Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2018

Kybernetická trestná činnost prostupuje dnes již takřka všemi druhy trestné činnosti – od násilné, mravnostní, majetkové až po činnost organizovaných zločineckých skupin. Závažnost této trestné činnosti stoupá, o čemž svědčí zvyšující se nápad těchto případů na úrovni vrchních státních zastupitelství.

Celková kriminalita mezi lety 2011 až 2017 poklesla o 40%.[1] Naopak kybernetická kriminalita ve stejném období vzrostla o téměř 300% - přeneseno do číselné podoby v roce 2011 bylo zaznamenáno 1 502 skutků a v roce 2017 již 5 654 skutků, jde tedy nárůst o více jak 4 000 deliktů. V roce 2018 byl zaznamenán meziroční nárůst deliktů asi o dalších 1300 případů. Odborníci odhadují, že tato čísla tvoří jen špičku ledovce a většina této trestné činností zůstává nezjištěna a nehlášena. Jednou z příčin poklesu čísel celkové kriminality tak může být právě přesun trestné činnosti (především obchodu s nelegálním obsahem všeho druhu) do kyberprostoru, kde je mnohem těžší ji odhalit a je těžší se jí bránit.

Problém definice kybernetické kriminality

Definice kyberkriminality přímo souvisí se statistikou páchání jednotlivých druhů trestné činnosti. Jak již bylo uvedeno v předchozích zprávách, definice kybernetické kriminality je v oblasti trestního práva prozatím neukotvená, a z tohoto důvodu je i trestná činnost do kybernetické kriminality spadající, ne zcela jednoznačně specifikována. S ohledem na absenci této definice byla proto pro potřeby Policie České republiky kybernetická kriminalita definována jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí, kde předmětem útoku je samotná oblast informačních a komunikačních technologií nebo je trestná činnost páchána za výrazného využití informačních a komunikačních technologií, jakožto významného prostředku k jejímu páchání[2].

Kromě statistiky má definice kyberkriminality význam mimo jiné pro určení agendy specializovaných policejních jednotek, na což navazují jejich personální a materiální zabezpečení a požadavky, ale i na vyčlenění specializovaných státních zástupců a nápadu jejich práce. Agenda spadající do kompetence specializovaných jednotek byla v roce 2018 předmětem diskuzí, z nichž vyplynul na jedné straně zájem (podporovaný ze strany státních zástupců) na koncentraci vyšetřování na „ryzí“ kybernetickou kriminalitu, kdy předmětem útoku jsou samotné technologie (hacking, DDoS, apod.) ale také například provozování tržišť s nelegálním zbožím na Darknetu, zneužívání virtuálních měn, atd. Na druhé straně byl obhajován názor (především členy některých specializovaných jednotek), že podvodná jednání, která

[1] Data byla získána od Policie ČR - Národní centrály pro organizovaný zločin.
[2] viz Pokyn policejního prezidenta č. 103/2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení

jsou nyní nejrozšířenějším druhem kyberkriminality (zejm. podvodné e-maily, apod.), by měla do této agendy spadat, neboť je jednak veřejnost vnímá nejcitlivěji a nejčastěji a jednak i v případech vyšetřování těchto podvodů je třeba odborný postup a znalosti specialistů.

Závěrem roku 2018 došlo například k významnému odhalení provázaného řetězce e-shopů v komerční doméně i v národních internetových doménách několika států. Podvodné portály nabízely oblečení, dresy známých klubů, apod. značně pod reálnou cenou. Ve skutečnosti však sloužily tyto obchody jen k vylákání identifikátorů platebních karet. Tento případ je úspěchem oddělení kybernetické kriminality PČR KŘ JmK, který byl realizován v době předvánoční nákupní špičky.

V oblasti personální bylo přitom u Policie ČR vytvořeno nových 195 tabulkových míst jak pro regionální tak i centrální úroveň, která se úspěšně daří zaplňovat. Problematice kybernetické kriminality se tak bude věnovat více než 300 policistů - specialistů na odhalování, prověřování, vyšetřování a forenzní zkoumání kybernetické trestné činnosti v celé České republice (na centrálním pracovišti sekci kybernetické kriminality NCOZ SKPV 59 policistů). Připravovány jsou rovněž změny policejního vzdělávání, jejichž cílem bude předání základních poznatků z oblasti kybernetické kriminality i policistům sloužícím mimo problematiku kybernetické kriminality.

Charakteristika trendů kyberkriminality v roce 2018

Ačkoliv zájem o kryptoměny výrazně oslabil, a to především díky hlubokému opakovanému poklesu směnného kurzu Bitcoinu i dalších kryptoměn, jsou odhalovány případy jejich zneužívání k daňovým únikům na dani z příjmu a DPH. Problematickou je zejména otázka dokazování na straně správců daně i omezené možnosti, ve srovnání s orgány činnými v trestním řízení, použití účinných procesních nástrojů. Nejvyšší správní soud se v nedávném rozsudku ze dne 31. 7. 2018, č. j. 5 Afs 252/2017 – 31 zabýval případem, kdy správce daně odmítl přiznat daňovému subjektu z přijatých zdanitelných plnění nárok na odpočet daně z přidané hodnoty. Správce daně tvrdil, že daňový subjekt věděl nebo vědět měl, že se účastní řetězce transakcí, které jsou zatíženy podvodem na dani z přidané hodnoty. Nejvyšší soud však tento názor vyvrátil a konstatoval, že je na správci daně, aby prokázal, že daňový subjekt nebyl v dobré víře a byl zapojen v řetězci obchodních převodů, které byly vytvořeny pouze za účelem vylákání daňové výhody v podobě odpočtu na dani z přidané hodnoty. V případě obchodů s kryptoměnami (často vytvořenými ad hoc právě za účelem provedení nákupu a prodeje) je tak ze strany správců daně téměř nemožné prokázat jinou hodnotu provedeného obchodu, než tu, kterou dokládají daňové subjekty – účastníci transakce. Často je správce daně nucen přijmout jako potvrzující dokumenty o provedené transakci například výtisky z monitoru počítače, aniž by bylo možno transakci zpětně kontrolovat nebo vyvrátit. Důkazní břemeno daňových subjektů zůstává, podle citovaného rozhodnutí Nejvyššího správního soudu, v rozsahu daňového přiznání.

Virtuální měny jsou stále častěji využívány k vyvádění a převádění prostředků získaných trestnou činností (zejm. podvody), neboť jsou díky anonymitě k tomuto účelu ideálním prostředkem.

Prostředí služeb anonymní sítě TOR dalo možnost k trvajícímu vzestupu mravnostní trestné činnosti, především šíření dětské pornografie. Pachatelé využívají zejména komunikační prostředí různých chatů, uzavřených skupina komunikačních fór (na internetu i v síti TOR).

V souvislosti s migrační vlnou došlo k rozšíření výskytu jednak nenávistných projevů na Internetu, ale také poplašných a dezinformujících zpráv, tzv. „hoaxů“, které bývají spojeny s phishingovými útoky. Lze vypozorovat nárůst phishingových útoků zaměřených na získání přístupu k bankovním účtům a následnému odčerpání finančních prostředků.

Jelikož bezpečnostní nástroje se v poslední době zaměřují na řešení problémů způsobených ransomwarem, na jejich detekci a eliminování důsledků škodlivé činnosti, někteří útočníci používají rozruch vyvolaný ransomwarem jako techniku pro skrytí jiné záměru, snahy dosáhnout zisku jiným způsobem, například použitím keyloggerů nebo těžbou kryptoměny.

Jako trend lze označit i prodej a výměnu ICS dat a citlivých údajů, které byly ukradeny z průmyslových podniků. Na černém trhu se tato data obchodují společně s nabídkou botnetů z „průmyslových“ počítačů. Stále častěji se tak lze na černém trhu lze setkat s trestnou činností v podobě nabídky služeb jako jsou: „*malware-as-a-service*“, „*attack-vector-design-as-a-service*“, „*attack-campaign-as-a-service*“ a dalšími.

Síť specializovaných státních zástupců

Členství specializovaných státních zástupců v neformální síti bylo ze strany jednotlivých krajských a vrchních státních zastupitelství opětovně potvrzeno. Síť se sešla v prosinci minulého roku v prostorách Justiční akademie, a to podle osvědčeného modelu společně s vedoucími všech oddělení informační kriminality Policie ČR a s vedoucími pracovníky sekce kybernetické kriminality NCOZ. Setkání koordinovali náměstek nejvyššího státního zástupce, národní korespondent pro kybernetickou kriminalitu a ředitel sekce kybernetické kriminality NCOZ.

Hlavními tématy jednání sítě byla příprava nové policejní metodiky k zajišťování virtuálních měn a přeshraniční přístup k elektronickým důkazům, včetně problematiky přímé spolupráce se zahraničními poskytovateli služeb, která není doposud uspokojivě vyřešena.

Na základě předchozí dohody a plánu a především díky spoluprací technologických pracovníků Policie ČR a státního zastupitelství se podařilo zřídit pro většinu členů sítě přístup k elektronickému portálu NCOZ, kde je k dispozici řada aktualizovaných informací.

Česko-Bavorský dialog o kyberkriminalitě

Ve dnech 25. – 26. 10. 2018 se skupina vybraných státních zástupců a pracovníků Sekce kybernetické kriminality NCOZ zúčastnila studijní návštěvy Bavorského centrálního úřadu pro stíhání kybernetické kriminality v Bambergu. Kromě účastníků z ČR se setkání účastnilo několik státních zástupců a odborných pracovníků výše uvedeného bavorského úřadu. Hlavními tématy byla problematika kryptoměn, vyhledávání a analýza otevřených online zdrojů, streamování placených televizních kanálů, zneužívání platebních karet k páchání trestné činnosti na internetu a další témata prezentovaná na konkrétních případech.

Podle dohody na úrovni Bavorského centrálního úřadu, NSZ i samotných účastníků budou další setkání zaměřená na výměnu metod s bojem s kybernetickým zločinem, řešení vybraných právních problémů a možnosti společného postupu navazovat v roce 2019.

Evropská justiční síť pro boj proti kyberkriminalitě (EJCN)

Síť pro boj proti kyberkriminalitě se sešla v dubnu a v listopadu 2018, jejího jednání se za ČR účastnil národní korespondent. Síť v minulém roce řešila například skutečnost, že v důsledku směrnice GDPR od 25. května 2018 nemá značná část policejních jednotek policie a další OČTŘ přístup do neveřejné části databáze WHOIS (mapuje především uživatele konkrétních IP adres). Komise EU chystá dohodu s WHOIS, která však zatím nebyla uzavřena a termín jejího uzavření naráží na různé technické a právní překážky.[3]

Síť dále přijala řadu pravidel pro svá jednání a průběžně řešila operativní otázky týkající se např. šifrování dat, virtuálních měn i konkrétních bezpečnostních hrozeb.

Evropská justiční síť státních zástupců pro ochranu práv k duševnímu vlastnictví (EIPPN)

Tato síť se sešla v dubnu 2018, jednání se za ČR účastnil národní korespondent. Na plenární zasedání sítě navazovalo setkání vybraných členů se zástupci Číny.

Podle výzkumu EUIPO rostou nelegální obchody v EU 10x rychleji, než retailový prodej. Přitom, jak již bylo uvedeno v předchozích zprávách, masivní podíl na tomto růstu mají online obchody s nelegálním zbožím, pirátská vysílání na internetu, apod. Jeden rok výzkumu se skrývá ve studii UNICRI týkající se přítomnosti malwaru na takových stránkách (“Identification and Analysis of malware on Selected copyright infringing websites”). Tato studie je přístupná na webu UNICRI. Další studii týkající se internetových televizí a nelegálního vysílání vypracoval úřad EUIPO (EUIPO

[3] K tomu viz také prohlášení sítě ECJN dostupné z http://www.eurojust.europa.eu/press/News/News/Documents/2018-05-25_EJCN-statement_EN.pdf

momentálně připravuje studii o vzniku a výpočtu škody v těchto případech) – studie jsou dostupné na webových stránkách Observatory. Nicméně již ve zprávě Observatory z roku 2016 je popsán model porušování IP práv online z technického pohledu. Zpráva také obsahuje taxonomii jednotlivých trestných jednání. Momentálně se pracuje na aktualizaci této zprávy. Uvedený model se se testoval na vzdělávacích akcích EUIPO určených pro soudce, kde byl kladně přijat a zdá se tedy, že má potenciál. V návaznosti na tento model byla vypracována zpráva, která mapuje situaci v některých zemích EU. Týká se jmen domén, jejich „krádeží a zneužívání k nelegálním obchodům. V další fázi na uvedený model a zprávu má dojít ke zkoumání pirátského vysílání, respektive zprostředkování vysílání legálního vysílání (tzv. IPTV Crime and Cardsharing). Práci provede univerzita (jejíž identitu prozatím úřad EUIPO drží v tajnosti) a výsledkem má být, kromě zprávy o výzkumu, také podrobný manuál k vyšetřování tohoto druhu trestné činnosti.

Spolupráce s Masarykovou univerzitou

V srpnu 2018 proběhla již tradiční prezentace pro skupinu zahraničních studentů, kteří se pod záštitou MU a organizace ELSA účastnili letní školy IT práva na MU. Tentokrát prezentaci provedl a zaštítil zástupce národního korespondenta společně s vedoucím oddělení kybernetické kriminality Krajského ředitelství PČR Jihomoravského kraje. Studenti vyslechli společnou přednášku a v prostorách Policie ČR debatovali na dané téma.

NSZ nadále spolupracuje na projektu C4e jehož hlavním realizátorem je Ústav výpočetní techniky MU. Náplní projektu je výzkum zaměřený na nakládání s elektronickými důkazy, klasifikaci a kvalifikaci počítačové trestné činnosti a mezinárodní spolupráce při vyšetřování a stíhání kyberkriminality, jakož i sdílení znalostí a výsledků výzkumu například také s NSZ.

Spolupráce s Ministerstvem spravedlnosti na přípravě legislativy

Specializovaní státní zástupci se účastní jednání pracovní skupiny k elektronickým důkazům, která se konají na půdě Ministerstva spravedlnosti.

Činnost skupiny se koncentruje na komplexní přístup k elektronickým důkazům v trestním řízení, z čehož i nadále vyplývá její budoucí dlouhodobější trvání.

Spolupráce s Justiční akademií a s Evropskou akademií práva (ERA)

Státní zástupci vystupovali jako přednášející na seminářích pořádaných Justiční akademií pro soudce a státní zástupce.

Pokračovala spolupráce s Evropskou akademií práva, kde do dvou cyklů přednášek na téma elektronických důkazů přispěl národní korespondent přednáškou na téma přístupu k datům ve vzdálených úložištích. Tento cyklus bude v dalším roce pokračovat na různých místech EU, včetně ČR.

Judikatura a vývoj v oblasti

I. V případě kryptoměn je třeba poukázat na situaci v Německu, která často ovlivňuje právní názory českých soudů vyšších instancí. Německý federální orgán pro finanční dohled (BaFin) nedávno klasifikoval Bitcoin jako finanční nástroj, avšak následné rozhodnutí soudu tuto kategorizaci zamítlo. Soud rozhodl, že kryptoměny podle zákona o bankovnictví (KWG) tuto definici nesplňují.

Berlínský odvolací soud v září 2018 odmítl vést trestní řízení proti provozovateli místní platformy obchodování s měnou Bitcon. Německé orgány stíhaly správce platformy za to, že umožnil obchodování s finančními nástroji jako je Bitcoin bez povolení BaFin. Zatímco soud Berlín-Tiergarten odsoudil obviněného, Berlínský regionální soud zrušil rozsudek a prohlásil, že BaFin nesprávně vyložil právní status Bitcoinu.

Odvolací soud citoval Článek 1(11) zákona o bankovnictví (KWG) a uvedl, že Bitcoin nevydává ani centrální banka, ani žádný jiný státní orgán a nejde o všeobecně uznávanou měnu, která navíc postrádá stálou hodnotu umožňující její použití ke srovnání cen zboží a služeb. Na rozdíl od názoru publikovaného orgánem pro finanční dohled (BaFin) soud judikoval, že Bitcoin nemůže být považován za zúčtovací jednotku nebo za finanční nástroj.

Citovaný rozsudek také objasnil záležitosti týkající se prodeje a nákupu Bitcoinu v Německu. Soud rozhodl, že obchodování s Bitcoin není předmětem povolení ani licencí a obchodování s ním bez licence nemůže tedy být trestným činem. Odvolací soud kritizoval orgán pro finanční dohled (BaFin) za to, že překročil svoji kompetenci federálního orgánu a provedl extenzivní výklad trestního práva hmotného.

Rozhodnutí uvedeného německého soudu dále prohloubilo nesrovnalosti v národních interpretacích směrnic EU přijatých proti praní špinavých peněz.

II. Za podstatné **pro oblast kryptoměn** je třeba považovat rozhodnutí Krajského soudu v Brně (rozsudek ze dne 9. 10. 2017 č. j. 50T 4/2017) a navazující rozhodnutí Vrchního soudu v Olomouci (rozsudek ze dne 30. 5. 2018, č. j. 5 To 8/2018).

Podle soudních rozhodnutí měl pachatel v období od 1. 2. 2013 do 30. 11. 2013 provozovat v anonymní síti Tor internetový obchod *Sheep Marketplace*. Skrze toto tržiště docházelo ke zprostředkování prodeje různého zboží či služeb, především návykových látek a jedů. Pachatel přitom nedisponoval potřebným povolením a jednotlivé platby probíhaly prostřednictvím digitální měny Bitcoin. Obžalovaný rovněž zneužíval tržiště k odcizení Bitcoinů dalších uživatelů. Vedle toho navíc držel doma nemalé množství zbraní a střeliva. Pachatel měl takto získat prospěch více než 16 milionů korun. Krajský soud jakožto soud prvního stupně po výslechu obžalovaného, provedl důkaz znaleckým posudkem odborníka z oboru kybernetiky a výpočetní techniky ohledně fungování a principů dotčeného anonymního tržiště, softwarového systému, „peněženek“ a profilů jednotlivých uživatelů. Stejně tak byl posuzován počítač a telefon obžalovaného, které sloužily k provozu a monitorování tržiště. V další části byla skrze druhý znalecký posudek rozvedena problematika

samotného Bitcoinu, směnárny Bitstamp, anonymních transakcí a kryptografie. Po řešení otázky původu Bitcoinů obžalovaného pak obžalovaný vysvětloval konkrétní aspekty jeho operování na tržišti a s anonymní měnou. Další části byly věnovány omamným látkám a jedům, jakož i držení zbraní a střeliva bez příslušných povolení. Soud nakonec rozhodl, že obžalovaný spáchal zvlášť závažný zločin nedovolené výroby a jiného nakládání s omamnými a psychotropními látkami a s jedy, zvlášť závažný zločin krádeže a přečin nedovoleného ozbrojování, za což mu byl vyměřen trest ve výši devíti let ve věznici se zvýšenou ostrahou, jakož i propadnutí věci v podobě části Bitcoinů, zbraní, střeliva a finančních prostředků. Jedná se o vůbec první rozhodnutí v otázce bitcoinového trhu v České republice, a to jak v rozsahu využívání takového trhu, šifrování měny, tak samotného bitcoinového zločinu, které do jisté míry předestírá cestu, jakou se bude rozhodovací praxe ubírat. Rozhodnutí navíc obsahuje vymezení tohoto prostředí a jeho jednotlivých aspektů, které může být pro svou bohatost a kvalitu do budoucna argumentační oporou v obdobných sporech. Rozhodnutí odvolacího soudu je v neposlední řadě důležité pro účely výpočtu prospěchu (případně škody) získaného prostřednictvím kryptoměny Bitcoin.

III. Nejvyšší soud ČR judikoval (usnesení ze dne 13. 12. 2017, sp. zn. 5 Tdo 1085/2017) v kauze týkající se zejména § 230 a § 248 trestního zákoníku. Soud konkrétně uvedl, že za **neoprávněné užití uložených dat** lze považovat takové jejich užití, které je v rozporu s právní normou nebo je činěno v rozporu se stanoveným účelem, popř. bez vědomí či souhlasu oprávněné osoby. Předmětem ochrany tohoto přečinu je primárně integrita a dostupnost počítačových dat a systémů, ochrana je poskytována počítačovým datům a počítačovým programům před neoprávněnými zásahy, které mohou mít vliv na existenci, kvalitu, správnost dat, a ustanovení chrání i před neoprávněným užíváním uložených počítačových dat. Neoprávněným užitím dat (neboli počítačovou špionáží) je jakákoli nedovolená manipulace s daty uloženými v počítačovém systému nebo na nosiči informací. Neoprávněné bude takové užití, které je v rozporu s právní normou nebo je činěno v rozporu se stanoveným účelem, popř. bez vědomí či souhlasu oprávněné osoby. Získáním přístupu se rozumí takové jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo nosičem informací a využití jeho informačního obsahu. Získat přístup k počítačovému systému nebo nosiči informací lze neoprávněně, ale i oprávněně. Nezáleží na důvodu, který vedl k získání přístupu (může to být náhoda, plnění pracovních úkolů, využití počítače pro zábavu, odcizení nosiče informací atd.).

IV. Za důležité **pro oblast práv k duševnímu vlastnictví** lze považovat rozhodnutí Soudního dvora EU ze dne 29. 11. 2017 (Věc: C-265/16 (VCAST) týkající se **ukládání televizního vysílání v cloudu.**

Společnost VCAST poskytuje zákazníkům na internetu systém nahrávání videozáznamů vysílání italských televizních společností (včetně společnosti RTI) do cloudového úložiště. Uživatel si může vybrat určitý program nebo časový interval a systém společnosti VCAST následně zachytí signál pomocí vlastních antén a nahraje vysílání do úložiště dle výběru uživatele. Vznikl spor mezi společnostmi VCAST a RTI. Společnost VCAST podala proti RTI žalobu v Itálii, kterou se

domáhala, aby bylo určeno, že její činnost je v souladu s právem. Soud však částečně vyhověl návrhu společnosti RTI na předběžné opatření a společnosti VCAST v podstatě zakázal pokračovat v její činnosti. Následně položil Soudnímu dvoru dvě předběžné otázky týkající se výkladu unijního práva, zejména interpretace čl. 5 odst. 2 písm. b) směrnice č. 2001/29 (dále jen „Směrnice“), který stanovuje, kdy mohou členské státy určit výjimky nebo omezení práva na rozmnožování autorských děl. Soud předložil Soudnímu dvoru dvě hypotézy, přičemž jedna předpokládá, že vnitrostátní úprava zakazuje poskytování služby umožňující pořizovat soukromé rozmnoženiny děl chráněných autorským právem nahráváním videozáznamů na dálku technikou zvanou cloud computing, druhá, že vnitrostátní úprava danou činnost povoluje. Podle čl. 5 odst. 2 písm. b) Směrnice je možné, aby členské státy stanovily výjimky z práva na rozmnožování nebo toto právo omezily u rozmnoženin na jakémkoliv nosiči vytvořených fyzickou osobou pro soukromé užití a pro účely, které nejsou přímo ani nepřímo komerční. Podle Soudního dvora pro uplatnění čl. 5 odst. 2 písm. b) stačí, aby byla třetí osobou poskytnuta rozmnožovací služba, není nutné, aby dotyčné osoby vlastnily vybavení, přístroje či nosiče pro rozmnožování. V tomto případě služba plní dvě funkce – zajišťuje pořizování rozmnoženin a zpřístupňuje díla a předměty, jichž se týká. Dále se jedná o sdělování veřejnosti - z judikatury Soudního dvora v tomto ohledu vyplývá, že se pojem „veřejnost“ týká blíže neurčeného počtu potenciálních diváků či posluchačů a kromě toho vyžaduje dosti vysoký počet osob. Původní přenos prováděný vysílacím subjektem a přenos prováděný poskytovatelem služeb jsou však dvě odlišná sdělování veřejnosti a tyto přenosy jsou určeny každý vlastnímu publiku. Ke každému z nich tak musí dotyční nositelé práv udělit svolení. Soudní dvůr na základě výše uvedeného judikoval, že Směrnice musí být vykládána tak, že brání vnitrostátní právní úpravě, která podnikatelskému subjektu dovoluje poskytovat jednotlivcům bez svolení nositele práv službu umožňující pořizovat soukromé rozmnoženiny děl chráněných autorským právem nahráváním videozáznamů na dálku do cloudu s pomocí výpočetního systému a při aktivním zásahu do vyhotovování záznamů.

V. Poukázat je možno na rozhodnutí Evropského soudu pro lidská práva ze dne 24. 3. 2018 v kauze Benedik v. Slovenia (podání č. 62357/14), ve kterém soud rozhodl, že slovinská policie porušila právo na soukromí podatele, když k vydání tzv. **informací o uživateli týkajících se dynamické IP adresy** nevyžádala svolení soudu. Obě strany se nicméně mohou proti rozhodnutí odvolat.

VI. V roce 2018 nelze pominout **vydání ruského hackera Jevgenije Nikulina do USA** a s tím spojené kauzy u Nejvyššího správního a u Ústavního soudu. Všechny stížnosti Jevgenije Nikulina byly zamítnuty. Tato kauze je podstatná spíše pro oblast mezinárodní právní pomoci, nicméně s trestní politikou v oblasti kybernetické kriminality je úzce spjata.

VII. Stále probíhá řízení u Ústavního soudu, jehož výsledkem bude rozhodnutí o návrhu skupiny poslanců týkající se zrušení některých ustanovení zákona o elektronických komunikacích a trestního řádu týkajících se **podstaty plošného uchování dat**.

VIII. V neposlední řadě je nutno zmínit i novou metodiku Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), podle které státní úřady mohou při vypisování veřejných zakázek na komunikační technologie brát v potaz rizika, která plynou z používání systémů čínských firem Huawei a ZTE. Postup zadavatele v konkrétních případech nicméně bude nadále posuzovat Úřad pro ochranu hospodářské soutěže.

IX. Problematika přímé spolupráce se zahraničními poskytovateli přesahuje rozsah této výroční zprávy. Lze pouze konstatovat, že řešení v podobě nové směrnice EU je hledáno na pracovních skupinách Rady EU, přičemž vydání nového právního předpisu reagujícího zejména na tzv. zákon „CLOUD Act“ v USA je možno očekávat počátkem roku 2019. Totožná jednání probíhají na půdě Rady Evropy, kde by měla být přímá spolupráce se zahraničními poskytovateli řešena cestou dodatkového protokolu k tzv. Budapešťské úmluvě. Vzhledem však ke zdlouhavému ratifikačnímu procesu nelze odhadnout, kdy je účinné řešení na této půdě možno očekávat.

X. Dne 1. 2. 2019 nabude účinnosti novela trestních předpisů č. 287/2018 Sb., která v novém ustanovení § 7b trestního řádu a v § 65a a 65b zákona č. 104/2013 Sb. upravuje příkaz k uchování dat.

Dne 31. 1. 2019
Mgr. Petr Klement