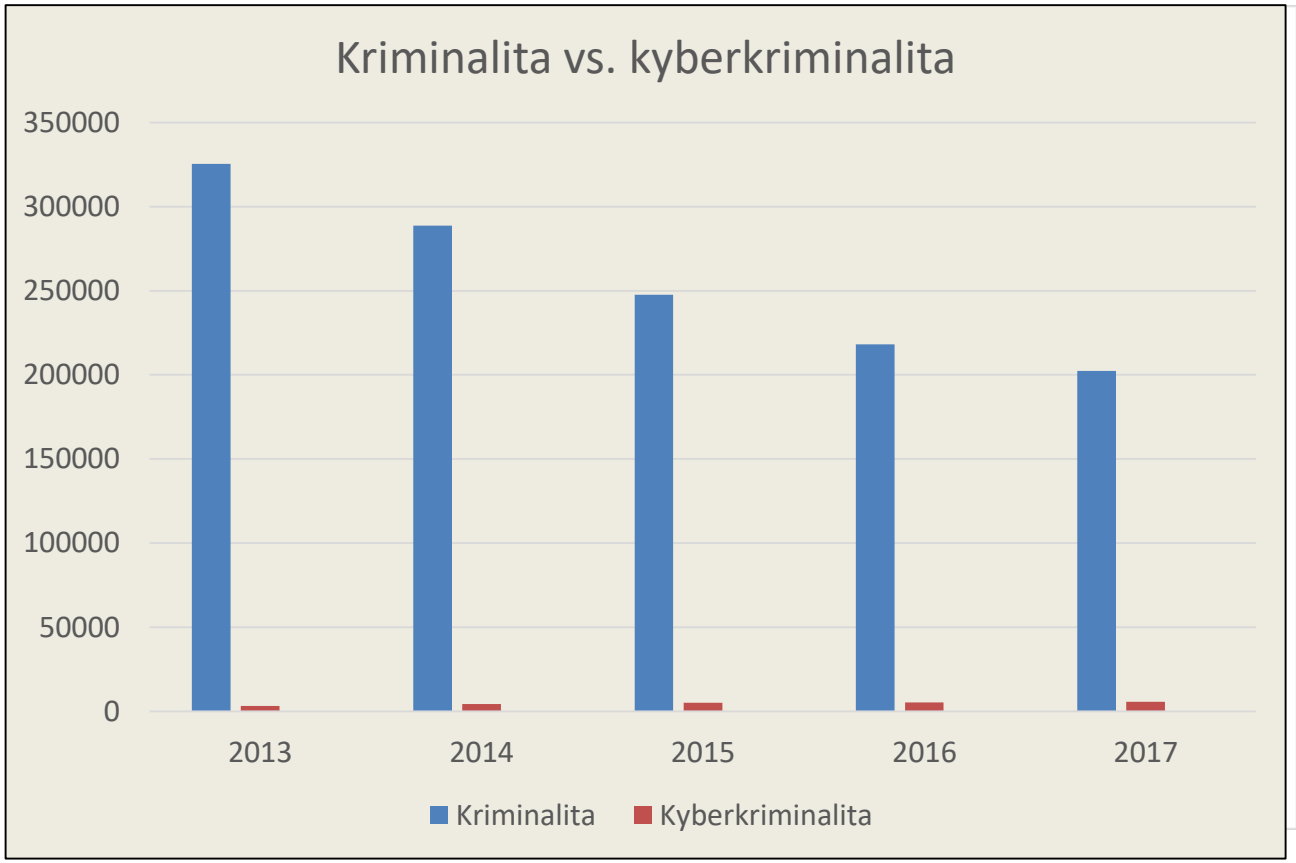
Kyberkriminalita
(a elektronické důkazy)

Jakub HARAŠTA

Kyberkriminalita

Cybercrime is on the rise!



Kriminalita celkově – cca 200 000 (2017);
leden-listopadu 2018 cca 180 000

Data:

https://www.policie.cz/clanek/kyberkriminalita.aspx [3.11.2019] https://www.policie.cz/statistiky-kriminalita.aspx [5.11.2019]

K soudům se dostávají „hlouposti“

- *„In the Czech Republic, the criminal offences associated with cybercrime that are dealt with by the courts are not representative of the breadth of cybercrime in today's society.“*

GŘIVNA, Tomáš a Jakub DRÁPAL. Attacks on the Confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digital Investigation,* 2019, vol. 28, March 2019, p. 1-13.

KYBERKRIMINALITA OBECNĚ

Typy (obecně)

- Úmyslné útoky proti CIA
  - Např. §230 Neoprávněný přístup k počítačovému systému a nosiči informací
- Trestné činy páchané prostřednictvím ICT
  - Např. §191 Šíření pornografie
- Trestné činy související s ICT
  - Např. §233 Padělání a pozměnění peněz

Typy dle 104/2013 Sb.

- Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů
  - §230 odst. 1 Neoprávněný přístup k počítačovému systému a nosiči informací
- Trestné činy související s počítačem
  - §230 odst. 2 Neoprávněný přístup k počítačovému systému a nosiči informací
- Trestné činy související s obsahem
  - §192 Výroba a jiné nakládání s dětskou pornografií
- Trestné činy týkající se poručení autorského práva a práv souvisejících s právem autorským
  - §270 Porušení autorského práva, práv souvisejících s právem autorských a práv k databázi

„Klasická“ kyberkriminalita

- §182 Porušení tajemství dopravovaných zpráv
- §230 Neoprávněný přístup k počítačovému systému a nosiči informací
- §231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- §232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
- (§234 Neoprávněné opatření, padělání a pozměnění platebního prostředku)

Široké pojetí (např. PČR)

- TČ proti uloženým informacím
  - §230 TZ Neoprávněný přístup k počítačovému systému nebo nosiči informací
  - §231 TZ Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
  - §232 TZ Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
- TČ ve vztahu k datům, kde je PC prostředkem pro páchání
  - §191 TZ Šíření pornografie
  - §192 TZ Výroba a jiné nakládání s dětskou pornografií
  - §193b TZ Navazování nedovolených kontaktů s dítětem
  - §270 TZ Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
  - §355 TZ Hanobení národa, rasy, etnické nebo jiné skupiny osob
  - §356 TZ Podněcování nenávisti vůči skupině osob nebo k omezování jejich práv a svobod
  - §357 TZ Šíření poplašné zprávy
  - §184 TZ Pomluva
  - §175 TZ Vydírání
  - „a mnohé další.“

KYBERKRIMINALITA KONKRÉTNĚ

§182 odst. 1 písm. b)

- Úmyslné poručení tajemství datové, textové, hlasové, zvukové nebo obrazové zprávy posílané prostřednictvím sítě elektronických komunikací
  - Datová zpráva – informační tok
  - Textová zpráva – Skype, ICQ, chat
  - Hlasová zpráva – Skype, Hangout
  - Zvuková zpráva – Skype, Hangout
  - Obrazová zpráva – Skype, videochat
  - Síť elektronických komunikací – § 2 písm. h) ZoEK
    - Družicové sítě, pevné sítě s komutací okruhů nebo paketů, mobilní zemské sítě, sítě pro rozvod elektrické energie, sítě pro rozhlasové a televizní vysílání, sítě kabelové televize

§182 odst. 1 písm. c)

- Úmyslné porušení tajemství neveřejného přenosu počítačových dat do systému, z něj nebo v jeho rámci, včetně elmag. vyzařování
  - Rekonstrukce obrazu na monitoru

§230 odst. 1 TZ

- *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části…“*
  - Primárně důvěrnost
  - Překonání bezpečnostního opatření a zároveň neoprávněnost přístupu
  - Široké chápání počítačového systému (server, PC, mobilní telefon, router, webkamera)
  - Bezpečnostní opatření – heslo, firewall, šifrování – nezáleží na „síle“

§230 odst. 2 TZ

- Kdo získá přístup a data neoprávněně užije NEBO data neoprávněně vymaže, zničí, poškodí, změní, potlačí, sníží jejich kvalitu NEBO data padělá a pozmění tak, aby byla považována za pravá NEBO neoprávněně vloží data do počítačového systému
  - Primárně integrita a dostupnost
  - Nezávisí na překonání bezpečnostního opatření nebo oprávnění použití systému

§ 231 TZ

- Vyrobení, uvedení do oběhu, dovoz, vývoz, nabízení, zprostředkování prodání nebo jiné zpřístupnění zařízení nebo hesla/kódu/dat v úmyslu spáchat §182 odst. 1 písm. b) nebo §230 odst. 1 nebo §230 odst. 2
  - Přístupové zařízení – hardware – např. čtečky bankovních karet – k trestnosti stačí držení části; sériová/individuální
  - Postup – „kuchařka“ jak odposlouchávat monitor pomocí antény
  - Nástroj – mechanický prostředek – klíč
  - Počítačový program – skenery pro zjišťování otevřených portů počítače, sniffery, 0-day exploity
  - Mohou sloužit i k legálnímu účelu, proto se provazují s úmyslem spáchat trestný čin.

§ 232 TZ

- Zničení/poškození/pozměnění dat nebo zásah do technického/programového vybavení počítače porušením povinnosti (zaměstnání/ postavení/funkce/ze zákona/smluvně) z hrubé nedbalosti
  - Např. zákaz používat bez souhlasu zaměstnavatele prostředky zaměstnancem
  - Subsidiarita trestní represe!

§234 TZ

- *„Kdo sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává … elektronické peníze …“*
  - Pohledávka za vydavatelem elektronických peněz uchovávaná elektronicky, která je vydávána proti přijetí peněžních prostředků v hodnotě ne nižší, než je hodnota vydávaných elektronických peněz, která je přijímána jako platební prostředek jinými osobami, než jejich vydavatelem.
  - Elektronické peněženky (dříve široký výklad pojmu platební karty) např. na In Kartě ČD

Elektronické důkazy

DOKAZOVÁNÍ

Hledání pravdy

- Nedosažitelná materiální pravda vs. „Dosažitelná“ formální pravda
  - Objektivně vnímatelná formalizace materiální pravdy
  - Absolutní pravda je „tam někde“ – relativní pravda je v soudním rozhodnutí
  - Dokonalý zločin
  - Svědek vs. znalec vs. soudce

Vyšetřování

- Snaha dosáhnout zjištění materiální pravdy, která bude nutně neúspěšná, ale musíme vyvinout maximální možnou snahu
- Důkaz jako prostředek, kterým lze zjistit stav věci

- Otcovství
  - Nemáme dokonalou (Boží) jistotu; ale máme rodné listy a testy DNA

Postup

- Důkaz vs. důkazní materiál

- Nalezení, shromáždění
- Analýza
- Komunikace

Práce s důkazy u soudu

- Volné hodnocení důkazů
- Zákonná teorie důkazní

Volné hodnocení důkazů

- Soudce může důkazy hodnotit volně
  - Přisuzování důkazní hodnoty
  - Přijetí důkazů za pravdivé / nepravdivé

- Důkazem může být cokoli, co může přispět k objasnění věci

Zákonná teorie důkazní

- Rigorózní úprava dokazování
- Pravidla dokazování (*rules of evidence*) fungují jako podrobný standard
  - Upravuje způsob získání a použití důkazu
  - Částečně obsahuje hodnocení důkazní spolehlivosti

- Důkazem může být jen to, co je jako důkaz uvedeno

Zákonnost důkazu

- Je důkaz opatřen tak, jak stanovuje/připouští zákon?
  - Např. opatření věcných důkazů při nepovolené domovní prohlídce
  - Např. opatření záznamu hovorů nad rámec povolení soudu
- Je důkaz opatřen a proveden oprávněným procesním subjektem?

- Absolutní neúčinnost důkazu (neodstranitelné)
- Relativní neúčinnost důkazu (odstranitelné)

- Může otrávený strom rodit zdravé plody?

Standard dokazování

- „Beyond reasonable doubt“ (USA, UK), „nejsou důvodné pochybnosti“ (ČR)

- Odlišný důkazní standard v trestním a civilním řízení?

ELEKTRONICKÉ DŮKAZY

Elektronický důkaz

- Anglicky *digital evidence* (spíše) nebo *electronic evidence*
- Důkazní informace uložená nebo přenášená v digitální formě

- E-maily, digitální fotografie, IM historie, textové dokumenty, účetní programy, spisová služba, palubní jednotky v autech, video a audio záznamy, lokalizační údaje, provozní údaje, obsah webových stránek atd.

Elektronický důkaz II

- Virtuální jako odraz reálného
- Obrovská výtěžnost

- Co je instalováno? Kdo s tím manipuloval? Jaké stránky byly navštěvovány? Co bylo vyhledáváno (jaké dotazy pokládány)? Nakolik SW plní deklarovanou funkci (losovací nástroje u veřejných zakázek)?
- Přiznání v rámci „náhodných“ služeb (WoW, USA) + domluvy na setkání/předání (kanibalismus, Německo).
- Artefakty v kódu („rukopis“ programátora nebo „školy“)

„Normální“ důkaz

- Viditelný
  - Nůž/otisk prstu vs. Metadata
- Stálý
  - Dopis vs. RAM
- Většinou méně rozsáhlý
  - Spisovna vs. eDiscovery
- Relativně jednoduše dostupný
  - Zamčené dveře vs. kryptografie

Obecné otázky…

- Co tu je?
  - Co tu je a nemá být?
- Co tu není?
  - Co tu není a má být?
- Co bylo změněno?
  - Přesun

… a specifické postupy

- Bitová kopie
- Kontrolní součet
  - Zachování integrity důkazu
- Odbor kriminalistické techniky a expertiz (OKTE) a Útvar zvláštních činností (ÚZČ)

Shromažďování důkazů

- Interní vyšetřování incidentu
  - CERT/CSIRT, forenzní postupy, vlastní majetek
- Civilní řízení
  - Strany opatřují a nesou své důkazní břemeno; důkaz nesmí být proti zákonu
- Trestní řízení
  - OČTŘ opatřují důkazy a musí dokázat vinu; důkaz musí být v souladu se zákonem

Procesní postupy OČTŘ

- Zákon č. 141/1961 Sb., trestní řád
  - §8 Součinnost
  - §78 Povinnost k vydání věci
  - §88 Odposlech
  - §88a Záznam telekomunikačního provozu
  - §158d Sledování osob a věcí

§8 TŘ

- Povinnost součinnosti

- Sdělte nám informaci XYZ
  - Státní orgány, PO, FO, bez úplaty

§78 TŘ

- Hmotná věc důležitá pro trestní řízení
- Často v kombinaci s domovní prohlídkou
- Data + věc
  - 7 Tz 9/2000 (NS), 1/2015 (NSZ)
- SR
  - §89 (vydanie veci) vs. §90 (uchovanie a vydanie počítačových údajov)
- Alternativy
  - Předložení

§ 88 TŘ

- Bez příkazu (se souhlasem účastníka odposlouchávané stanice – obchodování s lidmi, vydírání); soudní příkaz
- Jako důkaz pouze, pokud je k němu připojen protokol s uvedením údajů o místě, čase, způsobu a obsahu provedeného záznamu. Také identifikace orgánu.
- 4 měsíce; opakované prodlužování
- §88 odst. 8 – informování po pravomocném skončení věci (ESLP Klass v. Germany, 1978)
- Fungování: de facto legální MitM útok (§97 odst. 1 ZEK) + ÚZČ (PČR)
- Náhrady

§88a TŘ

- Provozní a lokalizační údaje
- Metadata (BTS, kdo komu a jak často apod.)

- ZEK (§97 odst. 3 a 4) stanovuje povinnost – pokud povinnost, tak přístup podle §88a TŘ

- Založeno směrnicí EU, ta později zrušena; zrušení povinnosti v ZEK (Pl. ÚS 24/10) i práva v TŘ (Pl. ÚS 24/11); pak opětovná úprava (kratší doba + jen pro určité trestné činy)
- ÚZČ
- Náhrady

§158d TŘ

- Při sledování lze pořizovat zvukové, obrazové a jiné záznamy – povolení státního zástupce.
- Lze zasahovat do nedotknutelnosti obydlí, do listovního tajemství nebo záznamů uchovaných v soukromí za použití technických prostředků – povolení soudce.
- Součinnost provozovatelů telekomunikační činnosti a jejich zaměstnanců.

ROZHODOVACÍ PRAXE I OBECNĚ

Hodnověrné/nehodnověrné důkazy

I. ÚS 3094/08

- Volné hodnocení důkazů neznamená absolutní volnost. Důkaz musí být odrazem skutečných událostí a situací. Jednotlivce musí být uznán vinným pouze na základě objektivních a skutečnosti odpovídajících zjištění.
- Nelze vyvozovat skutková zjištění, která z provedeného důkazu nevyplývají.
- Veškerá předání mezi orgány musí být protokolována, aby byla spolehlivě vyvrácena záměna či manipulace.
- Mechanoskopie.

Nepřímá povaha IP adresy

1 As 90/2008-189

- IP adresa je důkaz nepřímý – analogie s tím, že dopravní přestupek byl spáchán při jízdě určitým dopravním prostředkem. Tam ale není možné majitele bez dalšího považovat za pachatele. Je to významné vodítko, ale samo o sobě nestačí.
- S odkazem na předchozí rozhodnutí (8 As 10/2006-48): Nepřímé důkazy musí tvořit ucelený logicky provázaný důkazní řetězec, v němž žádný důkaz nezpochybňuje pravost a přesvědčivost důkazů ostatních
- Není nutné zvát znalce.

Náležitost příkazu podle §88 TŘ

II. ÚS 615/06

- Odposlech je prolomení distributivního práva. Jako takový musí být odůvodněný. Musí existovat alespoň minimální indicie o tom, že trestný čin se stal nebo mohl stát.
- Příkaz musí být individualizovaný ke konkrétní osobě, která užívá telefonní stanici. V případě, že to není jisté, musí být odůvodněno, na základě čeho se tak OČTŘ domnívá.
- Je potřeba specifikovat, jaké informace významné pro TŘ mají být zjištěny.

Zvukový záznam mimo §88 TŘ (§89 odst. 2 TŘ)

5 Tdo 459/2007

- §89 odst. 2 – za důkaz může sloužit vše / fakt, že důkaz nevyhledal OČTŘ není důvodem k odmítnutí.
- Přípustnost je nutné posuzovat s ohledem na respektování práva na soukromí a práva na nedotknutelnost osoby a jejího soukromí.

Dobrá praxe

4 Tdo 1482/2012

- Sice jen nepřímé důkazy, ale v množství a provázanosti, která dostačuje.
- IP adresa, ze které by mail odeslán + subjekty, kterým byly jednotlivé IP adresy přiděleny + korelace IP adres na všechny tři využité e-mailové adresy / z posudku znalce provázání mezi domácím PC a počítačem na pracovišti obviněného (přidělené stejné IP, které přistupovaly do mailových schránek) + obsáhlejší provoz související s běžným pracovním nasazením

ROZHODOVACÍ PRAXE II
STARÝ PŘEDPIS A NOVÝ SVĚT

Věc a data

7 Tz 9/2000

- §78 a §79 prolamuje tajemství již doručených zpráv
- Veškerá data, která jsou v době odnětí/vydání je možné použít

§158d TŘ a sledování dat

III. ÚS 3812/12

- §158d TŘ slouží k získávání poznatků o osobách a věcech. Probíhá utajovaným způsobem.
- Podstatné je, aby byl dostatečně specifikován okruh počítač, které mají být sledovány.
- Předmětem sledování jsou data. Lze opatřit jejich otisk použitím operativně pátrací techniky. Nelze použít pro data o telekomunikačním provozu, ale pro data uložená.

„jiné prostory“ a elektronická data

Tpjn 306/2014

- Účelem je ochrana listin, ke kterým se váže mlčenlivost advokáta. Místem, kde se tyto listiny mohou legitimně nacházet („jiné prostory“) jsou i elektronická úložiště nenacházející se fyzicky v místech běžného provozu. Tato místa může provozovat osoba odlišná od advokáta.
- Těžiště informací se přesunulo do elektronické podoby. Data, na která se vztahuje povinnost mlčenlivosti tak je prakticky možné mít kdekoli.
- ESLP klade elektronická data na roveň tištěným dokumentům – mají minimálně stejnou, v některých případech i vyšší ochranu.
- Cloudové úložiště má povahu nosiče dat.

Záznam z Facebooku

III. ÚS 3844/13

- Facebook není soukromý ani veřejný.
- Záleží na konkrétních uživatelích, nastavení míry soukromí u uživatelů nebo jednotlivých příspěvků, využití veřejného nebo soukromého komunikačního kanálu.
- S různou mírou soukromí se pojí různá míra oprávnění k zásahu do něj (různé instituty).

ZNALEC

Úloha znalce

- Vysvětlit soudu, co se technicky stalo a co to znamená
- Chápat techniku + umět ji vysvětlit někomu, kdo jí nerozumí
  - *„Je možné, aby bylo na jednotlivém počítači více Seznamů?“*
  - *„Obhajoba namítá pozměnění videozáznamu ve smyslu XYZ. Je možné, aby byl záznam v minulosti tímto způsobem pozměněn?“*

Děkuji Vám za pozornost!

jakub.harasta@law.muni.cz