VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

INFORMAČNÍ KRIMINALITA A JEJÍ PREVENCE

Autor práce: Lukáš Drozda, DiS.

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: Ing. Mgr. Martin Černý

Katedra: Katedra právních oborů a bezpečnostních studií

2018

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucímu bakalářské práce Ing. Mgr. Martinovi Černému, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

DROZDA, L., DiS. Informační kriminalita a její prevence: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2018. 84 s. Vedoucí bakalářské práce: Ing. Mgr. Martin Černý.

Klíčová slova: definice informační kriminality, úmluva o počítačové kriminalitě, typy protiprávního jednání, hackerské programové nástroje a techniky, trestné činy informační kriminality, telekomunikační provoz, procesní úkony při odhalování informační kriminality

Objektem bakalářské práce je informační kriminalita. Hlavním cílem práce je teoreticko-praktickým vhledem popsat pojem informační kriminality. Definovat základní pojmosloví a informační kriminalitu z pohledu Úmluvy o počítačové kriminalitě se zařazením jednotlivých trestných činů trestního práva hmotného do jejích okruhů, charakterizovat telekomunikační provoz a popsat základní procesní úkony trestního práva procesního, které jsou nejčastěji užívány k objasňování této kriminality. Vedlejším cílem je poskytnou praxeologický vhled do zkoumané problematiky popsáním vybrané kazuistiky konkrétního případu a blíže přiblížit postup policejního orgánu při jeho objasňování. Dalším vedlejším cílem je komparativní metodou porovnat a vyhodnotit statistická data informační společnosti a informační kriminality v posledních letech. Na základě těchto vyhodnocených dat potvrdit hypotézu o vzrůstající tendenci informační kriminality. Současně je dalším vedlejším cílem věnování se prevenci a bezpečnosti v zájmu ochrany před informační kriminalitou. Souhrnně se dá říci, že cílem bakalářské práce je poskytnout dostupné poznatky zejména z praxe, ale také ze samotné teorie informační kriminality.

ABSTRACT

DROZDA, L., DiS. Cybercrime and its prevention: Bachelor thesis. České Budějovice: The College of European and Regional Studies, 2018. 84 p. Supervisor: Ing. Mgr. Martin Černý.

Key words: definition of cybercrime, convention on cybercrime, types of infringement, hacking software tools and techniques, crimes of cybercrime, telecommunication traffic, procedural steps to detect cybercrime

The subject of the bachelor thesis is cybercrime. The main aim of the thesis is to describe the concept of cybercrime in a theoretical and practical way. Define basic terminology and cybercrime from the point of view of the Convention on Cybercrime with the inclusion of individual crimes of substantive criminal law in its circuits, characterize telecommunication operations and describe the basic procedural acts of criminal procedural law that are most frequently used to elucidate this crime.

The secondary aim is to provide a praxeological insight into the subject under investigation by describing the selected case-history of a particular case, and to further approximate the procedure of the police body in its elucidation. Another secondary objective is to compare and evaluate the statistic data of the information society and cybercrime in recent years by a comparative method.

On the basis of these evaluated data, confirm the hypothesis of the increasing tendency of cybercrime. At the same time, it is another secondary goal of dedicating prevention and security to protect against cybercrime.

In summary, the aim of the bachelor thesis is to provide the available knowledge, especially from practice, but also from the theory of cybercrime itself.

Obsah

ÚVOD **9**

CÍL A METODIKA BAKALÁŘSKÉ PRÁCE **10**

1 DEFINICE INFORMAČNÍ KRIMINALITY **11**

2 ÚMLUVA O POČÍTAČOVÉ KRIMINALITĚ **12**

2.1 ROZDĚLENÍ INFORMAČNÍ KRIMINALITY Z POHLEDU ÚMLUVY O POČÍTAČOVÉ KRIMINALITĚ 12

2.1.1 TRESTNÉ ČINY PROTI DŮVĚRNOSTI, INTEGRITĚ A POUŽITELNOSTI POČÍTAČOVÝCH DAT A SYSTÉMŮ 13

2.1.2 TRESTNÉ ČINY SOUVISEJÍCÍ S POČÍTAČEM 14

2.1.3 TRESTNÉ ČINY SOUVISEJÍCÍ S OBSAHEM 14

2.1.4 TRESTNÉ ČINY TÝKAJÍCÍ SE PORUŠENÍ AUTORSKÉHO PRÁVA. 15

3 TYPY PROTIPRÁVNÍHO JEDNÁNÍ **16**

3.1 HACKING 16

3.2 CRACKING 17

3.3 POČÍTAČOVÉ PIRÁTSTVÍ 17

3.3.1 WAREZ 18

3.3.2 FTP SERVERY 19

3.3.3 P2P SÍTĚ 19

3.3.4 DATOVÁ ÚLOŽIŠTĚ 19

3.4 ŠÍŘENÍ MATERIÁLŮ SE ZÁVADNÝM OBSAHEM 20

3.5 ZNEUŽITÍ INTERNETOVÝCH STRÁNEK 20

3.6 SPAMMING 20

3.6.1 SCAM 21

3.6.2 SCAM 419 21

3.6.3 PODVODNÉ NABÍDKY 22

3.7 SNIFFING 22

3.8 PHREAKING 23
3.9 CYBERSQUATING 23
3.10 PHISHING A PHARMING 23
3.10.1 SPEAR PHISHING 24
3.10.2 VISHING 25
3.10.3 SMISHING 25
3.11 KYBERNETICKÉ VÝPALNÉ 25
3.12 KYBERŠIKANA, KYBERSTALKING, KYBERGROOMING 26
3.12.1 KYBERŠIKANA 26
3.12.2 KYBERSTALKING 26
3.12.3 KYBERGROOMING 26
3.13 ŠKODLIVÉ ŠÍŘENÍ INFORMACÍ 26
3.14 SOCIÁLNÍ INŽENÝRSTVÍ 27
4 HACKERSKÉ PROGRAMOVÉ NÁSTROJE A TECHNIKY 29
4.1 PROLAMOVAČE HESEL 29
4.2 BACKDOORS 29
4.3 SKENERY 29
4.4 SNIFFERY 30
4.5 ROOTKITY 30
4.6 NÁSTROJE DOS 30
4.7 TROJSKÝ KŮŇ 31
4.8 NÁSTROJE PRŮZKUMU SÍTĚ 31
4.9 DEBUGGER 32
5 NĚKTERÉ DALŠÍ VÝSLEDKY HACKERSKÉ ČINNOSTI 33
5.1 MALWARE 33
5.2 POČÍTAČOVÝ VIRUS 33
5.3 POČÍTAČOVÝ ČERV 33
5.4 KEYLOGGER 34

5.5 RANSOMWARE 34
5.6 SPYWARE 35
5.7 ADWARE 35
6 TELEKOMUNIKAČNÍ PROVOZ 36
7 PROCESNÍ PROSŤREDKY PRO ODHALOVÁNÍ A OBJASŇOVÁNÍ INFORMAČNÍ KRIMINALITY 40
7.1 ODPOSLECH A ZÁZNAM TELEKOMUNIKAČNÍHO PROVOZU 40
7.2 SLEDOVÁNÍ OSOB A VĚCÍ 41
8 EMPIRICKÁ ČÁST 42
8.1 CÍL EMPIRICKÉ ČÁSTI 42
8.2 PREVENCE A BEZPEČNOST DĚTÍ 42
8.2.1 ZABEZPEČENÍ A UŽIVATELSKÉ PŘÍSTUPY 43
8.2.2 INTERNET A SOCIÁLNÍ SÍTĚ 44
8.3 PREVENCE A BEZPEČNOST DOSPĚLÝCH 45
8.3.1 INTERNETOVÉ OBCHODY 47
8.4 ROZBOR STATISTICKÝCH DAT 48
8.5 POPIS PŘÍPADU KAZUISTIKY 49
8.5.1 ROZBOR PŘÍPADU 50
8.6 NÁVRH ČESKÉ PIRÁTSKÉ STRANY KE ZRUŠENÍ UCHOVÁVÁNÍ TELEKOMUNIKAČNÍHO PROVOZU 52
8.6.1 KOMENTÁŘ 58
ZÁVĚR A NÁVRH DE LEGE FERENDA 61
SEZNAM POUŽITÝCH ZDROJŮ 63
SEZNAM PŘÍLOH 65

ÚVOD

Volba tématu Bakalářské práce byla ovlivněna praxeologickými zkušenostmi zpracovatele, který je služebně zařazen na službě kriminální policie a vyšetřování se zaměřením na odhalování a vyšetřování informační kriminality. Informační kriminalita svým rozsahem každoročně zvyšuje svůj podíl na celkovém počtu registrovaných skutků kriminality. Důvodem je, že výpočetní zařízení a moderní komunikační prostředky jsou součástí našeho života na každém kroku a jejich absenci si již nedokážeme představit. Důležitým faktorem pro odhalování informační kriminality jsou velmi dobré znalosti výpočetních zařízení a moderních komunikačních technologií. Tyto potřebné nutné znalosti stěžují odhalování informační kriminality a současně umožňují právě pachatelům, mající tyto znalosti, snadnějšího získání prospěchu ku škodě poškozených osob nemajících dostatečné znalosti, ba dokonce u nichž tyto znalosti zcela absentují, čím se snadněji tyto neznalé osoby dostávají do postavení poškozených. Její páchání je pro pachatele snadnější. Pachatelé se v tomto případě nemusí dopouštět trestné činnosti fyzicky na „ulici“, kde jim hrozí riziko snížení anonymity při „face-to-face“ páchání trestné činnosti a kde jsou nuceni překonat alespoň z části své možné osobnostní zábrany. Forma trestné činnosti na „ulici“ neposkytuje dostatek času k zakrytí této trestné činnosti do doby jejího prověřování či objasnění. Stejně tak výnos nedosahuje v současné době takové výše jako v případě informační kriminality. Informační kriminalita poměrně snadno svým pachatelům odbourává zmíněné překážky.

V teoretické části je nejprve osvětleno základní pojmosloví informační kriminality, její typy, hackerské programové nástroje, techniky a další výsledky hackerské činnosti. Autor dále rozděluje informační kriminalitu z pohledu Úmluvy o počítačové kriminalitě a zasazuje jednotlivé trestné činy trestního práva hmotného do jejích okruhů. Dále se věnuje pojmu telekomunikační provoz a uvádí nejčastěji vyžadované úkony trestního práva procesního za účelem objasnění informační kriminality.

V empirické části se autor zaměřuje na statistické výstupy Českého statistického úřadu a Policie České republiky. Dále v této části práce popisuje kazuistiku konkrétního případu informační kriminality včetně přiblížení postupu policejního orgánu při jejím objasňování. Autor se dále věnuje návrhu de lege ferenda.

CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Hlavním cílem práce je teoreticko-praktickým vhledem popsat pojem informační kriminality. Definovat základní pojmosloví a informační kriminalitu z pohledu Úmluvy o počítačové kriminalitě se zařazením jednotlivých trestných činů trestního práva hmotného do jejích okruhů. Dále je v rámci informační kriminality cílem charakterizovat telekomunikační provoz a popsat základní procesní úkony trestního práva procesního, které jsou nejčastěji užívány k jejímu objasňování. Vedlejším cílem je poskytnou praxeologický vhled do zkoumané problematiky informační kriminality popsáním vybrané kazuistiky konkrétního případu informační kriminality a blíže přiblížit postup policejního orgánu v konkrétním příkladu postupu základního objasňování trestné činnosti. Dalším vedlejším cílem bakalářské práce je komparativní metodou porovnat a vyhodnotit statistická data informační společnosti a informační kriminality v posledních letech. Na základě těchto vyhodnocených dat potvrdit hypotézu o vzrůstající tendenci informační kriminality. Současně je dalším vedlejším cílem věnování se prevenci a bezpečnosti v zájmu ochrany před informační kriminalitou. Souhrnně se dá říci, že cílem bakalářské práce je poskytnout dostupné poznatky zejména z praxe, ale také ze samotné teorie informační kriminality.

V práci budou použity metody:

- Rozbory dokumentů právní úpravy týkající se informační kriminality

- Porovnání statistických dat komparativní metodou

- Popis kazuistiky konkrétního vybraného příkladu

- Analyticko-syntetizující metoda k objasnění základních východisek pojmosloví.

1 DEFINICE INFORMAČNÍ KRIMINALITY

Informační kriminalitou je označována skupina trestných činů mající stejný charakter a v níž určitým způsobem figuruje počítač či jakékoli výpočetní zařízení. V informační kriminalitě může tedy počítač či jakékoli jiné výpočetní zařízení figurovat jako předmět či jako nástroj. Tj. počítač může být cílem útoku (resp. nejčastějším terčem útoku jsou právě data v něm uložená), nicméně počítač jako technický prostředek je také vznikající nástroj trestné činnosti.[1]

V širším okruhu pak informační kriminalitou můžeme označit protiprávní jednání, k jehož spáchání je použité jakéhokoli výpočetní zařízení, specifický prvek počítačové sítě či elektronická data způsobilá dopustit se zamýšleného protiprávního jednání případně, zda ke spáchání protiprávního jednání jsou tyto zmíněné prvky užity pro zakrytí identity pachatele. Z pohledu evropského práva a zejména orgánů činných v trestním řízení zpravidla informační kriminalitou označujeme specifické stěžejní trestné činy, které budou uvedeny v další kapitole.

V poslední době tak jako pojem počítačová kriminalita nahradil pojem informační kriminalita, je v současné době informační kriminalita označována jako kybernetická kriminalita neboli cybercrime či kyberzločin a to vzhledem k rozsahu a podílu této trestné činnosti v celkovém počtu registrovaných skutků kriminality.

[1] MATOUŠKOVÁ, I. *Aplikovaná forenzní psychologie*. Praha: Grada, 2013. 304 s. ISBN 978-80-247-4580-0, s. 154.

2 ÚMLUVA O POČÍTAČOVÉ KRIMINALITĚ

Vzhledem k postupnému nárůstu užívání informačních technologií ze strany obyvatel celého světa vlivem pokrokového rozvoje na poli informačních technologií, které začaly provázet stále sofistikovanější a časté cílené útoky na zařízení informačních technologií s rozsáhlými ekonomickými škodami, v některých případech ohrožující i svrchovanost samostatných států, bylo jen na čase, kdy tento globální problém informační kriminality bude řešen na mezinárodní úrovni. Výborem ministrů Rady Evropy pak byla dne 23.11.2011 v Budapešti otevřena k podpisu Úmluva o počítačové kriminalitě.

Cílem Úmluvy je vytvořit mezinárodní právní rámec pro účinné potírání počítačové kriminality prostřednictvím harmonizace prvků skutkových podstat v oblasti počítačové kriminality za účelem zajištění adekvátního postihu pachatelů, stanovení nezbytných vnitrostátních vyšetřovacích pravomocí pro zajišťování důkazů v elektronické formě a vyšetřování počítačové kriminality, jakož i zavedení pohotového a efektivního režimu mezinárodní spolupráce ve vztahu k trestným činům souvisejícím s informačními technologiemi.[2]

2.1 ROZDĚLENÍ INFORMAČNÍ KRIMINALITY Z POHLEDU ÚMLUVY O POČÍTAČOVÉ KRIMINALITĚ

Úmluva o počítačové kriminalitě rozděluje trestné činy v oblasti informační kriminality do čtyř oblastí:

a) trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů,
b) trestné činy související s počítačem,
c) trestné činy související s obsahem,
d) trestné činy týkající se porušení autorského práva.[3]

[2] ČESKO. Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě (Budapešť, 23. listopadu 2001). In *PARLAMENT ČESKÉ REPUBLIKY POSLANECKÁ SNĚMOVNA*. 24 s. 2013, VI. volební období, 890/0, s. 3. Dostupné také z WWW: <http://www.psp.cz/doc/00/13/95/00139513.pdf>

[3] FRANCIE. Council of Europe. *Convention on Cybercrime - ETS no. 185. Budapest*. [online]. Council of Europe, © 2001 [cit. 2017-12-06]. Dostupné z WWW: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>.

Zařazení níže uvedených skutkových podstat trestných činů do uvedených čtyř oblastí není nikterak přesně vymezené. Do uvedených oblastí lze zařadit i jednání vykazující znaky přestupku a to až do okamžiku, než je jeho trestně právní kvalifikací spolehlivě vyloučeno, že se nejedná o jednání naplňující některou ze skutkových podstat trestných činů uvedených ve zvláštní části trestního zákoníku. V praxi se jedná o případ evidování celkových počtů registrovaných skutků kriminality po celém území České republiky ze strany policejního orgánu, v tomto případě Policie České republiky, který v těchto evidencích eviduje jak registrované trestné činy, tak i rovněž jednání vykazující znaky přestupku. Tento policejní orgán pak ověřováním ve svých evidencích zjišťuje, zda nejsou dány důvody pro konání společného řízení, kterými může být například vztah ke způsobené škodě, čímž dojde ke změně trestně právní kvalifikace a postupu ve smyslu ustanovení § 158 odst. 3 trestního řádu. Policejní orgán tak zahájí úkony trestního řízení pro konkrétní skutkovou podstatu trestného činu uvedené ve zvláštní části trestního zákoníku. K samotnému zařazení skutkových podstat trestných činů do uvedených čtyř oblastí je třeba uvést, že toto není dogmatem, když je zřejmé, že trestná činnost může být páchána v souběhu jak se všemi níže uvedenými skutkovými podstatami trestných činů, tak rovněž může dojít k souběhu i s jinými skutkovými podstatami trestných činů uvedených ve zvláštní části trestního zákoníku. V tomto ohledu je problematika informační kriminality zcela různorodá.

2.1.1 TRESTNÉ ČINY PROTI DŮVĚRNOSTI, INTEGRITĚ A POUŽITELNOSTI POČÍTAČOVÝCH DAT A SYSTÉMŮ

V rámci informační kriminality můžeme mezi trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů uvést stěžejní trestné činy uvedené v zákoně č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a to:

§ 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.

2.1.2 TRESTNÉ ČINY SOUVISEJÍCÍ S POČÍTAČEM

V rámci informační kriminality můžeme mezi trestné činy související s počítačem uvést stěžejní trestné činy uvedené v zákoně č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a to:

§ 180 Neoprávněné nakládání s osobními údaji,

§ 181 Poškození cizích práv,

§ 182 Porušení tajemství dopravovaných zpráv,

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,

§ 184 Pomluva,

§ 209 Podvod.

2.1.3 TRESTNÉ ČINY SOUVISEJÍCÍ S OBSAHEM

V rámci informační kriminality můžeme mezi trestné činy související s obsahem uvést stěžejní trestné činy uvedené v zákoně č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a to:

§ 191 Šíření pornografie,

§ 192 Výroba a jiné nakládání s dětskou pornografií,

§ 352 Násilí proti skupině obyvatelů a proti jednotlivci,

§ 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob,

§ 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod,

§ 403 Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka,

§ 404 Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka,

§ 405 Popírání, zpochybňování, schvalování a ospravedlňování genocidia.

2.1.4 TRESTNÉ ČINY TÝKAJÍCÍ SE PORUŠENÍ AUTORSKÉHO PRÁVA

V rámci informační kriminality lze z pohledu našeho právního řádu mezi trestné činy související s obsahem zařadit trestný čin uvedený v zákoně č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a to § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.

3 TYPY PROTIPRÁVNÍHO JEDNÁNÍ

3.1 HACKING

Zjednodušeně bychom v současném pojetí mohli definovat hacking jako proniknutí do počítačového nebo řídícího systému jinou než standartní cestou při obejití nebo prolomení jeho bezpečnostní ochrany.[4]

Za účelem proniknutí do počítačového nebo řídícího systému užívá hacker různé hardwarové či softwarové nástroje. Hacking můžeme rozdělit na dva typy a to hacking etický a nelegální.

Etický hacking spočívá v tom, že profesionální hacker za úplatu prostřednictvím např. formou tzv. penetračních testů testuje komerční produkt s cílem vyhledat slabinu počítačového nebo řídícího systému v podobě nedostatečně vytvořené bezpečnostní ochrany. Při jejím zjištění tento poznatek předává objednateli, případně vytvoří a naprogramuje konkrétní záplatu tak, aby byl komerční produkt dostatečně bezpečnostně ochráněn. Tyto zjištěné informace o bezpečnostní hrozbě však nevyužije a neposkytne třetí straně. V opačném případě by se již jednalo o hacking nelegální a trestně právně postižitelný.

V případě nelegálního hackingu hacker působí za pomoci hardwarových a softwarových nástrojů na vytipované cíle. Zpravidla je mu útěchou kladné obejití nebo prolomení bezpečnostní ochrany počítačového nebo řídícího systému bez motivace finančního zisku, tato činnost je mu zábavou.

Hackeři mají v oblibě v současné době i další nástroj v podobě tzv. sociálního inženýrství, když se v tomto případě snaží přimět svoji předem vytipovanou oběť k tomu, aby mu své přístupové údaje ke konkrétnímu účtu počítačového systému sdělila zcela dobrovolně, čímž si tak hacker jednoduchým způsobem opatří heslo, jež současně poté přechovává. K sociálnímu inženýrství hacker zejména přistupuje prostřednictvím sociálních sítí, kde se snaží pod smyšlenou legendou či identitou (smyšlenou či odcizenou) obelstít konkrétní vytipovanou oběť tak, aby mu uvěřila a své přístupové údaje jednoduše poskytla. V některých případech pak dále využívá chyb obětí, které

[4] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2, s. 102.

důležité údaje v dobrém úmyslu zveřejnili, avšak se může jednat o údaje, které by měli být před veřejností zůstat utajené, neboť se může jednat o osobní či obchodním tajemství.

3.2 CRACKING

Ačkoli je cracking úzce spojen s hackingem, hlavní rozdíl mezi těmito činnostmi tkví v tom, že cracker, mající znalosti hackera, je motivován záměrně způsobit škodu komerční společnosti a to takové, která je výrobcem a nositelem autorského práva ke svému komerčnímu dílu, zpravidla softwaru. I přesto, že tyto komerční společnosti opatřují svůj software ochrannými prvky v podobě zabezpečení svého softwaru před možností jeho kopírováním, nutností jeho registrací na sériové číslo, šifrováním, zpřístupnění softwaru pod verzemi jako např. trialware, shareware či demoverze, je právě cracker motivován k tomu, aby jako hacker obešel nebo prolomil bezpečnostní ochrany v podobě tohoto ochranného prvku a následně jako cracker vytvořil software umožňující následné překonání ochranného prvku všem uživatelům, kterým tento software poskytne. Činnost, kdy je neoprávněně šířeno komerční dílo právě s crackerským softwarem dalším uživatelům s cílem užívat plnohodnotně toto komerční dílo a způsobit tak škodu jejímu výrobci, je nazýváno jako warez. Výsledek činnosti crackera v podobě jeho vytvořeného softwaru umožňující překonání bezpečnostní ochrany může být:

- ✓ **crack** - software sloužící k překonání bezpečnostní ochrany, který v originálním komerčním produktu přepíše potřebné údaje tak, aby byl poté pro jeho neoprávněného uživatele plně spustitelný se svými všemi funkcemi
- ✓ **keygen** - software generující různé kombinace sériových čísel potřebných pro registraci originálního komerčního produktu tak, aby byl poté pro jeho neoprávněného uživatele plně spustitelný se svými všemi funkcemi.

3.3 POČÍTAČOVÉ PIRÁTSTVÍ

Ve většině případů si pod pojmem informační kriminality představíme právě počítačové pirátství. Počítačové pirátství se zejména v České republice rozvíjelo již v době prvních počítačů. Tehdejší uživatelé se snažili vyhnout pořizování drahých licencí

za počítačové programy, hudbu či dokonce filmy. Mezi uživateli probíhala výměna nelegálních dat, která dále sdíleli, kopírovali a vypalovali na datová média. V minulosti se tento postup ve velké míře například odehrával mezi vysokoškolskými studenty elektrotechnických oborů, kteří měli přístup k veřejné síti internet prostřednictvím počítačových sítí vysokých škol, neboť na počátku vývoje nebyla veřejná síť internet rozšířena do běžných domácností našich rodin. Dnes se ruku v ruce vývoj počítačového pirátství výrazně posunul a to i s ohledem na nepřeberné množství jakýchkoli titulů, když v současnosti je zcela běžné, aby si uživatelé veřejné sítě internet běžně jakákoli tato nelegální data v podobě chráněných titulů stáhnuli do svých zařízení, neboť připojení k veřejné síti internet dnes již máme odkudkoli a kdekoli.

Počítačové pirátství je neoprávněné šíření nelegálních chráněných titulů v oblasti software a hudebních či filmových titulů a to zejména pomocí datových médií nebo jejich sdílením ve formě:

- ✓ **warez**
- ✓ **na FTP serverech**
- ✓ **P2P sítích**
- ✓ **datových úložištích**

nebo jejich zveřejňování například na webových stránkách v on-line přehrávačích či šíření a zveřejňování jejich internetových odkazů za účelem jejich stažení ze stran uživatelů těchto webových stránek. S vývojem počítačového pirátství se zcela jistě vyvíjí i crackerská činnost, když u chráněných titulů v oblasti software je třeba rovněž tvořit a šířit software umožňující překonání bezpečnostní ochrany těchto chráněných titulů.

3.3.1 WAREZ

Za účelem ztížení odhalitelnosti před veřejností si uživatelé warezu mezi sebou zřizují různé webové stránky s warezovými fóry či diskuzemi, kde mají své příspěvky roztříděny do jednotlivých sekcí dle konkrétního zaměření. Najdeme zde jak poradenské služby, nelegální chráněné tituly, tak rovněž i pornografický obsah a například i přístupová hesla na různé jinak placené webové služby. Samozřejmostí těchto warezových skupin je organizovanost jejich vzájemných postavení. Zpravidla jsou tyto warezová fóra či diskuze financovány z darů vlastních uživatelů, případně ze zisků z

prodeje reklamy, kterou na tyto stránky umísťují. Na těchto warezových fórech zpravidla funguje i směnný systém, tzn. může být zřízena elektronická měna, kterou si uživatelé mezi sebou zakupují buď za skutečné finanční prostředky, případně za provedené služby si mohou uživatelé část této elektronické měny darovat.

3.3.2 FTP SERVERY

Jedná se o zpřístupnění dat na jakémkoli serveru, když přístup k tomuto serveru a přenos souborů je realizován FTP protokolem (File Transfer Protocol), který je zabezpečen přístupovými právy a k tomuto zřízenému FTP serveru je uživateli zpravidla přistupováno prostřednictvím FTP klienta. Uživatel, který na FTP server přistoupí, pak vidí všechny sdílené složky se soubory, které mu jsou zpřístupněny. Obdobným řešením jsou rovněž tzv. cloudová úložiště, které jsem se rozhodl zařadit zde. Cloudová úložiště jsou službou různých poskytovatelů, kdy mezi ty největší patří např. Google, Microsoft či DropBox, kteří na svých serverech uživateli vyhradí prostor určité velikosti, kam můžou být uživatelem ukládána data. K této službě cloudového úložiště a jejímu přístupu slouží rovněž obdobní klienti. Za větší prostor úložiště je možné si připlatit. Přístupové údaje k této službě cloudového úložiště mohou uživatelé mezi sebou rovněž sdílet a přistupovat tak ke zde uloženým datům.

3.3.3 P2P SÍTĚ

Jedná se o počítačovou výměnou síť, ve které mezi sebou komunikují její uživatelé navzájem. Prostřednictvím této sítě uživatelé sdílí své soubory prostřednictvím klientů na tzv. Direct Connect sítích. Množství těchto klientů je mnoho, mezi nejčastější např. DC++, BCDC++, StrongDC++, CzDC či LinuxDC++. Právě pomocí těchto snadno ovladatelných klientů se uživatelé připojují na konkrétní P2P sítě, komunikují s uživateli těchto sítí a zjednodušeně řečeno si mezi sebou nabízí své sdílené soubory.

3.3.4 DATOVÁ ÚLOŽIŠTĚ

V současnosti mezi nejvyužívanější datová úložiště, kam uživatelé nahrávají svá data, jsou např. datová úložiště www.sdilej.cz či www.uloz.to a další. Obdobných platforem je nepřeberné množství a to zejména v zahraničí. Na těchto datových úložištích je možné i bez vlastní registrace za pomoci webového vyhledávače vyhledat konkrétní data a tyto stáhnout, kdy přenosová rychlost je omezená. V případě registrace

a předplacení registrovaného účtu je možné konkrétní data stahovat neomezenou rychlostí v závislosti na rychlosti připojení tohoto uživatele.

3.4 ŠÍŘENÍ MATERIÁLŮ SE ZÁVADNÝM OBSAHEM

Za šíření materiálu se závadným obsahem řadíme všeobecně problematiku šíření obtěžujícího, hanlivého obsahu, obsahu proti lidské důstojnosti, obsahu diskriminujícího proti náboženství, vyznání, rasy, pohlaví, obsahu propagujícího násilí, protiprávní jednání, extremismus a rovněž obsahu šířícího pornografii.

3.5 ZNEUŽITÍ INTERNETOVÝCH STRÁNEK

V tomto směru můžeme považovat jednání mající pomluvný charakter, zveřejnění osobních údajů a porušení jejich práva na ochranu, sdělení telefonního kontaktu na danou osobu, znevážení osoby vystavením nevhodné fotografie či jiného snímku, zveřejněním jejích kontaktních údajů např. na erotické seznamce či např. zveřejnění nepravdivé interpretace osoby s ohledem na protiprávní podtext.

3.6 SPAMMING

Spam je produkt společnosti Hormel Foods. Jedná se o masovou konzervu obsahující vepřové, mechanicky separované kuřecí maso, šunku, sůl, cukr, vodu, koření a dusitan sodný. V podstatě se jedná o lančmít vyráběný v USA, který se proslavil zejména během 2. světové války a po ní, kdy nahrazoval chybějící maso. Díky své trvanlivosti se mohl skladovat téměř po neomezenou dobu. Ostatně i na webu *http://store.spam.com/spam-classic* se dočtete: The original. The timeless.

Díky britské komediální skupině Monthy Python bude SPAM skutečně nadčasový a věčný. Právě skeč pojednávající o objednávání jídla (dostupný z: *http://www.youtube.com/watch?v=nZG6lQPQKlI*) zapříčinil následně tu skutečnost, že byl pojem spam použit pro označení nevyžádaného produktu, v ICT zejména pro označení nevyžádané komunikace.[5]

[5] KOLOUCH, J. *Cybercrime.* Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 231.

Pro spam je příznačné, že se jedná o sdělení, které je zaslané elektronicky, hromadně a zejména bez vyžádání.[6]

3.6.1 SCAM

Spam obsahující kriminální či jiný podvodný obsah je označován jako scam (z anglického „scam“ – podvod, švindl). Scamy tvoří v současnosti podstatnou část spamu a jejich účelem je, typicky za použití sociálního inženýrství, získat důvěru uživatele a donutit ho vykonat požadované úkony (např. otevření přílohy e-mailu, navštívení zobrazeného URL aj.).[7]

3.6.2 SCAM 419

SCAM 419 je označení pro druh podvodu u nás známého spíše jako Nigerijské dopisy. Tyto podvody nejsou žádnou novinkou, existovaly již dříve buď ve formě klasického dopisu nebo byly rozesílány faxem.

Rozvoj e-mailové komunikace umožnil za velice nízké náklady oslovit v krátkém časovém období milióny uživatelů. se tyto podvody masově rozšířily, ale princip zůstává stejný: osloví vás neznámý člověk, že zdědil, získal nebo dokonce spravuje něčí majetek ve výši několika desítek miliónů dolarů a potřebuje pomoc při jeho převodu ze země. Za to je slíbená tučná odměna ve výši několika desítek procent z celkové částky. Princip podvodu spočívá v tom, že oběť musí neustále platit nečekané administrativní poplatky a převod majetku se stále oddaluje.

S rozvojem internetových a elektronických služeb vymýšlejí podvodníci stále nové triky, jak vylákat z neopatrných uživatelů peníze. Někdy jsou to falešné nabídky neexistujícího zboží v internetových aukcích, podvodné inzeráty na prodej levného automobilu nebo pronájem bytů. Podvodníci se neštítí zneužívat různá neštěstí nebo přírodní katastrofy k nachytání dalších obětí.

Některé podvody bývají v principu jednoduše provedeny, ale velmi často bývají propracovány i do drobných detailů, jako jsou profesionálně vytvořeny webové stránky neexistujících společností a bankovních institucí. Obětem bývají zasílány i podvržené falešné dokumenty a certifikáty.

[6,7] KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 232,235.

K získání peněz a zametení stop slouží tzv. bílí koně (nebo také mules, arrow). Ti vyberou peníze z účtu, kam je oběť pod různými záminkami poslala a převedou na jiný účet. Bílí koně bývají nalákáni nabídkou na zajímavou a jednoduchou práci, která spočívá pouze v občasném převedení peněz. Tyto nabídky opět většinou chodí jako nevyžádaná pošta. U bílých koní stopa většinou končí a jsou to právě oni, kdo pyká za podvod jehož byli i nevědomky spolupachateli.[8]

3.6.3 PODVODNÉ NABÍDKY

Velmi úspěšnou formou scamu jsou různé podvodné nabídky, které mohou být rozesílány hromadně či cíleně. V současnosti jsou takovéto nabídky rozesílány nejen prostřednictvím e-mailů, ale i pomocí jakýchkoliv instant messengerů, sociálních sítí, aukčních portálů atd. Pokud jde o hromadné rozesílání podvodných nabídek, je možné si pod tímto pojmem představit celou řadu aktivit na principu „pyramida“ či „letadlo“, nabídky výhodných prací z domova, „zaručené“ metody zhodnocení peněz (s nejvyššími úroky), nabídky na půjčku (s nejnižšími úroky), „skvělé“ pracovní příležitosti aj.[9]

3.7 SNIFFING

Sniffing je metoda nelegálního odposlechu dat procházejících počítačovou sítí při komunikaci mezi poskytovanou službou a počítačovým systémem prostřednictvím tzv. snifferu.

Technicky sniffing znamená odchytávání a čtení TCP paketů. Z bezpečnostního pohledu je sniffing možné označit také jako monitoring sítě, či monitoring provozu sítě a jedná se o jeden ze standardních prostředků pro diagnostiku sítě, respektive diagnostiku anomálií v síťovém provozu. Monitoring sítě je pak schopen zobrazit například nestandardní komunikaci počítačového systému napadeného malwarem atp. Vlastní činnost správců sítě v případě monitoringu sítě není nelegální (pokud se nedopustí dalšího jednání, které by mohlo případnou právní odpovědnost zakládat – např. instalace keylogger, či jiného malware do počítačového systému bez vědomí uživatele), neboť umožňuje udržet a spravovat počítačovou síť.

[8] SCAM419. Josef Džubák & HOAX.cz [online]. © 2000-2017 [cit. 2017-12-07]. Dostupné z WWW: <http://www.hoax.cz/scam419/co-je-to-scam-419>.
[9] KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 240.

Pro to, aby bylo možné sniffing subsumovat pod jeden z projevů kyberkriminality, je třeba, aby osoba provádějící tuto činnost jednala nelegálně, typicky bez souhlasu či vědomí uživatele. Z dat zachycených sniffingem je útočník schopen extrahovat a složit citlivé informace o uživateli, např. přihlašovací údaje (uživatelské jméno a heslo), e-mailovou či VoIP komunikaci, informace o používaných službách aj. Ke sniffingu může být využit i malware v podobě trojských koní, keyloggerů nebo například spyware.[10]

3.8 PHREAKING

Jedná se o neoprávněné zneužívání telekomunikačních služeb tak, aby jejich neoprávněný uživatel nehradil služby jejímu poskytovateli. V daném případě se může ze strany neoprávněného uživatele jednat o využití bezpečnostní chyby umožňujícímu zneužívat tyto telekomunikační služby, případně tento překoná bezpečnostní ochranný prvek, který byl původně zřízen, aby takovému protiprávnímu jednání zamezil.

3.9 CYBERSQUATING

Pod tímto záhadným názvem se skrývá donedávna legální blokování internetových domén. Zaregistrování domén s názvem velkého podniku, instituce nebo produktu a spekulace s prodejem tohoto jména má již svůj zenit za sebou a dobíhající legislativa už asi nebude mít co postihovat. Svůj význam měl cybersquatting v době, kdy velké firmy na internet vstupovaly, nebo se rozhodovaly uvést na internetu své výrobky.[11]

3.10 PHISHING A PHARMING

Samotný phishing má základ v anglickém slově fishing a ve spojení s informační kriminalitou je zřejmé, že se bude jednat o snahu "chytit" svoji oběť. Klasickým principem phishingu je zaslání elektronické pošty jejímu příjemci, který je vyzván v jejím textu na kliknutí na odkaz pod podvodnou legendou např. k přihlášení do internetového bankovnictví. Příjemce, v tomto případě tedy oběť, na tento odkaz klikne,

[10] KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 294.
[11] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2, s. 107.

přičemž se mu v prohlížeči otevře podvodná webová stránka pod názvem obdobné webové adresy skutečného internetového bankovnictví tvářící se na první pohled jako skutečné webové stránky internetového bankovnictví příjemce. Příjemce v domnění, že se jedná o skutečné internetové bankovnictví, vyplní své přihlašovací údaje a pokusí se do internetového bankovnictví přihlásit. Vzhledem k tomu, že se jedná o podvodné internetové stránky, zpravidla tyto nahlásí chybu, avšak těmito přihlašovacími údaji neoprávněně disponuje již třetí strana.

Samotný pharming je již vyspělejší podvodnou metodou, která v případě, že oběť zadá do okna svého prohlížeče konkrétní stránky svého internetového bankovnictví, pharming za pomoci napadeného DNS záznamu uvedeného počítače přepíše cílovou IP adresu webových stránek internetového bankovnictví, které chtěla oběť navštívit a přesměruje oběť na podvodné internetové stránky tvářící se na první pohled jako skutečné webové stránky např. internetového bankovnictví a to za účelem, aby opět oběť zadala své přihlašovací údaje, kterých se poté třetí strana zmocní. Pharming je nebezpečný právě v tom, že ačkoli je oběť sebeobezřetnější, nedozví se ihned, že je přesměrována na podvodné internetové bankovnictví, a to i přesto, že do pole pro zadání webové adresy skutečně sama ručně požadovanou webovou adresu zadala.

3.10.1 SPEAR PHISHING

Spear phishing je jednou z forem phishingového útoku, avšak s tím rozdílem, že spear phishing je přesně cílený útok, na rozdíl od phishingu, který je útokem spíše plošným (nahodilým). Cílem útoku bývá konkrétní skupina, organizace nebo jednotlivec, konkrétně informace a data, která se v této organizaci nacházejí (např. duševního vlastnictví, osobní a finanční údaje, obchodní strategie, utajované informace aj.).

U spear phishingu oproti klasickému phishingu je rozdíl v tom, kdo je odesílatelem předmětných zpráv. V počátku útoku je to vlastní útočník, který využije otevřené zdroje, aby zjistil co nejvíce informací o napadané organizaci, její struktuře atd. Dále vytvoří velmi kvalitní e-mail či jinou zprávu a začne komunikovat s osobou zevnitř organizace jako s kolegou. Tuto osobu pak útočník využije jako prostředek pro šíření dalších zpráv (např. infikovaných malware) v rámci organizace. Jelikož se jedná o

osobu obětem „známou“, nemají problém s ní komunikovat a méně, pokud vůbec, prověřují její zprávy.[12]

3.10.2 VISHING

Pojem vishing označuje telefonický phishing, při kterém útočník využívá technik sociálního inženýrství a snaží se od uživatele vylákat citlivé informace (např. čísla účtů, přihlašovací údaje – jméno a heslo, čísla platebních karet, aj). Útočník se záměrně snaží zfalšovat svoji identitu. Útočníci se často představují jako zástupci skutečných bank či jiných institucí, aby u uživatele vyvolali co nejmenší podezření. Vishing se používá ve VoIP (Voice over Internet Protocol) telefonii.[13]

3.10.3 SMISHING

Smishing funguje na podobném principu jako vishing či phishing, ale k distribuci zpráv využívá SMS zprávy. V rámci smishingu jde primárně o snahu donutit uživatele zaplatit částku (například zavolat na placenou linku, poslat dárcovskou SMS aj.) nebo kliknout na podezřelé URL odkazy. Pokud uživatel uvedené URL navštíví, je přesměrován na stránku, která zneužívá určité zranitelnosti počítačového systému, případně je uživatel vyzván k zadání citlivých údajů či k instalaci malware.[14]

3.11 KYBERNETICKÉ VÝPALNÉ

Jakkoli se zdá toto slovní spojení nesmyslné, jedná se o nový typ trestné činnosti založený na strachu z prezentované hrozby průniku do spravovaného nebo vlastněného systému s následujícím zneužitím nebo zničením dat. I když ze strany vyděrače to mnohdy může být pouze využití neznalosti vydírané strany, je to zcela nová projekce klasického deliktu do počítačového prostředí, kterou se zejména může rozmáhat organizovaný zločin.[15]

V největší míře se tohoto jednání užívá při šíření tzv. ransomware, který bude popsán dále.

---

[12] KOLOUCH, J. *Cybercrime.* Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 264.
[13,14] KOLOUCH, J. *Cybercrime.* Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 265,266.

[15] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2, s. 102-103.

3.12 KYBERŠIKANA, KYBERSTALKING, KYBERGROOMING

3.12.1 KYBERŠIKANA

Tímto termínem označujeme nebezpečné komunikační jevy realizované prostřednictvím informačních a komunikačních technologií (např. pomocí mobilních telefonů nebo služeb v rámci internetu), jež mají za následek ublížení nebo jiné poškození oběti. Toto ublížení či poškození může být jak záměrem útočníka, tak důsledkem např. nevhodného vtipu, nedorozumění mezi obětí a útočníkem, nedomyšlením důsledků jednání ze strany útočníka atd. Oběť je poškozována opakovaně, ať už původním útočníkem či osobami, které se do kyberšikany zapojí později. Kyberšikana je druhem psychické šikany.[16]

3.12.2 KYBERSTALKING

Stalking (lov, pronásledování) označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu. Pronásledovatel svou oběť například dlouhodobě sleduje, bombarduje SMS zprávami, e-maily, telefonáty či nechtěnými pozornostmi (dárky). Útočník u oběti vyvolává pocit strachu. Ve spojení s využitím informačních technologií u útočníka hovoříme o termínu kyberstalking.[17]

3.12.3 KYBERGROOMING

Tento termín označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod. Kybergrooming je druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií.[18]

3.13 ŠKODLIVÉ ŠÍŘENÍ INFORMACÍ

Škodlivé šíření informací se nazývá jako tzv. hoax. Hoax je specifická forma spamu, falešná či žertovná poplašná zpráva (mystifikace), vyzývající adresáta, aby něco

[16,17,18] KOPECKÝ, K., KREJČÍ, V. *Rizika virtuální komunikace: příručka pro učitele a rodiče.* 1. vyd. Olomouc: NET UNIVERSITY, s.r.o., 2010. 34 s. ISBN 978-80-254-7866-O, s. 5,24,14.

učinil, nejčastěji, aby ji předal dál (nejlépe na několik adres), čímž se její šíření stává řetězovým.[19] Jako ideální příklad lze uvést řetězovou výzvu s doporučením, že jakmile se ocitneme v situaci a musíme pod nátlakem násilníka vybrat své peníze z bankomatu, máme zadat svůj PIN opačně, když dojde vyjma vydání finanční hotovosti rovněž k přivolání policie na pomoc. Ve skutečnosti však dojde k pouze zadání špatného PINu.

3.14 SOCIÁLNÍ INŽENÝRSTVÍ

Pokud bychom chtěli definovat pojem sociální inženýrství, bylo by možné říci, že jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli. Smyslem je v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je.

Hlavní myšlenkou sociálního inženýrství je nevyužívat různé ryze technické přístupy či nástroje například k prolomení hesla, když mnohem jednodušší je uvést oběť v omyl, ve kterém sama dobrovolně toto heslo prozradí. Nejslabším článkem bezpečnostního systému je a vždy bude člověk (uživatel). Jelikož na světě nemůže existovat počítačový systém, který by alespoň v nějaké fázi nebyl závislý na člověku (ať již jde o zprovoznění, nastavení, či údržbu počítačového systému), je nejjednodušší cestou získat potřebné informace právě od člověka. Právě jednoduchost útoku zacíleného na nejslabší článek celého systému z něj zpravidla činí tu nejúčinnější formu.

Pro sociální inženýrství je jedním z klíčových faktorů zisk co největšího množství informací o cíli útoku (ať již počítačovém systému, právnické či fyzické osobě). Mnohdy dochází k dlouhodobému působení na klíčovou osobu a budování „důvěry“ mezi útočníkem a obětí před vlastním útokem, přičemž útočník typicky využívá lidské neopatrnosti, důvěřivosti, ochoty pomoci jiným, lenosti, slabosti, strachu (např. aby se osoba nedostala do problémů), neodpovědnosti, hlouposti aj.

Útoky sociálního inženýrství jsou zpravidla vedeny třemi způsoby, přičemž tyto způsoby jsou navzájem kombinovány:

1) Sběr volně (veřejně) dostupných dat o cíli útoku,

[19] ČESKO. Základní definice, vztahující se k tématu kybernetické bezpečnosti. In *Ministerstvo vnitra České republiky*. 6 s. 2013, s. 5. Dostupné také z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>

2) Fyzický útok (útočník se například vydává za pracovníka servisní agentury – např. servis tiskáren, pracovník údržby aj.), při kterém se útočník snaží získat co nejvíce informací „zevnitř“ společnosti, případně citlivé informace o jednotlivých pracovnících (včetně např. prohledávání odpadků aj.),

3) Psychologický útok.

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit: podvodný e-mail či falešná webová stránka, telefonický hovor, útok „tváří v tvář“, prohledávání odpadků, prohledávání webu, sociálních sítí, tedy veřejně dostupných informací online, doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči, ponechání paměťového média v zájmové oblasti (např. firmě, u domu zaměstnance aj. toto médium pak typicky obsahuje malware), nabídka vyzkoušení služby online (např. nabídka cloudového úložiště, či některé zajímavé služby zdarma aj.), dodávka či nalezení zařízení (počítačového systému), falešný servisní technik a jiné.[20]

[20] KOLOUCH, J. *Cybercrime.* Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 186-188.

4 HACKERSKÉ PROGRAMOVÉ NÁSTROJE A TECHNIKY

4.1 PROLAMOVAČE HESEL

Prolamovače hesel jsou jedním z nejstarších nástrojů používaných hackery. Slouží, jak již název napovídá k prolomení ochrany nebo autorizace, která je prováděna statickým heslem. Princip jejich práce je jednoduchý - zkouší nejrůznější kombinace znaků, které podle uvážení autora prolamovače nebo jeho uživatele připadají v úvahu a pokud autorizace projde, je nalezené správné heslo odesláno hackerovi. Existují dva základní druhy útoků realizovaných prolamovači hesel:

- ✓ **slovníkové útoky**, které zkouší použít známá slova z vlastní databáze slov
- ✓ **útoky hrubou silou**, které postupně generují všechny možné kombinace potřebné délky z vybraných znaků a zkouší, zda náhodou nevyhovují zadanému heslu.[21]

4.2 BACKDOORS

Backdoors neboli zadní vrátka jsou velmi výstižným názvem pro kódy, které po instalaci na cílový počítač umožňují jeho vzdálené řízení. Jedná se o oblíbený hackerský nástroj a jakmile hacker objeví bezpečnostní díru, jeho prvním krokem je nainstalování backdoors. Typický hacker má vždy v záloze několik počítačů s tajně nainstalovaným nástrojem pro vzdálené řízení a čím je lepší, tím více strojů má k dispozici. Tyto, tzv. kompromitované stroje jsou pak používány k podnikání dalších útoků na cílový stroj. Často tento řetěz mezi útočníkem a cílovým strojem může mít i deset nebo více zkompromitovaných strojů, které izolují a chrání původního útočníka před odhalením.[22]

4.3 SKENERY

Skenery slouží pro zjištění otevřených portů počítače, a tedy i služeb, které na něm běží. Skener tak útočníkovi velmi rychle zjistí základní informace o cílovém

[21,22] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2, s. 62,63.

počítači a může sloužit i k získávání informací o operačním systému. Sken otevřených portů může být předzvěstí potencionálního útoku, a proto systémy se snaží tyto tzv. portskeny detekovat a spojení s možným útočníkem na nějakou dobu přerušit nebo učinit jiná bezpečnostní opatření.[23]

4.4 SNIFFERY

Sniffery jsou programy odposlouchávající síťový provoz a "čmuchající", co se kde děje. Nejedná se přímo o nástroj útoku, spíše prostředek k shromáždění informací potřebných pro přípravu útoku. Práce snifferu je jednoduchá, přepne síťové rozhraní do tzv. promiskuitního módu, a tak přijímá všechny pakety, které se na síti pohybují bez jakékoli další filtrace. Tyto pakety jsou zaznamenány a dále analyzovány - typ protokolu, IP adresy, MAC adresy, nastavění příznaků apod. Součástí analýzy je vydělení datové části s obsahem přenášené zprávy. Tak je možno odposlechnout komunikaci v síti, zachytit otevřeně přenášená hesla nebo jiné citlivé údaje.[24]

4.5 ROOTKITY

Rootkity jsou soubory technik pro skrývání činností prováděných na operačním systému. Na rozdíl od backdoors, které budou pravděpodobně brzo odhaleny, rootkit zůstává po kompromitaci účtu superuživatele stále v utajení. Jedná se o běžně užívané systémové programy, které jsou modifikovány tak, aby administrátor nic nepoznal a hacker měl ke stroji neomezený přístup.[25]

4.6 NÁSTROJE DOS

Zkratka DoS znamená "Denial of Service", neboli potlačení služby. Od základního potlačení služby se dále odvozují specifické útoky podobného ražení, jako např. potlačení přístupu DoA - "Denial of Access". Myšlenka tohoto útoku je jednoduchá - pokud nemohu zaútočit přímo na cílový stroj, zaútočím na jeho spojovací cesty. Existuje několik základních metod DoS:

[23,24,25] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2, s. 64,65.

- ✓ v zahlcení odesíláním jalových paketů z více strojů (tzv. DDoS - Distributed Denial of Service)
- ✓ v zahlcení příkazem ping do sítě cílového stroje,
- ✓ v zahlcení volných systémových prostředků.[26]

V každém případě tento útok způsobí na cílovém stroji jeho nemožnost odpovídat na síti jeho legitimním uživatelům, čímž je po dobu útoku znemožněn přístup k jeho službám.

4.7 TROJSKÝ KŮŇ

Už jeho historický název již vypovídá o jeho zvláštní funkci a účelu. Trojský kůň patří mezi nejoblíbenější hackerský nástroj současnosti. Jedná se o malé programy, které jsou zabaleny do volně stažitelného kódu utility nebo do nové bezplatně poskytované hry. Trojské koně se používají na nejrůznější účely, od pouhého monitorování činnosti cílového počítače až po zneužití pro útok DoS. Zajímavou variantou trojských koní jsou "dataminery" neboli programy, které po nainstalování monitorují činnost uživatele a zajímavé údaje odesílají do sběrného místa. Ty rozlišuje podle předem známých kritérií, např. při přihlašování k účtu v bance zaznamená stisknuté klávesy, a tak prozradí hackerovi přístupové kódy k manipulaci s účtem.[27]

Trojský kůň je podmnožinou malware, který bude popsán dále.

4.8 NÁSTROJE PRŮZKUMU SÍTĚ

Nástroje průzkumu sítě jsou většinou jednoduché programy, které zjišťují propojení a další technologické vlastnosti elementů cílové sítě. I obyčejný příkaz ping nebo tracert vede k získání celé řady informací o cílové síti. Hackeři tyto nástroje automatizovali, doplnili grafikou a lze je stáhnout nebo spustit přímo na internetu.

[26,27] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2, s. 66,67.

Úplným pokladem pro útočníka jsou špatně nakonfigurované DNS servery se záznamy o struktuře celé obsluhované sítě.[28]

4.9 DEBUGGER

Debbuger je nástroj používaný běžně při ladění nového programu, je neodmyslitelnou pomůckou každého hackera. Postup je obvykle takový, že útočník se snaží vložit svůj kód do místa, které chce využít. Debugger umožní ověření správné funkce kódu, ale mnohdy i nalezení nevhodnějšího místa pro uložení odskoku a výkonného kódu útočníka. Toho lze využít i při odhalování částí kódu pro kontrolu platné licence k programu. V tomto případě útočník zjišťuje, kde se ukrývá podprogram, kontrolující zda přidělené číslo licence odpovídá správnému číslu, a tedy zda program je provozován jeho původním vlastníkem. Crackeři používají debugger na nalezení tohoto podprogramu a jeho následné odstranění, čímž zbaví program jeho ochranných prvků.[29]

[28,29] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2, s. 67,68.

5 NĚKTERÉ DALŠÍ VÝSLEDKY HACKERSKÉ ČINNOSTI

5.1 MALWARE

Malware je souhrnný pojem pro jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na konkrétní naprogramovanou spouštěcí událost (např. na okamžik, kdy oprávněný uživatel otevře zprávu v rámci elektronické pošty).[30]

5.2 POČÍTAČOVÝ VIRUS

Počítačový virus, podmnožina malware, je parazitující soubor, který se připojí k určitým programům nebo systémovým oblastem, které pozmění. Může se nekontrolovatelně rozšiřovat, nebo po svém spuštění zahájit destrukční proceduru (poškození, změnu či zničení dat, degradaci funkce operačního systému, stahování dalšího malware atd.). Existují viry, které mohou zároveň plnit funkci trojského koně a (nebo) vytvářet tzv.„zadní vrátka“ do napadeného systému. Počátek šíření počítačového viru může být distribuován v prostoru ohnisek, vytvořených na již kompromitovaných (zavirovaných) počítačích, což nesmírně urychluje celý proces šíření infekce. [31]

5.3 POČÍTAČOVÝ ČERV

Počítačový červ, podmnožina malware, je autonomní program, schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů (sítí), kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.[32]

[30,31,32] ČESKO. Základní definice, vztahující se k tématu kybernetické bezpečnosti. In *Ministerstvo vnitra České republiky*. 6 s. 2013, s. 2,3. Dostupné také z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>

5.4 KEYLOGGER

Keylogger, podmnožina malware, je program implantovaný do systému bez vědomí oprávněného uživatele, monitorující specifické činnosti, o které projevuje útočník zájem. Zaznamenává např. znaky, které oprávněný uživatel stiskl na klávesnici (zejm. hesla) nebo stránky, které navštívil. Tyto údaje předává útočníku k dalšímu zpracování. Ten tak může získat přístupové informace k webovým stránkám, bankovním účtům nebo kontům elektronické pošty. Může se jednat i o textový editor, který zároveň ukládá text, který byl jeho prostřednictvím napsán, do skryté části systému, odkud může být vyzdvižen autorem.[33]

V minulosti se užíval rovněž jako hardwarový prostředek, připojen na konektor klávesnice do počítače, zaznamenávající činnost klávesnice.

5.5 RANSOMWARE

Do skupiny malware se řadí i tzv. vyděračský malware, pro nějž se ustálilo označení ransomware441 (z anglického „ransom“ – výkupné, někdy také označovaný jako rogueware nebo scareware). Ransomware je malware, který brání či omezuje uživatele v řádném užívání počítačového systému do doby, než dostane útočník zaplaceno „výkupné“. Ransomware se nejčastěji dostane do počítače pomocí malware (trojského koně či červa), který je umístěn na webových stránkách, nebo je přílohou e-mailu. Jakmile je tento malware bezpečně „usídlen“ v počítačovém systému, dojde ke stažení vlastního ransomware.

Obecně je možné rozlišovat dva typy ransomware podle toho, jak moc zasahují do vlastního chodu počítačového systému. Prvním typem je ransomware, který omezí funkčnost celého počítačového systému a neumožní uživateli tento systém vůbec využívat (např. zabráněním spuštění operačního systému či zablokováním systémové obrazovky. Typickým příkladem tohoto typu je „policejní ransomware“). Druhým typem pak je ransomware, jenž ponechá počítačový systém funkční, avšak dochází k uzamčení a znepřístupnění dat uživatele.

[33] ČESKO. Základní definice, vztahující se k tématu kybernetické bezpečnosti. In *Ministerstvo vnitra České republiky*. 6 s. 2013, s. 3. Dostupné také z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>

V současnosti dochází spíše k využívání druhého typu ransomware, který je známý pod označením crypto-ransomware. Účelem tohoto malware je zašifrovat pevný disk nebo vybrané typy souborů v počítačovém systému, přičemž primárně má tento malware za cíl zašifrovat soukromé soubory uživatele jako jsou obrázky, textové či tabulkové dokumenty, videa aj. Po skončení šifrování se zpravidla uživateli zobrazí zpráva, že jeho soubory jsou zašifrovány, a pokud je chce získat zpět (dešifrovat), musí poslat určitý obnos na účet útočníka. K transakcím jsou obvykle využívány virtuální měny jako je Bitcoin nebo různé předplacené služby. Ve většině případů je stanovena časová lhůta pro zaplacení. Po uplynutí této lhůty dochází k smazání klíče, jenž může zašifrované soubory otevřít.[34] Typickým příkladem je CryptoLocker či WannaCry.

5.6 SPYWARE

Spyware, podmnožina malware, je program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítačová hra), s jehož funkcí však nesouvisí.[35]

5.7 ADWARE

Pojem adware je zkratka z anglického slovního spojení „advertising supported software“, což lze do českého jazyka volně přeložit jako software podporující reklamu. Jedná se o nejméně nebezpečnou, avšak výnosnou formu malware. Adware zobrazuje reklamy na počítačovém systému uživatele (např. pop-up okna v operačním systému nebo na webových stránkách, reklamy zobrazované společně se software aj.). Byť jde ve většině případů o produkty, které pouze obtěžují uživatele neustálými reklamními sděleními, která „vyskakují“ na obrazovce, může být adware spojen i se spyware, jehož účelem je sledovat činnost uživatele a odcizit důležité informace.[36]

[34] KOLOUCH, J. *Cybercrime.* Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 221.
[35] ČESKO. Základní definice, vztahující se k tématu kybernetické bezpečnosti. In *Ministerstvo vnitra České republiky*. 6 s. 2013, s. 2. Dostupné také z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>
[36] KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8, s. 205.

6 TELEKOMUNIKAČNÍ PROVOZ

Telekomunikačním provozem můžeme chápat jakoukoli komunikaci mezi dvěma zařízeními. Jednoduše si telekomunikační provoz můžeme vysvětlit na principu vysílače a přijímače. Jakákoli komunikace mezi těmito prvky je telekomunikačním provozem. Telekomunikační provoz nás samozřejmě provází v současné době zejména v podobě výpočetní techniky a mobilních telefonů s internetovým připojením. Toto samé platí rovněž v případě intranetu, zabývat se však budu internetovým připojením k veřejné síti internet. Jakákoli naše činnost na veřejné síti internet popřípadě intranetu je zaznamenávána, neboť přístup z naší výpočetní techniky či mobilních telefonů na konkrétní cílový server v podobě například určité webové stránky provází zejména skutečnost potřeby přidělení IP adresy v konkrétním čase ze strany našeho poskytovatele internetového připojení, tzv. Internet Service Provider, pro přístup k síti internet. Pod touto IP adresou jsme identifikováni v síti internet právě pro cílový server, který rovněž činnost naší výpočetní techniky či mobilního telefonu s přidělenou IP adresou zaznamenává. Náš poskytovatel internetového připojení tedy zpravidla zaznamenává přidělení konkrétní IP adresy v konkrétním čase naší výpočetní technice a rovněž cílový server zpravidla zaznamenává v konkrétním čase IP adresy všech zařízení, které provádí komunikaci směrem k němu. Současně je zpravidla zaznamenávána i opačná komunikace. Tento telekomunikační provoz je automatizován prostřednictvím síťových protokolů.

Samotný telekomunikační provoz je legislativně upraven zákonem č. 127/2005 Sb., zákon o elektronických komunikacích, ve znění pozdějších předpisů.

Ustanovení § 97 tohoto zákona uvádí ve svém prvním odstavci skutečnost, že právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna na náklady žadatele zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv Policii České republiky, Bezpečnostní informační službě a Vojenskému zpravodajství a to pro účely stanovené zvláštním právním předpisem. Následně druhý odstavec uvádí, že tyto orgány prokazují své oprávnění k odposlechu a záznamu zpráv předáním písemné žádosti, která obsahuje číslo jednací, pod kterým je rozhodnutí soudu u tohoto orgánu vedeno, a která je podepsána osobou odpovědnou u těchto orgánů za vykonání odposlechu a záznamu

zpráv. V případě odposlechu a záznamu zpráv Policií České republiky podle zvláštních právních předpisů se v písemné žádosti uvádí číslo jednací, pod kterým je souhlas uživatele odposlouchávané stanice u Policie České republiky veden.

V odstavci třetím je uvedena skutečnost, že právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout jak orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem, tak rovněž Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem a dále rovněž Bezpečnostní informační službě, Vojenskému zpravodajství a České národní bance pro účely a při splnění podmínek stanovených zvláštním právním předpisem. Po uplynutí doby 6 měsíců je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud tento zákon nestanoví jinak.

Provozní údaje definuje tento zákon v ustanovení § 90 v jeho prvním odstavci tak, že těmito provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.

Lokalizační údaje definuje tento zákon v ustanovení § 91 v jeho prvním odstavci tak, že těmito lokalizačními údaji se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.

Ustanovení § 97 tohoto zákona uvádí ve svém čtvrtém odstavci skutečnost, že provozními a lokalizačními údaji podle odstavce třetího jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace. Rozsah provozních a lokalizačních údajů uchovávaných podle odstavce třetího, formu a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu a způsob jejich likvidace stanoví prováděcí právní předpis. V praxi se rovněž tyto provozní a lokalizační údaje odborně označují jako tzv. data retention.

Ustanovení § 97 tohoto zákona v odstavci pátém a šestém rovněž dále uvádí, že právnická nebo fyzická osoba poskytující veřejně dostupnou telefonní službu je povinna na žádost poskytnout informace z databáze všech svých účastníků veřejně dostupné telefonní služby orgánu oprávněnému k jejich vyžádání podle zvláštního právního předpisu, a to na jeho náklady. Formu a rozsah poskytovaných informací stanoví prováděcí právní předpis. Zavede-li právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací při této činnosti kódování, kompresi, šifrování nebo jiný způsob přenosu vedoucí k nesrozumitelnosti přenášených zpráv, je povinna zajistit, aby v koncových bodech pro připojení zařízení uvedených v odstavci prvním byly požadované zprávy a s nimi spojené provozní a lokalizační údaje poskytovány srozumitelným způsobem.

Ustanovení § 97 tohoto zákona v odstavci osmém uvádí, že právnická nebo fyzická osoba a její zaměstnanci jsou povinni zachovávat mlčenlivost o vyžádaném nebo uskutečněném odposlechu a záznamu zpráv podle odstavců prvního a druhého a vyžádání a poskytnutí údajů podle odstavců třetího a pátého a s tím souvisejících skutečnostech.

Ustanovení § 89 tohoto zákona v odstavci prvním uvádí, že podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost

zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak. To nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv, aniž by byla dotčena zásada důvěrnosti.[37]

Zcela bezesporu jsou provozní a lokalizační údaje o telekomunikačním provozu základním kamenem při odhalování a vyšetřování trestné činnosti v podobě informační kriminality, neboť bez těchto údajů jen stěží orgán činný v trestním řízení odhalí pachatele této trestné činnosti. V některých typech výše zmíněných protiprávních jednáních jsou mnohdy provozní a lokalizační údaje o telekomunikačním provozu jediným možným způsobem, jak odhalit pachatele této trestné činnosti. V praxi je však doba, po kterou se tyto provozní a lokalizační údaje o telekomunikačním provozu uchovávají, tedy doba 6 měsíců, mnohdy zcela hraniční a to v případech, kdy například poškozená osoba oznámí opožděně podezření z trestné činnosti orgánu činném v trestním řízení či dále v případech oznámených jednotlivých případů po celém území České republiky vykazujících znaky přestupků, kdy s odstupem času dojde jejich následným ověřováním k zjištění skutečností a důvodů pro konání společného řízení, kterými může být například vztah ke způsobené škodě, čímž dojde ke změně trestně právní kvalifikace a postupu ve smyslu ustanovení § 158 odst. 3 trestního řádu, tedy že policejní orgán zahájí úkony trestního řízení pro konkrétní skutkovou podstatu trestného činu uvedené ve zvláštní části trestního zákoníku. V uvedeném případě pak snadno dojde k nemožnosti tyto provozní a lokalizační údaje o telekomunikačním provozu vyžadovat, když zákonná doba 6 měsíců k možnosti tyto údaje vyžádat, již uplynula. Dalším problémem je účast zahraničních subjektů poskytujících služby, které jsou zneužity pro páchání informační kriminality, kdy jen samotná doba případného vyžádání informací cestou mezinárodní právní pomoci znemožňuje v případě zjištění IP adresy (na území České republiky) možnost vyžadovat lokalizační údaje k pachateli, když zákonná doba 6 měsíců zpravidla uplyne během doby vyžadování této mezinárodní právní pomoci.

[37] ČESKO. Zákon č. 127/2005 Sb. o elektronických komunikacích, ve znění pozdějších předpisů. In Sbírka zákonů, Česká republika. 2005, částka 43, s. 1330-1408.

7 PROCESNÍ PROSŤREDKY PRO ODHALOVÁNÍ A OBJASŇOVÁNÍ INFORMAČNÍ KRIMINALITY

V rámci odhalování, prověřování a vyšetřování předmětné informační kriminality jsou orgánu činnému v trestním řízení dány mimo jiné oprávnění uvedená zvláštním právním předpisem, v tomto případě zákonem č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů, a to zejména odposlech a záznam telekomunikačního provozu a sledování osob a věcí.

7.1 ODPOSLECH A ZÁZNAM TELEKOMUNIKAČNÍHO PROVOZU

Ustanovení § 88 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů, ve svém prvním odstavci uvádí mimo jiné, že je-li vedeno trestní řízení pro zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, pro trestný čin pletichy v insolvenčním řízení podle § 226 trestního zákoníku, porušení předpisů o pravidlech hospodářské soutěže podle § 248 odst. 1 písm. e) a odst. 2 až 4 trestního zákoníku, zjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě podle § 256 trestního zákoníku, pletichy při zadání veřejné zakázky a při veřejné soutěži podle § 257 trestního zákoníku, pletichy při veřejné dražbě podle § 258 trestního zákoníku, zneužití pravomoci úřední osoby podle § 329 trestního zákoníku nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, může být vydán příkaz k odposlechu a záznamu telekomunikačního provozu, pokud lze důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené. Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení Policie České republiky. Ustanovení § 88 tohoto zákona ve svém druhém odstavci dále uvádí mimo jiné, že nařídit odposlech a záznam telekomunikačního provozu je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce.[38]

[38] DRAŠTÍK A., FENYK J., a kol. *Trestní řád (č. 141/1961 Sb.) - Komentář*, Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-600-7.

Ustanovení § 88a tohoto zákona ve svém prvním odstavci uvádí mimo jiné, že je-li třeba pro účely trestního řízení vedeného pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), pro trestný čin podvodu (§ 209 trestního zákoníku), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), pro trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), pro trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), pro trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), pro trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené, nařídí v řízení před soudem jejich vydání soudu předseda senátu a v přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce.[39]

7.2 SLEDOVÁNÍ OSOB A VĚCÍ

Ustanovení § 158d zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů, ve svém třetím odstavci uvádí, že pokud má být sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků, lze je uskutečnit jen na základě předchozího povolení soudce. Při vstupu do obydlí nesmějí být provedeny žádné jiné úkony než takové, které směřují k umístění technických prostředků.[40]

[39,40] DRAŠTÍK A., FENYK J., a kol. Trestní řád (č. 141/1961 Sb.) - Komentář, Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-600-7.

8 EMPIRICKÁ ČÁST

8.1 CÍL EMPIRICKÉ ČÁSTI

Cílem empirické části práce je se věnovat prevenci a bezpečnosti dětí a dospělých před dopady informační kriminality, rozboru statistických dat a konkrétnímu vybranému případu kazuistiky. V rámci prevence a bezpečnosti dětí a dospělých před dopady informační kriminality budou přiblíženy základní zásady bezpečnosti a naší ostražitosti tak, abychom zamezili možnosti stát se obětí informační kriminality, případně abychom mohli odvrátit či minimalizovat následky a dopady informační kriminality. Rozborem statistických dat bude poukázáno na vrůstající tendenci jak v případě užívání počítačů, internetu, sociálních sítí, nakupování na internetu, tak i na vrůstající tendenci registrovaných skutků od roku 2013. V případě konkrétně vybraného případu kazuistiky bude cílem laické veřejnosti přiblížit činnost a procesní aspekty věcně a místně příslušného policejního orgánu. Za tímto účelem byl vybrán konkrétní případ informační kriminality v současné době prověřovaný na Policii České republiky, Městském ředitelství policie Plzeň, Oddělení hospodářské kriminality Služby kriminální policie a vyšetřování. Vzhledem ke skutečnosti, že se jedná o reálně prověřovaný případ, jsou uváděny smyšlené osobní údaje, neoznačující žádnou konkrétní osobu a časové údaje jsou rovněž pozměněny za účelem omezení zpětné dohledatelnosti.

8.2 PREVENCE A BEZPEČNOST DĚTÍ

V první řadě prevence a bezpečnost dětí musí vycházet z preventivní činnosti rodiny, konkrétně rodičů, na kterou by měla navazovat preventivní činnosti základních a středních škol v rámci výuky hodin předmětů informatiky. Souběžně s rodinnou a školní prevencí by měla probíhat preventivní činnost státu prostřednictvím centrálních preventivních projektů v rámci mediálních činností, např. reklamní spoty v televizi a kině. Vrcholem této preventivní činnosti by měla být rovněž preventivní činnost Policie České republiky formou školních besed. Tato preventivní činnost Policie České republiky by pro svojí efektivitu a zaujetí u dětí neměla být činností obecného charakteru, nýbrž by bylo vhodné, aby Policie České republiky čerpala ze své služební praxe z registrovaných skutků informační kriminality. Na mysli mám zejména preventivní činnost uváděnou na zcela praktických případech z praxe, tak aby

preventivní činnost nebyla pro děti nudou. Děti by si měly již od mladého věku uvědomovat možnost nebezpečí informační kriminality z příkladů běžné každodenní činnosti. Okruhy preventivní činnosti Policie České republiky bych s ohledem na současný vývoj informační kriminality tedy zaměřil na základní prvky zabezpečení jejich informačních technologií a zásady vystupování na veřejné síti internet, zejména bezpečné chování na sociálních sítí a komunikaci s neznámými osobami, tak aby si děti uvědomovaly skutečnost, že nemohou nikdy důvěřovat cizímu uživateli veřejné sítě internet.

8.2.1 ZABEZPEČENÍ A UŽIVATELSKÉ PŘÍSTUPY

U dětí se můžeme v největší míře setkat v případě informačních technologií s chytrými telefony, stolními počítači nebo notebooky či jejich obdobou. Všechna tyto zařízení by měla obsahovat pro největší zabezpečení proti informační kriminalitě vždy aktualizovaný operační systém s aktualizovanými aplikacemi, vybavený souběžně s aktualizovaným antivirovým, anti-spyware a firewall programem. Takto zabezpečené informační technologie minimalizují škody v případě útoku, infikace škodlivým softwarem jako jsou trojské koně, počítačové viry, počítačové červy, malware apod. K jejich infikování dochází v první řadě při navštěvování neověřených webových stránek, stahováním neověřených dat z veřejné sítě internet či užíváním datových disků, které nebyly při okamžitém připojení k zařízení ověřeny aktualizovaným antivirovým programem. Shora uvedené softwarové prostředky jsou dostupné jak v placených i bezplatných verzích.

O tyto informační technologie, které jsou zpravidla dětem darovány ze strany jejich rodičů, a o jejich zabezpečení by se měli v případě nízkého věku dítěte postarat jejich rodiče ještě před jejich darováním.

Rodiče při zprovozňování informačních technologií, které darují svým dětem, by dále rovněž měli využít některých bezpečnostních opatření, které nabízejí operační systémy v podobě tzv. rodičovské kontroly či zámku, což je vhodné užívat v případě nízkého věku dítěte. Rodičovská kontrola či zámek nám umožňuje nastavovat uživatele daného zařízení, udělovat či odebírat konkrétní oprávnění v daném operačním systému, používat vybrané aplikace, hry a souběžně lze nastavit i možný čas, po který našim dětem dovolíme přístup k uvedenému zařízení. Další šikovnou funkcí je i možnost sledování aktivity dětí na daném zařízení, konkrétně jejich aktivitu při navštěvování

webových stránek. Rovněž je možné některé webové stránky dětem blokovat. Samotnou instalaci potřebných programů a her by měly provádět děti vždy ve spolupráci se svými rodiči. U laiků by bylo vhodné, aby si před provedením instalace přečetli licenční podmínky, aby si uvědomili podmínky užívání, neboť v některých případech může docházet k odesílání informací o naší činnosti právě výrobcům programů a her. V případě užívání rodičovské kontroly či zámku tak snadno můžeme odepřít dítěti právo jakékoli instalace, minimalizujeme tak další riziko. Tato opatření známe ve formě zabezpečení ze strany zaměstnavatele.

Rodiče by své děti měli vychovávat tak, aby nevěřily cizím uživatelům a jejich projevům na veřejné síti internet. V případě vyhledávání informací pro školní potřeby by se měly tyto informace naučit vyhledávat na ověřených webových stránkách, popřípadě se naučit ověřování zveřejněných informací na dalších webových stránkách.

Za účelem zřízení jakýchkoli účtů na webové stránky či sociální služby by měly děti využívat pomoc rodičů, kteří by je měli poučit o skutečnosti nikomu nesdělovat přístupové údaje, tyto neuchovávat uložené ve svých zařízeních. Přístupová hesla by měla být volena dostatečně silná, aby nebylo tyto možné snadno překonat. Tedy, aby obsahovala alfa numerické znaky (malá a velká písmena, číslice) a rovněž i speciální znaky (např. ?,!,@ a další). Je-li možné nastavit ochranu proti zneužití kontrolní otázkou, je vhodné tuto ochranu využít a odpověď volit takovou, aby nebyla nikomu známa a snadno zjistitelná. Je třeba minimalizovat okruh osob, které by mohly odpověď znát. Pro tento účel je tak dále nutné, nikdy tuto informaci, sloužící jako kontrolní odpověď, o sobě nikde nezveřejňovat z důvodu možné dohledatelnosti třetí osobou. U sociálních sítí je vhodné využít ochranu v podobě záchranné e-mailové adresy, kam bude odesláno nové přístupové heslo v případě jeho zapomenutí. Není vhodné mít přístupová hesla na sociální sítě a do e-mailových schránek shodná, v případě překonání hesla tak přicházíme o ztráty našich dalších přístupů. Další ochranou přístupových hesel může být jejich pravidelná obměna.

8.2.2 INTERNET A SOCIÁLNÍ SÍTĚ

V případě zřizování účtů na sociálních sítích ze strany samotných dětí by toto rodiče měli vědět. Měli by své děti poučit k jejich budoucím projevům na těchto sociálních sítích a zveřejňování zejména jejich fotografií a videí. Dítě by si mělo uvědomovat, ostatně i rodič, že jakákoli zveřejněná informace ať už textová nebo

obrazová je viditelná pro určitý okruh lidí a v případě, že není nastavené zviditelnění jen pro přátele a je označena jako veřejná, k těmto údajům se dostane jakákoli třetí osoba, která těmito informacemi může disponovat. Samotným uvedením této informace dále disponuje rovněž i samotný provozovatel služby. Obecně pravidla užívání jsou rovněž uvedeny opět v licenčních podmínkách, které jsou vždy uživatelům nabídnuta při jejich registraci ze strany provozovatelů služeb. V některých případech je možné, že na některých službách mohou být zveřejněné informace užity ze strany jejich provozovatelů k jejich obchodním účelům, což uživatel odsouhlasí registrací a stvrzením licenčních či obchodních podmínek. Pro lepší kontrolu dětí může být vhodné, aby rodiče měli na stejné sociální sítí také svůj profil spřátelený s profilem jejich dítěte, tak aby bylo možné průběžně kontrolovat jeho činnost na sociálních sítích. Samozřejmě je možné, že dítě si rodiče z přátel odebere a v daném případě je třeba, aby rodiče vhodným výchovným způsobem poučili své děti.

V případě sociálních sítí umožňující video hovory prostřednictvím webové kamery je nutné, aby si děti uvědomovaly možná rizika při provádění daného video hovoru zejména, aby hovory uskutečňovaly jen s ověřenými přáteli. Riziko samo o sobě může nést i samotná webkamera, kterou může útočník využít napadením našeho zařízení a současně vzdáleným přístupem může dojít k její aktivaci včetně mikrofonu. Proto je vhodné ji například při jejím nevyužívání zakrýt. Pro minimalizaci rizika zde platí další hlavní zásada a to udržovat informační technologie, konkrétně jejich operační systémy a antivirové, anti-spyware a firewall programy v aktualizovaném stavu.

Pro funkční prevenci a bezpečnost dětí na internetu je nutné, aby děti měly se svými rodiči takový vztah, aby se nikdy nebály svým rodičům přiznat podezřelé dění či komunikaci. V jakémkoli podezřelém jednání či činnosti by se neměly ostýchat před svými rodiči dojít si pro radu či pomoc. Přeci jenom již samotným přístupem rodičů k nastalému problému se opět snižuje případné riziko na poli informační kriminality.

8.3 PREVENCE A BEZPEČNOST DOSPĚLÝCH

V předešlé podkapitole v zaměření prevence a bezpečnosti dětí byly ve větší míře uvedeny základní podmínky činnosti na zařízeních informačních technologií, kdy doporučení v činnosti rodičů nad dohledem svých dětí se samozřejmě vztahují i na chování a činnost všech dospělých užívajíce tyto informační technologie.

Samotná prevence a bezpečnost dospělých by měla v první řadě navazovat na preventivní činnost státu prostřednictvím centrálních preventivních projektů v rámci médií, např. reklamní spoty v televizi a kině, kterou by měli dospělí, i jako rodiče, vnímat. Vzhledem ke skutečnosti, že převážný část života dospělí prožijí pracovní činností, mělo by docházet k jejich školení, jako zaměstnanců, ze strany jejich zaměstnavatelů - podniků.

Je v zájmu podniků své zaměstnance pravidelně preventivně k bezpečnosti na poli informační kriminality školit, neboť jejich zaměstnanci mohou pracovat na důležitých projektech či spravovat finanční prostředky podniku. Příkladem může být účetní přistupující pravidelně k internetovému bankovnictví podniku, přijímající veškerou e-mailovou korespondenci, přičemž v případě neproškolení, neznalosti a neopatrnosti může dojít k úniku dat podniku směrem k třetí osobě, která může získat přístupové údaje k internetovému bankovnictví podniku, či dokonce může účetní přijmout infikovanou e-mailovou korespondenci, na základě níž dojde k odstavení podnikové sítě apod. Samozřejmostí je, že podnik by měl mít určeného bezpečnostního managera, případně správce sítě, který v prvé řadě provede opatření v zabezpečení informačních technologií aktualizovanými operačními systémy, aktualizovanými antivirovými, anti-spyware a firewall programy, když na jednotlivých zařízeních současně nastaví různá bezpečnostní oprávnění, tedy jejich uživatelům udělí či odebere jednotlivá oprávnění na tato zařízení, oprávnění k přístupu k aplikacím, databázím, internetovému bankovnictví, apod. Rovněž může přistoupit k provedení tzv. penetračních bezpečnostních testů jejich sítě a systémů (hledání slabin ve zranitelnosti, nevhodné konfiguraci). Již ze samotné pracovní činnosti těchto dospělých by mělo dojít k jejich řádnému proškolení, tak aby si tyto bezpečnostní kroky přenesli i do osobního života, čímž se rovněž docílí k vhodné prevenci nad jejich dětmi. Problém však nastává v méně slabší sociální vrstvě dospělých, kteří se k prostředkům informačních technologií nedostanou a tudíž ze své praxe nemohou být poučeni o bezpečnostních zásadách při jejich budoucí činnosti na veřejné síti internet. V tomto ohledu nezbývá, než spoléhat na centrální preventivní projekty státu. V neposlední řadě nesmíme zapomenout na seniory, kteří samozřejmě nemohli během života projít celým vývojem informačních technologií. I v dnešní době můžeme vyhledat vcelku dobře veřejně dostupné jednotlivé kurzy pro seniory, kde dochází k jejich školení v užívání informačních technologií. Tyto kurzy provozují jak soukromé subjekty, tak i stát

prostřednictvím školství v rámci kurzů celoživotního vzdělávání. Jistě každý z nás v okruhu své rodiny zná osoby seniorů případně starších dospělých, kteří se snaží jít s dobou, nevyhýbají se těmto technologiím a snaží se jim porozumět. Této generaci lze v prevenci a bezpečnosti na poli informační kriminality dopomoci rovněž centrálními projekty ze strany státu a rovněž preventivní činnosti Policie České republiky formou besed.

8.3.1 INTERNETOVÉ OBCHODY

Nakupování na internetových obchodech, tzv. e-shopech, je činností, v jejíž větší míře dochází k podvodným jednáním případně jednáním poškozující spotřebitele ve smyslu porušení obchodních podmínek plynoucích z občanského zákoníku č. 89/2012 Sb., jehož ustanoveními se právě řídí smluvní podmínky mezi prodejcem a zákazníkem jako spotřebitelem.

V první řadě bychom si měli uvědomit, že pro zamezení jakýchkoli problémů s naším nákupem v internetovém obchodě, je nejlepší vždy nakupovat na ověřených internetových obchodech. Výběr internetového obchodu volíme dle vlastních zkušeností či podle zkušeností ostatních uživatelů – zákazníků - spotřebitelů. U většiny internetových obchodů již v dnešní době nalezneme mnoho recenzí jejich zákazníků tak, jak je tomu například u největšího nákupního portálu a srovnávače cen na českém internetu www.heureka.cz. U jednotlivých internetových obchodů zde nalezneme jak uvedené recenze jejích zákazníků, tak rovněž certifikace (ceny) udělené tímto portálem, což samo o sobě poukazuje na to, že se jedná o spolehlivý internetový obchod. Samozřejmostí je, že i v případě nakupování na těchto ověřených internetových obchodech, je nutné se seznámit podrobně s obchodními podmínkami těchto internetových obchodů a to zejména s okolnostmi, kterými se řídí vrácení, reklamace, doručování a platba zboží.

Přirozenou vlastností člověka je snaha vyhledat konkrétní zboží za tu nejnižší cenu, což v nás může vyvolat ztrátu obrany schopných prostředků a to i jen pouhou myšlenkou výhodné koupě a ušetření finančních prostředků. Snaha ušetřit nás mnohdy zavede na scestí, neboť snahou ušetřit můžeme nalézt či být odkázáni na neověřené internetové obchody. K tomu, abychom zamezili jakékoli možnosti podvodného jednání případně jednání poškozující spotřebitele ve smyslu porušení obchodních podmínek, je třeba postupovat velmi obezřetně. V první řadě při návštěvě těchto neověřených

internetových obchodů se vždy zaměříme na grafický vzhled a uspořádání internetového obchodu. Funkční, ověřené a stálé internetové obchody si potrpí vždy na adekvátní grafické zobrazení dle vývoje trendů. Vždy bychom v uspořádání internetového obchodu měli nalézt odkaz na všeobecné obchodní podmínky upravující podmínky obchodního ujednání řídícího se dle zákonných podmínek občanského zákoníku ve smyslu vrácení, reklamace, doručování a platby zboží. Zcela jistě bychom zde dále měli nalézt identifikaci provozovatele v podobě jména, názvu, identifikačního čísla osoby, sídla, adresy pobočky a kontaktu na prodejce. V tomto případě bychom si měli rovněž uvědomit, že tyto informace ve vztahu k osobám s identifikačním číslem osoby lze veřejně nalézt v obchodním popřípadě živnostenském rejstříku. Tyto údaje je vhodné si ověřit, zda se zakládají na pravdě, a rovněž je vhodné si uvědomit, že tyto údaje mohl stejným způsobem nalézt a ověřit právě i možný pachatel provozující tento internetový neověřený obchod. V neposlední řadě je vhodné si tyto údaje ve vztahu k internetovému obchodu ověřit v internetových vyhledávačích, například www.google.cz, a to pro případ, že by vyhledávač mohl nalézt jakékoli varování a negativní recenze uživatelů. V poslední řadě jsme již tedy provedli všechna nutná opatření a v případě, že cena zboží není zcela nepřiměřená než obvyklá, což může být také podezřelým vodítkem, můžeme přistoupit k objednávce zboží. U zavedeného internetového obchodu by mělo být možné zboží objednat a nechat jej zaslal s platbou na dobírku, tak abychom v případě prvního nákupu na námi neověřeném internetovém obchodě nemuseli užívat platební údaje ve spojitosti s platební kartou, internetovým bankovnictvím apod.

Závěrem je třeba uvést, že všechna tyto opatření nemusí vyloučit podvodná jednání, avšak svým jednáním jsme vyvinuli dostatečně velkou snahu a zájem riziko těmito opatřeními zcela jistě minimalizovat. V případě, že by nebylo tohoto postupu využito, můžeme jednoznačně říci, že by nákup zboží byl proveden zcela bezhlavě.

8.4 ROZBOR STATISTICKÝCH DAT

V rámci práce byla porovnána statistická data informační kriminality, viz příloha číslo 1 až 10, který byla získána ze zveřejněných údajů Českého statistického úřadu, Policejního prezidia České republiky a dále Národní centrály proti organizovanému zločinu Služby kriminální policie a vyšetřování, které autor získal vlastním šetřením. Z dat Českého statistického úřadu je zřejmé, že užívání počítačů a internetu v domácnostech má stále vzrůstající tendenci, u jednotlivců napříč věkem a vzděláním

vzrůstá obliba užívání sociálních sítí, užívání internetového bankovnictví a nakupování na internetu. Tato vzrůstající tendence byla zaregistrována nejen u mladších a středních ročníků, ale také u seniorů. Z dat Policie České republiky je zřejmé, že informační kriminalita má od roku 2013 vzrůstající tendenci, meziročně vzrůstá tak jako její projevy v podobě podvodných jednání, hackingu, mravnostních deliktů, autorskoprávních deliktů, násilných projevů apod.

8.5 POPIS PŘÍPADU KAZUISTIKY

Dne 18.10.2016 u policejního orgánu podal trestní oznámení Jan NOVÁK, jako jednatel obchodní společnosti Dodejce zboží s.r.o. s tím, že ze strany neznámého pachatele došlo na veřejné síti internet pravděpodobně k narušení tajemství dopravované zprávy osoby Bruno TRIMO, žijícího v předmětné době v Itálii, který ze své e-mailové schránky @noname.it odesílal osobě Jan NOVÁK, žijícího v předmětné době v Plzni, e-mailovou korespondenci, jejíž přílohou byl elektronický dokument formátu *.pdf s vystavěnou proforma fakturou na celkovou částku 70.444 amerických dolarů, kterou neznámý pachatel zachytil, její přílohu v podobě elektronického dokumentu formátu *.pdf pozměnil v její spodní části v místě platebních údajů, když zde původně uvedený bankovní účet podvrhl uvedením IBAN bankovního účtu v Anglii, přičemž tento pozměněný podvržený e-mail následně odeslal dne 17.10.2016 z e-mailové adresy bruno.trimo@email.com osobě Jan NOVÁK, načež následně došlo v důsledku tohoto podvrženého e-mailu ke skutečnosti, že Jano NOVÁK prostřednictvím internetového bankovnictví obchodní společnosti Dodejce zboží s.r.o. zadal mezinárodní platbu ve prospěch tohoto podvrženého bankovního účtu v celkové částce 21.133,60 amerických dolarů, neboť dle obchodní dohody měl uhradit celkem 30% podíl jako zálohu za provedenou objednávku zboží, čímž tak neznámý pachatel svým jednáním úmyslně porušil tajemství dopravované zprávy zasílané prostřednictvím elektronických komunikací a sebe nebo jiného obohatil tím, že uvedl Jana NOVÁKA v omyl, když rovněž musel získat přístup k počítačovému systému, aby tak data pozměnil, aby byla považována za pravá, přičemž pravděpodobně získal přístup do e-mailových schránek těchto osob včetně přístupových hesel, která v uvedenou dobu přechovával, neboť v případě zaslání e-mailu osobou Bruno TRIMO z e-mailové schránky @noname.it osobě Jan NOVÁK, došlo k jejímu automatickému vymazání v e-mailové schránce v okamžiku jeho doručení osobě Jan NOVÁK, čímž tak byla způsobena škoda

na cizím majetku a to v celkové částce 21.133,60 amerických dolarů, dle přepočtu v částce 507.586,80,- Kč, když dále neznámý pachatel s osobou Jan NOVÁK komunikoval bez jakýchkoli diakritických chyb v italském jazyce z e-mailové schránky bruno.trimo@email.com. V daném případě Jan NOVÁK uvedenou finanční částku odeslal bez jakéhokoli podezření, neboť s osobou Bruno TRIMO telefonicky hovořil a skutečně mezi nimi mělo dojít k odeslání tohoto dokumentu a jeho úhradě ve výši 30% na základě vystavené proforma faktury. Jan NOVÁK si telefonicky u osoby Bruno TRIMO skutečně ověřoval, zda je na faktuře uveden správný účet, což mu Bruno TRIMO potvrdil, aniž by si byl vědom, že během cesty odeslaného e-mailu došlo k pozměnění výlučně jen bankovního účtu, když ostatní údaje na faktuře včetně objednávky byly uvedeny v nezměněné podobě.

8.5.1 ROZBOR PŘÍPADU

Policejní orgán na základě uvedeného oznámení ihned dne 18.10.2016 zahájil úkony trestního řízení podle § 158 odst. 3 trestního řádu pro podezření ze spáchání přečinu porušování tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), odst. 3 písm. c) trestního zákoníku, zločinu podvod podle § 209 odst. 1,4 písm. d) trestního zákoníku, přečinu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. b,c), odst. 4 písm. b,e) trestního zákoníku a přečinu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 odst. 1 písm. a,b), odst. 2 písm. b) trestního zákoníku, jehož se měl dopustit neznámý pachatel výše uvedeným jednáním.

Ačkoli ze strany osoby Jan NOVÁK došlo k provedení reklamace mezinárodní platby u bankovního ústavu s cílem již odeslanou mezinárodní platbu zastavit, policejní orgán z důvodu neodkladnosti kontaktoval za účelem spolupráce Ministerstvo financí, Finančně analytický útvar (dnes Finančně analytický úřad), přičemž se podařilo urychlit upřednostnění požadavku reklamace a navrácení platby, když z okolností souhry náhod tato mezinárodní platba neodešla přímo transakcí do Anglie, nýbrž přes Spojené státy americké z důvodu mezinárodní transferové služby, čímž se oddálilo její okamžité doručení do Anglie, když se nakonec skutečně podařilo tuto platbu navrátit zpět do České republiky do příslušného bankovního ústavu v plné výši, což Jan NOVÁK potvrdil a dále předložil další e-mailovou komunikaci s neznámým pachatelem, který vyčkával na obdržení této zachráněné platby a snažil se dále přimět Jana NOVÁKA

k zaslání další platby na jiný bankovní účet v Anglii. Navrácení platby rovněž později potvrdil i Finančně analytický útvar svým přípisem.

Ve věci došlo dne 18.10.2016 k přibrání soudního znalce k vypracování posudku z oboru kybernetika, odvětví výpočetní technika, kdy ze strany tohoto došlo k vykopírování kompletní e-mailové komunikace z notebooku používaným oznamovatelem Janem NOVÁKEM. Soudním znalcem byla dále na uvedeném notebooku nalezena jediná instalace škodlivého softwaru, kdy se jednalo o "Gen:Variant.Symmi.62690[ZP] (DB)". Jedná se o škodlivý software přidávající tzv. pop up okna do webového prohlížeče. Jeho další činností může být shromažďování osobních údajů uživatele (hesla pro internetové bankovnictví apod.) a tyto dále odesílá třetí osobě. Znalec nenalezl záznamy o připojování do zajištěného počítače.

V rámci prověřování bylo Janem NOVÁKEM sděleno, že správu e-mailového serveru obchodní společnosti Dodejce zboží s.r.o. má na starost obchodní společnost SprávaIT s.r.o., konkrétně Petr PAVEL, se kterým Jan NOVÁK v době trestního oznámení hovořil, přičemž bylo jeho vstupem do serverového rozhraní zjištěno, že u obchodního e-mailu objednávky@dodejcezbozi.cz bylo provedeno jeho přesměrování na cizí e-mailovou schránku u poskytovatele yahoo.com. Následně Jan NOVÁK uvedl, že ačkoli provedl opatření ve změně přístupových práv k firemním e-mailovým schránkám spočívající ve změně hesla, nadále zjišťuje komunikaci, kdy obchodní e-mailovou adresou mají být odesílány asi i další e-maily. Později pak Petr PAVEL uvedl, že po předchozí spolupráci s Janem NOVÁKEM ověřil e-mailový server, když od doby změny za nové heslo nebyly zjištěny cizí přístupy, změna hesla skutečně pomohla. Dále uvedl, byl zjištěn neoprávněný přístup na e-mailový server Dodejce zboží s.r.o. dne 17.10.2016, když jej neznámý pachatel užil pro odesílání pravděpodobně spamových e-mailů. Ze strany neznámého pachatele byla užita zahraniční IP adresa, tak jako v případě dále zkoumaných hlaviček e-mailů. Neznámý pachatel vystupuje pod IP adresou registrované dle databáze RIPE v Nigérii, přičemž údaje o poskytovaných rozsazích IP adres nejsou v Nigérii aktualizované, není možné zjistit bližšího tamního poskytovatele internetového připojení. Vyžádání mezinárodní právní pomoci je v této zemi nereálné bez možnosti zjistit bližší skutečnosti.

Ve věci bylo provedeno oslovení Federal Bureau od Investigation, Legal Attaché Office - Prague, CZE (dále FBI), kdy však ze strany FBI nebyl sdělen žádný relevantní výsledek.

Ve věci došlo k vyžádání informací prostřednictvím mezinárodní právní pomoci týkajících se bankovních účtu evidovaných u bankovního ústavu v Anglii. Dále byl zaslán požadavek o provedení výslechu majitelů a disponentů uvedených bankovních účtů. K bankovním účtům bylo zjištěno, že byly zřízeny v Anglii na osoby ženského pohlaví, když doložené kopie dokladů k 1. bankovnímu účtu byly pravděpodobně padělané z důvodu stejných čísel dokladů a doložené kopie dokladů k 2. bankovnímu účtu jsou hlášeny jako odcizené/ztracené nebo neoprávněně užívané. Z britské strany bylo dále sděleno, že tamní šetření nadále pokračuje.

Během prověřování se podařilo vyslechnout i osobu Bruno TRIMO, který shodou okolností měl zahraniční cestu přes Českou republiku. Bruno TRIMO potvrdil veškeré sdělení učiněné Janem NOVÁKEM, kdy nad rámec tohoto sdělil, že podal trestní oznámení na Poštovní policii v Itálii dne 28.11.2016, kdy dříve jej podat nemohl, jelikož si musel měsíc předem sjednat schůzku. Tento následně ke spisovému materiálu poskytl originál elektronického dokladu ve formátu *.pdf.

V předmětné věci došlo k provedení "data-freeze" (zamražení dat pro pozdější vyžádání) týkající se e-mailové adresy @yahoo.com, když následně byl vydán podnět k vydání mezinárodní právní pomoci ke společnosti Yahoo.com, za účelem vyžádání registračních, provozních a lokalizačních údajů k této e-mailové schránce. V dané věci již tak nezbývá vyčkat na výsledek prověřování, mezinárodní právní pomoc ke společnosti Yahoo.com je tak posledním možným procesním postupem k možnosti objasnění této informační kriminality, avšak co se týče lokalizačních údajů, lze předpokládat, že neznámý pachatel ke vstupu do této e-mailové schrány rovněž užívá IP adresu Nigérie.

8.6 NÁVRH ČESKÉ PIRÁTSKÉ STRANY KE ZRUŠENÍ UCHOVÁVÁNÍ TELEKOMUNIKAČNÍHO PROVOZU

Dne 20.12.2017 Česká pirátská strana uvedla, že se ji podařilo nasbírat potřebný počet podpisů pro podání návrhu k Ústavnímu soudu České republiky, kterým chce zrušit plošné sledování občanů. Konkrétním cílem je dle jejího vyjádření zrušení

několika zákonných ustanovení, které umožňují "plošné šmírování lidí" a uchovávání osobních dat. Jan Vobořil z neziskové právní organizace Iuridicum Remedium (IuRe) podotýká, že "plošné sledování" nevedlo k zefektivnění práce policie a je zjevné, že trestné činy lze vyšetřovat i bez těchto dat: „Za loňský rok přitom žádaly oprávněné orgány údaje jen o mobilních telefonech v téměř půl milionech případů, což je víc než dvojnásobek oproti roku 2015. Přitom není žádný posun v objasněnosti případů ani v míře kriminality. Navíc náklady na šmírování představují pro stát výdaje v řádech několika stovek milionů ročně. Občané si ve výsledku daněmi připláceli za to, že je stát měl za sprosté podezřelé.“ Předkladatelé návrhu se opírají o dvě rozhodnutí Soudního dvoru EU, který naposledy v prosinci 2016 rozhodl, že státy nemají právo plošně uchovávat data o uživatelích komunikačních sítí. Rovněž se předkladatelé návrhu opírají k nálezům Ústavního soudu týkajících se uchovávání a využívání provozních a lokalizačních údajů v trestním řízení, který vyslovil požadavek, aby údaje byly využívány v obdobném režimu jako jsou nařizovány odposlechy. Využití údajů by tak mělo být dle Ústavního soudu možné pouze v případech „zvlášť závažných trestných činů“. Vzhledem k tomu, že Ústavní soud například v nálezu sp. zn. Pl. ÚS 24/10 přímo odkazuje na úpravu odposlechů (bod 48), je dle navrhovatelů nezbytné tento pojem „zvlášť závažné trestné činy“ vykládat právě v souvislosti s úpravou odposlechů v § 88 trestního řádu.

Předkladatelé návrhu uvádí, že je zřejmé, že zákonodárce při přípravě nové právní úpravy nerespektoval toto vymezení přípustnosti zásahu do práva na informační sebeurčení v případě žádostí orgánů činných v trestním řízení o provozní a lokalizační údaje, když odposlechy dle § 88 je možné nařídit v případech trestných činů s horní hranicí minimálně 8 let a dalších uvedených trestných činů, zatímco provozní a lokalizační údaje lze vyžadovat u trestných činů s horní hranicí trestní sazby 3 roky a dalších vymezených trestných činů včetně například hojného trestného činu podvodu dle § 209, kde je horní hranice základní trestní sazby v odst. 1 dva roky. Navrhovatelé mají za to, že uvedená úprava neodpovídá požadavkům formulovaným ze strany Ústavního soudu a je tedy rovněž v rozporu s Listinou základních práv a svobod a tedy i ústavním pořádkem České republiky, neboť jednotlivci je dle Listiny základních práv a svobod zaručena nedotknutelnost osoby a jejího soukromí, když omezena může být jen v případech stanovených zákonem, ochrana před neoprávněným zasahováním do soukromého a rodinného života, ochrana před neoprávněným shromažďováním,

zveřejňováním nebo jiným zneužíváním údajů o své osobě, když nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, tak jako tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením, s výjimkou případů a způsobem, které stanoví zákon, a právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

Překladatelé návrhu se domnívají, že je zřejmé, že údaje jsou zejména v trestním řízení vyžadovány zcela rutinně. Navrhovatelé mají za to, že stávající právní úprava zjevně neposkytuje efektivní záruku toho, aby nedocházelo k nadužívání žádostí o provozní a lokalizační údaje. Absenci dostatečné právní úpravy, jež je ve smyslu ustanovení čl. 4 odst. 2 Listiny předpokladem omezení základních práv a svobod v obecné rovině, přitom nelze nahradit ani soudním přezkumem (k tomu viz Nález ÚS ve věci sp. zn. Pl. ÚS 24/11) a dle navrhovatelů nelze tento problém vyřešit ani ústavně konformním výkladem. Tento podaný návrh směřuje proti ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a prováděcí vyhlášce č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. Jakož i proti § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů a § 88a zákona č. 141/1961 Sb., trestního řádu, ve znění pozdějších předpisů.

Předkladatelé návrhu se snaží napadnout ustanovení zákona o elektronických komunikacích, kdy právnická nebo fyzická osoba, vedená v registru tohoto zákona a zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, když těmito provozními a lokalizačními údaji jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace. Předkladatelé návrhu se snaží v této souvislosti i napadnout skutečnost, že v těchto případech se dále uchovávají také údaje jako jméno, příjmení a adresa účastníka nebo registrovaného uživatele uvedená ve smlouvě nebo adresa umístění telekomunikačního koncového zařízení. Rovněž je poukazováno na ustanovení § 2 odst. 4, odst. 5, odst. 6 vyhlášky č. 357/2012 Sb., dle kterého se uchovávají také údaje o všech telefonních automatech, údaje o všech základnových stanicích včetně geografických souřadnic, údaje o vzájemných vazbách

mezi telefonními čísly a identifikátory IMSI, jakož i identifikátory mobilních zařízení, údaje o aktivaci u předplacených služeb či údaje o poskytovatelích služeb.

Dle návrhu předkladatelů se u veřejných telefonních sítí s přepojováním okruhů se uchovávají tyto provozní a lokalizační údaje:

a) telefonní číslo volajícího a volaného, telefonní čísla, která se zúčastnila konferenčního volání, identifikátor telefonní karty použité ve veřejném telefonním automatu,

b) datum a čas zahájení komunikace,

c) délka komunikace,

d) datum a čas odeslání textové zprávy SMS,

e) použitá telefonní služba (např. přesměrování hovoru, hlasová schránka apod.)

f) stav komunikace,

u veřejných mobilních telefonních sítí se uchovávají

a) identifikátor IMSI volajícího a volaného,

b) identifikátor mobilního přístroje volajícího a volaného,

c) datum a čas odeslání multimediální zprávy MMS,

d) označení základnové stanice Start a základnové stanice Stop,

u služby přístupu k internetu z pevného připojení

a) typ připojení,

b) telefonní číslo nebo označení uživatele,

c) identifikátor uživatelského účtu,

d) adresa MAC zařízení uživatele služby,

e) datum a čas zahájení a ukončení připojení k internetu,

f) označení přístupového bodu u bezdrátového připojení k internetu,

g) adresa IP a číslo portu, ze kterých bylo připojení uskutečněno,

u služby přístupu k internetu z mobilního připojení

a) typ připojení,

b) telefonní číslo uživatele,

c) identifikátor mobilního zařízení,

d) datum a čas zahájení a ukončení připojení k internetu,

e) označení základnové stanice Start a základnové stanice Stop,

f) adresa IP a číslo portu, ze kterých bylo připojení uskutečněno,

u služby přístupu ke schránce elektronické pošty

a) adresa IP a číslo portu, ze kterých bylo připojení uskutečněno,

b) identifikátor uživatelského účtu,

c) datum a čas zahájení připojení ke schránce elektronické pošty,

d) datum a čas ukončení připojení ke schránce elektronické pošty,

e) identifikátor protokolu elektronické pošty,

u služby přenosu zpráv elektronické pošty

a) adresa IP a číslo portu zdroje a cíle přenášené zprávy,

b) datum a čas odeslání zprávy,

c) adresa elektronické pošty odesílatele,

d) adresy elektronické pošty příjemců,

e) stav přenosu zprávy,

f) identifikátor protokolu elektronické pošty,

u služby IP telefonie

a) adresa IP a číslo portu zdrojového zařízení,

b) adresa IP a číslo portu cílového zařízení,

c) transportní protokol,

d) datum a čas zahájení a ukončení komunikace,

u služby přístupu k internetu podle písmene z pevného či mobilního připojení s překladem adres IP

a) privátní adresa IP,

b) veřejná adresa IP a číslo portu, nebo přidělený rozsah portů,

c) datum a čas zahájení překladu adres,

d) datum a čas ukončení překladu adres.

Předkladatelé návrhu se dále snaží napadnout ustanovení, kdy Policie České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, a dále útvar policie, jehož úkolem je boj s terorismem, je oprávněna si vyžádat provozní a lokalizační údaje od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací způsobem umožňujícím dálkový a nepřetržitý přístup. Jak již bylo uvedeno, dále se snaží napadnout ustanovení § 88a zákona č. 141/1961 Sb., trestního řádu, když cílem tohoto návrhu je nález Ústavního soudu o zrušení všech těchto uvedených ustanovení.

Předkladatelé návrhu dále uvádí možnou alternativu k vyžadování těchto údajů a to tzv. **quick freeze systém**, jenž se liší od uchovávání údajů zejména tím, že při něm nejsou uchovávány plošně údaje o veškeré komunikaci, ale jsou uchovávány pouze údaje o komunikaci podezřelých osob, které jsou vyžádány ze strany oprávněných orgánů a se souhlasem soudu. Uchovávání tak začíná až ve chvíli, kdy o toto požádá

oprávněný orgán, podobně jako je tomu například u odposlechů, případně lze vyžádat i údaje uchovávané operátory za účelem vyúčtování služeb.[41]

8.6.1 KOMENTÁŘ

Při zveřejnění tohoto návrhu lze jen říci, že bylo jen otázkou času, kdy se nově zvolená politická strana do Poslanecké sněmovny Parlamentu České republiky pokusí tento návrh za účelem zrušení uvedených ustanovení prosadit. Předkladatel tohoto návrhu nebere však v potaz, že ačkoli Listina základních práv a svobod, tedy ústavní pořádek České republiky, uvádí, že i přes zaručená práva na ochrany jedince, nemůže státní orgán do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a zejména nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných. V daném případě tak jsou dle tohoto ustanovení skutečně zákonem stanoveny možnosti prolomení této ochrany, což jsou v daném případě právě ta ustanovení, která se předkladatel návrhu snaží zrušit. Bude-li Ústavním soudem formou nálezu vyhověno tomuto návrhu, pohrává si tento návrh s bezpečností obyvatel České republiky, byť v elektronickém světě, a rozhodně těm slušným občanům nepomůže před následky trestných činů, pokud však předkladatel nedokázal zamezit páchání trestné činnosti potažmo terorismu. Vždyť právě bezpečnost je v demokratickém zřízení realizována skutečností, že jsou všem dány zákonem některé povinnosti, omezení a oprávnění. Pokud tyto povinnosti, omezení a oprávnění zmizí, nelze bezpečnost realizovat, není zadarmo. Bezpečnost je ústupek vůči ústupku na druhé straně, je o dosažení rovnováhy. V současné době nelze ani říci, že se naše společnost nachází v období míru, hrozeb na naši společnost máme mnoho kolem sebe. Na zajištění bezpečnosti je třeba vynaložit prostředky, které stále všude chybí, zejména finanční prostředky. Operuje-li tu předkladatel návrhu s "plošným šmírováním a sledováním slušných občanů" je třeba k uvedenému říci, že nelze uchovávání telekomunikačního provozu brát jako šmírování či sledování. Uchovávat se nerovná sledovat. Pod tímto pojmem si lze představit sledování přes kukátko s tím, že vím o každém, co činí. Tak to v elektronickém světě ale nefunguje, tedy alespoň v našem právním státě. Předmětné údaje jsou dotazovány až v případě prověřování konkrétní trestné činnosti, jež se dopustil právě podezřelý. Tedy

[41] Návrh Pirátů a IuRe a zrušení plošného sledování. Jan Vobořil & Česká pirátská strana [online]. © 2017 [cit. 2017-12-23]. Dostupné z WWW: <https://www.pirati.cz/tiskove-zpravy/navrzeno-zruseni-smirovani.html>.

jsou vyžadovány údaje o podezřelých osobách, potažmo o poškozených v případě jejich souhlasu, aby se policejní orgán dostal k údajům pachatele (např. zneužité elektronické účty poškozených). Trestná činnost, zejména informační kriminalita dle uvedených statistických výstupů, je na vzestupu, je pochopitelné, že když vzrůstá trestná činnost, roste i rozsah dotazů k těmto údajům. Tvrzení předkladatele návrhu o tom, že lze tyto trestné činy vyšetřovat i bez těchto dat jen potvrzuje skutečnost, že předkladatel nezná rozdíl mezi prověřováním a vyšetřováním. Vyšetřování jako úsek trestního stíhání konkrétního obviněného nelze bez těchto údajů vést, neboť by došlo k důkazní nouzi a nebylo by možné trestnou činnost obviněnému prokázat. Od toho, prověřování bez těchto údajů lze vést, avšak toto zpravidla skončí meritorním rozhodnutím o odložení, neboť pokud není možné tyto údaje vyžádat, nelze pak proti podezřelé osobě zahájit trestní stíhání. Samozřejmě jsou situace, kdy v prověřování se ukážou náhody, kdy lze zajistit jiné listinné údaje či lze využít operativně pátrací prostředky, avšak v současné době se prověřování trestné činnosti páchané ryze v elektronickém světě bez těchto údajů neobejde. Jak pak poškozeným vysvětlit, že prověřování bude odloženo, neboť není žádná možnost, jak údaje o pachateli v elektronickém světě získat a k nim dám provádět prověřování.

Co se týče navrhovaného zrušení ustanovení § 88a trestního řádu s odůvodněním, že tyto data by měla být vyžadována za podmínek jako např. § 88 trestního řádu v případě zvlášť závažných zločinů, lze jen sdělit, že ustanovení § 88 trestního řádu je odposlechem komunikace, tedy zjišťujeme obsah a to vždy do budoucna, eventuálně dále postup sledování osob a věcí podle § 158d odst. 3 trestního řádu. V případě současného ustanovení § 88a trestního řádu zjišťujeme údaje do minulosti a to jen základní identifikátory, když nám není znám obsah této komunikace. V daném případě je tak toto vyžadování výrazně odstupňováno, nad to, je zde dohled ze strany soudu, který k těmto vydává soudní příkaz a v případě sledování osob a věcí pak předchozí souhlas soudce. Předkladatel návrhu si tyto pojmy zřejmě plete, když například navrhuje zrušení ustanovení § 88a trestního řádu avšak navrhuje možnou alternativu tzv. quick freeze systém, jenž se liší od uchovávání údajů zejména tím, že při něm nejsou uchovávány plošně údaje o veškeré komunikaci, ale jsou uchovávány pouze údaje o komunikaci podezřelých osob, které jsou vyžádány ze strany oprávněných orgánů a se souhlasem soudu. Uchovávání tak začíná až ve chvíli, kdy o toto požádá oprávněný orgán, což de facto naplňuje ustanovení § 88 trestního řádu. Nad to

předkladatel návrhu nezmiňuje v případě ustanovení § 88a trestního řádu skutečnost, že vyžadování údajů i ke zde výslovně neuvedeným trestným činům je možné právě s odkazem na mezinárodní smlouvu, což v daném případě je Úmluva o počítačové kriminalitě. Smutným faktem je zde i skutečnost, že předkladatel návrhu navrhuje možnost policejnímu orgánu zrušit oprávnění předmětná data vyžadovat v případě zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, což je zejména v případě hledání osob značně nebezpečné a v případě pohřešování je tak tento návrh špatnou zprávou například pro rodiče pohřešovaných dětí, když nad to ochrana života a zdraví v tomto případě by měla být nadřazena ochraně práv jedincům zaručených jim Listinou základních práv a svobod. Přeci jenom dle této Listiny základních práv a svobod, když každý má právo na život a na ochranu zdraví, když i právě pro tuto ochranu Listina základních práv a svobod stanoví, že ostatní práva lze omezit právě mimo jiné pro ochranu života a zdraví.

Případná skutečnost, že předkladatelé návrhu poukazují i na skutečnost, že jsou dále uchovávány také údaje jako jméno, příjmení a adresa účastníka nebo registrovaného uživatele uvedená ve smlouvě nebo adresa umístění telekomunikačního koncového zařízení, lze jen konstatovat, že je na dobrovolnosti jedince s kým vstoupí do obchodního vztahu a za jakých obchodních podmínek. Zákazník si nemusí tuto službu zřizovat, pokud nechce, aby tyto údaje obchodníkovi sdělil.

Ihned po seznámení se zveřejněným prohlášením České pirátské strany na sociální síti Facebook, se autor této práce snažil v komentáři pod tímto příspěvkem výše uvedené ospravedlnit v zájmu průzkumu, jak dokáže tvrzení obhajovatelů tohoto návrhu zvrátit, když jeho hlavní příspěvek označilo „To se mi líbí“ celkem 11 uživatelů, přičemž v konverzaci nalezl pouze 3 osoby, které stejným tvrzením odporovaly podanému návrhu. V ostatních případech si to občané nenechali vysvětlit s obavou, že jsou sledováni, potažmo se od myšlenky návrhu odklonili stížnostmi na jiná politická témata. Snaha autora práce je uvedena v příloze č. 11.

ZÁVĚR A NÁVRH DE LEGE FERENDA

Informační kriminalita každoročně vzrůstá spolu se vzrůstající tendencí informační společnosti. Telekomunikační údaje jsou důležitým prvkem v boji nejen proti informační kriminalitě, jsou součástí elektronického světa, tak jako listiny ve světě reálném. Nelze se k telekomunikačním údajům obracet. Informační technologie a i telekomunikační údaje mají za cíl vše sblížit, zjednodušit, urychlit. Ve vztahu k informační kriminalitě lze zařadit i jednání vykazující znaky přestupku a to až do okamžiku, než je jeho trestně právní kvalifikací spolehlivě vyloučeno, že se nejedná o jednání naplňující některou ze skutkových podstat trestných činů uvedených ve zvláštní části trestního zákoníku. Zde je naráženo na smutnou okolnost, že v případě, že dojde ke svázání jednotlivých přestupkových jednání, zpravidla na základě výši škody, vůči konkrétní osobě podezřelého, tedy již zjištěného pokračujícího trestného činu, je ve vztahu k uplynulé době skoro nemožné vyžadovat telekomunikační údaje. V tomto vztahu **autor navrhuje změnu de lefa ferenda a to konkrétně ustanovení § 97 odst. 3 zákona č. 127/2005 Sb.** o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) **v tomto znění:**

"Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat **po dobu 12 měsíců (1 roku)** provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout

a) orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem,

b) Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem,

c) Bezpečnostní informační službě pro účely a při splnění podmínek stanovených zvláštním právním předpisem),

d) Vojenskému zpravodajství pro účely a při splnění podmínek stanovených zvláštním právním předpisem,

e) České národní bance pro účely a při splnění podmínek stanovených zvláštním právním předpisem.

Po uplynutí doby podle věty první je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud tento zákon nestanoví jinak (§ 90)."

SEZNAM POUŽITÝCH ZDROJŮ

Bibliografické zdroje

DRAŠTÍK A., FENYK J., a kol. Trestní řád (č. 141/1961 Sb.) - Komentář, Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-600-7.

JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

KOLOUCH, J. Cybercrime. Praha: CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8.

KOPECKÝ, K., KREJČÍ, V. Rizika virtuální komunikace: příručka pro učitele a rodiče. 1. vyd. Olomouc: NET UNIVERSITY, s.r.o., 2010. 34 s. ISBN 978-80-254-7866-O.

MATOUŠKOVÁ, I. Aplikovaná forenzní psychologie. Praha: Grada, 2013. 304 s. ISBN 978-80-247-4580-0.

Elektronické zdroje

ČESKO. Základní definice, vztahující se k tématu kybernetické bezpečnosti. In Ministerstvo vnitra České republiky. 6 s. 2013, s. 5. Dostupné také z WWW: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx.

Návrh Pirátů a IuRe a zrušení plošného sledování. Jan Vobořil & Česká pirátská strana [online]. © 2017 [cit. 2017-12-23]. Dostupné z WWW: <https://www.pirati.cz/tiskove-zpravy/navrzeno-zruseni-smirovani.html>.

SCAM419. Josef Džubák & HOAX.cz [online]. © 2000-2017 [cit. 2017-12-07]. Dostupné z WWW: <http://www.hoax.cz/scam419/co-je-to-scam-419>.

Legislativní dokumenty

FRANCIE. Council of Europe. Convention on Cybercrime - ETS no. 185. Budapest. [online]. Council of Europe, © 2001 [cit. 2017-12-06]. Dostupné z WWW: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

ČESKO. Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě (Budapešť, 23. listopadu 2001). In PARLAMENT ČESKÉ REPUBLIKY POSLANECKÁ SNĚMOVNA. 24 s. 2013, VI. volební období, 890/0, s. 3. Dostupné také z WWW: http://www.psp.cz/doc/00/13/95/00139513.pdf.

ČESKO. Zákon č. 127/2005 Sb. o elektronických komunikacích, ve znění pozdějších předpisů. In Sbírka zákonů, Česká republika. 2005, částka 43, s. 1330-1408.

SEZNAM PŘÍLOH

Příloha č. 1: Český statistický úřad: Domácnosti v ČR s počítačem celkem

Příloha č. 2: Český statistický úřad: Domácnosti v ČR s připojením na internet

Příloha č. 3: Český statistický úřad: Jednotlivci v ČR používající sociální sítě

Příloha č. 4: Český statistický úřad: Jednotlivci v ČR používající internetové bankovnictví

Příloha č. 5: Český statistický úřad: Jednotlivci v ČR nakupující na internetu

Příloha č. 6: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2013 do 31.12.2013

Příloha č. 7: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2014 do 31.12.2014

Příloha č. 8: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2015 do 31.12.2015

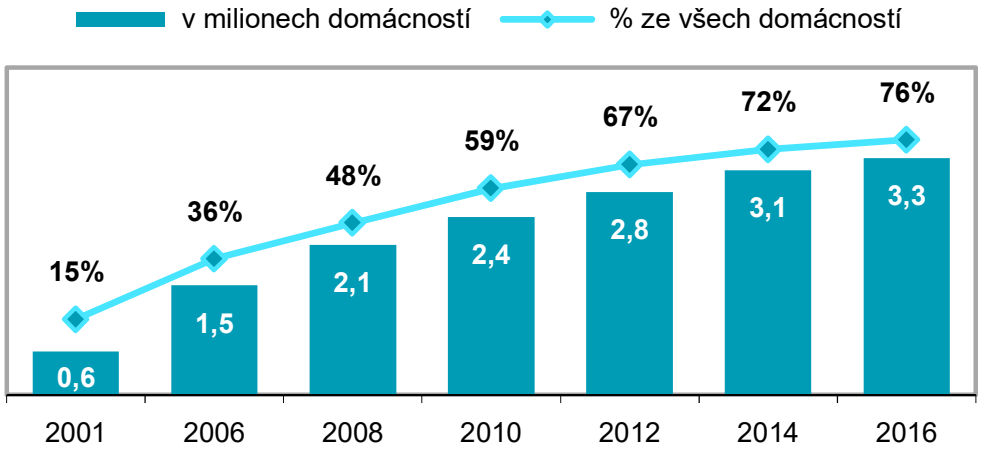
Příloha č. 9: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2016 do 30.11.2016

Příloha č. 10: Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování: Statistiky informační kriminality 2011-07/2017

Příloha č. 11: Vlastní komentář a komunikace k Návrhu České pirátské strany ke zrušení uchovávání telekomunikačního provozu

Příloha č. 1: Český statistický úřad: Domácnosti v ČR s počítačem celkem

			%
	2012	**2014**	**2016**
Celkem	**67,3**	**72,4**	**75,6**
Celkem (s alespoň 1 členem do 74 let)	74,6	79,4	81
podle typu domácnosti			
domácnosti bez dětí celkem	58,5	64,7	68,4
osob mladších 40 let	86,7	95	91,5
osob starších 65 let	12,3	23,8	29,5
domácnosti s dětmi	91,1	93,7	94,6

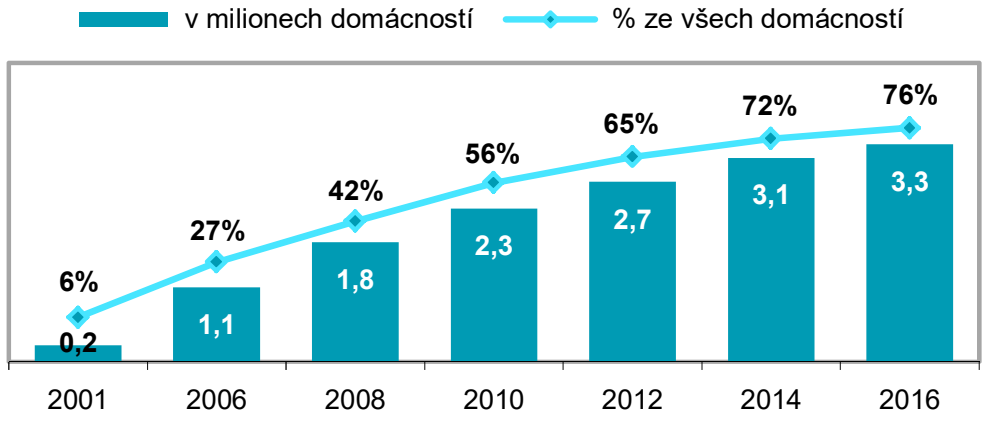


(Zdroj: https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2014-2016 ke dni 23.12.2017)

Porovnáním zveřejněných statistických výstupů Českého statistického úřadu zaměřených na domácnosti s počítačem v České republice můžeme konstatovat, že jejich počet plynuje rok od roku vzrůstá a to i včetně u osob starších 65 let.

Příloha č. 2: Český statistický úřad: Domácnosti v ČR s připojením na internet

			%
	2012	**2014**	**2016**
Celkem	**65,4**	**72,1**	**76,1**
Celkem (s alespoň 1 členem do 74 let)	72,6	79,2	81,7
podle typu domácnosti			
domácnosti bez dětí celkem	56,5	64,6	68,8
osob mladších 40 let	85,2	95,6	94,6
osob starších 65 let	11,2	22,7	29
domácnosti s dětmi	89,6	93	95,3



(Zdroj: https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2014-2016 ke dni 23.12.2017)

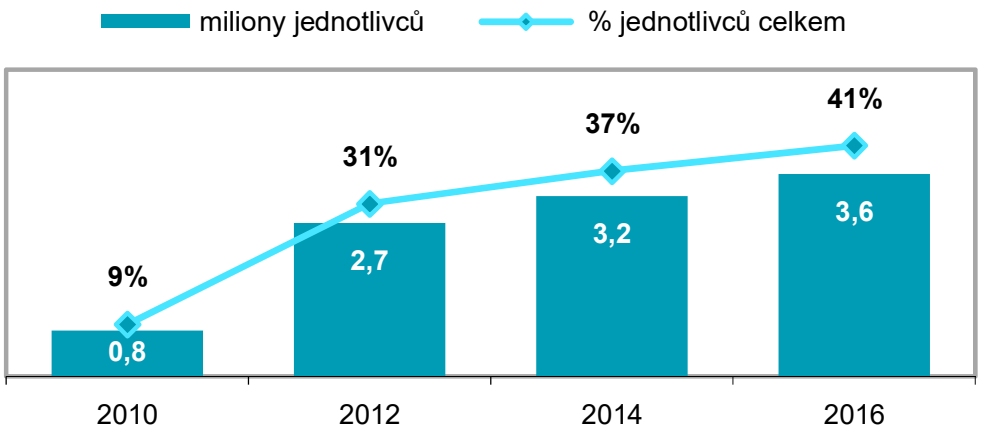
Porovnáním zveřejněných statistických výstupů Českého statistického úřadu zaměřených na domácnosti s připojením na internet v České republice můžeme konstatovat, že jejich počet plynuje rok od roku vzrůstá a to i včetně u osob starších 65 let. Rovněž můžeme vidět, že téměř většina domácností s dětmi je již k internetu připojena.

Příloha č. 3: Český statistický úřad: Jednotlivci v ČR používající sociální sítě

%

	2012	2014	2016
Celkem 16+	**30,3**	**36,9**	**41,4**
Celkem 16–74	32,8	40	45,1
podle pohlaví			
muži 16+	31,3	37,7	40,7
ženy 16+	29,4	36,1	42,1
podle věkových skupin			
16–24 let	79,4	90,1	91,4
25–34 let	57,9	71,7	77,8
35–44 let	32,4	43,1	53,0
45–54 let	17,0	23,9	33,0
55–64 let	7,9	10,5	14,1
65+	1,3	3,5	4,9
podle dokončeného vzdělání (25+)			
základní	6,7	8,3	13,2
střední bez maturity	16,6	20,7	26,8
střední s maturitou	30,8	35,4	44,1
vysokoškolské	38,4	46,8	51,3
podle specifické skupiny populace			
ženy na rodičovské dovolené	47,9	65,2	72,1
studenti 16+	84,9	93,5	94,0

starobní důchodci	1,6	4,1	5,5



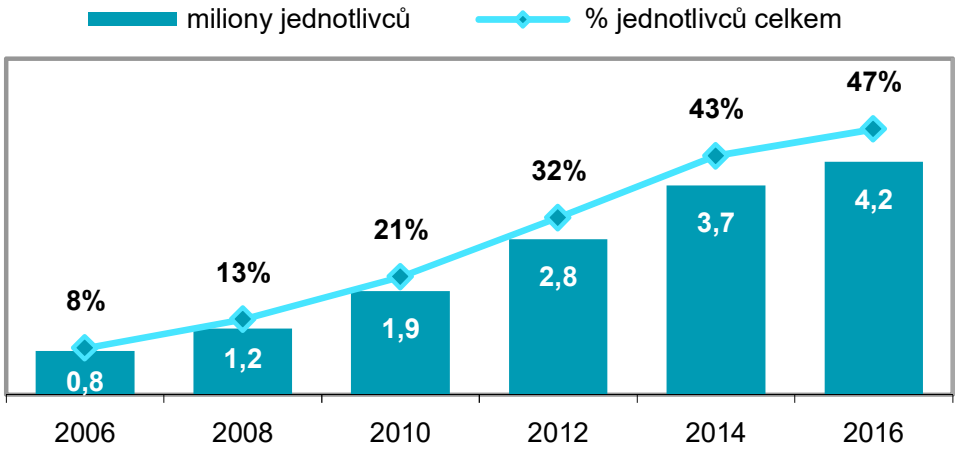
(Zdroj: https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2014-2016 ke dni 23.12.2017)

Porovnáním zveřejněných statistických výstupů Českého statistického úřadu zaměřených na jednotlivce v České republice používající sociální sítě můžeme konstatovat, že jejich počet plynuje rok od roku vzrůstá a to celým věkovým spektrem i spektrech dle dokončeného vzdělání. Pozadu v oblasti sociálních sítí nezůstávají ani senioři, jejich počet pomalu rovněž přibývá.

Příloha č. 4: Český statistický úřad: Jednotlivci v ČR používající internetové bankovnictví

			%
	2012	**2014**	**2016**
Celkem 16+	**32,3**	**42,6**	**47,4**
Celkem 16–74	34,2	46,0	51,4
podle pohlaví			
muži 16+	34,3	45,4	48,8
ženy 16+	30,4	40,0	46,0
podle věkových skupin			
16–24 let	26,0	38,5	40,3
25–34 let	57,2	68,6	69,4
35–44 let	46,6	62,0	71,0
45–54 let	38,6	49,8	58,5
55–64 let	22,3	31,1	36,7
65+	3,7	9,2	12,3
podle dokončeného vzdělání (25+)			
základní	5,8	6,9	9,8
střední bez maturity	20,1	27,1	36,2
střední s maturitou	45,6	55,5	61,1
vysokoškolské	62,8	76,0	73,7
podle specifické skupiny populace			
ženy na rodičovské dovolené	50,6	69,0	68,5

studenti 16+	22,6	28,9	33,6
starobní důchodci	5,2	10,5	12,9



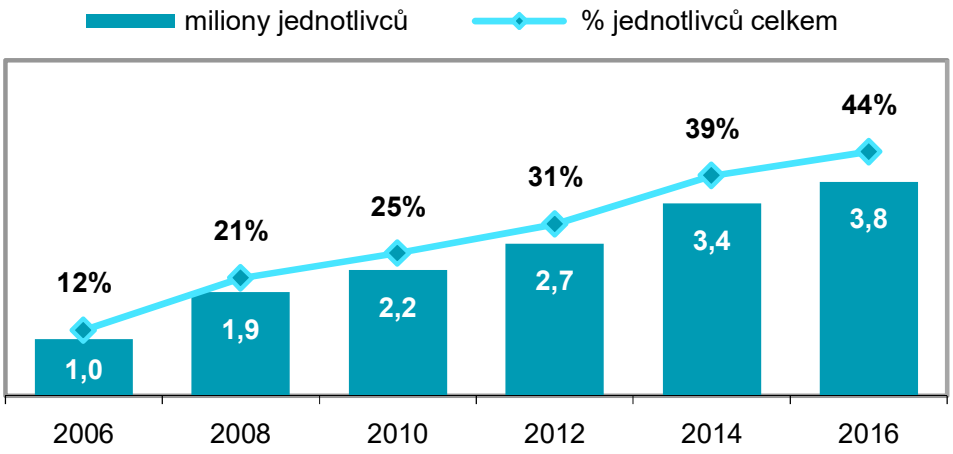
(Zdroj: https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2014-2016 ke dni 23.12.2017)

Porovnáním zveřejněných statistických výstupů Českého statistického úřadu zaměřených na jednotlivce v České republice používající internetové bankovnictví můžeme konstatovat, že jejich počet plynuje rok od roku vzrůstá a to celým věkovým spektrem i spektrech dle dokončeného vzdělání. Pozadu v oblasti internetového bankovnictví nezůstávají ani senioři, jejich počet pomalu rovněž přibývá.

Příloha č. 5: Český statistický úřad: Jednotlivci v ČR nakupující na internetu

			%
	2012	**2014**	**2016**
Celkem 16+	**30,6**	**39,3**	**43,6**
Celkem 16–74	32,5	42,5	47,4
podle pohlaví			
muži 16+	31,5	40,5	42,3
ženy 16+	29,8	38,1	44,9
podle věkových skupin			
16–24 let	46,3	62,2	58,7
25–34 let	54,3	63,2	72,0
35–44 let	43,1	52,6	59,4
45–54 let	27,9	40,1	46,6
55–64 let	15,7	21,7	28,3
65+	3,9	7,6	9,7
podle dokončeného vzdělání (25+)			
základní	6,0	6,3	8,3
střední bez maturity	18,7	23,5	30,5
střední s maturitou	38,5	45,9	55,2
vysokoškolské	50,7	61,4	61,5
podle specifické skupiny populace			
ženy na rodičovské dovolené	51,0	64,6	72,4
studenti 16+	46,9	62,5	58,3

starobní důchodci	4,2	8,2	11,4



(Zdroj: https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2014-2016 ke dni 23.12.2017)

Porovnáním zveřejněných statistických výstupů Českého statistického úřadu zaměřených na jednotlivce v České republice nakupujících na internetu můžeme konstatovat, že jejich počet plynuje rok od roku vzrůstá a to celým věkovým spektrem i spektrech dle dokončeného vzdělání. Pozadu v oblasti nakupování na internetu nezůstávají ani senioři, jejich počet pomalu rovněž přibývá.

Příloha č. 6: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2013 do 31.12.2013

TSK	Název	Zjištěno	Objasněno	Stíháno, vyšetřováno osob					Škody v tis. Kč	
				Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let	Ženy	celkem	zajištěno
828	Poruš. tajemství doprav. zpráv	45	25	11	1	0	0	7	0	0
863	Poruš. autor. práva, k datab.a padělání díla	338	201	152	21	0	2	10	125480	86
865	Pošk. a zneuž. záz. na nos. infor.	301	76	57	8	5	3	17	595	0
	celkem:	684	302	220	30	5	5	34	126075	86

TSK = Takticko statistická klasifikace kriminality Policie ČR.

(Zdroj: http://www.policie.cz/soubor/12-celkova-kriminalita-za-obdobi-od-01-01-2013-do-31-12-2013.aspx ke dni 23.12.2017)

Policejní prezidium České republiky neeviduje přesnou statistiku ryze informační kriminality ani jejich jednotlivých trestných činů, případně trestných činů, které jsou přímo páchány informační kriminalitou (např. podvod spáchaný na poli informační kriminality x podvod obecného charakteru). Uvedené statistické výstupy tak nejsou kompletními statistickými výstupy jednotlivých trestných činů informační kriminality.

Příloha č. 7: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2014 do 31.12.2014

TSK	Název	Zjištěno	Objasněno	Stíháno, vyšetřováno osob					Škody v tis. Kč	
				Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let	Ženy	celkem	zajištěno
828	Poruš. tajemství doprav. zpráv	33	17	18	3	0	0	7	0	0
863	Poruš. autor. práva, k datab.a padělání díla	358	212	114	12	0	0	9	74757	0
865	Pošk. a zneuž. záz. na nos. infor.	669	192	86	12	5	3	24	15936	0
	celkem:	1060	421	218	27	5	3	40	90693	0

TSK = Takticko statistická klasifikace kriminality Policie ČR.

(Zdroj: http://www.policie.cz/soubor/12-celkova-kriminalita-za-obdobi-od-01-01-2014-do-31-12-2014.aspx ke dni 23.12.2017)

Policejní prezidium České republiky neeviduje přesnou statistiku ryze informační kriminality ani jejich jednotlivých trestných činů, případně trestných činů, které jsou přímo páchány informační kriminalitou (např. podvod spáchaný na poli informační kriminality x podvod obecného charakteru). Uvedené statistické výstupy tak nejsou kompletními statistickými výstupy jednotlivých trestných činů informační kriminality.

Oproti roku 2013 bylo zjištěno o 376 skutků více, objasněno jich bylo o 119 více.

Příloha č. 8: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2015 do 31.12.2015

TSK	Název	Zjištěno	Objasněno	Stíháno, vyšetřováno osob					Škody v tis. Kč	
				Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let	Ženy	celkem	zajištěno
828	Poruš. tajemství doprav. zpráv	56	39	23	5	0	1	8	0	0
863	Poruš. autor. práva, k datab.a padělání díla	399	272	114	9	0	1	5	25080	0
865	Pošk. a zneuž. záz. na nos. infor.	707	144	127	19	14	14	36	12463	0
	celkem:	1162	455	264	33	14	16	49	37543	0

TSK = Takticko statistická klasifikace kriminality Policie ČR.

(Zdroj: http://www.policie.cz/soubor/statistiky-od-01-01-2015-do-31-12-2015-zip.aspx ke dni 23.12.2017)

Policejní prezidium České republiky neeviduje přesnou statistiku ryze informační kriminality ani jejich jednotlivých trestných činů, případně trestných činů, které jsou přímo páchány informační kriminalitou (např. podvod spáchaný na poli informační kriminality x podvod obecného charakteru). Uvedené statistické výstupy tak nejsou kompletními statistickými výstupy jednotlivých trestných činů informační kriminality.

Oproti roku 2013 bylo zjištěno o 478 skutků více, objasněno jich bylo o 153 více.

Příloha č. 9: Policejní prezidium České republiky: Statistický výkaz - kriminalita za období od 01.01.2016 do 30.11.2016

TSK	Název	Zjištěno	Objasněno	Stíháno, vyšetřováno osob					Škody v tis. Kč	
				Celkem	Recidivisté	Nezletilí 1-14 let	Mladiství 15-17 let	Ženy	celkem	zajištěno
828	Poruš. tajemství doprav. zpráv	29	17	15	5	0	0	7	0	0
863	Poruš. autor. práva, k datab.a padělání díla	262	157	110	7	0	1	9	22995	0
865	Pošk. a zneuž. záz. na nos. infor.	590	141	197	56	15	15	33	470027	0
	celkem:	881	315	322	68	15	16	49	493022	0

TSK = Takticko statistická klasifikace kriminality Policie ČR.

(Zdroj: http://www.policie.cz/soubor/statistiky-od-01-01-2016-do-30-11-2016-zip.aspx ke dni 23.12.2017)

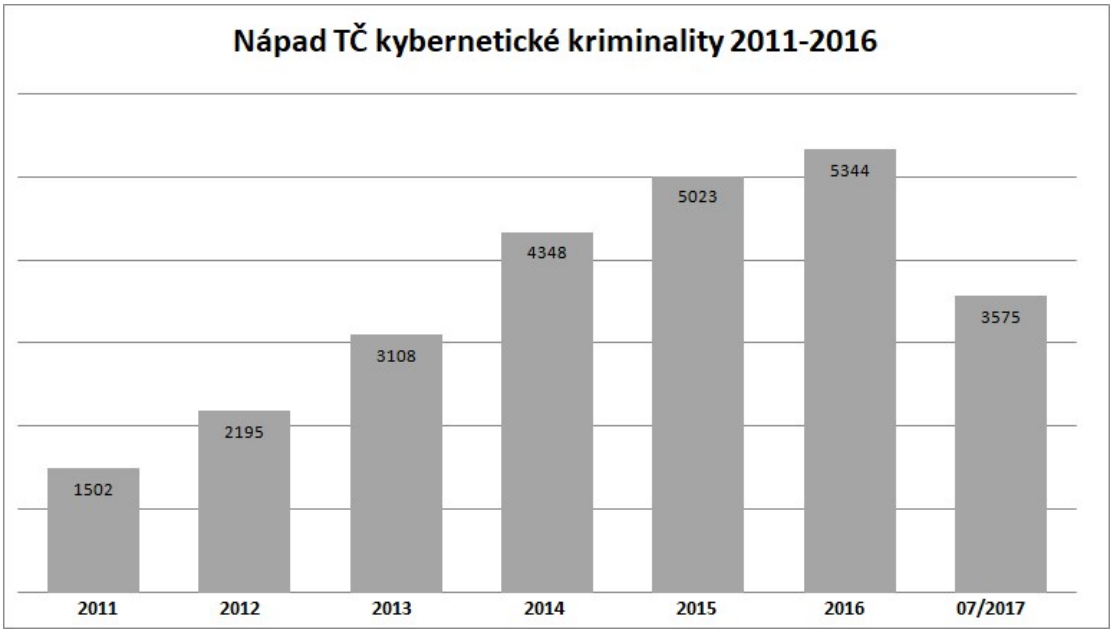
Policejní prezidium České republiky neeviduje přesnou statistiku ryze informační kriminality ani jejich jednotlivých trestných činů, případně trestných činů, které jsou přímo páchány informační kriminalitou (např. podvod spáchaný na poli informační kriminality x podvod obecného charakteru). Uvedené statistické výstupy tak nejsou kompletními statistickými výstupy jednotlivých trestných činů informační kriminality.

Oproti roku 2013 bylo do listopadu 2016 zjištěno o 197 skutků více, objasněno jich bylo o 13 více.

Příloha č. 10: Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování: Statistiky informační kriminality 2011-07/2017

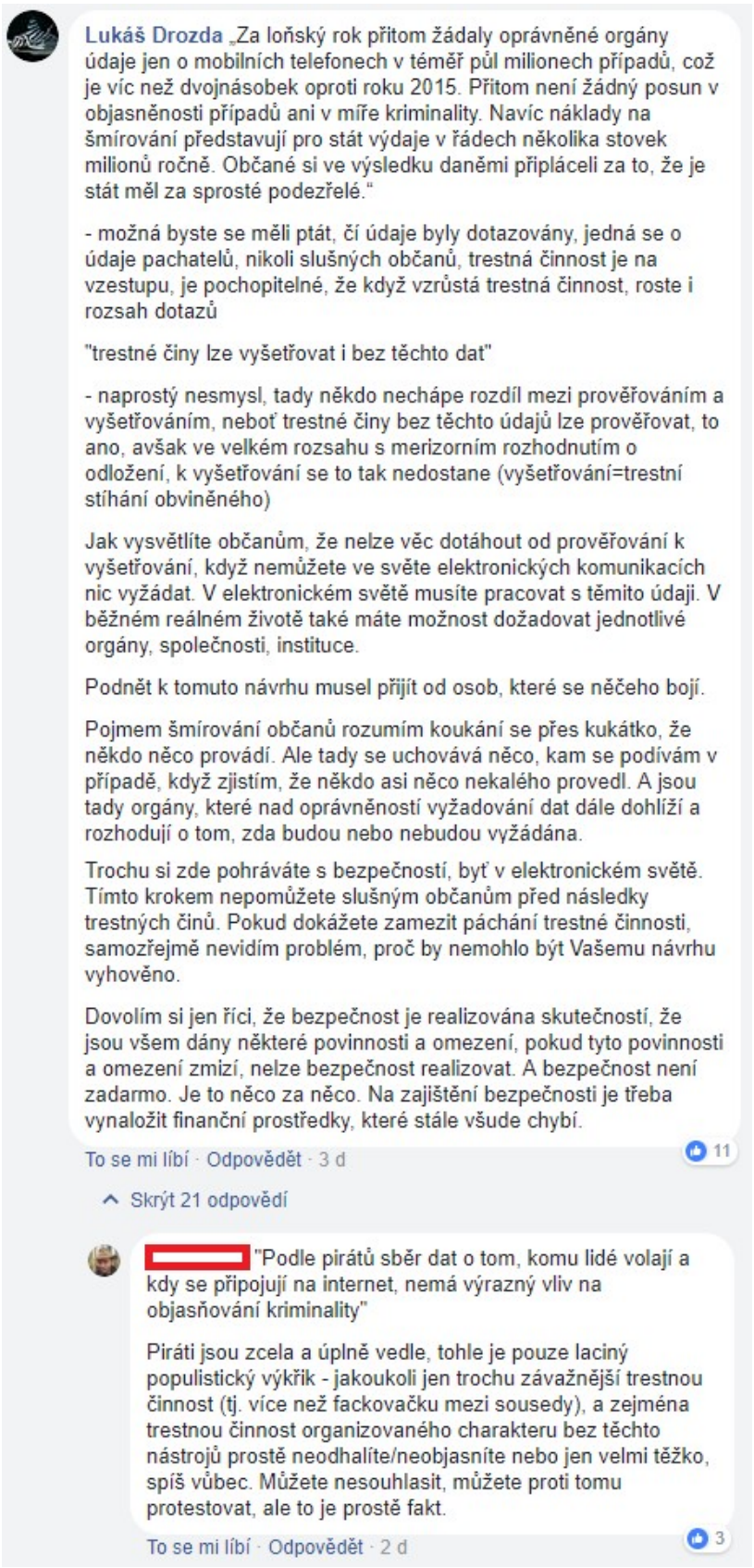
Struktura nápadu	2011	2012	2013	2014	2015	2016	07/2017
podvodná jednání	917	1303	1863	2478	2932	3235	1931
tj. %	*61,05*	*59,36*	*59,94*	*56,99*	*58,37*	*60,54*	*54,01*
hacking	66	112	220	555	578	534	398
tj. %	*4,39*	*5,10*	*7,08*	*12,76*	*11,51*	*9,99*	*11,13*
mravnostní delikty	132	161	261	314	351	344	358
tj. %	*8,79*	*7,33*	*8,40*	*7,22*	*6,99*	*6,44*	*10,01*
autorskoprávní delikty	155	241	181	262	315	237	173
tj. %	*10,32*	*10,98*	*5,82*	*6,03*	*6,27*	*4,43*	*4,84*
násilné projevy + hate crime	86	111	155	202	230	265	217
tj. %	*5,73*	*5,06*	*4,99*	*4,65*	*4,58*	*4,96*	*6,07*
ostatní	146	267	428	537	617	729	498
tj. %	*9,72*	*12,16*	*13,77*	*12,35*	*12,28*	*13,64*	*13,93*

Celkem nápad IT	**1502**	**2195**	**3108**	**4348**	**5023**	**5344**	**3575**



(Zdroj: Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování – autor vlastním šetřením)

Příloha č. 11: Vlastní komentář a komunikace k Návrhu České pirátské strany ke zrušení uchovávání telekomunikačního provozu



Lukáš Drozda „Za loňský rok přitom žádaly oprávněné orgány údaje jen o mobilních telefonech v téměř půl milionech případů, což je víc než dvojnásobek oproti roku 2015. Přitom není žádný posun v objasněnosti případů ani v míře kriminality. Navíc náklady na šmírování představují pro stát výdaje v řádech několika stovek milionů ročně. Občané si ve výsledku daněmi připláceli za to, že je stát měl za sprosté podezřelé."

- možná byste se měli ptát, čí údaje byly dotazovány, jedná se o údaje pachatelů, nikoli slušných občanů, trestná činnost je na vzestupu, je pochopitelné, že když vzrůstá trestná činnost, roste i rozsah dotazů

"trestné činy lze vyšetřovat i bez těchto dat"

- naprostý nesmysl, tady někdo nechápe rozdíl mezi prověřováním a vyšetřováním, neboť trestné činy bez těchto údajů lze prověřovat, to ano, avšak ve velkém rozsahu s merizorním rozhodnutím o odložení, k vyšetřování se to tak nedostane (vyšetřování=trestní stíhání obviněného)

Jak vysvětlíte občanům, že nelze věc dotáhout od prověřování k vyšetřování, když nemůžete ve světe elektronických komunikacích nic vyžádat. V elektronickém světě musíte pracovat s těmito údaji. V běžném reálném životě také máte možnost dožadovat jednotlivé orgány, společnosti, instituce.

Podnět k tomuto návrhu musel přijít od osob, které se něčeho bojí.

Pojmem šmírování občanů rozumím koukání se přes kukátko, že někdo něco provádí. Ale tady se uchovává něco, kam se podívám v případě, když zjistím, že někdo asi něco nekalého provedl. A jsou tady orgány, které nad oprávněností vyžadování dat dále dohlíží a rozhodují o tom, zda budou nebo nebudou vyžádána.

Trochu si zde pohráváte s bezpečností, byť v elektronickém světě. Tímto krokem nepomůžete slušným občanům před následky trestných činů. Pokud dokážete zamezit páchání trestné činnosti, samozřejmě nevidím problém, proč by nemohlo být Vašemu návrhu vyhověno.

Dovolím si jen říci, že bezpečnost je realizována skutečností, že jsou všem dány některé povinnosti a omezení, pokud tyto povinnosti a omezení zmizí, nelze bezpečnost realizovat. A bezpečnost není zadarmo. Je to něco za něco. Na zajištění bezpečnosti je třeba vynaložit finanční prostředky, které stále všude chybí.

To se mi líbí · Odpovědět · 3 d 11

Skrýt 21 odpovědí

[redacted] "Podle pirátů sběr dat o tom, komu lidé volají a kdy se připojují na internet, nemá výrazný vliv na objasňování kriminality"

Piráti jsou zcela a úplně vedle, tohle je pouze laciný populistický výkřik - jakoukoli jen trochu závažnější trestnou činnost (tj. více než fackovačku mezi sousedy), a zejména trestnou činnost organizovaného charakteru bez těchto nástrojů prostě neodhalíte/neobjasníte nebo jen velmi těžko, spíš vůbec. Můžete nesouhlasit, můžete proti tomu protestovat, ale to je prostě fakt.

To se mi líbí · Odpovědět · 2 d 3

[redacted] Pokud budou sledovat konkrétního podezřelého a jeho kontakty, fajn. Ale proč by měli sledovat všechny? Takové údaje jsou celkem nebezpečné v rukou špatných lidí a zabezpečit je na 100% není možné...

To se mi líbí · Odpovědět · 2 d

2

[redacted] Protože ne vždy víš předem, kdo je konkrétní podezřelý a identifikovat ho lze dle zaznamenaného provozu z doby, kdy trestnému činu došlo. A tohle zaznamenáš jen plošným screeningem. K získání takových nebezpečných údajů navíc vede celkem dlouhá a komplikovaná cesta přes několik hrází. Jakékoliv informace jsou nebezpečné v rukou špatných lidí. Včetně těch ve Tvém mailu. A přesto všechno ten mail máš a používáš ho. Nebo jsi taky pro jeho zakázání?

To se mi líbí · Odpovědět · 2 d

1

[redacted] Tady někdo nechápe rozdíl mezi vyšetřováním podezřelého a plošným sledováním.

Plošné sledování nemá ve svobodné a demokratické společnosti prostě co dělat a názor "nic špatného nedělám, může mi to být jedno" je v dobách míru naprosto neopodstatněný. Z principu platí a musí platit "nic špatného nedělám, tedy nejsem nijak a nikým sledován". Navíc stát bude chtít jen víc a víc. Nikdy se nevzdá moci nad občany kterou získal. Bude toho jen víc a víc. Za 10, 15 let budeme mít centrální systém co agreguje kamerové a digitální záznamy /plošně zaznamenávané/ protože "teroristé, slušní občané atd..." kde bude naprosto celý denní život každého jednotlivce snadno dostupný, a lidi jako vy tomu zatleskaj a zase napíšou podobnou z prstu vycucanou pitomost jako je toto:

"- možná byste se měli ptát, čí údaje byly dotazovány, jedná se o údaje pachatelů, nikoli slušných občanů, trestná činnost je na vzestupu, je pochopitelné, že když vzrůstá trestná činnost, roste i rozsah dotazů"

Piráti mají naprostou pravdu, pošné sledování je extrémní řešení pro extrémní případy, a nikoliv usnadňovák pro neschopnou státní moc.

Abych vás parafrázoval, "Slušný člověk nemá co být sledován!!!"

To se mi líbí · Odpovědět · 2 d

2

Lukáš Drozda Uchovávat se nerovná sledovat. Sleduji podezřelého podle jeho uchovaných dat až když vím, že je lump. A jestli se to někomu nelíbí, tak nechte změnit trestní právo hmotné, smažte trestné činy, aby nebyla potřeba kvůli nim tyto údaje vyžadovat a hledat ... Zobrazit více

To se mi líbí · Odpovědět · 2 d

Lukáš Drozda Ještě si přečtěte zákon o elektronických komunikacích na ty svátky, abyste věděli, jak se to všechno vlastně všude plošně uchovává každým a kolik staletí jsou ty data uchovávána a jak je jednoduché se k těm datum dostat. Ach jo, i ty osobní, bankovní data nemají takovou ochranu, jako ty elektronická. A zamyšlete se, s čím vším jste v obchodních podmínkách souhlasili např. zde s touto sociální službou, a zcela dobrovolně a nikdo Vás nenutil. Až jednou vycestujete do nejdemokratičtější země a budete chtít vízum, možná vás napadne, k čemu se může tamní politický systém dostat z důvody bezpečnostních prověrek.

To se mi líbí · Odpovědět · 2 d · 1

[redacted] Představ si, že by se po celé ČR vypnuly bezpečnostní kamery, které mimo pohyb pachatelů přirozeně zaznamenávají i pohyb běžných občanů. Tohle je naprosto to stejné s tím rozdílem, že abys získal a hlavně identifikoval někoho dle záznamu provozu, musíš kvůli tomu jít za soudcem dozorujícím prověřovaný případ, a ten zváží, je-li to vůbec nutné. Na normální kameře Ti stačí znát jen obličeje osob na záznamu, abys je identifikoval. Tady je to mnohem těžší a nad oprávněností a účelností takových žádostí je zvýšený dozor.

Stavět zákony na základě nereálných hypotéz a nesouvisejících statistikách je zhovadilost a ukazuje to tak maximálně amatérství Pirátů.

To se mi líbí · Odpovědět · 2 d · Upraveno · 1

Lukáš Drozda Co je mír, máme ho kolem sebe? Já nevím, na každém kroku samá hrozba.

To se mi líbí · Odpovědět · 2 d

[redacted] Mnohem lepší je příklad, kdy krom kamer před policejní stanicí, na soukromém pozemku atp. si musíš povinně nechat nainstalovat kamery do celého svého bytu a nechat se sledovat, protože co kdybys chtěl spáchat teroristický útok? Jenže když ho budeš chtít spáchat, stejně se kamerám nějak vyhneš a najdeš si místo a způsob, jak se se spolupachatelem sejít a domluvit se. Ve vodách internetu se tomu říká šifrování.

To se mi líbí · Odpovědět · 2 d

[redacted] Jenže problémem je, že ze zákona nelze do těchto dat nahlížet plošně (naštěstí), ale pouze se dotazovat na konkrétní osoby. Tudíž musíš mít podezřelého, nemůžeš ho hledat namátkou. A pokud máš podezřelého, tak ho můžeš stejně dobře nechat odposlouchávat a nemusí se zbytečně sledovat všichni.

To se mi líbí · Odpovědět · 2 d

Lukáš Drozda To ale lze jen u telefonu, ne u IP. Jak chceš odposlouchávat pachatelův provoz po IP, když nikdy dle vašeho názoru nezjistíš jakou má, protože by to nikdo nevěděl.

To se mi líbí · Odpovědět · 2 d · 1

Lukáš Drozda Jak říkám, nejdřív si to nastudujte, než se začnete cítit dotčení ničím.

To se mi líbí · Odpovědět · 2 d · 1

[redacted] Plosne shromazdovani dat ale znamena, ze nas policie povazuje uplne vsechny za potencialne podezrele. At si shromazduji data na zaklade pozadavku soudu na konkretni sim kartu. Ne uplne vsem.

To se mi líbí · Odpovědět · 2 d

[redacted] Já mluvím z praxe, Ty z čisté domnělé teorie. Pak se spolu dál nemáme o čem bavit

To se mi líbí · Odpovědět · 2 d · 1

[redacted] Další diskuse asi nemá cenu. Z celého srdce ale přeji všem paranoidním křiklounům, aby si v případě, že data retention bude zrušené, rozbili na takové bezpečnostní díře tlamičky jako první právě oni.

To se mi líbí · Odpovědět · 2 d · 1

[redacted] To navrhované zrušení se týká i logování NATu, že?

To se mi líbí · Odpovědět · 2 d

[redacted] Víte, já když čtu vám podobné názory, mám pocit jak je potom možné, že jsme doteď nevymřeli, že jsme se nepozabíjeli navzájem a že ulice nebyly doteď plné gangsterů kteří si bez kamer dělali divoký západ.

Kamera má smysl tam kde je zvýšené riziko - např. křižovatka nebo samosebou letiště. Už ale nemá smysl jen tak jí dávat na každý chodník, a už absolutně není žádný důvod zavádět to co tam dnes s velkým úspěchem cpou - software co si vás "podává" z kamery na kameru, sleduje vás a vyhodnocuje automaticky vaší nenormálnost chování (kdo nevěří, tohle je zavedeno už docela dlouho na letištích a i v některých městech).

Jak je tohle ospravedlnitelné vaší povýšeneckou logikou člověka "z praxe", a nikoliv "utopistických teorií"?

Celý ten problém je v tom že digitální retence a kamery a software za tím vším nezaznamenávají pachatele. V 99.9xxx% případů totiž zaznamenávají nevinné. Je úplně jedno kolik na to nabalíte povolení, já prostě nechci takovýhle svět, protože je mi jasné kam to povede, a protože hlavně demokratická země takový svět NEPOTŘEBUJE ani pro svou bezpečnost, ani pro vymáhání spravedlnosti. A ne, nejsem opravdu praštěný konspirační utopistický hipísák.

To se mi líbí · Odpovědět · 2 d · Upraveno

[redacted] Mimochodem, ve švýcarsku pokud vím žádný takový zákon není. Asi to budou paranoidní zpátečníci.

A mimochodem, podle rozhodnutí evropského soudního dvoru z roku 2014 je plošný data retention neopodstatněný a nezákonný (http://curia.europa.eu/juris/document/document.jsf?text=...)

Asi to taky budou paranoidní idioti co nemaj poznatky z masopsovy praxe.

CURIA - Documents

„Elektronické komunikace – Směrnice 2006/24/ES – Veřejně dostupné služby…

CURIA.EUROPA.EU

To se mi líbí · Odpovědět · 2 d · 1

[redacted] Tady ale nedochází k plošnému šmírování. To že jsou data k dispozici ještě neznamená, že si je orgány činné v trestním řízení mohou prohrabávat jak chtějí. K tomu musí žádat státní zastupitelství, které dále žádá obvodního sou... Zobrazit více

To se mi líbí · Odpovědět · 1 d

Lukáš Drozda [redacted] jediní se chápeme. Děkuji Ti za to.

Už to nemá cenu komentovat. Netvrdil jsem, že dochází k plošnému šmírování, tvrdím celou dobu, že to žádné šmírování není, a navíc rozhodně ne plošné viz zákon o elektronických komunikacích, logování se vztahuje na osoby - subjekty pod ZEK.

To se mi líbí · Odpovědět · 1 d

[redacted]

Lekce přítomnosti:
http://www.bbc.com/.../in-your-face-china-s-all-seeing-state

Lekce budoucnosti:
https://technet.idnes.cz/sledovani.../sw_internet.aspx...

A bude hůř.

Jestli si myslíte že budoucnost naší a našich dětí ochrání nějaký řetěz rozhodování s obvodním soudem v ČR... good luck. Já takovej svět nechci a v demokracii není potřeba a nesmí existovat.

In Your Face: China's all-seeing state

BBC.COM

To se mi líbí · Odpovědět · 1 d

Je vybraná možnost Hlavní komentáře. Některé odpovědi se nemusí v tomto filtru zobrazovat.

Napište odpověď...

[redacted] Asi je to uzitecne, ale chce to hlavne jine zakony: - aby si kazdy mohl chranit svuj majetek pomoci kameroveho zaznamu. Tedy za jizdy autem, svuj byt, svojo garaz, svoje vozodlo na verejnem parkovisti. Jiste jakekoliv neopravnene a napadene zverejneni ... Zobrazit více

16

To se mi líbí · Odpovědět · 3 d

6 odpovědí