926—943

Neoprávněný přístup na online účty (internetové bankovnictví, sociální sítě) a dekriminalizace jednoho z počítačových trestných činů

Kateřina Kudrlová* – Jiří Vlach**

Abstrakt: Online účty představují dnes již nedílnou součást každodenního života. Mezi ty nejdůležitější patří na jedné straně internetové bankovnictví sloužící ke správě financí a na straně druhé profil na sociální síti sloužící ke komunikaci s širokým okolím. Protože jde o počítačové systémy, neoprávněný přístup k nim lze postihnout jako počítačový trestný čin dle § 230 odst. 1 tr. z. Reprezentativní dotazníkové šetření realizované v roce 2020 v ČR však ukázalo, že k neoprávněným přístupům dochází poměrně často, a to zejména mezi partnery nebo v rámci úzkého rodinného kruhu. Útočníci získávají přístup zejména s využitím přihlašovacích údajů, které uživatelé online účtů relativně běžně sdílejí s dalšími osobami, a samotná neoprávněnost přístupu může být v řadě případů sporná. Cílem článku je proto poukázat na nesoulad právní normy s běžnou uživatelskou praxí a navrhnout možnou úpravu de lege ferenda tak, aby lépe odpovídala sociální realitě. Při zohlednění mezinárodních závazků by mohlo dojít k částečné dekriminalizaci počítačového trestného činu dle § 230 odst. 1 tr. z. změnou výrazu „překoná" na „poruší" a přidáním dalšího znaku k této základní skutkové podstatě – jednání „s úmyslem získat počítačová data nebo s jiným nečestným úmyslem". Závěrem uvádíme stručná doporučení pro prevenci neoprávněných přístupů k online účtům.

Klíčová slova: neoprávněný přístup, internetové bankovnictví, sociální sítě, dekriminalizace, počítačový trestný čin, online účty

Úvod

Online účty. Snad každý dnes disponuje hned několika, od sociálních sítí přes herní účty až po e-shopy a nepřeberné množství rozličných aplikací. A samozřejmě mezi ně patří v širším smyslu i internetové bankovnictví a účty v online světě nejstarší – e-mailové. Zcela běžně uživatelé využívají vícero účtů určitého typu, typicky několik e-mailových účtů, profily na sociálních sítích, herní účty i internetová bankovnictví.[1] Obvykle však některé z nich vynikají svým významem pro uživatele – internetové bankovnictví, hlavní e-mail coby brána do virtuálního světa uživatele,[2] nejvíce využívaný profil na sociální síti jakožto významný sociální a komunikační prostředek. Právě o internetovém bankovnictví a sociálních sítích tento článek pojednává.[3]

* Mgr. Kateřina Kudrlová, Ph.D., Institut pro kriminologii a sociální prevenci, odpovědná řešitelka výzkumného úkolu *Posouzení trendů kyberkriminality*. E-mail: kkudrlova@iksp.justice.cz. ORCID: https://orcid.org/0000-0001-8911-1134.

** Mgr. Jiří Vlach, Institut pro kriminologii a sociální prevenci, řešitel výzkumného úkolu *Posouzení trendů kyberkriminality*. E-mail: jvlach@iksp.justice.cz. ORCID: https://orcid.org/0000-0002-7295-4677.

1 „Online účet" ve spojení s internetovým bankovnictvím odkazuje na bankovnictví jedné banky spadající pod jednoho uživatele bez ohledu na množství bankovních účtů, které má k sobě přidružené.

2 KUDRLOVÁ, K. Kybernetická kriminalita – dílčí poznatky z výzkumu II. In: ŠČERBA, F. (ed.). *Kriminologické dny 2018*. Olomouc: Iuridicum Olomoucense, 2018, s. 148–157.

3 Obsah článku byl nastíněn autory spolu s Mgr. Lukášem Kutilem na odborné konferenci *Vliv nových technologií na trestní právo* pořádané 24. března 2022 katedrou trestního práva Právnické fakulty Univerzity Karlovy.

Vychází přitom z poznatků získaných v rámci dvou výzkumných úkolů věnujících se kyberkriminalitě a řešených v Institutu pro kriminologii a sociální prevenci (dále jen IKSP).[4] První z nich, *Identifikace a posouzení druhů a trendů kriminality páchané prostřednictvím Internetu, případně dalších sociálních sítí*, řešený v letech 2016–2019, se zabýval zejména analýzou vybraných trestních spisů vedených o počítačových trestných činech, dále pak přípravou rozsáhlého dotazníkového šetření.[5] Výsledky šetření jsou v současnosti předmětem analýz v rámci druhého ze zmíněných výzkumných úkolů, a to *Posouzení trendů kyberkriminality*, řešeného v letech 2020–2023.[6] Dále čerpáme z veřejně dostupných statistických údajů a právních dokumentů. V následujícím textu uvádíme nejprve podrobnosti ke sběru vlastních dat. Dále pak analýzu relevantních hmotněprávních ustanovení *de lege lata* a naproti tomu zjištěné poznatky z uvedených výzkumů. Závěrem nastíníme možnou úpravu *de lege ferenda* a přidáme doporučení pro prevenci.

Analýza trestních spisů naznačila, že neoprávněné vstupování na cizí online účty není zdaleka ojedinělé, přičemž údaje z dotazníkového šetření tento trend potvrdily (a to dle vyjádření aktérů na obou stranách). Z právního hlediska může být neoprávněný vstup na cizí online účet počítačovým trestným činem (§ 230 zák. č. 40/2009 Sb., trestní zákoník, dále jen tr. z.), uvedené jednání však bývá vysoce latentní (ostatně jako převážná část protiprávního jednání online). Pokusíme se zde ukázat, že stávající formulace skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 odst. 1 tr. z. neodpovídá přiměřeně současné sociální realitě.

1. Zdroje dat – analýza trestních spisů a dotazníkové šetření

Sledované trestní spisy zahrnovaly věci, ve kterých byla podána obžaloba pro naplnění skutkové podstaty některého z počítačových trestných činů a trestní řízení pravomocně skončilo v roce 2015.[7] V drtivé většině z nich šlo o neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací dle § 230 tr. z., případně v souběhu s dalšími trestnými činy. Ostatní skutkové podstaty počítačových trestných činů dle § 231 a § 232 tr. z. nachází uplatnění jen sporadicky. Zpracováno bylo 66 trestních spisů z celkového počtu 71 věcí pravomocně skončených v roce 2015, jednalo se o 68 obviněných. Získané údaje sloužily jako významný zdroj informací při přípravě dotazníkového šetření. Přesto je třeba brát data s určitou rezervou především s ohledem na vysokou míru latence.

Při sběru dat ze spisů jsme sledovali zhruba 50 položek zahrnujících především základní údaje o obviněném, trestném činu samotném a o průběhu trestního řízení. Výjimečně ten či onen údaj chyběl, vždy však šlo o pouze ojedinělou absenci.

---

4 IKSP je výzkumnou organizací zřízenou Ministerstvem spravedlnosti ČR zabývající se kriminologickým výzkumem.

5 Celý výzkumný úkol a jeho výsledky podrobně shrnuje monografie VLACH, J. – KUDRLOVÁ, K. – PALOUŠOVÁ, V. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020. Dostupná též online z: <http://www.ok.cz/iksp/docs/463.pdf>.

6 Druhou částí uvedeného projektu je pokračování analýzy trestních spisů vedených o počítačových trestných činech.

7 Přesněji řečeno jde o ta pravomocně skončená řízení, jejichž údaje (statistické listy trestní) byly v roce 2015 odeslány do evidence statistiky Ministerstva spravedlnosti, tedy s určitým převisem z roku 2014 a bez věcí odeslaných až začátkem roku 2016.

Následná analýza sebraných dat sestávala z běžných statistických operací, ovšem s tříděním nejvýše 2. stupně (vzhledem k počtu případů na samé hraně statisticky zpracovatelných dat). Mimoto bylo podrobněji kvalitativně analyzováno několik typických či naopak vyjímajících se kauz.[8]

Na základě takto získaných poznatků jsme vytvořili dotazník *Zkušenosti obyvatel ČR s vybranými jevy v online prostředí*, samotný sběr dat realizovala jako veřejnou zakázku společnost ppm factum research s. r. o. Po prvotních úskalích spojených s omezeními v souvislosti s pandemií covidu-19[9] proběhl sběr dat v listopadu roku 2020. Většina otázek směřovala na „uplynulých 12 měsíců", a tak lze hovořit o zkušenostech uživatelů zhruba v roce 2020 (dále jen 2020*). Respondenti byli vybíráni na základě kvót předem určených dle údajů Českého statistického úřadu a informací Sdružení pro internetový rozvoj. Jednalo se o české uživatele internetu ve věku 16–74 let (nikoliv tedy o obecnou populaci ČR). Při reprezentativním výběru respondentů byly použity jako kvótní znaky pohlaví, věk, nejvyšší dosažené vzdělání, velikost místa bydliště a kraj, kde se nacházelo. Pro sběr dat byla použita metoda CAWI (Computer Assisted Web Interviewing), tj. dotazování prostřednictvím interaktivního webového dotazníku. Celková velikost souboru činila 6811 osob. Analýza získaných dat v současnosti stále probíhá.

Dotazník se obrací na respondenty coby běžné uživatele, zaměstnance, oběti i útočníky (self-report).[10] Zjištění tak poskytují ojedinělý obrázek zahrnující do jisté míry obě strany.[11] Dotazované oblasti zahrnovaly vybrané bezpečnostní návyky uživatelů, zařízení používaná k přístupu na internet a jejich ochranu (při rozlišování soukromých, zaměstnaneckých a podnikatelských zařízení), obchodování online (s rozlišením e-shopů a inzertních portálů), internetové bankovnictví, ransomware, phishing, e-maily, sociální sítě (samotné používání sociálních sítí, zneužívání profilů a zkušenosti s falešnými profily), herní účty (při rozlišení hazardních her, počítačových her a herních platforem), darkweb, porušování autorských práv, baiting a zneužití přístupu zaměstnancem.

V tomto článku pracujeme se zjištěnými poznatky z oblasti internetového bankovnictví, neboť kriminalita spojená s přístupem na cizí bankovní účet bývá obvykle (byť ne nutně) motivována snahou finančně se obohatit a lze ji považovat za jednání s jasným kriminálním záměrem. Dále pracujeme s informacemi o neoprávněných přístupech na účty na sociálních sítích,[12] kde bývá naopak motivace rozmanitější a hranice mezi kriminálním a nekriminálním jednáním se z hlediska pachatele může jevit jako mlhavá. Tyto dvě oblasti proto považujeme za dobrou demonstraci neoprávněných přístupů na různé online účty. Zdrojem dat v grafech je výše uvedené dotazníkové šetření.

---

8 Veškeré poznatky i podrobnější metodologické informace lze nalézt souhrnně v již zmíněné monografii VLACH, J. – KUDRLOVÁ, K. – PALOUŠOVÁ, V. *Kyberkriminalita v kriminologické perspektivě*.

9 Vyloučena byla původně předpokládaná metoda osobního dotazování (CAPI). K podrobnějším informacím ohledně realizace dotazníkového šetření viz KUDRLOVÁ, K. – KUTIL, L. – VLACH, J. Výzkumné šetření IKSP „Zkušenosti obyvatel České republiky s vybranými jevy v online prostředí". *Kriminalistika*. 2022, č. 2, s. 139.

10 Na některé otázky odpovídali všichni respondenti bez rozdílu, jiné byly selektivní dle předchozích odpovědí respondentů.

11 K možnostem i omezením vyplývajícím z metody self-reportu viz např. TOMÁŠEK, J. *Self-reportové studie kriminálního chování*. Praha: Institut pro kriminologii a sociální prevenci, 2013.

12 Nutno pro úplnost podotknout, že tyto poznatky se v obecné rovině prakticky shodují s poznatky o neoprávněných přístupech k soukromým emailovým schránkám.

2. Nezákonnost neoprávněných přístupů de lege lata

„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán […].“ Tak zní první ze dvou základních skutkových podstat trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 odst. 1 tr. z.[13] Dopadá tedy na jakýkoliv neoprávněný přístup k počítačovému systému za předpokladu překonání bezpečnostního opatření majícího za úkol přístup omezit.[14] Další jednání (typicky manipulace s daty) již pro naplnění této základní skutkové podstaty není třeba.[15]

Naplnění objektivní stránky této skutkové podstaty může být samotným cílem pachatele (např. chce zjistit z profilu oběti na sociální síti podrobnosti o jejím soukromém životě, aniž by měl v úmyslu se zjištěnými daty jakkoliv manipulovat či k nim přidat data jiná). Nikoliv výjimečně však slouží jako příprava k dalšímu jednání, zejména v podobě neoprávněného nakládání s daty, tedy naplnění objektivní stránky základní skutkové podstaty uvedené v druhém odstavci § 230 tr. z. Zde již nezáleží na oprávněnosti získání přístupu k počítačovému systému. Může tedy jít o přístup oprávněný (např. přístup administrátora spravujícího firemní síť v rámci pracovněprávních povinností), stejně tak jako neoprávněný, kterým je zároveň naplněna skutková podstata dle prvního odstavce § 230 tr. z. Ta však bude v takových případech pravděpodobně (nikoliv však nutně) fakticky konzumována.[16]

Z hlediska subjektivní stránky vyžadují obě základní skutkové podstaty § 230 tr. z. úmyslné zavinění. U kvalifikovaných skutkových podstat se úmysl vyžaduje pro naplnění skutkové podstaty dle § 230 odst. 3 písm. a) i b) tr. z., stejně tak dle § 230 odst. 4 písm. a) tr. z. (vyplývá z povahy věci), ve všech ostatních případech postačí nedbalostní zavinění okolnosti zvlášť přitěžující, zde vždy v podobě těžšího následku [srov. § 17 písm. a) tr. z. a § 230 odst. 4 písm. b), c), d) a e), odst. 5 tr. z.]. Všechny tři počítačové trestné činy jsou zařazeny v rámci hlavy páté tr. z. Kromě kvalifikované skutkové podstaty dle § 230 odst. 1 a/nebo 2, odst. 5 tr. z., kdy jde o zločin, se jedná o přečiny (srov. § 14 odst. 2 a 3 tr. z.).

Objektem počítačových trestných činů (§ 230–232 tr. z.) je *„zájem na ochraně počítačových systémů a jejich částí, dále dat v nich uložených a dat uložených na nosičích informací a také na ochraně počítačů nebo jiných technických zařízeních pro zpracování dat před neoprávněnými přístupy a zásahy“*.[17] Klíčová je tedy jednak bezpečnost samotných zařízení, jednak bezpečnost informací a dat – slovy zákona o kybernetické bezpečnosti jejich důvěrnost, integrita a dostupnost [§ 2 písm. c) zák. č. 181/2014 Sb.]. Ve spojení s informacemi dostupnými prostřednictvím internetového bankovnictví pak jde zároveň o finanční stránku (např. zneužitelnost informací o finančních transakcích uživatele)[18] a v neposlední řadě o osobnostní stránku v podobě soukromí uživatele. Ta vystupuje do popředí

13 KRUPIČKA, J. Trestné činy proti majetku. In: ŠÁMAL, P. a kol. *Trestní právo hmotné*. 8. vydání. Praha: Wolters Kluwer ČR, 2016, s. 696.

14 GŘIVNA, T. Komentář k § 230. In: ŠÁMAL, P. a kol. *Trestní zákoník II: Zvláštní část (§ 140–421). (komentář)*. 2. vydání. Praha: C. H. Beck, 2012, s. 2305.

15 To potvrzuje i usnesení Nejvyššího soudu ze dne 29. 11. 2017, sp. zn. 7 Tdo 1469/2017.

16 Viz např. KUDRLOVÁ, K. *Kriminalita spojená s využíváním nových médií dětmi*. Dizertační práce. Praha: Právnická fakulta Univerzity Karlovy, 2019. Dostupné z: <https://dspace.cuni.cz/handle/20.500.11956/111603>; nebo SMEJKAL, V. *Kybernetická kriminalita*. 3. vydání. Praha: Aleš Čeněk, 2022.

17 KRUPIČKA, J. *Trestné činy proti majetku*, s. 695.

18 Nemluvě o případných neoprávněných finančních transakcích a jiných aktivitách.

zvlášť palčivě v případě narušování soukromí prostřednictvím neoprávněných vstupů na profily na sociálních sítích, na něž bývá mnohdy navázána významná část sociálních kontaktů uživatele.[19]

2.1 Překonání překážky a svolení poškozeného

Dle prvního odstavce § 230 tr. z. se zmíněného trestného činu dopustí ten, *„kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části […].“* Jednou z podmínek je zde tedy překonání bezpečnostního opatření, přičemž úroveň zabezpečení není rozhodující. Již sama existence jakéhokoliv bezpečnostního opatření postačuje. Základním opatřením majícím za úkol zabránit zejména malwarovým útokům na samotné fyzické zařízení (hardware) či jeho programové vybavení (software) je v současnosti firewall, obvykle též zároveň doplněný o antivirový ochranný software, případně antispyware.[20] Bezpečnostních opatření si uživatel nemusí ani být zcela vědom (např. má jen neurčité povědomí o tom, že jeho zařízení používá nějaký antivirus). Druhým stupněm ochrany, tentokrát obsahu či přístupu, je především heslo, bez ohledu na jeho snadnou prolomitelnost (např. heslo „12345“) či naopak sílu (např. kombinace nejméně 8 různých znaků atp.).

Pro oblast osobních účtů je klíčový judikát Nejvyššího soudu ze 4. 11. 2020 ve věci 7 Tdo 1134/2020. V něm Nejvyšší soud deklaruje, že jakýkoliv neoprávněný přístup do osobního účtu bez ohledu na způsob, jakým bylo heslo či jiné bezpečnostní opatření překonáno, je překonáním bezpečnostního opatření dle § 230 tr. z.

V bodě 40 odůvodnění zmíněného rozhodnutí je citováno vcelku trefné přirovnání, jež uvedla státní zástupkyně ve svém vyjádření k dovolání. *„Facebook je v podstatě virtuální prostor a má podobnou povahu jako ‚obydlí‘, jehož ‚dveře‘ tvoří počítačový systém, či jiný nosič informací, přičemž ‚klíčem‘ k těmto ‚dveřím‘ je bezpečnostní opatření, jimiž je lze odemknout. Trestní zákon při ochraně ústavou zaručeného práva na soukromí sankcionuje jakýkoli neoprávněný vstup do obydlí, a to i za pomoci shodného klíče, aniž by pachatel musel dveře do domu prolamovat násilím. Obdobně je tedy nutno postihovat případy, kdy pachatel prolomí ‚dveře‘ do virtuálního prostoru například za pomoci hesla, které znal z dřívější doby, či za pomoci telefonního čísla, na které jsou tyto soukromé účty navázány. Rozhodující je – obdobně jako u porušování domovní svobody – že v okamžiku, kdy pachatel tohoto způsobu narušení soukromí využívá, ví, že do toho důvěrného prostoru vstupuje neoprávněně, a je s tímto následkem přinejmenším srozuměn. Za překonání ‚bezpečnostního opatření‘ ve smyslu § 230 odst. 1 trestního zákoníku je proto možno považovat i využití duplikátu telefonní SIM karty, na kterou jsou tyto soukromé účty vázány, s jejímž využitím lze do důvěrného prostoru vstupovat přímo, nebo za pomoci nově vygenerovaných hesel.“* Nelze proto pochybovat o tom, že překonáním bezpečnostní překážky ve smyslu ustanovení § 230 odst. 1 tr. z. tak bude i využití přístupových údajů tzv. zapamatovaných v zařízení, poznamenaných na papírku, uhodnutých, pachateli známých atp. Nemluvě o časté situaci, kdy pachatel využije přihlašovací údaje poskytnuté samotnou obětí, avšak za jiným účelem (viz dále).

19 KUDRLOVÁ, K. *Kriminalita spojená s využíváním nových médií dětmi.*

20 Malware znamená škodlivý software, antivirus ochranný software sloužící k detekci a eliminaci malwaru. Antispyware se zaměřuje na sledovací malware a může i nemusí být součástí antiviru.

Právě hojné využívání cizích přístupových údajů pachateli známých (viz dále) vybízí k úvaze nad protiprávností jednání s ohledem na institut svolení poškozeného (§ 30 tr. z.). Svolení musí být dáno osobou oprávněnou, dobrovolně, určitě, vážně a srozumitelně. Může být dáno i následně jako důvodně předpokládaný a následně udělený souhlas. Za pozornost ovšem stojí určitá úskalí jeho aplikace.

Oprávnění ke svolení lze zpochybnit u použití cizích přístupových údajů k internetovému bankovnictví, neboť banky zpravidla smluvně stanovují prostřednictvím všeobecných obchodních podmínek přístup ke svým službám pouze na základě smlouvy či písemného zmocnění. Použití cizích přístupových údajů se tak dotýká nejen majitele účtu, ale i provozující banky, která předpokládá přístup ke svým službám pouze ze strany daného klienta (či disponenta nebo zmocněnce). Zvlášť pak, když banka potvrzuje identitu svého klienta coby tzv. bankovní identitu při komunikaci se státními orgány.[21] Neoprávněně přistupující osoba by tak mohla jednat v omylu ohledně oprávněnosti majitele účtu bez dalšího udělit souhlas s jeho použitím.

Z hlediska dobrovolnosti, určitosti, vážnosti ani srozumitelnosti svolení by neměly v praxi vznikat větší pochybnosti. Dotčené osoby[22] zpravidla reagují na zjištěný neoprávněný přístup ke svému online účtu jednoznačně (změna přístupových údajů, podání trestního oznámení aj.), kdy je nesouhlas zřejmý, anebo nereagují vůbec, což lze považovat za konkludentní, dostačující souhlas.[23] Problém nastává, když se dotčená osoba o neoprávněném přístupu ke svému účtu nedozví (pachatel si např. pouze prohlédne obsah) – v takovém případě nelze o souhlasu poškozeného vůbec uvažovat (respektive o jeho následném udělení).

2.2 Inspirace pro stávající právní úpravu

Důvodová zpráva k návrhu nového tr. z.[24] se k počítačovým trestným činům (tehdy § 228–230 namísto současných § 230–232 tr. z.) vyjadřuje poměrně stroze, když pouze poukazuje na závazky plynoucí z Úmluvy o počítačové kriminalitě[25] (dále jen Úmluva), zejména její články 2–11.

Na Úmluvu o počítačové kriminalitě pochopitelně odkazuje i odborná literatura, která vždy zmiňuje patero jednání, které se signatářské státy zavázaly kriminalizovat: protiprávní přístup (§ 230 odst. 1 tr. z.), neoprávněný zásah do dat nebo počítačového systému [§ 230 odst. 2 písm. a), b), d) tr. z.], falšování údajů související s počítači [§ 230 odst. 2 písm. c) tr. z.], podvod související s počítači [§ 230 odst. 3 písm. a) tr. z.] a neoprávněný

21 Vytrácí se tak společenská prospěšnost institutu svolení poškozeného spočívající v odpadnutí zájmu na stíhání odsouhlaseného jednání. Viz např. LUKÁŠOVÁ, M. Institut svolení poškozeného a jeho uplatnění nejen v judikatuře. *Trestněprávní revue*. 2019, č. 3, s. 60. Prospěšnost institutu svolení poškozeného je zde převážena zájmem na ochraně důvěrnosti a autenticitě komunikace mezi státem a obyvateli.

22 K problematickému označení dotčených osob za „poškozené" v případě uplatnění institutu svolení poškozeného viz např. KLAPAL, V. Svolení poškozeného jako okolnost vylučující protiprávnost. *Trestněprávní revue*. 2005, č. 10, s. 259.

23 GŘIVNA, T. Komentář k § 30. In: ŠÁMAL, P. a kol. *Trestní zákoník I: Obecná část (§ 1–139) (komentář)*. 2. vydání. Praha: C. H. Beck, 2012, s. 424.

24 VLÁDA ČR. *Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník*. 25. 2. 2008.

25 Convention on Cybercrime, ETS No. 185. Vznikla na půdě Rady Evropy v roce 2001 a vstoupila v účinnost 1. 7. 2004, Česká republika ji podepsala 9. února 2005 a ratifikovala 22. srpna 2013. Viz RADA EVROPY. Chart of Signatures and Ratifications of Treaty 185. In: *Council of Europe*. [cit. 2022-12-29]. Dostupné z: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>.

zásah do systému [§ 230 odst. 3 písm. b) tr. z.].[26] Pro znění § 230 odst. 1 tr. z. je v rámci Úmluvy klíčový požadavek kriminalizace neoprávněného přístupu do počítačového systému nebo jeho části dle čl. 2. Signatářským státům se ponechává na zvážení, zda podmíní trestnost jednání mimo jiné překonáním bezpečnostních opatření, což ČR činí.

Mimoto zavazovalo ČR k postihu protiprávního přístupu i Rámcové rozhodnutí Rady EU 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům, které požadovalo v čl. 2 kriminalizaci protiprávního přístupu k informačním systémům [čl. 1 písm. a), d) a čl. 2, odpovídajícím ustanovením je v českém právním řádu § 230 odst. 1 tr. z.]. I zde měly zavázané státy možnost podmínit trestnost překonáním překážky (čl. 2 odst. 2). Toto rámcové rozhodnutí bylo s účinností od 3. září 2013 nahrazeno směrnicí Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (dále jen Směrnice). Ta požaduje kriminalizaci neoprávněného přístupu k informačním systémům v čl. 3 a tentokrát je zde již výslovně uvedeno porušení bezpečnostního opatření jako podmínka požadované kriminalizace. Všechny uvedené právní dokumenty se vyjadřují i ke kriminalizaci pokusu a účastenství, nicméně vzhledem k trestněprávnímu pojetí vývojových stádií trestného činu a účastenství v ČR není třeba se jimi zde podrobněji zabývat.[27]

3. Poznatky – internetové bankovnictví

Zhruba v 15 % analyzovaných trestních spisů mělo být zneužito internetové bankovnictví. Nutno podotknout, že zneužití internetového bankovnictví bylo zřejmě častější, a to i v praxi justičních orgánů (mimo latentní kriminalitu) – některé případy mohly být právně kvalifikovány např. pouze jako podvodné jednání (typicky podvod dle § 209 tr. z. nebo úvěrový podvod dle § 211 tr. z.), bez souběhu s § 230 tr. z.

V dotazníkovém šetření se k vlastnímu internetovému bankovnictví přihlásilo 93 % respondentů (6338 osob), přičemž 3 % z nich (199 osob) uvedlo, že jejich internetové bankovnictví někdo v roce 2020* (pravděpodobně)[28] zneužil, z toho v téměř polovině případů opakovaně. Naproti tomu 9 % respondentů v rámci self-reportu vypovědělo, že v roce 2020* používali internetové bankovnictví někoho jiného,[29] z toho 29 % (191 osob) tak činilo bez výslovného svolení majitele účtu.

Kdo byl útočníkem, vědělo 38 % napadených (75 osob). Podle nich se nejčastěji jednalo o nejbližší osoby: za pachatele označili respondenti především své stávající partnery,[30] bývalé partnery či osoby z úzkého rodinného kruhu[31] (20, 12 a 8 %). Signifikantně často označovali své partnery za pachatele muži (29 %), ženy naopak někoho zcela jiného (55 %),

---

26 GŘIVNA, T. *Komentář k § 230*, s. 2304. Dále např. SMEJKAL, V. *Kybernetická kriminalita*; KUDRLOVÁ, K. *Kriminalita spojená s využíváním nových médií dětmi*; GŘIVNA, T. – POLČÁK, R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008; nebo KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016.

27 Pro podrobnější informace k mezinárodněprávním dokumentům zavazujícím ČR k postihu kyberkriminality viz např. KUDRLOVÁ, K. Vliv práva EU na trestněprávní postih kyberkriminality v ČR. In: JELÍNEK, J. – IVOR, J. a kol. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, s. 285.

28 Souhrn odpovědí, kdy si respondenti byli napadením jisti, spolu s odpověďmi, kdy se domnívali, že k napadení pravděpodobně došlo.

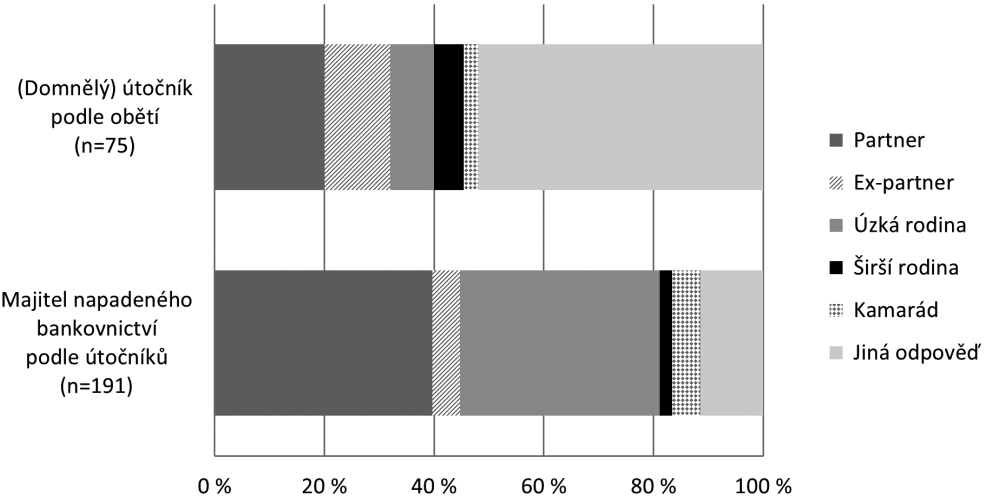
29 Nejčastěji tak činily osoby mladší 29 let, přičemž s věkem počet osob používajících internetové bankovnictví někoho jiného postupně klesá.

30 V rámci zjednodušení uvádíme vždy pouze „partneři" namísto „partneři či partnerky" atp.

31 Výlučně děti, rodiče, prarodiče, vnoučata, sourozenci.

častou odpovědí byl v tomto případě neznámý hacker. Podobně uvažovaly i osoby starší 45 let (ve věku 45–59 let to bylo 60 %, ve věku 60–74 let 77 %).

I z pohledu osob používajících cizí internetové bankovnictví bez výslovného svolení oprávněného uživatele nacházíme na druhé straně především stávající partnery a osoby z úzkého rodinného kruhu (45 a 41 %), avšak výrazně méně bývalých partnerů (6 %). Pro zajímavost doplníme, že motivace neoprávněného přístupu k cizímu internetovému bankovnictví (respektive přístupu bez výslovného svolení jeho majitele) nebyla zdaleka pouze finanční (27 %), nýbrž šlo i o prostou zvědavost (12 %).[32] Statisticky významně často hovořili o zvědavosti osoby mladší 29 let (22 %). Zvědavosti a finanční motivaci odpovídá i další otázka zaměřená na samotnou aktivitu po (neoprávněném) přístupu, když respondenti uváděli nejčastěji zjištění finanční situace majitele účtu (61 %) a převod peněz na jiný účet (45 %), ostatní možnosti byly jen minoritní.



Graf č. 1: Aktéři neoprávněného vstupu do internetového bankovnictví

Ze 75 respondentů, kteří vědí, kdo v roce 2020* nejméně jednou[33] zneužil jejich internetové bankovnictví, jich 45 % dobrovolně pachateli poskytlo své přihlašovací údaje. Nejčastěji (62 %) z důvodu jednorázové výpomoci (např. zjištění zůstatku). Ostatní důvody byly pouze minoritní, za zmínku stojí snad jen trvalá péče o internetové bankovnictví (např. vnuk spravující internetové bankovnictví prarodičů) – 15 %.

V rámci self-reportu uváděli respondenti ještě vyšší poměr známých přístupových údajů, když jich 80 % uvedlo, že je znají přímo od majitelů (neoprávněně) navštívených účtů. Dále jich 16 % uvedlo, že získali přístup prostřednictvím zařízení, na kterém bylo internetové bankovnictví přihlášené (statisticky významně často osoby mladší 29 let, 28 %),

[32] 45 % respondentů uvedlo „jinou" motivaci, často nějakou formu pomoci – (ne)oprávněnost jejich přístupu je proto diskutabilní.

[33] Pakliže bylo takových incidentů více, otázky v dotazníku směřovaly vždy jen na incident, jenž byl z pohledu respondenta nejzávažnější.

ostatní způsoby získání přístupu byly jen sporadické. I pachatelé uvádí jako důvod poskytnutí přihlašovacích údajů žádost samotného majitele účtu (72 %), především tak byli žádání respondenti mladší 29 let (84 %, jejich poměr s věkem setrvale klesá) a vysokoškolsky vzdělané osoby (83 %). Třetina (33 %) pak uvádí trvalou péči o internetové bankovnictví někoho jiného.[34]

Když se přitom podíváme na odpovědi všech respondentů (bez ohledu na viktimizaci nebo neoprávněné přístupy) ohledně dobrovolného poskytování přihlašovacích údajů k vlastnímu internetovému bankovnictví jiným osobám, jde o jednání relativně časté. Své přihlašovací údaje k internetovému bankovnictví někdy poskytlo 8 % uživatelů (495 osob), z toho 23 % dokonce více než jednomu člověku (především osoby mladší 29 let, 31 %). Své přihlašovací údaje poskytují statisticky významně často ženy (9 %), osoby mladší 29 let (10 %) a osoby se základním vzděláním nebo vyučené bez maturity (12 a 10 %). Přihlašovací údaje bývají poskytnuty především stávajícím partnerům (72 %) a/nebo někomu z úzkého rodinného kruhu (29 %). Muži a osoby ve věkové skupině 30–44 let, kteří poskytli své přihlašovací údaje více osobám, je sdělovali statisticky významně často svým partnerům, kdežto ženy a osoby mladší 29 let nebo starší 60 let je sdělovaly někomu z úzkého rodinného kruhu.

Nejčastějším důvodem poskytnutí přihlašovacích údajů je i v této skupině jednorázové použití internetového bankovnictví (74 %), dále pak trvalá správa internetového bankovnictví (21 %). Statisticky významný vztah zde vykazuje pouze kategorie respondentů ve věku 45–59 let, kteří nechávají někoho pečovat o své internetové bankovnictví trvale. Respondenti starší 60 let (respektive ve věku 60–74 let) nejčastěji uváděli jako důvod umožnění dlouhodobého přístupu dané osobě obavu z náhlé nehody, vlastní invaliditu či jinou zdravotní překážku.

4. Poznatky – sociální sítě

Co se týče zneužívání sociálních sítí z pohledu analyzovaných trestních spisů za rok 2015, zdaleka převažovala protiprávní jednání spojená s Facebookem (zhruba 27 %), zneužívání jiných sociálních sítí bylo v posuzovaných věcech jen občasné (4 %).

Stejný trend potvrdili i respondenti v rámci dotazníkového šetření, kteří měli zkušenosti se zneužíváním sociálních sítí zejména v případě Facebooku a dále též Messengeru.[35] Zhruba 80 % všech respondentů používalo v roce 2020* nějakou sociální síť, z toho 7 % (377 osob) mělo zkušenost s (pravděpodobným) napadením jejich účtu v uvedeném období, z toho 36 % zřejmě opakovaně. Celkem 250 osob hovořilo o napadení jejich účtu na Facebooku, 19 osob o účtu v Messengeru.[36] Statisticky významně často měly zkušenost s napadením svého profilu na sociální síti ženy, osoby mladší 29 let a osoby s pouze základním vzděláním.

Povědomí o útočníkovi mělo pouze 16 % napadených respondentů (59 osob), častěji to věděli muži, zatímco ženy naopak nikoliv. Opět označovali především stávající i bývalé

34 Zde i na jiných místech měli respondenti možnost vybrat více odpovědí, pokud se vzájemně nevylučovaly.

35 Messenger, dříve navázaný na účet uživatele na Facebooku, slouží jako komunikační platforma podobná aplikaci WhatsApp.

36 Účty na Facebooku a Messengeru mohou splývat, nicméně respondenti byli tázáni ohledně incidentu, který oni sami považují za nejzávažnější.

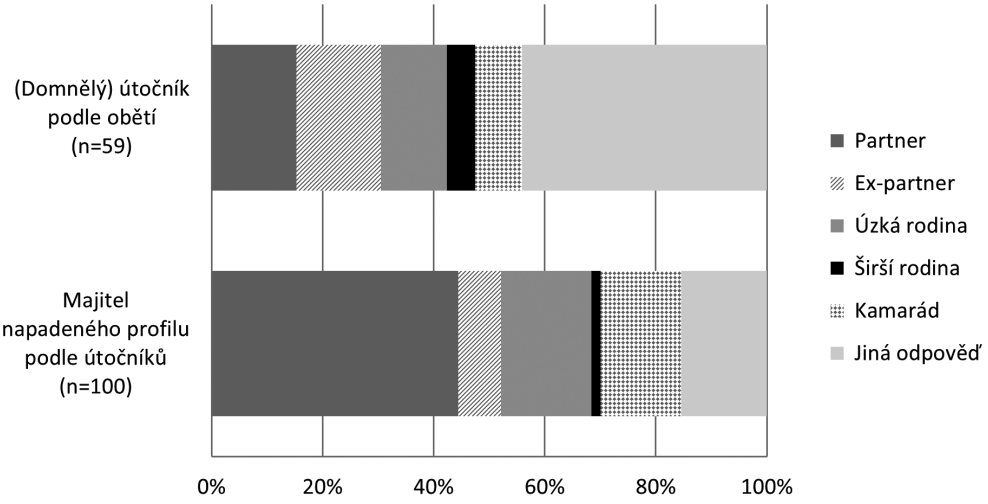
partnery a osoby z úzkého rodinného kruhu (15, 15 a 12 %). Častěji se u sociálních sítí objevil v pozici (domnělého) útočníka i kamarád.

U domnělého způsobu získání přístupu dominovalo z pohledu napadených respondentů uhádnutí přihlašovacích údajů (24 % napadených), dále použití zařízení napadeného respondenta s otevřenou příslušnou aplikací či účtem (7 %), ovšem i zde řada respondentů poskytla své přihlašovací údaje útočníkovi z vlastní vůle (5 %). V rámci otevřených odpovědí uvedlo zhruba 15 % napadených respondentů, že jejich účet někdo „hacknul".

Napadení respondenti věděli především o vložení obsahu na jejich profil a/nebo převzetí jejich identity[37] (37 %). Útočníci měli také často měnit přihlašovací údaje, potažmo zamezit přístupu oprávněného uživatele (23 %). Dále mazali a stahovali si nějaký obsah (9 a 7 %). Nejjistější si byli ohledně formy zneužití jejich účtu respondenti mladší 29 let. Kupodivu v případě neoprávněných přístupů na cizí profily na sociálních sítích hrála z pohledu napadených hlavní roli majetková motivace (15 %). Následuje pouhá zvědavost (11 %). Významný podíl zaujímá souhrnně virtuální násilí – žárlivost, stalking, osobní nenávist a nesnášenlivost obecně považovalo za hlavní motivaci celkem 30 % napadených.

V rámci self-reportové části dotazníku byli respondenti dotázáni, zda použili něčí účet na sociální síti bez výslovného svolení jeho majitele. V roce 2020* tak učinilo 100 osob (2 % všech respondentů), z toho 86 % použilo jen jeden účet jedné osoby. Opět šlo především o Facebook a Messenger (75 a 18 %).

(Neoprávněně) navštívené účty patřily převážně stávajícím partnerům a osobám z úzkého rodinného kruhu (52 a 19 %),[38] jen v několika případech bývalému partnerovi (9 %). Naopak celých 17 % vypovědělo o neoprávněném přístupu k účtu kamaráda.



Graf č. 2: Aktéři neoprávněného vstupu do profilu na sociální síti

37 Typicky např. odeslání zprávy jejich jménem.

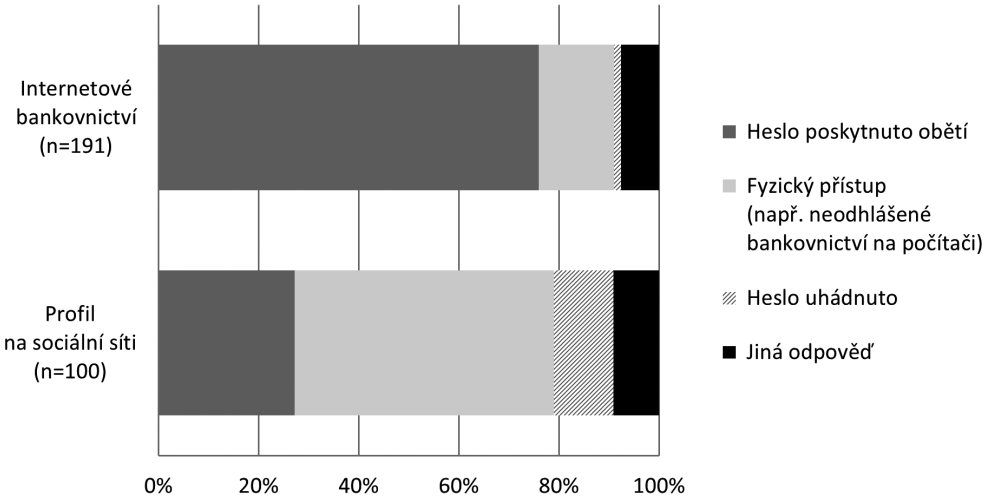
38 Statisticky významně často tak odpovídaly ženy – ty mnohdy přistupovaly na profily svých potomků. V takových případech dost dobře nelze (ne)oprávněnost přístupů dovozovat bez dalšího (např. znalosti věku dohlížené osoby, resp. její rozumové a volní vyspělosti).

Na rozdíl od domněnek napadených respondentů hovořili respondenti-pachatelé převážně o získání přístupu díky použití zařízení napadené osoby, na kterém byl daný profil či účet přihlášený (57 %). Ve třetině případů (30 %) znali útočníci přihlašovací údaje od samotné napadené osoby[39] a pouze ve 13 % je uhádli.

Během přístupu bez výslovného svolení majitele účtu si respondenti zdaleka nejčastěji prohlíželi obsah (78 %). Případně si nějaký obsah stáhli (14 %), smazali nebo vložili vlastní (shodně 9 %). Statisticky významně často si obsah prohlížely osoby ve věku 30–44 let. Tomu odpovídá i motivace uváděná respondenty navštěvujícími cizí účty, a to převážně zvědavost (68 %), o peníze šlo pouze u 10 % případů. K dalším častějším pohnutkám patřila zábava/žert a žárlivost.

5. De lege ferenda

Na jedné straně máme právní úpravu, která postihuje jakýkoliv neoprávněný přístup k online účtu, ať už půjde o internetové bankovnictví, profil na sociální síti či jiný účet.[40] Podstatná je neoprávněnost přístupu určená překonáním překážky, a to i v případě, že dotyčný „má klíč" (zná přihlašovací údaje). Zejména, když ona překážka chrání soukromý prostor či obsah, o čemž lze v případě internetového bankovnictví a profilu na sociální síti pochybovat jen výjimečně.[41]



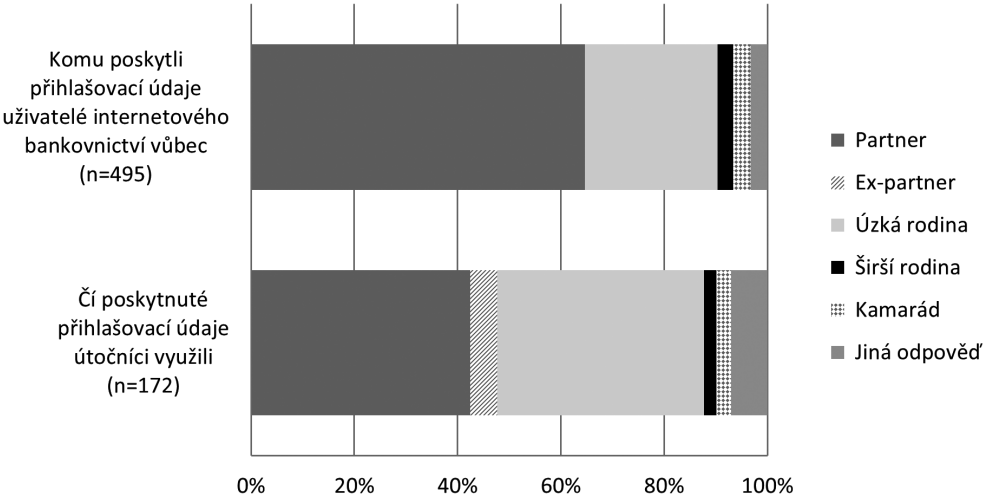
Graf č. 3: Získání přístupu k napadenému účtu podle útočníků

[39] 63 % bylo požádáno o nějakou jednorázovou aktivitu (např. poslání zprávy), 40 % spravovalo daný profil trvale (nicméně i tito zde odpovídali výlučně ohledně přístupu bez výslovného svolení majitele daného účtu).

[40] Zejména emailový.

[41] I zcela veřejně přístupný profil na sociální síti k sobě může mít např. navázané soukromé zprávy. Na druhou stranu nelze pominout, že většina online účtů vyžaduje přihlášení prostřednictvím přihlašovacích údajů bez ohledu na to, zda o to uživatel stojí, či nikoliv. Samotná existence bezpečnostního opatření tedy nemusí vypovídat o snaze uživatele zabránit neoprávněnému přístupu.

Na straně druhé leží každodenní praxe mnoha uživatelů, kteří dobrovolně sdílejí své přihlašovací údaje, včetně přístupu k internetovému bankovnictví. V nezanedbatelném množství případů pak zakouší neoprávněný přístup k jejich účtům i sami neoprávněně přistupují k účtům cizím, byť si mnohdy pouze ze zvědavosti prohlédnou určitý obsah.[42] Lze se přitom domnívat, že řada takových uživatelů si není vůbec vědoma, že se dopustili či by se mohli dopustit protiprávního jednání.[43]



Graf č. 4: Sdílení přihlašovacích údajů k internetovému bankovnictví

Je tedy zřejmé, že obsah právní normy vtělený do § 230 odst. 1 tr. z. neodpovídá příléhavě sociální realitě (přinejmenším v této oblasti). Nelze samozřejmě volat po zrušení skutkové podstaty trestného činu krádeže s odůvodněním, že řada osob krade, a jde tedy o „normální" jednání. Stejně tak by nemělo smysl volat po zrušení skutkové podstaty § 230 odst. 1 tr. z. pouze s odůvodněním, že některé osoby se takového jednání dopouštějí (koneckonců by v podobném duchu ztratil opodstatnění celý trestní zákon). Namístě je však zamyšlení, zda je pro společnost vůbec žádoucí postihovat prostředky trestního práva jednání, které často z pozice aktérů na obou stranách není vůbec chápáno jako protiprávní, natož trestné. Naopak je docela dobře možné, že oběti přinejmenším některých oblastí kyberkriminality si v řadě případů ani nepřejí trestněprávní postih útočníka, třeba z důvodu přetrvávajícího vztahu, absence negativních dopadů atp.[44] Navíc ani zákonodárce

42 Koneckonců i „pouhé" prohlédnutí si obsahu však může představovat významný zásah do soukromí.

43 Domněnka vychází z analýzy trestních spisů, rozhovorů s experty i řady kurzů bezpečného chování online vedených autorkou.

44 Ilustrací budiž nizozemský projekt zabývající se šířením intimních snímků mladých obětí bez jejich souhlasu. Mimo jiné se zde ukázalo, že oběti by před trestním sankcionováním pachatele daly přednost tomu, aby byla pachateli uložena povinnost absolvovat osvětový kurz zaměřený na dopady daného jednání na oběti. Blíže k metodologii výzkumu a jeho výsledkům viz projekt @ntidote a program 3. dne (22. listopadu 2022) konference Human Factor in Cybercrime (2022), abstrakt vystoupení A. Gilen, C. Van de Heyning a M. Walrave. The Non-consensual Dissemination of Intimate Images (NCII): Victims' Rationales behind not Reporting This Crime and Their Perspective on How to Legally Conserve NCII. Viz BELSPO BRAIN-be 2.0. *@ntidote*. [cit. 2023-01-26]. Dostupné z: <https://www.antidoteproject.be>; a HFC CONFERENCE (2022). *HFC conference*. [cit. 2023-01-08]. Dostupné z: <https://www.hfc-conference.com>.

sám nepovažoval za nutné či vhodné uvést jiný důvod stávající právní úpravy než mezinárodní závazky.[45]

Za zvážení proto stojí jiná cesta, která by omezila erozi právní normy plynoucí z jejího nepochopení, neznalosti a nedodržování. Takovou, která by zároveň zohlednila i skutečnost, že některé oblasti kyberkriminality vyžadují značné úsilí ze strany (všech) orgánů činných v trestním řízení k jejímu odhalení, vyšetření a odsouzení, zatímco „řešení" daného jednání ze strany samotného napadeného uživatele může být výrazně rychlejší, efektivnější i preventivní. Nízkému zájmu napadených osob na řešení značné části útoků prostřednictvím orgánů činných v trestním řízení odpovídá i vysoká latence takového jednání – na policii se v roce 2020* obrátilo kvůli neoprávněnému přístupu do jejich internetového bankovnictví pouhých 15 % napadených respondentů, v případě účtů na sociálních sítích to bylo dokonce jen 5 %.[46]

5.1 Částečná dekriminalizace

Z důvodů výše uvedených se nabízí zvážení částečné dekriminalizace, respektive legislativní úprava § 230 odst. 1 tr. z.[47] Již několikrát zmíněné mezinárodní závazky ponechávají sice v tomto směru jen relativně malé možnosti, nicméně určitý prostor zde je.

Předně se podívejme na Úmluvu. V článku 2 vyžaduje kriminalizaci úmyslného neoprávněného přístupu[48] k počítačovému systému nebo jeho části, přičemž trestnost lze podmínit porušením bezpečnostních opatření, úmyslem získat počítačová data nebo jiným nečestným úmyslem nebo jednáním ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem.

Úmluva – článek 2 – Nezákonný přístup
„[…] aby […] byl trestným činem, pokud je spáchán úmyslně, neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části. Strana může stanovit, že bude považovat tento čin za trestný, jen pokud je spáchán porušením bezpečnostních opatření, s úmyslem získat počítačová data nebo s jiným nečestným úmyslem, nebo ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem."

Stávající právní úprava v ustanovení § 230 odst. 1 tr. z. zmiňuje toliko překonání bezpečnostních opatření. V úvahu proto připadá dekriminalizace úpravou subjektivní a/nebo objektivní stránky základní skutkové podstaty § 230 odst. 1 tr. z. vložením dalšího znaku.

Jedním takovým znakem může být v souladu s čl. 2 Úmluvy *„úmysl získat počítačová data nebo jiný nečestný úmysl"*, tedy znění např.: *„Kdo překoná bezpečnostní opatření s úmyslem získat počítačová data nebo s jiným nečestným úmyslem, a tím neoprávněně*

45 VLÁDA ČR. *Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník*. 25. 2. 2008.

46 Několik dílčích poznatků ohledně latence různých typů online útoků je dostupných prostřednictvím tiskové zprávy ze zasedání Republikového výboru pro prevenci kriminality z května roku 2021 v její příloze č. 1 nazvané Kybernetická kriminalita v ČR z kriminologické perspektivy – IKSP, viz MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Tisková zpráva ze zasedání Republikového výboru pro prevenci kriminality*. Květen 2021 [cit. 2023-01-08]. Dostupné z: <https://www.mvcr.cz/clanek/tiskova-zprava-ze-zasedani-republikoveho-vyboru-pro-prevenci-kriminality-713175.aspx>, příloha č. 1, s. 5.

47 Záměrně vztahujeme úvahy k první základní skutkové podstatě § 230 tr. z. uvedené v odstavci 1 – neoprávněnému přístupu, a nikoliv zároveň ke druhé základní skutkové podstatě uvedené v odstavci 2, který se již věnuje různým formám neoprávněné manipulace s daty.

48 Úmluva výraz „neoprávněný přístup" blíže nespecifikuje.

získá přístup k počítačovému systému nebo k jeho části, bude potrestán […].“ Z uvedené formulace by zároveň z hlediska jazykového výkladu vyplývalo, že i samotný úmysl získat počítačová data by musel být nečestný (srov. „*nebo s jiným nečestným úmyslem*“), a tak by tato skutková podstata nedopadala bez dalšího automaticky na řadu jednání, jejichž (ne)oprávněnost je sama o sobě diskutabilní – typicky např. sledování facebookového profilu rodiči.

Dalším dekriminalizujícím znakem by mohlo být z hlediska Úmluvy spojení napadeného počítačového systému nebo jeho části s jiným počítačovým systémem,[49] které bychom ovšem ponechali stranou. Především proto, že jednání, o jejichž dekriminalizaci zde uvažujeme, se v drtivé většině odehrávají online, tedy v rámci propojených počítačových systémů. „Dekriminalizace“ přidáním znaku propojených počítačových systémů nebo jejich částí by proto fakticky žádnou dekriminalizací nebyla. Zároveň se nedomníváme, že „nepropojenost“ počítačového systému či jeho části s jiným počítačovým systémem neznamená bez dalšího jeho menší význam, potažmo nesnižuje závažnost neoprávněného přístupu k němu.

Směrnice uvádí v čl. 2 písm. d) definici „neoprávněného“ jednání, kam zařazuje mimo jiné přístup, který není povolen majitelem (či jiným držitelem práv k systému nebo k jeho části), a v čl. 3 upravuje regulaci neoprávněného přístupu.

> *Směrnice – článek 3 – Neoprávněný přístup k informačním systémům*
> *„[…] aby […] je-li spáchán úmyslně, byl trestným činem, je-li tím porušeno bezpečnostního opatření, a to alespoň tehdy, pokud se nejedná o méně závažný případ.“*

Směrnice je oproti Úmluvě mírnější, neboť na rozdíl od ní vyžaduje pro kriminalizaci neoprávněného přístupu kumulativní splnění podmínky úmyslu a porušení bezpečnostního opatření, kdežto Úmluva pouze umožňuje zavázaným státům zmírnit kriminalizaci přidáním podmínky porušení bezpečnostního opatření. Směrnice oproti Úmluvě zároveň předpokládá, že půjde o nikoli méně závažný případ neoprávněného přístupu. Jinými slovy nepožaduje kriminalizaci méně závažných případů.

Při zohlednění Směrnice i Úmluvy by tak bylo možno běžným legislativním procesem upravit znění skutkové podstaty v § 230 odst. 1 tr. z. tak, aby nedopadalo na úmyslný neoprávněný přístup k počítačovému systému (či nosiči informací) či jeho části, při němž sice bylo porušeno bezpečnostní opatření, ale je méně závažný a chybí u něj nečestný úmysl (včetně získání počítačových dat s nečestným úmyslem).[50] Pakliže by zákonodárce nechtěl použít široký pojem „nečestný úmysl“, inspiraci lze nalézt např. v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch [nyní odst. 3 písm. a) tr. z.], v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat [nyní odst. 3 písm. b) tr. z.], v zavrženíhodné pohnutce, v úmyslu narušit soukromí dítěte atp.

Nutno podotknout, že výraz „*získat počítačová data*“ lze v širším významu vykládat jako jakékoliv jejich zpřístupnění pro sebe, tedy včetně pouhého přečtení či prohlédnutí. Dekriminalizaci by naproti tomu odpovídal užší význam získání dat, a to zajištění si

---

49 Nemuselo by tak jít pouze o síťové propojení (typicky internetem, ale i jakoukoliv jinou sítí – např. uzavřenou firemní), ale de facto propojení jakýchkoliv dvou prvků – tedy např. i přímé spojení dvou zařízení.

50 V převážné většině případů zřejmě bude menší závažnost jednání dána již samotnou absencí nečestného úmyslu, nicméně nemusí tomu tak být vždy.

možnosti manipulace s daty – tzn. jejich okopírování, zjednání přístupu pro pozdější využití atp. Pouhé přečtení či prohlédnutí dat by tak nebylo jejich „získáním", a zároveň by ještě nenaplnilo základní skutkovou podstatu uvedenou v odst. 2 § 230 tr. z.

Za pozornost stojí i úvaha nad zúžením znaku *„překonání bezpečnostního opatření"*, tedy nějaké překážky mající za úkol zabránit neoprávněnému jednání. Zatímco tr. z. používá výraz „překonání", Úmluva i Směrnice mluví o „porušení" bezpečnostního opatření.[51] Úmluva v anglické verzi používá výraz *„infringing security measures"*, ve francouzské verzi *„en violation des mesures de sécurité"*. Adekvátním překladem je v obou případech „porušení bezpečnostních opatření" (samotný rozdíl v použití singuláru a plurálu zde nehraje velkou roli). Zároveň obvykle nepřichází v úvahu výraz „překonání",[52] lze se tedy domnívat, že zákonodárce zvolil slovo „překonání" namísto „porušení" záměrně. Oba výrazy se částečně významově liší, když „překonat" evokuje typicky překonání překážky, též ale např. ovládnutí, nabytí moci, zdolání, tedy určité přemožení – v kontextu neoprávněného přístupu přemožení autentizačního systému, včetně případů použití správného hesla.[53] Naproti tomu „porušit" odkazuje významově více k poškození.[54] S použitím správného hesla sice bezpečnostní opatření překonávám, ale neporušuji. Ono „porušení" znamená už nějaký zásah do systému. O nezákonnosti vniknutí v podobě úpravy zdrojového kódu daného systému není pochyb. Nicméně „porušením" by bylo např. i použití softwarového prolamovače hesel,[55] ba i prosté uhádnutí hesla bez předchozí znalosti. Někdo by snad namítl, že „porušení" v trestním zákoně znamená i prosté seznámení se s jinak nedostupným obsahem, viz § 182 tr. z., porušení tajemství dopravovaných zpráv.[56] Zde však hovoříme o samotném přístupu, nikoliv o následné aktivitě.[57]

Z hlediska trestního řízení by bylo namístě uvažovat o zařazení skutkové podstaty § 230 odst. 1 tr. z. mezi trestné činy, pro které lze zahájit a v již zahájeném trestním stíhání pokračovat pouze se souhlasem poškozeného dle § 163 odst. 1 zák. č. 141/1961 Sb., trestní řád (dále jen tr. ř.). A to zejména s ohledem na relativně četný výskyt neoprávněného přístupu do internetového bankovnictví i k sociálním sítím osobami v poměru rodinném či obdobném.[58] Procesněprávní normy nejsou předmětem tohoto článku, nicméně považujeme za vhodné tuto variantu pro úplnost uvést.

---

51 Překlad do češtiny uvádí na svém webu sama Rada Evropy, viz RADA EVROPY. *Council of Europe – Convention on Cybercrime (ETS No. 185) – Translations*. [cit. 2023-01-17]. Dostupné z: <https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations>. Směrnice coby právní dokument EU má vlastní oficiální znění i v češtině.

52 Různé slovníky se do jisté míry rozchází, nicméně z hlediska použití slova „porušení" a absence slova „překonání" se v překladech shodují. Viz např. OHEROVÁ, J. S. *Anglicko-český právnický slovník*. 4. vydání. Praha: LINDE, 2010, s. 261; TOMÁŠEK, M. *Čtyřjazyčný právnický slovník*. Antwerpen: MAKLU Uitgevers, 1997, s. 352; FRONEK, J. *Velký anglicko-český slovník*. Praha: LEDA, 2006, s. 791; nebo DeepL SE. *DeepL*. Dostupné z: <https://www.deepl.com/translator>.

53 Dotyčný „vyzraje" na systém, který nepředpokládá znalost hesla u nikoho jiného než oprávněného uživatele.

54 ÚSTAV PRO JAZYK ČESKÝ AKADEMIE VĚD ČR. *Internetová jazyková příručka*. [cit. 2023-01-17]. Dostupné z: <https://prirucka.ujc.cas.cz>. Blíže k tomu viz zde dostupný Slovník spisovné češtiny a Slovník spisovného jazyka českého, výrazy „porušit" a „překonat".

55 Tzv. brute-force útok, např. slovníkový útok (snaha získat přístup zkoušením všemožných slovních kombinací).

56 ŠÁMAL, P. Komentář k § 182. In: ŠÁMAL, P. a kol. *Trestní zákoník II: Zvláštní část (§ 140–421)*, s. 1809.

57 Při vstupu na cizí online účet nepochybně přichází v úvahu použití skutkové podstaty § 183 tr. z., porušení tajemství listin a jiných dokumentů uchovávaných v soukromí, nikoliv však nutně. Pachatel by musel zjištěný obsah nějakým způsobem „použít", což zřejmě nezahrnuje prosté seznámení se s ním. K „použití" obsahu viz např. ŠÁMAL, P. Komentář k § 183. In: ŠÁMAL, P. a kol. *Trestní zákoník II: Zvláštní část (§ 140–421)*, s. 1823.

58 Obdobný návrh se již objevil např. v souvislosti s etickým hackingem, viz HLAVÁČOVÁ, K. Institut svolení poškozeného a etický hacking. *Trestněprávní revue*. 2018, č. 3, s. 53.

6. Prevence

Při pokračování stávající kriminalizace veškerých neoprávněných přístupů k informačním systémům v nezměněné podobě dost dobře nelze zamezit výše zmíněnému nesouladu mezi sociální realitou a požadavky právní normy. V banálních případech se lze sice dovolat materiálního korektivu v podobě zásady subsidiarity trestní represe a principu ultima ratio (§ 12 odst. 2 tr. z.) v duchu *minima non curat praetor* – o drobné záležitosti se praetor nestará.[59] Nelze však pominout náklady spojené byť jen se zahájením a ukončením trestního řízení (zejména personální a časové).

Uvedený nesoulad vyplývá u řady osob z neznalosti právní normy a i případná dílčí dekriminalizace by ho pouze částečně omezila. Zmírnění by proto mohla přinést do jisté míry i vhodně realizovaná osvěta. V ideálním případě s takovým účinkem, aby povědomí o nezákonnosti neoprávněného přístupu k online účtu někoho jiného bylo tak samozřejmé jako např. povědomí o nezákonnosti krádeže.[60]

Primární prevence by se tak měla zaměřit zejména na potenciální pachatele. Cílem je informovanost o nezákonnosti neoprávněného přístupu, potažmo odrazení od neoprávněného přistoupení k cizímu online účtu.

Naproti tomu sekundární prevence by měla zacílit na ohrožené skupiny obětí. Podrobnější rysy obětí různých typů online deliktů se sice stále hledají,[61] obecně však můžeme hovořit o známých skupinách – především senioři a děti/dospívající. Překvapivě by ovšem měly být zahrnuty i osoby v partnerském vztahu, vzhledem k jejich nejčastějšímu aktérství na obou stranách. Osvěta by se měla zaměřit na ochranu vlastních přihlašovacích údajů, a to zejména jejich nesdílení s dalšími osobami a nepoužívání stejných hesel na různých místech.[62]

Mohlo by se zdát, že terciární prevence zde nenajde příliš uplatnění (protože pachatelé již vědí o nezákonnosti svého jednání a oběti jsou viktimizací motivované pro příště své účty lépe chránit). V nezanedbatelném množství případů však dochází k reviktimizaci, a to i v rámci jediného roku, jak ukázalo dotazníkové šetření (viz výše). Terciární prevence by tak měla učit oběti lepším bezpečnostním online návykům souvisejícím s jejich napadením.

Shrnutí

Článek vychází z výzkumného úkolu IKSP Posouzení trendů kyberkriminality. Čerpá především z dotazníkového šetření ohledně zkušeností českých uživatelů internetu ve věku 16–74 let v roce 2020* a analýzy trestních spisů vedených o počítačových trestných činech, pro něž byl pachatel pravomocně odsouzen v roce 2019. Byla použita kombinace metod kvantitativního i kvalitativního výzkumu, včetně analýzy právních dokumentů.

---

59 ŠÁMAL, P. Komentář k § 12. In: ŠÁMAL, P. a kol. *Trestní zákoník I: Obecná část (§ 1–139)*, s. 120. V procesní rovině by pravděpodobně v řadě takových případů přicházelo v úvahu i zastavení trestního stíhání s tím, že účelu trestního řízení bylo již dosaženo [§ 172 odst. 2 písm. c) tr. ř.].

60 Takže by stačila zcela hrubá představa bez zvláštních technických znalostí nad rámec běžných uživatelských schopností.

61 Typologie obětí kyberdeliktů bude čítat zřejmě desítky typů. Informace k významnému aktuálně probíhajícímu projektu v tomto směru zazněly na již zmíněné konferenci Human Factor in Cybercrime (2022), viz abstrakt vystoupení S. van 't Hoff-de Goede, A. Moneva a R. Leukfeldt nazvaného *Examining Risk Profiles for Cybercrime Victimization*. Viz HFC CONFERENCE (2022). *HFC conference*.

62 Další doporučené bezpečnostní prvky jako síla hesla už patří do relativně běžného povědomí.

Analýza trestních spisů poskytla východisko pro zde uvedené úvahy i realizaci dotazníkového šetření. To mimo jiné naznačilo, že osoby ve věku 16–29 let představují do jisté míry specifickou skupinu.[63] Latence zjišťovaných jednání online je sice značná (dosahuje až 99 %), přesto lze usuzovat na určitý stav. Ve zde sledovaných oblastech poskytlo odpovědi 199 obětí a 86 útočníků ohledně neoprávněného přístupu k internetovému bankovnictví a 377 obětí a 100 útočníků ohledně neoprávněného přístupu k profilům na sociálních sítích. Ve významném množství případů byli aktéry na obou stranách partneři, případně osoby z úzkého rodinného kruhu. Často byly využity k neoprávněnému přístupu přihlašovací údaje, které dříve poskytly útočníkům samy oběti.

Současné znění § 230 odst. 1 tr. z. se z hlediska výkladu i judikatury vztahuje také na neoprávněný přístup k online účtu chráněnému heslem, včetně případů, kdy pachatel heslo zná. Vychází z mezinárodních závazků – Úmluvy a Směrnice. Ty sice vyžadují kriminalizaci úmyslného neoprávněného přístupu po porušení bezpečnostních opatření, nicméně ponechávají i určitý prostor pro zúžení kriminalizace, který český zákonodárce zcela nevyužil. Jde zjednodušeně např. o přidání znaku nikoli menší závažnosti a znaku nečestného úmyslu. K tomu se přidává i do jisté míry se odchylující překlad, když Směrnice i Úmluva hovoří o „porušení" bezpečnostních opatření, zatímco pro naplnění skutkové podstaty § 230 odst. 1 tr. z. stačí i jejich „překonání".

Část neoprávněných přístupů k online účtům by tak bylo možné a žádoucí v souladu s mezinárodními závazky dekriminalizovat změnou znění § 230 odst. 1 tr. z. např. na *„Kdo poruší bezpečnostní opatření s úmyslem získat počítačová data nebo s jiným nečestným úmyslem, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán […]."*

Při dekriminalizaci i zachování stávající kriminalizace neoprávněného přístupu k online účtu se jeví jako žádoucí osvěta zaměřená na jedné straně na nezákonnost takového jednání (cílící na potenciální pachatele), na straně druhé pak na základní bezpečnostní návyky, konkrétně především nesdílení přihlašovacích údajů s dalšími osobami, byť těmi nejbližšími (cílená na potenciální oběti, pro online prostředí neobvykle s důrazem na osoby v partnerském vztahu, nejen seniory a děti/dospívající).

Závěr

Z obsahu článku je zřejmě patrné, že za nejvhodnější řešení napětí mezi sociální realitou a trestní normou jednoznačně považujeme částečnou dekriminalizaci § 230 odst. 1 tr. z. Legislativní proces však představuje nesnadnou cestu, zvláště když aktuální stav není tak palčivý jako řada jiných otázek a společenských problémů.

O to větší důraz by měl být kladen na osvětu, zejména zaměřenou na potenciální oběti a budování základních bezpečnostních návyků v online prostředí vůbec. Měla by mezi ně patřit i schopnost vypořádat se vlastními silami s neoprávněným přístupem: zabezpečit samotný účet (typicky změnou přihlašovacích údajů), informovat osoby, kterých se neoprávněný přístup mohl dotknout, zálohovat důležitý obsah atd. Důvodem vybízení k osvětě je i praktické hledisko, neboť zabezpečení svých online účtů může docílit nejlépe sám uživatel vlastními silami a s minimálními náklady (finančními, časovými i znalostními).

63 Pravděpodobně v důsledku vyšší orientace v online prostředí a zároveň vyšší důvěry vůči ostatním osobám ve vztahu k online prostředí, nicméně to je pouze domněnka.

Osvěta se také oproti právní dekriminalizaci vyhýbá posouzení (ne)oprávněnosti přístupu. Nemusí se zabývat spornými případy, kdy např. rodič dohlíží na profil svého dospívajícího potomka na sociální síti bez jeho souhlasu. Podobně jako případy, kdy je heslo natolik zřejmé a evidentní, že ačkoliv ho jiná osoba nezná, okamžitě jej bez jakéhokoliv úsilí uhodne. A nakonec ani těmi, kdy si neoprávněně přistupující osoba pouze prohlédne nějaký obsah, avšak pro oběť to představuje výrazný zásah do jejího soukromí.

Zde uvedené údaje mají samozřejmě svá omezení. Údaje z analýzy trestních spisů zachycují pouze malou část skutečných jednání (samotné orgány činné v trestním řízení se dozví pravděpodobně nejvýše o čtvrtině z nich, pouze část pachatelů se podaří identifikovat a ještě menší podíl obžalovat, natož odsoudit). Dotazníkové šetření naproti tomu zachycuje pouze ty informace, které byli respondenti ochotni sdělit (limit především u self-reportu).[64] Přesto se domníváme, že jejich vypovídací hodnota je nezanedbatelná, a to i s ohledem na fakt, že při zohlednění velikosti obou výzkumných souborů se poznatky z nich poměrně shodují. Další analýzy se zaměří na případnou souvislost mezi aktérstvím na kterékoliv straně jednání a viktimizacemi různým jednáním, dále též na vztah mezi bezpečnostními návyky a viktimizací vůbec.

Online prostředí představuje rychle se vyvíjející oblast, kterou se daří jen pozvolna zachycovat výzkumným úsilím napříč sociálněvědními obory, natož prostředky trestního práva. Zatímco některé instituty zůstávají neměnné bez ohledu na online či offline prostředí (typicky význam skutečně soukromého prostoru), jiné doznávají výrazných změn – např. kvazisoukromý prostor v podobě veřejného profilu na sociální síti. Zároveň se přítomnost v online prostředí stala samozřejmou součástí každodenní reality a nezdá se, že by měl její význam ustoupit. Je proto namístě zamyslet se nad vhodnou právní regulací tak, aby kyberprostor nebyl zbytečně svázán nedodržovanými právními normami, ale ani „Divokým západem“.

64 Zároveň referovaná jednání nemusí nutně bez dalšího naplňovat skutkovou podstatu § 230 odst. 1 tr. z.

Unauthorised Access to Online Accounts (Internet Banking, Social Networks)

Kateřina Kudrlová (https://orcid.org/0000-0001-8911-1134) –
Jiří Vlach (https://orcid.org/0000-0002-7295-4677)

Abstract: Online accounts are nowadays an inseparable part of everyday life. Among the most important ones are online banking for managing finances and a social network profile for communicating with the social networks community. As these are computer systems, unauthorised access to them can be punished as a computer crime under Section 230(1) of the Criminal Code. However, a representative questionnaire survey carried out in 2020 in the Czech Republic showed that unauthorised access occurs quite frequently, especially between partners or within a close family. In many cases, attackers gain access using login credentials that are relatively commonly shared with others by users of online accounts, and the unauthorised access itself may be questionable in many cases. The aim of this article is therefore to highlight the inconsistency of the legal norm with common user practice and to propose a possible legal modification to better reflect social reality. Considering international obligations, a partial decriminalisation of the computer offence under Article 230(1) of the Criminal Code could be achieved by changing the term "overcomes" to "infringes" and adding an additional element to this offence – acts "with the intent to obtain computer data or with other dishonest intent". Finally, we provide brief recommendations for preventing unauthorised access to online accounts.

Keywords: unauthorised access, internet banking, social networks, decriminalisation, computer crime, online accounts