ZAVRŠNIK, Aleš. Kyberkriminalita

Praha: Wolters Kluwer ČR, 2017, 148 s. ISBN 978-80-7552-758-5.

Veronika Skalická*

Publikace vydaná nakladatelstvím Wolters Kluwer ČR v roce 2017 si za primární cíl klade analýzu kyberkriminality ve Slovinsku. Druhotným cílem publikace je vysvětlení základních témat a pojmů souvisejících s kyberkriminalitou a spojených s internetem, výpočetní technikou a novými informačními společnostmi.

Autor Prof. Dr. Aleš Završnik, univ. dipl. prav. působí na Právnické fakultě Univerzity v Lublani jako docent a na Institutu kriminologie téže fakulty, současně rovněž jako hostující lektor na Collegium Helveticum Zürich. V rámci programu Evropské spolupráce ve vědě a technice (COST) se podílel na celé řadě akcí a v nedávných výzkumech se zaměřil na sledování drony. Své závěry shrnul v publikaci Drones and Unmanned Aerital systems: Legal and Social Implication for Security and Surveillance. Za knihu Crime and Transation in Central and Eastern Europe, na které se podílel jako spoluautor, získal ocenění od Slovinské výzkumné agentury za nejlepší vědecký počin v kriminologii. Stran rozsáhlé výzkumné a publikační činnosti se věnuje kyberzločinu, právu IT, sledování, regulaci kriminality a technologiím, etickým problémům v oblasti bezpečnosti a ICT. Řídil výzkumný projekt Law in the Age of Big Data, Regulating Privacy, transparency, secrecy and Other Competition Values in the 21st Century.

V publikaci se autor věnuje jednotlivé problematice kyberkriminality, od seznámení se se základními pojmy, přes rozvoj a dílčí obecná témata až po konkrétní specifické náměty. Primární pozornost publikace má být směřována k aktuálnímu stavu kyberkriminality ve Slovinsku, přičemž autor postupuje systematicky v rámci seznámení čtenáře s jednotlivými typickými aspekty kyberkriminality jednak z pohledu trestněprávního, tak rovněž kriminologického. Autor se pokouší reflektovat legislativní řešení přijatá ve Slovinsku, v rámci Rady Evropy nebo Evropské unie.

Právnické publikace zabývající se kyberkriminalitou na území České republiky z komplexního pohledu nenalezneme v hojném zastoupení. Výjimku tvoří monografie CybyrCrime od Jana Koloucha, která analyzuje kybernetickou kriminalitu, mimo právního pohledu současně i zahrnuje technickou část obsahující oblasti malware, phishingu, darknetu či botnetů, nebo Kybernetická kriminalita od Vladimíra Smejkala, která je zaměřena více prakticky i s podložením přiléhavé judikatury. V tomto ohledu lze poukázat

* Mgr. Veronika Skalická, doktorandka, Katedra trestního práva, Právnická fakulta, Masarykova univerzita, Brno / Department of Criminal Law, Faculty of Law, Masaryk University, Brno, Czech Republic / E-mail: skalicka.veronika@seznam.cz

spíše na monografie z dílčích oblastí kyberkriminality, ku příkladu Kryptografie (Milan Oulehla), CyberSecurity (Jan Kolouch, Bašta), Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti (Vladimír Smejkal, Tomáš Sokol, Jindřich Kodl) anebo komentářů zákonů (Zákon o elektronických komunikacích, Zákon o kybernetické bezpečnosti, aj.).

Monografie je uspořádána do sedmi kapitol, od vymezení jednotlivých pojmů jako je kyberkriminalita, kybernetická bezpečnost, kyberterorismus a kybernetické války, a rozvoj kyberkriminality, přes jednotlivé subtypy kyberkriminanality a její výskyt, až po reagování na kyberkiminalitu. Poslední dvě kapitoly se věnují praktickým otázkám kriminální politiky a aktuálním tématům souvisejícím s kyberkriminalitou.

První kapitola je jakýmsi obecným exkurzem a vymezením základních pojmů ve spojení s užíváním internetu v Evropě, a zvláště pak ve Slovinsku. Pojednává o rozvoji kyberkriminality a kriminality související s ní, jakož i o prvních mezinárodních právních aktech v této oblasti. Autor se věnuje Budapešťské úmluvě z roku 2001 a v ní rozdělení trestných činů. V zásadě se tak snaží vymezit pojem kyberkriminality a definovat jej za pomoci charakteristických znaků. Okrajově poukazuje na činnost Evropského centra pro boj proti kyberkriminalitě a projekt E3C First Year Report identifikující okolnosti ztěžující trestní stíhání. Prostřednictvím grafických znázornění se pokouší čtenáři osvětlit princip fungování internetu a pilíře kybernetické bezpečnosti na národní slovinské úrovni a úrovni Evropské unie včetně jednotlivých institucí a organizací (Europol, Eurojust, CEPOL, CERT, EC3, EDA, EEAS, ENISA, EP3R). Úvodní kapitolu uzavírá definicí pojmů kyberterorismu a kybernetické války s případovou studií rusko-estonského konfliktu. Autor tak dle mého názoru zdárně čtenáře uvedl do problematiky, jíž se bude celá publikace věnovat a za pomoci praxe vymezil základní milníky v kyberkriminalitě. První kapitola tak ničím zásadním nepřekvapuje, nicméně představuje důležitou a esenciální část knihy.

Druhá kapitola pojednává o rozvoji kyberkriminality jako takové ve třech fázích, rozvoji internetu a hackerské kultuře. Autor kapitole věnoval minimum obsahu celé publikace a z pohledu informovanosti čtenáře považuji právě druhou kapitolu za nejméně přínosnou a pro získání nových informací nikterak převratnou. Značná míra stručnosti, jež je pro tuto kapitolu charakteristická, tak ubírá na celkovém pozitivním hodnocení monografie.

Naopak podrobněji je rozebrána fenomenologie kybernetiky ve třetí kapitole. Autor prostřednictvím matice (tabulky) rozčlenil kyberkriminalitu do čtyř skupin podle trestných činů spojených s integritou, s počítači, s obsahem – obscénností a s obsahem – násilím. Protiprávní činy pak dále v rámci takového dělení rozřadil do třech podskupin podle příležitostí pro tradiční kriminalitu (více příležitostí a nové příležitosti) a pro novou formu kriminality. Poukazuje na čtyři diskurzy, zda kyberkriminalita představuje „problém“, jak ji definovat, jaké jsou její podoby a jak na ni reagovat. V souladu s Budapešťskou

úmluvou a jejím dělením kyberkriminality se autor v rámci jednotlivých podkapitol zabývá (i) kyberkriminlaitou spojenou s integritou informačního systému a dat, s definicí pojmů počítačová data a počítačový systém a konkrétními trestnými činy, i s poukázáním na úskalí trestního stíhání v této oblasti. Zde lze ocenit i teoretický přesah do právní praxe a upozornění na praktická úskalí. Dále se jedná o (ii) kyberkriminalitu spojenou s obsahem, v rámci níž se autor pokouší o přednes kyberkriminality se sexuálním obsahem, násilným obsahem a obsahem porušujícím právo duševního vlastnictví. V určitém smyslu se autor podrobně zabývá úskalími trestněprávních sankcí v podobě definic pojmů podstatných pro daný druh trestných činů (definice materiálu, sporných činů, utajenosti činů), extrémní pornografii, dětskou pornografii, šíření boje proti dětské pornografii. Autor probíranou problematiku podkládá jednotlivými právní předpisy – Evropskou směrnicí o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a dětské pornografii, Lanzarotskou úmluvou. V rámci subkapitoly spojené s násilným obsahem se publikace zaobírá kyberšikanou a nenávistnými projevy. Ani zde autor neopomněl odkázat na přiléhavé právní akty Rady Evropy a Evropské unie.

Třetí část dílčí kapitoly o kyberkriminalitě ve spojení s obsahem autor věnoval kyberkriminalitě spojené s porušováním duševního vlastnictví. Osobně tuto část považuji za nejvíce přínosnou z pohledu praktického využití nejen pro právníky, ale rovněž i pro laickou veřejnost, která je uživatelem internetu a služeb s ním spojených. Autor poměrně správně polemizuje nad škodou způsobenou porušováním práv duševního vlastnictví na internetu, neboť neopomíjí ani kladné dopady masového porušování práv duševního vlastnictví, kdy dochází k širšímu legálnímu užívání chráněných děl. Autorovi nelze upřít ani relevanci s názorem, zda v digitálním věku neopustit trestněprávní ochranu práv duševního vlastnictví. V rámci trestněprávních nástrojů na ochranu práv duševního vlastnictví stojí za zmínku autorův názor na boj o nadvládu mezi poskytovateli obsahu a internetovými/digitálními společnostmi s odkazem na směrnice IPRED a dohodu TRIPS, následně směrnici IPRED 2 a dohodu ACTA.

Závěrečná část kapitoly je věnována (iii) kyberkriminalitě spojené s počítači. Převážná část podkapitoly pojednává o krádeži identity i s jednotlivými způsoby přebrání identity pachatelem oběti. Dále jsou zde nastíněny i další typy podvodů na internetu: falešné internetové stránky obchodů, investiční podvody, webové aukční podvody, nigerijské podvody („podvody 419“), zneužívání pravidel trhu, špionské vybavení a nezákonný dohled nad zařízeními obětí. Autor upozorňuje současně na dopad v trestním stíhání, kdy je ziskovost podvodu na internetu mnohem vyšší a kriminální činnost probíhá pod dohledem orgánů činných v trestním řízení, přičemž významná může být až souhrnná viktimizace. Velmi okrajově se autor zabývá podvody s platebním stykem, což je dle mého názoru minimálně ku škodě čtenáře, neboť je ochuzen o významný a bez pochyby zajímavý podruh kyberkriminality.

Čtvrtou kapitolu lze považovat především za kriminologickou část monografie, v rámci níž autor rozebírá problematiku výskytu kriminality. Opět se jedná o obsahově méně rozsáhlou kapitolu. Ve své podstatě autor pouze uvádí některá data z výzkumů, avšak dle mého názoru postrádá vzájemné propojení a kontinuitu. Za pozitivně hodnocené považuji až vymezení čtyř hrozeb pro informační bezpečnost projevující se jako základní trendy. Jedná se o souhrnné, avšak ucelené konstatování nově vznikajícího problému, s nímž, domnívám se, se současná společnost a zejména orgány činné v trestním řízení musejí vyrovnat. Čtenáře tak autor nenásilným způsobem nutí k zamyšlení se nad cloud computingem, big daty, sociálními sítěmi a hrozbami s mobilními zařízeními. Za zmínku bezpochyby stojí i odhady výskytu kyberkriminality, resp. metodologická úskalí – údaje od největších výrobců ochranného software, na základě trestních oznámení, zkušenosti uživatelů ve speciálních výzkumech aj.

V páté, neobsáhlejší kapitole je čtenář seznámen pod názvem „Reakce na kyberkriminalitu" se základními prostředky, které napomáhají nastolit pořádek v kyberprostoru. V úvodu kapitoly autor uvádí sedm činitelů zajišťující pořádek v kyberprostoru. Za kladné považuji odkazy na případové studie o samoregulaci a úskalích spojených s vyšetřováním kyberkriminality. Přiléhavě pak poukazuje na skutečnost, že mezery v trestním právu hmotném vyúsťují zpravidla ve prospěch obviněných, avšak mezery v trestním právu procesním bývají často v neprospěch základních lidských práv obviněných. Za pozitivně hodnocenou lze považovat i zařazení podkapitoly o jurisdikci pro kybernetické trestné činy, kde zcela správně není opomenut přeshraniční charakter kyberkriminality, avšak jedná se pouze o povrchový, do hloubky nezacházející exkurs. Výrazněji není propracována ani další podkapitola zabývající se elektronickými důkazy, kdy se jedná spíše o vymezení pojmu elektronických důkazů.

Nikterak podrobně se autor nezaobírá rovněž problematikou získávání kybernetických forenzních dat od podezřelých skrytým dohledem, od poskytovatelů komunikačních služeb a od podezřelých na základě zabavování, zajišťování a analyzování počítačů a sítí. Přínosně mohu hodnotit vtipné a přiléhavé obrázky vztahující se k anonymitě na internetu, avšak po obsahové stránce není tato podkapitola pro čtenáře ničím novým. Výjimku tvoří pouze část o vybraných ustanoveních Budapešťské úmluvy, resp. o okamžitém zajištění údajů podle Budapešťské úmluvy. Ve vztahu ke Slovinské úpravě si však čtenář na základě textu autora nedokáže utvořit ucelenou představu o situaci ve Slovinsku, neboť autor se jí věnoval pouze ve dvou obsahově chudších odstavcích.

Za přínosné a obohacující lze považovat části páté kapitoly věnující se digitální forenzní analýze. Autor poukazuje na úskalí spojená s digitálními údaji – úskalí identity, fyzické loajality pachatele, integrity údajů, analýzy – podpořeno případovou studií se steganografií. Publikace obsahuje rovněž vymezení digitálního forenzního procesu, vymezení kybernetické forenzní vědy, základní zásady digitální forenzní analýzy (autentičnost, integrita, ověřitelnost), jakož i vlastnosti důkazů. Stručně jsou vymezeny digitální

vyšetřovací metody a techniky. Za zajímavou část můžeme považovat případovou studii aféry „Bunderstrojaner" a z ní vycházející dilemata spjatá s forenzními počítačovými systémy. Po povrchu je naznačena i problematika provádění elektronických důkazů v řízení před soudem. Vyzdvihnout je třeba závěr páté kapitoly zabývající se mezinárodní spoluprací a ochranou před kyberkriminalitou. Obsah kapitoly je vzhledem k ostatním podkapitolám pestřejší a hlouběji propracovaný. Za přínosné lze považovat jednak skutečnosti týkající se aktivit OECD, Rady Evropy a OSN, resp. nejstarší její agentury ITU a UNODC. Kladně hodnotím zejména přiloženou tabulky prvků národního programu kybernetické bezpečnosti, jež přehledně poukazuje na referenční model strategie kybernetické bezpečnosti. Stručně kapitola pojímá i činnost dalších mezinárodních organizací a v neposlední řadě obsahuje exkurs v rámci činnosti Evropské unie (EU Digitální agenda, Evropské středisko kyberkriminality, Evropská agentura pro bezpečnost sítí a informací), končící výčtem přiléhavých směrnic, což lze považovat minimálně za vhodný návod pro další hlubší samostudium.

Šestá kapitola je pouhým konstatováním a exkursem do oblasti kriminální politiky v oblasti kyberkriminality, avšak pro čtenáře dle mého názoru není tato kapitola výrazně přínosná. Za pozitivní aspekt však lze považovat poukazovanou případovou studii o vývoji inkriminovaného porušování hmotných autorský práv ve Slovinsku.

Za nejvíce přínosnou a zajímavou kapitolu považuji až kapitolu poslední, jež se věnuje vybraným aktuálním problémům. Srozumitelnou formou, byť stručněji, autor rozebírá správu internetu a internetové infrastruktury, zpravodajskou činnost a internet, hackerství, hacktivismus a politické využívání internetu, neutralitu internetu a vývoj uzavřených platforem, kryptoměny, deep web a dark web a v neposlední řadě i internet věcí. Autor vymezuje zejména pojmy internet, síťový protokol, IP adresy komunikací, doménová jména, aj. Zajímavou a novou informací byl pro mě výčet institucí spravujících základní stavební kameny internetu včetně krátkého popisu jejich činností a řízení internetu jako takového.

V podkapitole o zpravodajských službách autor rozebírá činnost Edwarda J. Snowdena, který odhalil zachycování provozních a lokalizačních údajů od poskytovatelů veřejných komunikačních služeb, kdy shromažďování údajů zahrnovalo i údaje o obsahu, což využilo hned několik zpravodajských služeb. Poukazuje na otázky, které po odhalení zpravodajských aktivit vyvstaly. Dále autor mapuje vývoj pojmu hacker, uvádí jednotlivé případy hacktivismu a politického využívání internetu z nedávné minulosti. Ocenit lze zmínku o uzavírání počítačové architektury, když původní počítače byly ve svém základě otevřené, jejich účel nebyl determinován a zakódován do technologie. Naopak nová zařízení nám umožňují mnohem větší kontrolu a bezpečnost, byť likvidují právo na soukromí v digitální době.

V rámci podkapitoly zabývající digitální měnou a kryptoměnou se z převážné většiny věnuje krypotoměně bitcoin, která existuje vedle 740 dalších kryptoměn. Autor

srozumitelně vysvětluje podstatu bitcoinu, jeho výhody i nevýhody, definici, srovnání s již zavedenými systémy, jakož i jeho vytěžování a hodnoty digitální měny v průběhu času.

Zejména o vyhledávači pojednává podkapitola deep web a dark web s konkrétními příklady při obchodování na černém trhu. Zcela okrajově a z mého pohledu ku škodě recenzované publikace autor řeší internet věcí. Lze souhlasit s tvrzeními, že v současné době jsou zabudovány senzory do různých předmětů a zařízení pro každodenní používání, které společně komunikují prostřednictvím internetu. Vyvstávají tedy nové otázky spočívající ve vymezení osobních údajů, otázkami anonymizace a nových algoritmů. Zajímavým poznatkem pro mě bylo, že Evropská komise v akčním plánu uváděla, že 80 % evropských domácností bude mít do roku 2020 chytré odečty elektřiny a s tím související i nově vznikajícími problémy se ztrátou soukromí. Nová chytrá zařízení tak s sebou přináší nová úskalí pojící se k ochraně soukromí a osobních údajů.

Monografie je psána stručně, avšak obsahuje zejména dostatečné informace pro navození představy a ponoření se do problematiky kyberkriminality. Čtenář tak není přehlcen informacemi a ze studia publikace si odnáší relevantní a základní poznatky. Nicméně za nedostatek lze považovat delší časový odstup vydání publikace (2017) od jednotlivých provedených vědeckých výzkumů (např. 2007).