KOLOUCH, J. CYBERCRIME

ZDENĚK JIŘÍ SKUPIN[*]

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC, 522 s. ISBN 978-80-88168-15-7.

CZ.NIC, z. s. p. o., se soustředí na provozování registru doménových jmen a jejich ochranu, vedle toho ale působí jako vydavatel odborné i populární literatury spojené s internetem a informačními technologiemi.[1] Jako svou 14. publikaci vydala v zimě 2016 edice CZ.NIC publikaci autora Jana Koloucha[2] nesoucí název CyberCrime,[3] jejímž cílem je, dle slov autora, shrnout jeho názory a zkušenosti na poli kybernetické kriminality a kybernetické bezpečnosti.

Autor se bezesporu pouští do tématu velmi aktuálního, o čemž svědčí i skutečnost, že na téma kybernetické kriminality a kriminality páchané v oblasti informačních technologií bylo již napsáno mnoho odborné i populární literatury, ať tuzemské, ať zahraniční. Na druhou stranu tato skutečnost klade na autora vyšší nároky, neboť není zajisté žádoucí opakovat stále stejné a mnohokrát zmíněné skutečnosti. S uspokojením musím ale konstatovat, přestože autor v publikaci využívá přepracované části již publikovaných textů a samotná monografie navazuje tématem na autorovo starší dílo Trestně právní ochrana před kybernetickou kriminalitou[4], že samotná publikace působí svěže, nově, neboť do ní autor zapracovává nově

[*] Autor je prezenčním doktorandem katedry trestního práva Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: 392870@mail.muni.cz

[1] Edice CZ.NIC [online]. [cit. 4.3.2017]. Dostupné z: https://knihy.nic.cz/

[2] Autor působí od roku 2003 jako vysokoškolský učitel katedry trestního práva Policejní akademie České republiky v Praze, kde přednáší zejména témata kybernetické kriminality a její prevence.

[3] Přestože je publikace nazvána CyberCrime, je psána česky.

nabyté zkušenosti, revizi svých původních názorů, ale například přidává řadu praktických případů, což umožňuje čtenáři lépe pochopit předkládanou matérii. Zmíněné tak mělo dopad na rozsah publikace, kterou je možno, i vzhledem k jejímu počtu 522 stran, označit za rozsáhlou.

Monografie je určena jak odborné veřejnosti právní, tak odborné veřejnosti zabývající se informačními technologiemi. Bezpochyby ale její hodnotu ocení jak studenti právních i neprávních oborů (jako například informačních technologií a další), tak i širší veřejnost. Zajímavou skutečností pro čtenáře může být i ten fakt, že je publikace poskytována v licenci Creative Commons (CC BY-ND 3.0 CZ) a v elektronické podobě je možné ji stáhnout na stránkách vydavatele zdarma.

Publikace je členěna do sedmi tematických kapitol, autor zvolil postup, jak je u vědeckých prací obvyklé, od obecného ke konkrétnímu. Zprvu tak ustanovuje a vykládá obsah pojmů, kterých dále v práci využívá a navazuje na ně. V rámci každé kapitoly a podkapitoly je pro zjednodušení uchopení matérie čtenářem uveden rozsáhlý výčet příkladů. Vhodně je zvolena i vazba na právní předpisy a jiné významné dokumenty, ať národní či mezinárodní. Zkušenosti autora v oblasti se projevují i tím, že ve většině kapitol uvádí své vlastní názory, a to i v kapitolách čistě popisných a definičních, zároveň tyto konfrontuje s názory ostatních autorů, což je bezpochyby přínosné i pro čtenáře, který si může vytvořit širší obraz o probírané problematice.

První kapitola se nese v duchu definic a pojmů. Autor seznamuje čtenáře s pojmem kybernetické trestné činnosti, kterou zasazuje do historických, mezinárodních i národních souvislostí. Kriticky přistupuje k definicím kybernetické kriminality a sám se snaží co nejpřesněji charakterizovat předkládaný pojem. Svůj výklad podporuje celou řadou konkrétních příkladů. Na samotný pojem kybernetické trestné činnosti navazuje podkapitolou souvisejících pojmů, která se nese v obdobném duchu jako podkapitola předchozí. Čtenáře tak seznamuje například s kyberprostorem a jeho specifiky. Vše zmíněné obohacuje o vlastní názory. Dále vysvětluje pojmy jako

[4] Publikaci autor napsal společně s JUDr. Petrem Voloveckým, Ph.D., vyšla v roce 2013 a její rozsah byl 117 stran, tudíž autor současnou publikaci výrazným způsobem rozšířil.

kybernetický útok, počítač, hardware, software atd. V následujících podkapitolách je čtenář seznámen s počítačovými sítěmi, jejich dělením, Internetem, souvisejícími technickými poznatky a poskytovatelem internetových služeb.

U první kapitoly je z formálního hlediska nutno vyzvednout přehlednost a věcnost, autor se nepouští do složitých souvětí či obratů, což umožňuje i čtenáři, který se neorientuje v oblasti informačních technologií, pochopit základní principy a funkce předkládaných pojmů. Z obsahového hlediska je nutno ocenit autorovu snahu zasadit vysvětlované pojmy do právního rámce. I přestože je kapitola ryze popisného charakteru, lze sledovat tendence o doplnění definic na základě vlastního výzkumu a zkušeností.

V druhé kapitole se autor soustředí na právní regulaci kyberprostoru, zejména zda a jakým způsobem regulovat tento virtuální svět a úskalí spojená s touto problematikou, což prezentuje na reálných příkladech. Zdůrazňována je problematika globálnosti internetu a omezení dopadu a působnosti národních právních úprav v jiných státech, zvláště pak při jejich rozdílnosti, nebo také problematika uchopení internetu tuzemským právem. Rozsah podkapitol vztahujících se k prostředkům ochrany jednotlivými právními odvětvími českého práva v případě odpovědnostních vztahů za protiprávní jednání v rámci internetu je spíše sporadický, ale umožňuje v hrubých rysech alespoň čtenářovu základní orientaci v matérii (pro účely a zaměření publikace se jedná o dostatečné rozpracování). Důraz je kladen na podkapitoly o poskytovatelích služeb informační společnosti a o odpovědnosti uživatelů. Autor neopomíná zmínit ani právní úpravu, a to jak na národní úrovni, tak na úrovni unijní. Vše doplňuje pro lepší orientaci grafickým znázorněním za pomocí diagramů.

Druhá kapitola se nese v duchu zasazení tématu do právního rámce, první část kapitoly obsahuje obecnou úpravu, kterou zejména ocení čtenáři bez právního vzdělání. Druhá část kapitoly poté přechází k úpravě speciální, založené na základě zákona o některých službách informační společnosti[5], příslušných směrnicích a judikaturních rozhodnutích Soudního

[5] Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů

dvora EU. V této části monografie lze sledovat výraznější právnickou mluvu a projev, což čtenáři bez právnického vzdělání může způsobovat mírné potíže, zejména v případě odborných právních termínů, avšak tuto skutečnost autor vyvažuje tím, že vhodně využívá poznámkového aparátu k případnému vysvětlování problematických skutečností a pojmů.

Třetí kapitola se nese znovu v duchu technického rázu, autor se v ní zaměřuje na anonymitu uživatele. Varuje čtenáře před shromažďováním informací o uživatelích aplikacemi (příp. třetími stranami), riziky a hrozbami s tím spojenými. Prostřednictvím tohoto seznamuje čtenáře s digitální stopou. Zároveň na různých příkladech demonstruje možnosti zjištění identity uživatele. Autor se v kapitole nesoustředí pouze na uživatele počítačů, ale i na uživatele smartphonů, tabletů, atd. Např. rozsah a druh sbíraných informací o uživateli autor prezentuje na příkladu společnosti Google Inc. V dalších podkapitolách se autor věnuje sociálním sítím a projektům, které jako pedagog společně se svými studenty v oblasti zjištění důvěry, přístupu k datům a informacím, chyb a útoků na uživatele sociálních sítí realizoval.

Třetí kapitola má bezpochyby svůj přínos a čtenáře zajisté zaujme skutečností, že autor publikuje vlastní výzkum a jeho výsledky, který společně se svými studenty provedl na sociální síti Facebook. Upozornil v něm na chyby a nedostatky, kterých se uživatelé těchto sítí dopouští, zároveň zdůraznil nebezpečí hrozící příslušným uživatelům, na což navazuje sérií doporučení při pohybu na sociálních sítích.

Nejrozsáhlejší je kapitola čtvrtá o projevech kyberkriminality. Autor v ní rozpracovává některé její druhy a jednotlivé projevy uvádí v příkladech, seznamuje tak čtenáře například s malwarem, spamem, phishingem, hackingem, crackingem, nebo také internetovým pirátstvím, krádeží identity, kyberterorismem a dalšími.

Čtvrtá kapitola pokračuje v nastoleném trendu, tedy tak, že příslušný výklad je proložen řadou příkladů a diagramů. Čtenář zajisté ocení řadu rad, více či méně konkrétních, jak zvýšit svou bezpečnost při pohybu

v kyberprostoru. Přínosná je i vazba na zákonná ustanovení trestního zákoníku[6].

V páté kapitole autor rozpracovává podrobněji trestněprávní ochranu před kyberkriminalitou, kterou započal již v kapitole druhé. Kapitolu tak lze rozdělit na tři části. První část sestává z podkapitol, které výčtovou metodou seznamují čtenáře s obsahem Úmluvy o kyberkriminalitě[7] a jejím protokolem, obojím přijatým na poli Rady Evropy. Poté následuje výčet nařízení a směrnic přijatých v rámci Evropské unie a výčet národních předpisů. Druhá část kapitoly se zaměřuje na podrobnější rozpracování jednotlivých ustanovení trestního zákoníku souvisejících s kyberkriminalitou. Vše je uváděno v rámci dopadu mezinárodní unijní úpravy. Třetí část se věnuje trestněprávní analýze výzkumů sdružení CZ.NIC v oblasti bezpečnostních testů počítačových sítí.

Druhá část páté kapitoly se nese v duchu komentáře příslušných skutkových podstat, i když v některých případech doplněných o autorovy názory a domněnky. Skutečnost, že vše autor doplňuje řadou příkladů, nenapomáhá tomu, aby zmíněná část nepůsobila jako komentářová literatura. Na druhou stranu, třetí část kapitoly přináší pohled na to, zda se sdružení CZ.NIC při svých výzkumech může dopouštět porušování předpisů trestního práva, a přikládá případná doporučení. Autor v této části provádí vlastní výzkum, který může čtenář využít, nachází-li se v obdobné pozici jako CZ.NIC.

Šestá kapitola se zaměřuje na oblast trestního práva procesního a kriminalistiky při odhalování, prověřování a vyšetřování kyberkriminality. Čtenář je zprvu seznámen s obsahem důležitých pojmů a specifiky důkazů a důkazních prostředků v prostředí kyberprostoru, a poté s postupem v přípravném řízení trestním, jak orgánů činných v trestním řízení, tak oznamovatele trestního činu, příp. poškozeného.

V kapitole je zejména nutno ocenit autorův přínos na poli poskytování rad čtenáři, jakým způsobem postupovat při podávání trestního oznámení,

[6] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník“)

[7] Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb., sjednání Úmluvy o počítačové kriminalitě

náležitosti podání, aj., nebo rad pro orgány činné v trestní řízení, jak modifikovat dokazování na oblast kyberkriminality, atd.

V sedmé a zároveň poslední kapitole se autor věnuje, jak je u obdobných prací obvyklé, návrhům *de lege ferenda.* Navazuje tak na již prezentované názory z předchozích kapitol, které rozpracovává a doplňuje. Kapitola je rozdělena na část hmotněprávní a část procesní. V části hmotněprávní navrhuje úpravu skutkových podstat, případně zavedení nových skutkových podstat, pro jednotlivé projevy kyberkriminality. Zároveň k tomu přidává vlastní paragrafové znění navrhované úpravy. V části druhé, věnované procesněprávní problematice, autor navrhuje implementaci institutů z Úmluvy o kyberkiminalitě, k tomu také doplňuje své znění příslušných paragrafů.

Závěrem je nutno zmínit jednu poznámku, a to že publikace je vydána k právnímu stavu ke dni 1. 8. 2016, což se projevuje ve čtvrté kapitole u kyberterorismu, jelikož není zohledněna novela trestního zákoníku č. 455/2016 Sb., která významnou měrou zasahuje a upravuje terorismus a přidruženou problematiku.
