SMEJKAL, V. KYBERNETICKÁ KRIMINALITA

MIROSLAV UŘIČAŘ[*]

SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Nakladatelství Aleš Čeněk, 2015, 636 str. ISBN 978-80-7380-501-2.

Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. se kromě klasické právnické literatury stále více profiluje jako vydavatelství děl z oblasti kriminalistiky. Pod vedením jedné z nejuznávanějších osobností tohoto oboru, prof. JUDr. Ing. Viktora Porady, DrSc., zde vyšla díla jako Kriminalistika (teorie, metody, metodologie), Kriminalistika (výzkum, pokroky, perspektivy) nebo Kriminalistika - Kriminalistická taktika a metodiky vyšetřování, bez nichž by tento vědní obor nebyl dokonale popsán.

Obdobně významné dílo, tentokráte coby průnik trestního práva a kriminalistiky na straně jedné a informačních technologií na straně druhé nyní v nakladatelství vydal prof. Ing. Vladimír Smejkal, CSc., LL.M., jeden ze zakladatelů oboru IT právo a IT kriminalistika v České republice, dlouholetý vysokoškolský pedagog a soudní znalec.

Kniha poměrně velkého formátu (B5) o celkem 636 stránkách názorně ukazuje, co vše lze napsat o kriminalitě spojené s počítači a počítačovými sítěmi. Dnes, kdy se informační technologie nacházejí prakticky v každém předmětu nejen v zaměstnání, ale i v domácnostech, to ovšem není nikterak překvapivé. Nemluvě o tom, že bezpečnost IS/IT je dnes jedním z nejčastěji skloňovaných pojmů, a to nejen v souvislosti s útoky hackerů páchajících

[*] Mgr. Miroslav Uřičař je ředitelem úseku práva, regulace, vnějších vztahů a bezpečnosti společnosti T-Mobile Czech Republic a.s. a předsedou legislativní komise České asociace pro soutěžní právo. Je dále členem představenstva Asociace provozovatelů mobilních sítí, členem výkonné rady UNICEF ČR a působí jako rozhodce Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky.

trestnou činnost v kyberprostoru, zcela běžně se již hovoří o kyberútocích vedených teroristickými skupinami a dokonce státy.

Zejména v tomto shledávám vysokou prospěšnost a výborné načasování díla prof. Smejkala, neboť otázka kybernetické kriminality je dnes jednou ze stěžejních otázek pro celé lidstvo. Nemusí totiž nastat výpadek dodávek elektrické energie; stačí jen když kyberteroristé zaútočí na elektronická zařízení (a data v nich) pomocí systémů typu HERF (high energy radio frequency) a EMPT bomby (electromagnetic pulse transformer) a zničí elektronické obvody v nich.

Autor v díle shrnul výsledky svého dlouholetého působení (v předmluvě uvádí, že první článek na toto téma publikoval s doc. JUDr. Martinem Vlčkem, CSc. již v roce 1988) jak v oblasti trestněprávní a kriminalistické teorie, tak i vlastní obsáhlé praxe, kdy se podílel jako znalec na vyšetřování nejzávažnějších případů počítačové kriminality u nás.

O čem tedy pojednává dílo nazvané *Kybernetická kriminalita*? Měli jsme zde kriminalitu počítačovou a ve svém předchozím díle, *Právo informačních a telekomunikačních systémů* prof. Smejkal zavedl termín „informatická kriminalita“. Nutno říci, že termín „počítačová kriminalita“ odpovídá zahraničnímu „computer crime“ a dlouho se držel v čele používané terminologie. Dnes se stejně často používá označení „kybernetická kriminalita“, a to jako synonymum. Pravdou je, že Smejkalův pojem „informatická kriminalita“ se příliš neprosadil, neboť vytváří dojem, že se jedná spíše o kriminalitu informatiků, nežli spojenou s informačními systémy. Přesto zřejmě bude mít pravdu, když vnímá kriminalitu kybernetickou jako něco komplexnějšího, nežli počítačovou. Je tomu tak, že kyberprostor (autor s ním pracuje zpočátku jako s notorietou a definuje jej až na straně 93) klade větší důraz na nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů nebo chceme-li, počítačů a počítačových sítí.

Autor přistoupil ke zpracování tématu klasickým vědeckým způsobem – od obecného (definice počítačové kriminality, kyberprostoru, kyberterorismu apod.) ke zvláštnímu (zevrubný popis jednotlivých skutkových podstat včetně forem a způsobů páchání trestných činů a detailního rozboru jednotlivých částí jejich definic podle trestního zákoníku). Vždy pak následuje obsáhlá judikatura, přičemž autor na rozdíl

od obvyklého způsobu prezentace judikatury neuvádí pouze právní větu, ale vybral ve většině případů i relevantní části odůvodnění, resp. parafrázoval je coby popis případu, vysvětlující čtenáři, oč v dané věci šlo a jaká byla geneze v rámci rozhodování zúčastněných soudů všech stupňů. Užitečnost tohoto přístupu zvyšují i vlastní komentáře autora, které hodnotí, zobecňují nebo naopak rozporují soudní rozhodnutí, zejména v kontextu s jinými, obdobnými případy.

Ještě před tento výklad ale autor předřadil kapitolu první, která je jakýmsi vysvětlujícím a definičním textem terminologie z oblasti ICT. Vysvětlujícím, aby text mohli bez problémů zvládnout i ti právníci, kteří nemají příliš vřelý vztah k moderním informačním technologiím. A definičním proto, aby IT odborníci vnímali, jak se s daným pojmem pracuje prismatem právních a technických norem. Najdeme zde definice základních stavebních kamenů kyberprostoru, jako jsou počítače (HW, SW), data, informace a informační systémy, počítačové sítě, Internet a dálkový přístup. Proto nejsou čtenáři, jejichž světem není IT, ale spíše soudní síně, ponecháni na pospas nesrozumitelné terminologii.

Těžiště výkladu představuje 460 stran kapitoly druhé nazvané *Kriminalita v prostředí informačních systémů a na Internetu.* Najdeme zde takové činy jako např. sabotáže, teroristické útoky a obecné ohrožení, poškození obecně prospěšného zařízení či cizí věci, neoprávněné užívání ICT zařízení, podvody, poškození cizích práv, či vydírání. Značná pozornost je věnována trestné činnosti spočívající v získávání a šíření informací. Zde autor popisuje sociální sítě, zabývá se odpovědností za obsah, ústavními základy ochrany soukromí a osobních údajů a konkrétní ochranou obsahu v sítích elektronických komunikací a osobních údajů. V rámci jednotlivých skutkových podstat je uvedeno neoprávněné nakládání s osobními údaji, šíření pornografie a dětská pornografie, porušování tajemství dopravovaných zpráv a dokumentů uchovávaných v soukromí, ohrožení utajované informace, vyzvědačství, šíření poplašné zprávy, nebezpečné vyhrožování a pronásledování (stalking), manipulace s kurzem investičních nástrojů, nekalá soutěž) a další možné trestné činy související se šířením informací.

Následující část kapitoly je věnována nehmotným statkům a duševnímu vlastnictví – průmyslovým a autorským právům. Velmi podrobně jsou

popsány výslovně počítačové trestné činy, jak jsou definovány v ust. § 230 – *Neoprávněný přístup k počítačovému systému a nosiči informací*, § 231 – *Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a* § 232 – *Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.*

Závěr druhé kapitoly tvoří ostatní trestné činy související s počítači, kde autor uvádí neoprávněné opatření, padělání a pozměnění platebního prostředku, výrobu a držení padělatelského náčiní, padělání a pozměnění veřejné listiny, zkreslování údajů o stavu hospodaření a jmění, poškození finančních zájmů Evropské unie, vývoz zboží a technologií dvojího užití a zahraniční obchod s vojenským materiálem. Souhrnně by se dalo říci, že prof. Smejkal provedl analýzu všech trestných činů podle platného trestního zákoníku a zamýšlel se nad možným výskytem počítače jako souhrnu technického a programového vybavení včetně dat, případně většího množství počítačů propojených do počítačové sítě, a to jako předmětu nebo jako nástroje trestné činnosti. Činil tak tedy zjevně v souladu s definicí počítačové kriminality, nacházející se na str. 20 knihy.

Je nutno ocenit pozornost, kterou autor věnoval jednomu z nejvýznamnějších fenoménů dneška – kyberterorismu, který ovšem zcela správně vnímá šířeji, a to vzhledem k naplnění dalších skutkových podstat s tímto jednáním souvisejících, jako jsou poškození a ohrožení provozu obecně prospěšného zařízení a poškození cizí věci. Tuto problematiku pojal autor značně do hloubky – od darkingu a phreakingu přes hackery a crackery až po kyberteroristy. V knize je navíc stručně popsán i zákon o kybernetické bezpečnosti, který nabyl účinnost těsně před jejím vydáním.

Třetí kapitola *Odhalování a vyšetřování kybernetické kriminality* nás z oblasti trestního práva přesouvá do kriminalistiky a jejích metod. Zde se autor zabývá kriminalistickou metodikou a expertizou v oblasti počítačové kriminality, přičemž značnou pozornost věnuje důkazům, dokazování a digitálním stopám. Ještě zajímavější je ale část, v níž prof. Smejkal popisuje hlavní současné problémy při odhalování a dokazování kybernetické kriminality: jsou to podle něj problém jurisdikce, problém odhalování trestné činnosti, problém dokazování a problémy související s dalším možným vývojem kyberkriminality. Jsou zde také popsány jednotlivé fáze trestního řízení a jejich specifika v souvislosti

s kybernetickou kriminalitou: od prověřování před zahájením trestního stíhání, přes vyšetřování a dokazování v prostředí ICT. Tato kapitola obsahuje i informace o pachatelích kybernetické kriminality a jejich nejčastějších motivech.

Zatímco v předchozích kapitolách nejdeme některé myšlenky, které již autor publikoval dříve, byť v méně propracované formě, čtvrtá kapitola *Prognóza dalšího vývoje kybernetické kriminality* soustředila velké množství nových, originálních informací a úvah autora. Lze ji v zásadě rozdělit do několika tematických oblastí. Jako první zde najdeme další úvahy o možnostech postihu útoků DoS/DDoS v rámci českého právního řádu; je otázkou, zda neměly být součástí výkladu již dříve k ust. § 230, ale faktem je, že aplikace tohoto ustanovení není zcela jednoznačná a autor zde diskutuje možnost postihu napříč celým trestním zákoníkem. Recenzent se nicméně přiklání k tomu, že odpověď na otázku, zda takové jednání vůbec stíhat a pokud ano, pak zda se snažit aplikovat § 228, § 230 nebo některá jiná ustanovení – za určitých okolností např. o nekalé soutěži – se zatím ještě vyvíjí a nemá tedy finální podobu.

Druhá část kapitoly je věnována virtuálním světům a virtuální kriminalitě. Je třeba ocenit, že autor nesklouzl k často používanému, leč chybnému ztotožnění kyberprostor = virtuální svět, který definuje jako „počítačově implementovaná simulovaná prostředí, která se nacházejí v prostředí kyberprostoru“. Především je však třeba ocenit, že zde diskutuje různé aspekty virtuality, jako jsou virtuální vlastnictví a virtuální majetek a jejich interakce se světem reálným. Dochází zde k závěru, že objekty ve virtuálním světě jsou produkty, které se za určitých okolností mohou stát zbožím, majícím svou tržní a směnnou hodnotu (cenu). Proto poměrně logicky navazuje další podkapitola, zabývající se virtuálními měnami, a to zdaleka ne pouze nejznámějšími z nich, tj. bitcoiny. Nejzajímavější je to, co uvádí hned na počátku: „*Ve skutečnosti ale hodnota peněz je dána především důvěrou uživatelů v ně, přičemž současné měny jsou tzv. fiat měny, tj. peníze existují na základě rozhodnutí státu (právních předpisů) a žádný stát ani centrální banka dnes nebude peníze vyměňovat za zlato ani za žádné jiné aktivum, a to přes různá oficiální tvrzení, mnohdy surrealistického charakteru.*“. Logicky z toho vyplývá závěr, že mohou existovat soukromé peníze a že démonizace virtuálních měn, zejména pak tzv. kryptoměn, mezi které patří

i bitcoiny, není zcela na místě. A to přesto, že vzhledem k jejich vlastnostem lze předpokládat, že budou existovat pokusy, jak využít virtuální měny pro páchání nejrůznější trestné činnosti, jako např. praní špinavých peněz, daňové úniky včetně online sázek, financování terorismu, nákupy drog, možná i podvody a jiné. Autor dále krátce zmiňuje virtuální sex a popisuje vizi roku 2050, kdy se sexuální robot/robotka více či méně chová jako reálný partner/partnerka a kdy místo prostitutek budou sexuální služby poskytovat roboti – androidi pod kontrolou magistrátu. Další část je věnována virtuální a skutečné kriminalitě ve virtuálním světě, tedy klasické kriminalitě ve vztahu k virtuálnímu prostoru a naopak. Podle prof. Smejkala již můžeme hovořit o vzájemném prolínání reálného a virtuálního světa i v oblasti kriminality, resp. trestního postihu. V další části kapitoly jsou zmiňovány nové aspekty IT/IS, které se začínají promítat do reálného života, a tedy i do trestní oblasti. Patří sem 3D tisk, který, přes své nesporné přínosy, může usnadňovat porušování práv duševního vlastnictví, ale i jiné trestné činy, např. nedovolené ozbrojování. V rámci dalšího předpokládaného vývoje kybernetické kriminality uvádí autor také další možné formy jednání: útoky na technologické řídicí systémy (SCADA a ICS), útoky prostřednictvím sociálních sítí a vysoká rizika spojená s tzv. Internetem věcí a BYOD (Bring Your Own Device) neboli používání vlastních zařízení ve firemním prostředí. Poněkud nesystematicky je sem zařazena i část věnovaná odpovědnosti za škodu způsobenou provozem nezabezpečeného informačního systému; je však otázkou, kam jinam toto téma, které rovněž souvisí s trestnou činností, zařadit.

Závěrečná část čtvrté kapitoly je věnována opět vysoce aktuálnímu tématu, kterým je střet mezi anonymitou a ochranou soukromí na Internetu. Zde autor diskutuje otázku prolamování ochrany soukromí, odposlechy a monitorování služeb elektronických komunikací a lokalizačních údajů jako součást boje proti trestné činnosti, samozřejmě nikoliv toliko kybernetické. Popisuje snahy států o prolamování ústavních práv občanů spočívající v povinnosti poskytnout státním orgánům svá vlastní hesla či šifrovací klíče, což podle autora představuje porušení zákazu sebeobviňování, resp. zákazu donucování k poskytnutí důkazů proti sobě samému. Uvádí, že nejvíce byla tato ochrana prolomena překvapivě ve Spojeném království Velké Británie a Severního Irska, kde podle zákona

RIPA (Regulation of Investigatory Powers Act) je možné vynutit vydání kryptografických klíčů nebo zpřístupnění požadovaných materiálů. Poněkud překvapivé, uvědomíme-li si, že jde o zemi, která byla jednou z prvních, jež ve svém právním řádu nastavila ochranu jednotlivce (Magna charta libertatum v roce 1215). Přitom podle Evropského soudu pro lidská práva patří právo nevypovídat a právo nepřispívat k obvinění proti sobě samému k obecně uznávaným mezinárodním principům.

V závěru svého obsáhlého díla prof. Smejkal zmiňuje další technologické novinky, které se mohou dostat do rozporu s ochranou soukromí nebo dalšími zájmy chráněnými podle trestního zákoníku. Uvádí zde „chytré šaty“ a šperky, monitorující životní pochody nositelů, létající roboty – drony, mikrominiaturní roboty (velikosti až mikroorganismů) a zdůrazňuje, že čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití musíme, bohužel, počítat.

Kniha *Kybernetická kriminalita* je zpracována na vysoké odborné úrovni, současně však velice přehledně a srozumitelně. Je obdivuhodnou syntézou oborů práva, kriminalistiky a informačních technologií a lze ji tedy doporučit čtenářům působícím ve všech těchto oblastech. Zcela samozřejmě by se měla stát základním zdrojem informací právníků všeho druhu – podnikových právníků nejen v IT firmách, advokátů, zaměstnanců orgánů veřejné moci, ale i osob působících v orgánech činných v trestním řízení, jako jsou policisté, státní zástupci, soudci. Nepostradatelnou bude i pro manažery IS/IT, specialisty na bezpečnost – od správců po auditory. Vysoce užitečná je pro výuku na všech typech vysokých škol, od právnických až po manažerské a informatické.