RECENZE

Smejkal Vladimír. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015, 636 s.

Loňského roku spatřila světlo světa mimořádně zdařilá rozsáhlá publikace o kybernetické kriminalitě. Autorem je *Vladimír Smejkal*, známý odborník v této oblasti a soudní znalec. Třeba říci, že obsáhlá kniha (636 stran) představuje literární završení dosavadních autorových odborných prací počínaje koncem 80. let. Kniha se tak stává zásadní literaturou, která by neměla chybět nikomu, kdo se zabývá trestním právem, ale i kriminalistickými technikami, forenzními disciplínami apod. Zejména mám na mysli orgány činné v trestním řízení, ale i advokáty, znalce apod. Autor patří mezi průkopníky oboru počítačového práva u nás. Dnes ale věcně správně již nehovoří o „počítačovém právu" či o „počítačové kriminalitě", nýbrž o „kriminalitě kybernetické", chápané v širokém pojetí kyberprostoru, zejména sítí elektronických komunikací. Změna názvu tak vystihuje i poslední věcný vývoj a jeho směřování. Srovnej například různé společenské sítě, elektronickou poštu apod., kde i sám pojem a význam počítače je tak trochu upozaděn (a zejména chápán velmi široce, vícefunkčně, včetně tzv. chytrých mobilních telefonů, tabletů apod.). Recenzovanou knihu můžeme řadit do poměrně širokého rámce prakticky uchopeného víceodvětvového oboru práva informačních a komunikačních technologií, pokud o jeho veřejnoprávní část a mimoprávní přesahy technické.

Po stránce obsahové kniha zahrnuje veškeré možné oblasti i témata, která se týkají kybernetické kriminality nebo širšího pojetí kyberprostoru samého. V úvodu jsou podrobně vysvětleny základní pojmy včetně různých definic, začasto ryze technických. Druhá kapitola je již věnována kriminalitě v prostředí informačních systémů a na internetu včetně jejích různých podob. Dozvíme se tak o kyberterorismu, kybernetickém bezpečí včetně poměrně nové české zákonné a podzákonné úpravy. Velmi podrobně jsou komentovány jednotlivé skutkové podstaty trestního zákoníku, které se týkají zvoleného tématu práce. Uváděny jsou přehledy judikatury včetně obsáhlých citací právních vět nebo částí celých rozhodnutí, což poskytuje čtenáři i jistý druh komfortu (skutečný odborný servis po ruce). Další kapitola je zaměřena na odhalování a vyšetřování kybernetické kriminality. Zabývá se například kriminalistickou expertízou, jednotlivými důkazy a dokazováním vůbec. Dovíme se mnohé i z kriminalistické historie daného oboru, která je přitom mladá. Do této kapitoly patří i relativně samostatná část o znalcích v režimu zákona o znalcích a tlumočnících. Zde musím, na okraj recenze, kriticky poukázat na znalecké postavení Kriminalistického ústavu, který spadá pod Policii České republiky, což není vhodné z hlediska možných pochyb o znalecké nezávislosti na policejních orgánech činných v trestním řízení. Kriminalistickému ústavu by slušela právní samostatnost, tzn. alespoň formální (ale i materiální) odloučení od policejních orgánů, služebních postupů apod. Různé právní formy právnických osob by se k tomu nabízely. Jedná se ovšem o politické (i finanční) rozhodnutí, které je v rukou Ministerstva vnitra. Nemalou část knihy zahrnuje prognóza dalšího vývoje kybernetické kriminality, která se týká i elektronických peněz a jiné „měny". Autor se zaobírá i právní povahou bitcoinů, které nesplňují veřejnoprávní měnová ani peněžní kritéria. Otázkou zůstává, zda a nakolik bychom vůbec mohli hovořit o pohledávkách na peněžní plnění. Bez ohledu na hospodářský význam. Jedná se „jen" o hru (§ 2881 o. z.)? Některé podobné otázky by si ještě vyžádaly podrobnější právní, zejména soukromoprávní, rozbory, zvláště z pohledu herního práva.

Výklad autora je koncipován ve stylu historie, současnost a budoucnost kybernetické kriminality. Veden je od obecného (definice) ke zvláštnímu (zevrubný popis jednotlivých skutkových podstat včetně forem a způsobů páchání trestných činů, které představují naplnění skutkových podstat kybernetické kriminality, nebo se vyskytují v souběhu s nimi.) Autor se ale neomezuje pouze na jednání, které je podřaditelné pod „kyberparagrafy", ale systematicky probírá všechna ustanovení zvláštní části trestního zákoníku, která komentuje z hlediska jejich možného vztahu k moderním informačním technologiím. Nalezneme zde skutky, které bychom zřejmě předpokládali (neoprávněné nakládání s osobními údaji, šíření a držení pornografie nebo porušování autorských práv). Daleko zajímavější je ale výklad toho, jak se skutkově i právně promítají informační a komunikační technologie do poškození a ohrožení provozu obecně prospěšného zařízení či cizí věci obecně, jaká může být trestná činnost spojená se získáváním a šířením informací nebo další trestné činy související s počítači; např. neoprávněné opatření, padělání a pozměnění platebního prostředku nebo vývoz zboží a technologií dvojího užití. Nejvíce je zřejmě třeba ocenit pozornost, kterou autor věnoval dnes nejpalčivější a nejaktuálnější problematice – kyberterorismu a asymetrickým hrozbám.

Každá podkapitola rozebírající jednotlivé skutkové podstaty je doplněna obsáhlou citací aktuální judikatury; zde autor neuvádí pouze právní větu, ale tam, kde to je účelné, zahrnul do textu i podstatné části odůvodnění soudního rozhodnutí. Judikaturu také opatřil vlastními poznámkami, které zaujímají stanovisko k průběhu věci anebo k vlastnímu rozhodnutí.

Neméně významná je další část knihy, která se zabývá metodologií odhalování a vyšetřování kybernetické kriminality. Autor vychází z vlastních rozsáhlých zkušeností, neboť se podílel na vyšetřování mnoha případů kybernetické kriminality. Jeho typologie pachatelů kybernetické kriminality a jejich motivace je proto podložena empirickými poznatky. Významná kapitola v této části je věnována problematice kriminalistické expertizy v oblasti kybernetické kriminality. Popsány jsou zde jednotlivé fáze trestního řízení a jejich specifika v souvislosti s kybernetickou kriminalitou, jakož i zvláštní charakter důkazů a dokazování v prostředí informačních technologií.

Od současnosti se ve čtvrté části knihy, nazvané *Prognóza dalšího vývoje kybernetické kriminality*, čtenář přesune do budoucnosti, kterou autor nevidí jako příliš vzdálenou a na podporu svých tvrzení uvádí skutečné případy, které se již odehrály. Nejedná se ale, jako konečně nikde v tomto díle, o „sběr zajímavostí z internetu", ale opět o systematicky koncipovaný výklad. Začíná úvahou o možnostech postihu útoků typu DoS/DDoS, s nimiž se potýkal náš stát před rokem, v rámci českého trestního zákoníku. Ještě zajímavější je následující část, zabývající se pojmy jako virtuální svět a virtuální kriminalita. Autor zde rozebírá různé aspekty virtuality, jako jsou virtuální vlastnictví a virtuální majetek a jejich interakce se světem reálným. Virtuální svět definuje jako „*počítačově implementovaná simulovaná prostředí, která se nacházejí v prostředí kyberprostoru*". Dále dochází k závěru, že objekty ve virtuálním světě jsou produkty, které se za určitých okolností mohou stát zbožím, majícím svoji tržní a směnnou hodnotu (cenu), což dokládá řadou příkladů. Nelze se proto divit, jestliže se v návaznosti na virtuální majetek v další části přesuneme k virtuálním měnám, což není pouze známý *bitcoin*. Profesor *Smejkal* definuje peníze veřejné a soukromé, upozorňuje na to, že dnešní veřejné (státní) 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*". Od toho logicky dochází k závěrům, že mohou existovat soukromé peníze a peníze virtuální. Protože kniha je zaměřena především na trestnou činnost, autor neopomíná upozornit na to, s čím se již dnes stále více setkáváme, tj. že tzv. kryptoměny mohou být užívány pro podporu a páchání trestné

činnosti, zejména pak praní špinavých peněz, daňové úniky včetně sázek online, financování terorismu, nákupy nelegálního zboží apod. Závěr této části je věnován novým technologickým jevům, které budou mít podle autora nepochybný vliv na zvýšení rizika v kyberprostoru a vytvoří další živnou půdu pro kybernetický zločin. Jsou to dnes tak populární cloudy, internet věcí anebo útoky na technologické řídicí systémy (od elektráren a pecí až po řízení letového provozu). Autor zdůrazňuje, že čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším nebezpečím zneužití musíme počítat.

V poslední kapitole najdeme i další témata, která nějakým způsobem s kybernetickým zločinem a kybernetickou bezpečností souvisí. Jsou to odpovědnost za škodu způsobenou provozem nezabezpečeného informačního systému, střet mezi anonymitou a ochranou soukromí v prostředí zejména internetu, včetně stále sílících pokusů různých států, označovaných jako demokratické, nejen sledovat veškerou komunikaci občanů jako takovou, ale i dalších kroků, jako je např. povinnost poskytnout hesla či šifrovací klíče. Autor recenzované práce toto chápe jako porušení zákazu sebeobviňování, respektive zákazu donucování k poskytnutí důkazů proti sobě samému.

Recenzovaná publikace do značné míry představuje až téměř encyklopedický souhrn všeho podstatného, co se jejího záběru týká. Můžeme ji používat i jako dílčí komentář k vybraným částem trestního zákoníku, které věcně souvisí nebo v praxi mohou alespoň potenciálně souviset s kybernetickou kriminalitou. Zároveň autor dílem proniká i do jiných právních oblastí, jako je zejména autorské právo nebo právní ochrana před nekalou soutěží na trhu. Užitečné jsou kupříkladu mnohé srovnávací tabulky, byť v nich autor nemusí přinášet nic nového. Důležité je již samo shrnutí kupříkladu různých definic a jejich vzájemné porovnání, a to i s ohledem na jejich možnou využitelnost v právní praxi (nebo naopak nevyužitelnost).

Na přínosu recenzované knihy nic nemění, že některé dílčí otázky mohou vést k odborným diskuzím. Tak kupříkladu diskuzní může být již sama otázka soukromoprávní povahy internetu neboli sítě elektronických komunikací. Autor dospívá k závěru, že se nejedná o věc v právním slova smyslu, a to ani v podobě veřejného statku určeného k obecnému užívání kýmkoli. Diskuzní může být, zda takováto síť sama o sobě (odmyslíme-li si k ní připojené koncové přístroje, obslužné počítače apod.) je či není ovladatelná. Na rozdíl od autora se domnívám, že síť jako taková (zasítěnost) je „něčím" ovladatelným, ať již signál proniká po kabelu (po drátě), anebo bezdrátově. Vlastnost ovladatelnosti se mi zde technicky jeví jako dokonce příznačná. Jiným znakem by mohlo být, zda se jedná o „přírodní" sílu. V širokém chápaném slova smyslu by sem spadaly veškeré ovladatelné energie včetně různých vln (vlnění). Srovnej též televizní a rozhlasový signál jako takový a kmitočet. Úvaha o tom, že by se v takovém případě mohlo jednat o věc nehmotnou ve smyslu občanského zákoníku, by proto nemusela být zcela od věci. Jinou otázkou by bylo, zda se jedná o veřejný statek určený k obecnému užívání kýmkoli, anebo nikoli, a to za stavu, kdy zde je poskytovatel signálu a jeho příjemce jakožto konkrétní osoby (strany závazku). Otázkou ale je, nakolik je tato záležitost vůbec právně významná. Zda se nejedná jen o „akademické" dělení, kterého ovšem není prost ani sám občanský zákoník, jenž k něčemu takovému dokonce přímo navádí. Jiný předmětový úhel právního pohledu na internet je naopak závazkový. Takovýto pohled víceméně rezignuje na rozdělení věcí z hlediska absolutních majetkových práv (systémově rušené různými atypy) a naopak zdůrazňuje předmět plnění, tedy sám signál jako předmět jeho dodávání. Předmět plnění (signál) tak může být například i vadný. Posledně zmíněný pohled přináší i bezprostřední právní význam z hlediska řádného a včasného (anebo naopak vadného) plnění závazku založeného smlouvou. Při různých diskuzích ohledně nového občanského zákoníku a jeho roztřídění věcí v právním smyslu spíše převážil, poněkud pragmaticky, právě pokud jde o internet, tento poslední právní náhled.

Kromě ryze právních témat se dočteme mnohé z mimoprávních oborů. Právě zde leží největší přínos recenzované publikace, totiž její obsahové prolnutí mezi právem a technikou. Málokterému autorovi a málokdy se něco takového podaří. Srovnej např. výhody a nevýhody *cloud computingu* (strana 56 a násl.). Poznatky tohoto druhu mohou mít bezprostřední vliv i na uzavření určité smlouvy, či nikoli.

Recenzovaná kniha je obsáhlým kompendiem, syntézou právních, kriminalistických a technologických aspektů nelegálních aktivit v kybernetickém prostoru. Jedná se o dílo na vysoké odborné úrovni, které by se mělo stát základním zdrojem informací z této oblasti pro právníky a bezpečnostní manažery.

Závěrem mi nezbývá nežli konstatovat, že recenzovaná publikace nejen shrnuje dosavadní stav poznání na pomezí mezi právem a technickou, ale zároveň jej rozhojňuje. Současně též provokuje k dalším odborným diskuzím. Již proto si zaslouží pozornost.

Ivo Telec*

* Prof. JUDr. Ivo Telec, CSc., Právnická fakulta Univerzity Palackého v Olomouci. E-mail: ivo.telec@upol.cz.