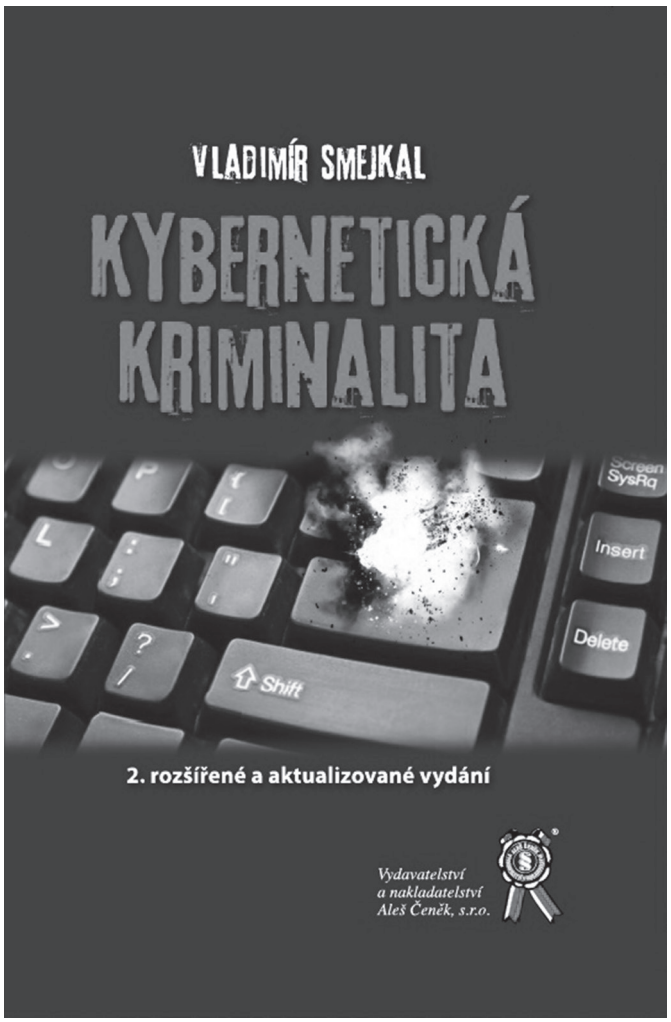
Recenze monografie „Kybernetická kriminalita“

Monograph Review „Kybernetická kriminalita“

Viktor Porada*

SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Nakladatelství Aleš Čeněk, Plzeň, 2018, 936 s.
ISBN 978-80-7380-720-7
Cena 990 Kč, v e-shopu vydavatele 891 Kč



Vědecká monografie prof. Ing. Vladimíra SMEJKALA, CSc., LL.M., DrSc. týkající se problematiky „kybernetické kriminality“, je svým pojetím mimořádně aktuální a systémově zaměřená na stěžejní a rozhodující aspekty této trestné činnosti v jejich komplexnosti, složitosti a širokém dopadu v současné, ale i budoucí kriminalisticko-právní praxi. Její druhé vydání představuje ve značném rozsahu aktualizované a rozšířené vydání monografie “Kybernetická kriminalita“ z roku 2015, a to co se týká jak nových, tak aktualizovaných vědeckých poznatků získaných převážně vlastním výzkumem této problematiky, včetně mnoha poznatků z praxe – zejména co se týká nových forem kybernetické trestné činnosti a judikatury. Obsah recenzované monografie tvoří čtyři na sebe logicky navazující kapitoly:

První kapitola obsahuje popis základních pojmů spojených s počítači, sítěmi, Internetem, virtuálními objekty, sociálními sítěmi, 3D tiskem a dalšími, pro dnešní dobu tak typickými fenomény. Navíc je v této kapitole zařazen odstavec 1.4.3.7, týkající se problematiky: Viditelný Web, Dark Web a Deep Web a zejména pak kapitola 1.5 Od robotů po Společnost 4.0. V ní je popsána problematika robotů – od autonomních systémů řízení vozidel, přes tzv. válečné roboty až po dnes tak módní pojmy, jako jsou Průmysl 4.0, Společnost 4.0, smart city apod. Tento výklad tvoří faktografický podklad k rovněž nové kapitole 4.4 Trestněprávní aspekty robotiky – viz dále.

Druhá kapitola se věnuje problematice kriminality v prostředí informačních systémů a na Internetu. Jsou v ní zařazeny problémy spojené s historií a současností počítačové kriminality a postupně, s velkým přehledem a podrobně rozebrány jednotlivé druhy skutků tak, jak se postupně v praxi a následně v teorii objevily a jak v různých formách v prostředí vymezeném počítačovou, resp. kybernetickou kriminalitou přetrvávají dosud. Výklad je pojat chronologicky – od prvních projevů počítačové kriminality, přes současnost a až po výhled do budoucnosti. Každá skutková podstata, která byla v minulosti, nebo je nyní zařazena do trestního zákoníku a v níž můžeme najít počítač či počítačovou síť jako cíl nebo nástroj útoku, je zde podrobně rozebrána. Podrobně je mj. popsána problematika kyberterorismu, což je zejména nyní téma vysoce aktuální. Nechybí ani problematika, jako jsou zločiny spojené s bitcoiny a virtuální zločiny ve virtuálním prostoru. V této kapitole je nově zařazena zejména problematika kybernetické války, diskutována zákonem zavedená cenzura obsahu sociálních sítí v SRN a zařazen celý blok týkající se ochrany osobních údajů podle GDPR a dalších předpisů EU. Aktualizován byl výklad k řadě dalších skutkových podstat, jako účast na sebevraždě, nekalá soutěž, zneužití informace v obchodném styku a některé další trestné činy související se šířením informací.

Třetí kapitola se zabývá odhalováním a vyšetřováním kybernetické kriminality. Jsou zde definovány digitální stopy a nově digitální důkazy, je uvedená tématika a problémy dokazování (fyzická versus logická přítomnost, čas, čitelnost dat, identifikace a autentizace, pravost důkazu a průkaznost důkazu) a kriminalistické počítačové expertizy. Dále je popsán rovněž postup před zahájením trestního stíhání (prověřování) a poté etapa vyšetřování a dokazování, a to z hlediska specifik souvisejících s vyšetřováním kybernetické trestné činnosti. V závěru jsou uvedeny a diskutovány perspektivy kontroly počítačové/kybernetické kriminality.

Korespondenční adresa: viktor.porada@mail.vsfs.cz

Ve čtvrté kapitole se autor zajímavým způsobem věnuje prognóze dalšího vývoje kybernetické kriminality. Nově jsou zařazeny ve značném rozsahu vysoce aktuální trestněprávní aspekty robotiky. Zde byly zcela poprvé, přinejmenším v České a Slovenské republice, publikovány myšlenky zabývající se deliktní odpovědností, zaviněním, nedbalostním jednáním a příčinnou souvislostí v oblasti trestných činů v robotice. Diskutována je problematika fyzických a právnických osob jako pachatelů „robotické“ kriminality a robot jako oběť trestného činu. nechybí ani dnes nejvíce diskutovaná otázka odpovědnosti za autonomní vozidla, tentokrát ale z pohledu přestupkového a trestního práva.

Autor při zkoumání využívá vybraných poznatků souvisejících vědních oborů, které vhodným způsobem aplikuje na svůj předmět zkoumání a vytváří tak kombinaci poznatků majících významný synergický efekt v zájmu úspěšného odhalování, vyšetřování a předcházení kybernetické kriminality. Publikace obsahuje vlastní zevrubnou analýzu jednotlivých skutkových podstat trestných činů, které souvisí nebo souviset mohou s počítači či celým kyberprostorem.

Monografie se zabývá novými, aktuálními a moderními kriminalistickými, právními a kybernetickými aspekty počítačové/ kybernetické kriminality. Je v ní uvedeno komplexní a unikátní systémové pojetí kriminalistické a právní vědy, z hlediska mé profese zaměřené především na důkazy a dokazování, digitální stopy, kriminalistickou počítačovou expertizu, postup orgánů činných v trestním řízení před zahájením trestního stíhání (prověřování), vyšetřování, znalce a znalecké posudky, judikaturu a další perspektivy kontroly počítačové/ kybernetické kriminality.

V práci je patrný heuristický přístup z hlediska symptomologie hraničního vědního poznání, jehož struktura a strategie se opírají o řadu vědních oborů a odvětví, jako jsou právo, zejména trestní právo, matematická logika, teorie systémů, teorie modelování, teorie umělé inteligence, teorie kognitivních systémů, výpočetní technika (kybernetika) a novodobé experimentální metody. Dílo vykazuje kvalifikovaný systémový přístup autora a jeho prokazatelnou erudici.

Prof. Smejkal ve svém díle soustředil a mimořádně poutavým způsobem zpracoval a srozumitelně podal problematiku obtížnou, aktuální a významnou, která oproti prvnímu vydání je rozšířena a aktualizována o 287 stran textu a která má značný vědecký přínos. Monografie je v tomto pojetí originálním dílem v české odborné literatuře se zřetelným přesahem do evropského prostoru. Je v převážné míře opřená o vlastní vědecký a výzkumný podíl autora publikace, viz seznam použité a citované literatury, ze které je zcela zřejmé, že autor se kybernetickou kriminalitou a kriminalistikou zabývá dlouhodobě a systematicky.

Monografie má dobrý didaktický styl. Je určená širokému okruhu specialistů-kriminalistických teoretiků, právníků, znalců, ale i vědecko-pedagogickým pracovníkům vysokých škol technického a právního zaměření, doktorandům a studentům právnických, technických a policejních vysokých škol a orgánům a subjektům bezpečnosti a justice. Kniha je navíc koncipována široce a mezioborově tak, aby zde našli potřebné informace i pracovníci CIO (Chief Information Officer) a další odborníci v oboru management informačních technologií, řízení rizik, podnikatelé i výkonní pracovníci bezpečnosti, analytici, programátoři a technologicky orientovaní odborníci.