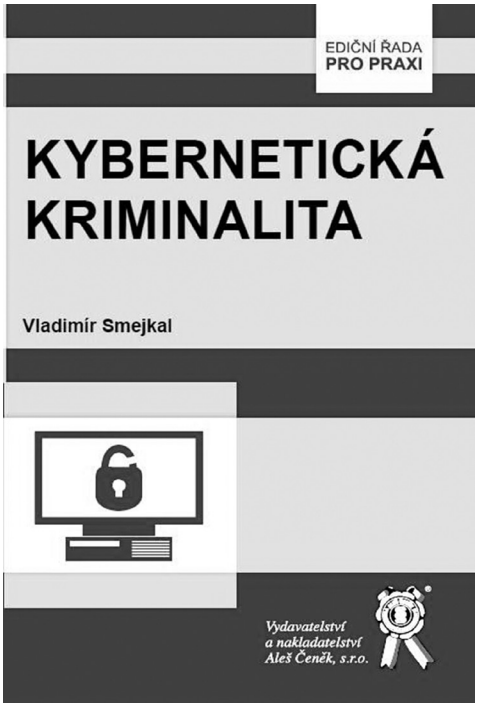
Reviews

SMEJKAL, V. Kybernetická kriminalita.
Plzeň: Nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. Cena 690 Kč.



Recenzovanou knihu byste snad ani neměli otevírat. Zejména nemáte-li hlubší vztah k počítačům, mobilům a další „elektronické havěti“, neboť zde jsou popsány s vysokou erudicí a značnou mírou podrobností všechny možné druhy trestné činnosti, která se odehrává kdekoliv v kyberprostoru.

Kniha prof. Smejkala, zakladatele oboru IT právo v České republice a dlouholetého pedagoga na VUT v Brně, má neuvěřitelných 636 stran. Autor zde shrnul svoje dlouholeté působení v oblasti právní teorie, ale i reálné praxe při praktickém odhalování a vyšetřování kybernetické kriminality.

Je záslužné, že autor před hlavní část výkladu, nacházející se ve druhé kapitole, předřadil úvodní část Počítače a počítačová kriminalita – základní pojmy, kde jsou stručně vysvětleny pojmy, které sice „ajťáci“ znají, ale každý je vnímá trochu jinak, což v momentě, kdy potřebujeme analyzovat obsah smlouvy či naplnění skutkové podstaty trestného činu, činí neskonalé potíže. A opačně – právníci většinou netuší, co se pod kterým z pojmů skrývá.

Těžiště knihy představuje 2. kapitola Kriminalita v prostředí informačních systémů a na Internetu, kde jsou podrobně popsány jednotlivé skutkové podstaty a doplněny jak praktickými příklady z reálného života, tak judikaturou. Nikoliv pouze judikaturou obsahující právní větu, jež je mnohdy nejasná a zavádějící, ale včetně relevantních částí zdůvodnění a často ještě doplněnou vlastním komentářem autora. To výrazně zvyšuje využitelnost tohoto díla pro právníky.

Najdeme zde např. teroristické útoky, poškození obecně prospěšného zařízení či cizí věci, neoprávněné užívání, podvody, vydírání, pornografii, porušování tajemství dopravovaných zpráv a dokumentů uchovávaných v soukromí, šíření poplašné zprávy, nebezpečné vyhrožování a pronásledování (stalking), nekalou soutěž a další trestné činy včetně porušování práv k duševnímu vlastnictví. Pochopitelně velmi podrobně jsou rozebrány počítačové tr. činy podle ust. § 230 – 232.

Třetí kapitola Odhalování a vyšetřování kybernetické kriminality patří spíše do oblasti kriminalistiky. Jsou zde charakterizováni typičtí pachatelé kyberkriminality a jejich motivy, popsány metody a postupy kriminalistické expertizy a diskutována dnes velmi aktuální témata jako digitální stopy, důkazy a dokazování nebo znalecké posudky.

Nesmírně zajímavá je pak 4. kapitola Prognóza dalšího vývoje kybernetické kriminality, zabývající se záležitostmi jako jsou útoky DoS, virtuální měny – bitcoiny útoky prostřednictvím sociálních sítí a dalšími technologickými novinkami, které se brzy objeví i v rukou zločinců (3D tisk nebo Internet věcí). Autor se odvážně pustil i do rozboru virtuálních světů a virtuální kriminality. Závěr kapitoly obsahuje témata, která rovněž souvisí s trestněprávní problematikou (k principu „ultima ratio“ a k zákazu donucování k poskytnutí důkazů proti sobě samému), ale zabrousil i do občanskoprávní oblasti (k odpovědnosti za škodu).

Kniha je přes vysoce složitou tématiku psána srozumitelně a to nejen právníkům, ale veškerým odborníkům, kteří se nějakým způsobem pohybují ve světě IT a jeho bezpečnosti. Podle názoru recenzentky by neměla chybět v knihovně žádného odborníka, zejména pak u manažerů v oblasti informačních technologií a jejich bezpečnosti. Její využitelnost pro výuku ve všech oborech informačních technologií a práva či managementu je vysoká.

JUDr. Hana Schelová Bachrachová Ph.D. LL.M.
advokát a vysokoškolský pedagog

SMEJKAL, V. Kybernetická kriminalita (Cybernetic Criminality).
Plzeň: Nakladatelství Aleš Čeněk, 2015, 636 pp. ISBN 978-80-7380-501-2. Price 690 CZK.

Perhaps it would be better not to open this book at all, particularly if you do not have a close connection with computers, mobiles and other "electronic pests", as it describes in considerable detail, and with great erudition, all the possible kinds of criminal activity conducted in cyberspace.

This book by Professor Smejkal, founder of the study field IT Law in the Czech Republic and long-time lecturer at Brno University of Technology, is comprised of an incredible 636 pages. The author has summarised his many years working in the field of legal theory and his practical work in uncovering and investigating cybernetic criminality in this publication.

The author deserves our praise for the fact that the main part of his book, found in the second chapter, is preceded by an introductory section entitled *Computers and Computer Criminality – Basic Terms* that gives a brief explanation of terms that are familiar to IT experts, though perceived slightly differently by each individual which causes infinite difficulties at the moment at which we want to analyse the content of a contract or the facts of a criminal case. Lawyers, on the other hand, generally don't have a clue of the meaning behind these terms.

The focal point of the book is its second chapter *Criminality in the Environment of Information Systems and the Internet* which gives a detailed description of the facts of individual cases supplemented both with practical examples from real life and with examples from the jurisprudence, and not merely the reasoning given for legal rulings, which may often be unclear and confusing, but with the inclusion of relevant parts of the legal grounds of individual cases, often supplemented by the author's own commentary. This significantly expands the usefulness of this work to lawyers.

The things we can find here include terrorist attacks, damage to public and private property, unauthorised use, fraud, extortion, pornography, violation of the confidentiality of private reports and documents, the spreading of hoaxes, dangerous threats and stalking, unfair competition and other criminal acts, including the violation of intellectual copyright. Computer-related criminal acts in accordance with the provisions of Sections 230–232 are, understandably, treated in great detail.

Chapter Three on the *Detection and Investigation of Cyber Crime* is devoted to the area of criminal science. A characterisation of typical perpetrators of cyber crime and their motives is given, their methods of criminal expertise described, and highly topical issues such as digital trails, evidence and expert judgements discussed.

Chapter Four on *The Prognosis for the Further Development of Cyber Crime* is extremely interesting and considers such things as DoS attacks, virtual currencies – Bitcoins, attacks over social networks and other technological innovations that are soon to appear in the hands of the criminals (3D printing and the Internet of Things). The author has bravely undertaken an analysis of virtual worlds and virtual criminality. The end of the chapter focuses on a topic that is also associated with criminal justice (the principle of "ultima ratio" and the ban on forcing people to provide evidence against themselves), though it also considers the area of civic law (responsibility for damage).

In spite of the enormous complexity of the topics covered, the book is written in a style that can be understood both by lawyers and by anyone working in the world of IT and IT security. In the view of this reviewer, it should not be missing from the shelves of any professional, and in particular those of managers in informational technology and security. It also offers great possibilities for use in teaching in all branches of information technology, law and management.

JUDr. Hana Schelová Bachrachová Ph.D. LL.M.
lawyer and university lecturer