Kapitola 12

Kybernetická kriminalita

Po prostudování kapitoly budete umět:

- definovat pojem kriminalita, kybernetická kriminalita,
- vysvětlit vybrané skutkové podstaty uvedené v trestním zákoníku.

Klíčová slova:

Kriminalita, počítačová kriminalita.

Kriminalita, nazývaná nejdříve počítačová, nyní pak nově kybernetická kopíruje technické vlastnosti i uživatelské možnosti počítačů, počítačových sítí, resp. celého kyberprostoru. Ze všeho nejdříve se počítače staly předmětem klasických kriminálních útoků, směřujících proti nim coby věcem movitým – krádeže, poškozování cizí věci atd., dále pak se jednání pachatelů posunulo směrem k neoprávněnému užívání. Následovaly útoky na data počítači zpracovávaná, a přes podvody jsme se dostali k dnešnímu stavu, kdy skutkových podstat spojených s počítači a počítačovými sítěmi nalezneme v současném trestním zákoníku mnoho a kdy variabilita jednání pachatelů v kyberprostoru je značná a neustále se rozšiřuje.

Označení „počítačová kriminalita“ má obdobný charakter jako pojmy „násilná kriminalita“, „kriminalita mladistvých“ apod. Takovýmito názvy jsou označovány skupiny trestných činů, mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty). Přitom ale – na rozdíl od jiných kategorií trestné činnosti – dlouho neexistovala jasná shoda v tom, co počítačovou kriminalitou je. Diskuse, která proběhla u nás v devadesátých letech, se přiklonila k názoru poprvé publikovaném kolektivem Smejkal, Sokol, Vlček[7], že pod pojmem „počítačová kriminalita“ je třeba chápat páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

a) jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité,
b) nebo jako nástroj trestné činnosti.

Počítač může být předmětem trestného činu; současně je ale také ke spáchání celé řady trestných činů ideálním prostředkem. Vzhledem k mnoha jeho vlastnostem, jakými jsou především:

- složitost principů, na nichž pracuje a nejednoduchost jeho ovládání;
- nakládání s informacemi, jež jsou nehmotné, přičemž mohou reprezentovat vysoké peněžní hodnoty nebo představovat citlivé osobní či ekonomické údaje;
- možnost jednoduchého skrývání a zahlazování těchto nehmotných stop;
- dostupnost prostředků pro utajování obsahu informací (šifrováním, přístupovými mechanismy – hesly, kartami, otisky prstů apod.);
- uplatnění distančního přístupu v prostředí počítačových sítí a elektronických komunikací, umožňující páchat trestnou činnost na dálku,

[7] Smejkal, V., Sokol, T., Vlček, M., *Počítačové právo*. Praha: C. H. Beck, 1995, s. 99.

je z hlediska páchání trestné činnosti používání počítačů pro pachatele vysoce přínosným.

Prvními trestnými činy zaměřenými na počítače, ať už si je představíme v jakékoliv podobě, byly sabotáže, které byly různě motivované – politicky i mstou zaměstnavateli.[8]

Velice brzy si ale uživatelé, kteří ani neměli přímý přístup k počítači, tehdy se nacházejícímu v klimatizovaných sálech pod dohledem vysoce kvalifikovaných specialistů, uvědomili další možnosti. Objevily se tzv. dokladové delikty, kdy stejným způsobem, jako měnili a falšovali údaje v běžných „papírových“ dokladech, začali zločinci měnit podklady připravené ke zpracování do počítače. Jednalo se o nejčastější odhalený počítačový zločin, jehož podstatou byly manipulace v mzdových účtárnách, zásobování, odbytech a na jiných pracovištích, kde pracovník měl možnost manipulovat s penězi (ať už v hotovosti nebo přes čísla účtů) či zbožím. Dnes jsou skutky tohoto typu obvykle kvalifikovány jako podvod podle § 209 trestního zákoníku obvykle v souběhu s trestným činem podle § 230 Neoprávněný přístup k počítačovému systému a nosiči informací.

Sjednocujícím kritériem takovýchto jednání je vždy více méně o využití něčího omylu ve svůj prospěch, přičemž v souvislosti s informačními systémy zde hraje nezanedbatelnou roli složitost problematiky a psychologická stránka věci. Na rozdíl od klasických manipulací s „papírovými“ doklady má manipulace s počítačovými daty pro pachatele několik výhod:

1. vymazání či přemazání údaje na magnetickém médiu je podstatně snazší a nezanechává prakticky žádné stopy;
2. člověk (zaměstnanec, auditor, zákazník apod.) z psychologického hlediska považuje výsledky z počítače za a priori správné a více jim (byť podvědomě) důvěřuje;
3. systém zpracování dat je natolik složitý, že málokdo má přehled o všech aspektech, procedurách, postupech a mechanismech, jež jsou používány a kontrola toho, co se odehrává ve výpočetním systému, je velmi obtížná;
4. objem zpracovaných, resp. přenášených dat je velmi velký;
5. zjištění stavu informačního systému v určitém, mnohdy časově vzdáleném okamžiku a prokázání odpovědnosti určité osoby za provedení operací v tomto IS je obtížné, ne-li nemožné;
6. lehkost provádění operací s počítačovými daty oproti reálnému životu; ukrást někomu z kapsy peněženku je výrazně obtížnější než napsat příkazový řádek na počítači – alespoň pro kvalifikovaného programátora;
7. morální aspekty jsou ve virtuálním světě poněkud potlačeny – daleko snadněji lze spáchat trestný čin kliknutím myši nežli namáhavým jednáním v reálném světě.

[8] Smejkal, V. a kol., *Právo informačních a telekomunikačních systémů*. 2. vydání. Praha, C. H. Beck, 2004, s. 703.

Tyto aspekty počítačové kriminality mají za následek vysokou úspěšnost trestných činů páchaných za využití výpočetní techniky. Právě značná důvěryhodnost výstupů z počítače, aniž bychom mnohdy byli schopni zjistit, jak se k těmto výstupům dospělo, je základním předpokladem úspěšného podvodu v prostředí informačních systémů.

Kromě toho se zde objevuje další aspekt podmiňující úspěchy počítačových zločinců, kterým je vysoká kvalifikace pachatelů tohoto druhu trestné činnosti. Ta se projevuje ve vysoké latenci tohoto druhu kriminality, neboť pachatelé mají daleko větší předpoklady k tomu, aby se vůbec nepodařilo spáchání trestného činu zjistit, případně aby se nepodařilo zjistit, kdo je pachatelem, a jak jsme se s tím již v nejednom případě setkali – aby nebylo podezřelému možno jeho trestnou činnost dokázat.

Teprve další dva technologické zlomy v oblasti počítačových systémů umožnily jejich hromadné využívání, a tudíž i neméně masivní trestnou činnost s počítači spojenou. Nová doba počítačového zločinu se datuje dvěma zásadními momenty:

1. nástupem osobních počítačů,
2. vznikem počítačových sítí a vzdáleného přístupu k počítačům, zejména prostřednictvím Internetu.
   K těmto dvěma faktorům musíme připojit ještě třetí, a to:
3. exponenciální růst možností mobilní telefonie a tomu odpovídající vybavenost občanů, včetně využívání anonymních, tzv. předplacených karet.

V rámci distančního přístupu prostřednictvím Internetu byly klasické podvody podle ust. § 209 TrZ zdokonaleny pomocí počítačů, případně se objevily zcela nové druhy podvodů – phishing, pharming apod.[9]

Dalšími delikty, které se objevily jako součást počítačové kriminality, byly a stále jsou:

a) padělky dokumentů, zhotovené pomocí moderních digitálních technologií;
b) padělky nosičů informací především v podobě různých karet obsahujících nosič dat – telefonních, kreditních (úvěrových), debetních (platebních), vstupních apod.

Nedlouho po masovém rozšíření počítačů a Internetu u nás se porušování autorských práv stalo takřka synonymem pro užívání počítačů. Nelegální užívání počítačů – hardware – bylo rychle dohnáno a předehnáno nelegálním užíváním software. Uvědomění si samotné existence nehmotných statků je spojeno až s pozdější dobou zhruba od poloviny devadesátých let, kdy se duševní vlastnictví ob-

[9] Smejkal, V., *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 137 a násl.

jevuje jako nehmotný majetek v obchodním majetku společností, v daňových zákonech, v novelizovaných zákonech na ochranu duševního vlastnictví a jako předmět obchodních vztahů i soudních sporů. Od té doby je ochraně práv autorských, průmyslových a práv jim podobných věnována stále větší pozornost (mj. i v důsledku intenzivnějších mezinárodních hospodářských vztahů). Dva druhy duševního vlastnictví – oba spadající pod ochranu autorským zákonem – se staly velice rychle masivním předmětem útoku zločinců: audiovizuální nahrávky a počítačové programy, později i databáze. Přitom většina počítačových programů a řada databází požívá ochrany podle autorského zákona, neboť podle § 2 odst. 2 AutZ se za dílo považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Za dílo souborné se považuje databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem.

Nelegální užívání software prošlo intenzívním nárůstem, kdy se hovořilo až o 80% nelegálně užívaného programového vybavení v České republice. Současná situace není tak dramatická a s rostoucími možnostmi zveřejňování audiových a audiovizuálních děl a jejich šíření prostřednictvím úložišť na Internetu se těžiště tr. činnosti podle § 270 stávajícího TrZ (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi) od software přesunulo k těmto dílům, případě ke zveřejňování děl literárních, zejména odborných nebo mimořádně populární beletrie obdobným způsobem[10].

S tím, jak stále více údajů je uloženo na magnetických médiích, roste zájem zločinců o obsah těchto nosičů informací. Těžiště jejich zájmu představují dnes zejména dvě oblasti:

a) osobní údaje občanů;
b) politicky nebo hospodářsky využitelné údaje (vyzvědačství a průmyslová špionáž).

Na přelomu let 1991–1992 došlo k velmi žádoucímu zařazení některých nových skutkových podstat do tehdejšího trestního zákona č. 140/1961 Sb., a to včetně skutkových podstat souvisejících s počítačovou kriminalitou. Jsou to ustanovení § 257a – Poškození a zneužití záznamu na nosiči informací a § 178 – Neoprávněné nakládání s osobními údaji.[11] Bylo to velmi prorocké, protože všechny tyto trestné činy doznaly značného rozšíření. Zejména pak neoprávněné nakládání s osobními údaji, podle stávající trestní úpravy pak § 180 tehdejšího TrZ.

Již v době platnosti předchozího tr. zákona se ale objevila další jednání, s nimiž si právní řád, a to nejen český, nevěděl příliš rady. Byly to zejména:

[10] Telec, I., *Zakázané těžení a nebezpečná situace na elektronických úložištích dat*, 2015, č. 1–2, s. 19–29; Smejkal, V., *Kybernetická kriminalita*, 2015, s. 352 a násl.

[11] Smejkal, V. a kol., *Právo informačních a telekomunikačních systémů*, 2. vydání. Praha, C. H. Beck, 2004, s. 730 a násl.

1. Obtěžování, které právě v souvislosti s ICT nabylo hrozivých rozměrů. K obtěžování dochází jednak formou elektronické pošty (e-mailů), jednak zasílám zpráv přes Internet (ICQ, chat, sociální sítě) nebo prostřednictvím mobilních telefonů (SMS), ale vyskytuje se i obtěžování formou klasických telefonických hovorů, faxů nebo různými zásilkami.
2. Tzv. hromadné útoky DoS, DDoS.[12]
3. Ještě problematičtější byl postih neoprávněného užívání počítače dálkovým způsobem, neboť podle ust. § 249 neoprávněné užívání cizí věci se předpokládalo, že se pachatel „zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu jich přechodně užívat, nebo na cizím majetku způsobí škodu nikoli malou tím, že neoprávněně takových věcí, které mu byly svěřeny, přechodně užívá“. Ani jedna skutková podstata se na variantu pachatele, připojeného ze svého osobního počítače v místě A k cizímu počítači v místě B plně nehodila.
4. S tím souvisela i možnost postihu pachatele, který pronikl do cizího počítače, aniž by jakkoliv poškodil či zničil údaje, v něm uložené. Pokud se hacker dostane do počítače a „koukne se“ na data v něm uložená, aniž by je následně využil (sdělil, okopíroval, zpracoval atd.), nelze hovořit o užití, a tudíž by pravděpodobně nedošlo k naplnění skutkové podstaty ust. § 257a písm. a).
5. Jelikož delikt podle § 257a neznal nedbalostní kvalifikaci, nebylo zřejmě jednoduše a podle tohoto ustanovení možné stíhat např. zaměstnance, který vložil zavirovanou disketu do počítačového systému svého zaměstnavatele, čímž došlo k vymazání obsahu pevného disku, neboť lze podle ust. § 257a stíhat pouze ty osoby, u nichž by úmysl byl prokázán.

Dne 23. 11. 2001 byla publikována Úmluva Rady Evropy o počítačové kriminalitě (dále jen Úmluva), která vstoupila v platnost 1. 7. 2004.756 Česká republika tuto Úmluvu podepsala v roce 2005, zohlednila ji v přípravě nového trestního zákoníku, leč ratifikovala až v 23. 8. 2013 s účinností od 1. 12. 2013.757 Celkově Úmluvu ratifikovalo 41 států z celého světa, dalších 12 ji zatím pouze podepsalo. Úmluva je poměrně dobrým základem pro postihování trestné činnosti v počítačových sítích, zejména na Internetu, neboť se kromě definování skutkových podstat zabývá i otázkami jurisdikcí a mezinárodní spolupráce[13].

Kromě deliktů ve vztahu k počítačovým systémům a počítačovým datům jsou do této kategorie podle Úmluvy řazeny i delikty páchané pomocí počítačů snadněji, a tudíž častěji a pravděpodobně s vyšší společenskou nebezpečností (typicky trestné činy související s dětskou pornografií nebo porušování autorského práva).

[12] Smejkal, V. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015, s. 534 a násl.

[13] Viz např. Gřivna, T.; Polčák, R. a kol., *Kyberkriminalita a právo*, 2008, s. 162 a násl.

Na jejím základě byly formulovány „počítačové“ skutkové podstaty v současném trestním zákoníku, zákonu č. 40/2009 Sb. ve znění pozdějších předpisů, a to:

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací,
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

Nová právní úprava je rozsáhlejší, pokud jde o popis postihovaných aktivit. Nadto se z původního jednoho ustanovení § 257a předchozího TrZ stala dvě ustanovení. Ustanovení § 230 postihující neoprávněný přístup k počítačovému systému a nosiči informací a § 231, který postihuje opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Přibyl i postih nedbalostního jednání podle § 232.

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat je definováno v ust. § 231 tak, že podle odst. 1 „*Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává*

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

b*ude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.*“. Detailní rozbor viz literatura. [14]

Ustanovení § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti nenalezneme v Úmluvě, ale bylo zařazeno na základě požadavků z praxe a poznatků orgánů činných v trestním řízení. U některých pachatelů bylo obtížné prokázat úmyslné jednání, přestože – vzhledem ke svému zaměstnání, postavení či funkci muselo být zřejmé, že svým jednáním způsobí škodu či jinou újmu a z kontextu vyplývalo, že si tohoto následku musel být plně

[14] Smejkal, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 411 a násl.

vědom. Rovněž zhojení se na hrubě nedbalém zaměstnanci, který svým jednáním spojeným s počítačem způsobil mnohamiliónovou škodu či mohl ohrozit samu existenci organizace, naráželo na limity dané zákoníkem práce[15].

Úmysl zákonodárců směřuje k ochraně majetku hrubě nedbalým jednáním osob, které doposud nepožívalo ochrany v rámci trestního práva a bylo je nutno řešit výlučně soukromoprávními prostředky. Důvodem je možnost značného ohrožení při nedbalém nakládání s počítačovými systémy, které dnes řídí výrobu, obchod, finance, ale i letový provoz nebo jednotky intenzivní péče, tedy kdy na jejich bezchybném provozu závisí majetek, zdraví i životy osob.

Trestnou činnost spojenou s počítačovými sítěmi a zejména s Internetem můžeme rozdělit do dvou základních kategorií:

1. zpřístupňování informací, které mohou někomu způsobit újmu nebo založit spáchání trestného činu nebo naopak shromažďování informací za účelem jejich pozdějšího nelegálního využití – neboli informační trestná činnost, neboť tato může být páchána i bez pomoci počítačů, byť značně obtížněji;
2. páchání trestné činnosti v kyberprostoru, a to takové činnosti, kterou lze páchat díky vlastnostem počítačů a počítačových sítí a jejich komponent (hardware, software, dat).

Do první oblasti ad a) lze zařadit zejména § 180 Neoprávněné nakládání s osobními údaji, § 316 Vyzvědačství, § 317 Ohrožení utajované informace, § 318 Ohrožení utajované informace z nedbalosti. Povaha Internetu jakožto prostředku, jehož prostřednictvím lze veřejně šířit informace, je významná v oblasti trestněprávní, konkrétně tam, kde se jedná o trestné činy, u nichž je veřejnost jejich znakem (např. § 184 Pomluva, § 191 Šíření pornografie, § 192 Výroba a jiné nakládání s dětskou pornografií, § 250 Manipulace s kurzem investičních nástrojů, § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi, § 352 Násilí proti skupině obyvatelů a proti jednotlivci, § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, § 357 Šíření poplašné zprávy, § 364 Podněcování k trestnému činu, § 365 Schvalování trestného činu, § 403 Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka, § 404 Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka, § 405 Popírání, zpochybňování, schvalování a ospravedlňování genocidia).

Páchání trestné činnosti v kyberprostoru jiné, nežli byla popsána výše, zahrnuje zejména různé druhy útoků na zařízení ICT, a to formou kyberterorizmu, vyvoláním stavu obecné ohrožení podle §

[15] Šámal, P. a kol., *Trestní zákoník II. § 140 až 421. Komentář*, 2012, s. 2320.

272–273, poškozením a ohrožením provozu obecně prospěšného zařízení podle § 276–277, poškozováním cizích věcí podle ust. § 228 TrZ a neoprávněným užíváním cizí věci podle § 207 TrZ. V poslední době se rozmáhá vydírání v prostředí ICT, které započalo pohrůžkami o zveřejnění osobních údajů a končí zaplacením „výpalného“ za odšifrování disků s daty, tzv. ransomware.[16]

Mezi ostatní trestné činy související s počítači můžeme zařadit ještě Neoprávněné opatření, padělání a pozměnění platebního prostředku, zejména platebních karet, resp. údajů z nich (§ 234), Výroba a držení padělatelského náčiní (§ 236) tvořeného prostředky ICT, případně padělání a pozměnění veřejné listiny (§ 348). Detailní rozbor kybernetické trestné činnosti viz literatura. [17]

V blízké budoucnosti můžeme počítat s trestnou činností související s virtuálními světy (vytvořenými v kyberprostoru), která bude zaměřena na virtuální vlastnictví a virtuální majetek, včetně tzv. virtuálních měn, jako jsou např. bitcoiny. Bude docházet k prolínání klasické kriminality ve vztahu k virtuálnímu prostoru a naopak. Také nové technologické fenomény, jako např. 3D tisk, „chytré šaty“ a šperky, monitorující životní pochody nositelů, létající roboti – drony či mikrominiaturní roboti budou představovat nejen přínos pro lidstvo, ale i rostoucí bezpečnostní rizika. Čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití musíme počítat. Proto trend IoT (Internet věcí) představuje extrémní hrozbu z hlediska kybernetické kriminality. Další velmi významnou oblastí je využívání trestné činnosti v kyberprostoru k páchání kybernetického terorizmu, útočícího na informační systémy sátu, klíčových podniků a poskytovatelů služeb obyvatelstvu včetně síťových služeb (telekomunikace, dodávky energie, vody apod.).

V kapitole je popsána problematika počítačové, resp. kybernetické kriminality. Jsou zde definovány skutkové podstaty těch trestných činů podle platného trestního zákoníku, které souvisejí s počítači a kyberprostorem. Závěrečnou část kapitoly tvoří prognóza dalšího vývoje kybernetické kriminality.

1. Jaký je rozdíl mezi počítačovou a kybernetickou kriminalitou?
2. Které jsou „počítačové“ skutkové podstaty v současném trestním zákoníku?
3. Podle jakého ustanovení trestního zákoníku jsou chráněny osobní údaje občanů?
4. Proč představuje Internet věcí vysokou hrozbu z hlediska kybernetické kriminality?

[16] Smejkal, V., *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 147 a násl.

[17] Smejkal, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015.

Literatura k tématu:

[1] SMEJKAL, V. *Kybernetická kriminalita*. 1. vyd. Plzeň: Aleš Čeněk, 2015. 640 s. ISBN 978-80-738-0501-2

[2] SMEJKAL, V. *Práva k počítačovým programům a databázím*. In: SRSTKA, Jiří a kol. *Autorské právo a práva související. Vysokoškolská učebnice.* Praha: Leges, 2017, s. 198-224. ISBN: 978-80-7502-240-0.

[3] TELEC, I., *Zakázané těžení a nebezpečná situace na elektronických úložištích dat*. *Bulletin advokacie*, 2015, č. 1–2, s. 19–29. ISSN 1210-6348.

[4] SMEJKAL, V. *Metodika vyšetřování kybernetické kriminality*. In: Porada Viktor a kol. *KRIMINALISTIKA. Technické, forenzní a kybernetické aspekty*. 1. vydání. Plzeň: Aleš Čeněk, 2016, s. 786–802. ISBN 978-80-7380-589-0.

[5] SMEJKAL, V. *Metodika vyšetřování softwarového pirátství.* In: Porada Viktor a kol. *KRIMINALISTIKA. Technické, forenzní a kybernetické aspekty*. 1. vydání. Plzeň: Aleš Čeněk, 2016, s. 803–824. ISBN 978-80-7380-589-0.

[6] JELÍNEK, J. a kol. *Terorismus – základní otázky trestního práva a kriminologie*. Praha: Leges, 2018, 224 str. ISBN978-80-7502-256-1.