**Název předmětu: Vybrané bezpečnostní aspekty ve veřejném právu**

**Téma č. 10: Nové trendy v bezpečnostně právní regulaci – kybernetická bezpečnost a robotika**

**ÚVOD**

Kriminalita patří k nejzávažnějším negativním společenským jevům, a proto je zapotřebí kriminalitě předcházet. Kriminalita se přizpůsobuje vývoji společnosti. S příchodem globalizace se sbližují nejen životní podmínky lidí přes hranice různých států, ale dochází i k internacionalizaci kriminality.

Nejdynamičtěji se rozvíjející kriminalitou je **kybernetická trestná činnost**. Je typickou trestnou činností, u níž dochází k potírání geografických a státně teritoriálních omezení.

1. **CHARAKTERISTIKA KYBERKRIMINALITY**

Kybernetická kriminalita nebo také kyberkriminalita je relativně nový interdisciplinární obor (v porovnání s obory jinými), zabývající se nelegálními a škodlivými aktivitami v kyberprostoru, které jsou založeny na použití nebo zneužití počítačové technologie.

Pojem kyberkriminalita nahradil dříve používané pojmy jako počítačová kriminalita nebo kriminalita v informační vědě. Počítačová kriminalita byla nejčastěji charakterizována jako „*páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroj trestné činnosti.“1*

V USA byl první počítačový trestný čin zaznamenán již v roce 1958[[1]](#footnote-1) [[2]](#footnote-2), ale samotný pojem „počítačová kriminalita“ („computer crime“) se jako obecně přijímaný pojem objevuje v právní a kriminologické terminologii vyspělých zemí až v sedmdesátých letech. Tehdy se odehrál i první čistě počítačový zločin v ČR, který spočíval v tom, že nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy na magnetických páskách.[[3]](#footnote-3)

Vývoj kybernetické kriminality lze rozdělit na následující etapy:

1. Etapa sólových, nedostupných počítačů.
2. Etapa nástupu osobních počítačů.
3. Etapa propojování počítačů do sítě.[[4]](#footnote-4)

**Kybernetická kriminalita je obvykle charakterizován jako souhrn takových trestných činů, které jsou páchány v kyberprostoru**. „*Těžištěm útoku již není počítač, ale kyberprostor tvořený počítačovými sítěmi a jejich jednotlivými prvky, ve kterém spolu komunikují veškerá zařízení ovládající protokol TCP/IP“.*[[5]](#footnote-5)

V současné době nemá kybernetická kriminalita žádný oficiálně definovaný obsah. **Jednotná definice neexistuje v teorii ani v platné právní úpravě.**

Dle dostupné odborné literatury jde v případě kybernetické kriminality, o taková kriminální jednání, při nichž bylo užito výpočetní techniky, informačních či komunikačních systémů:

1. jako předmět této trestné činnosti, tzn. cíl útoku pachatele, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité anebo
2. jako nástroj ke spáchání trestného činu.[[6]](#footnote-6)

Pojem kybernetické kriminality tedy nestaví do centra pozornosti počítač, nýbrž klade důraz na využívání komunikačních a informačních technologií a především na virtuální prostor, tedy kyberprostor, v jehož rámci se delikt uskutečňuje. Odráží tak technologický vývoj počítačových systémů a jejich funkcí. Z uvedeného je tedy zřejmé, že **těžištěm útoku** již není počítač, ale **kyberprostor.**

Kybernetický prostor pak věcný záměr zákona o kybernetické bezpečnosti vykládá jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními a komunikačními technologiemi, zahrnující připojení k veřejné síti (internet)“[[7]](#footnote-7)*

Kyberprostor tedy vzniká díky počítačovým systémům. Bez počítačů není ani kyberprostoru. Z tohoto úhlu pohledu bude v kybernetické kriminalitě vždy figurovat i počítač a každý případ kybernetické kriminality lze tedy označit i za počítačovou kriminalitu. Dalšími stavebními kameny kyberkriminality jsou kromě počítačů, informace a sítě. Takový přístup k definování kybernetických trestných činů nebude do budoucna udržitelný. S dalším rozvojem počítačových technologií se jejich využívání v každodenním životě natolik rozšíří, že bude možné podřadit pod takto široce pojatou definici kyberkriminality téměř vše. Tím okamžikem však uvedená definice ztratí svůj význam.

Dalším nedostatkem výše uvedené definice kyberkriminality je její navázání na výskyt počítače ve formě nástroje. Pak by každý trestný čin, v jehož rámci je počítač nějakým způsobem využit jako nástroj, bylo možné považovat za projev kyberkriminality, a tím by se pod kyberkriminalitu dostala obsáhlá množina trestných činů. Navíc není zvykem v právní teorii specifikovat kategorii trestných činů podle použitých prostředků.

Kyberkriminalitu definují tři hlavní novinky:

1. uskutečňuje se v novém „virtuálním“ prostoru,
2. obsahuje nová deviantní chování (podle eliminačního testu je „pravou“ kyberkriminalitou taková kriminalita, která by neexistovala bez internetu),
3. novinky v trestněprávních reakcích.[[8]](#footnote-8)

Mezi další nejvýraznější **specifika kyberkriminality[[9]](#footnote-9)** patří:

1. anonymita - znamená, že pachatel kyberkriminality se nemusí do kontaktu s obětí dostat, protože může trestnou činnost páchat z pohodlí domova. Každá interakce však zanechává v prostředí tzv. digitální stopu, a tudíž se jedná o znak zdánlivý.
2. globálnost neboli dosažitelnost - znamená, že internet je celosvětovou sítí, a tudíž interakce mají mezinárodní charakter.*„Kyberprostor existuje nezávisle na vůli jednotlivce 24 hodin 7 dní v týdnu“.* [[10]](#footnote-10)
3. síťovost,
4. informativnost,
5. distribuovanost - rozptýlenost,
6. automatizovanost - umožnění vzniku individuálních malých, na kumulované úrovni však velkých škod.

Evropské centrum pro boj proti kyberkriminalitě v EC3 First Year Report identifikoval z hlediska trestněprávních reakcí tyto nové charakteristiky kyberkriminality, které ve svém důsledku ztěžují jejich trestní postih. Jedná se o:

1. přeshraniční povahu internetu,
2. zvyšování počtu trestných činů na masovou úroveň,
3. větší možnost skrývání kyberkriminality (latence) - některé výzkumy uvádějí až 95% latentnosti,
4. široce rozvětvenou zločineckou síť vzniklou spoluprací zločineckých skupin na internetu.
5. **KATEGORIZACE KYBERKRIMINALITY**

Kybernetickou kriminalitu můžeme dělit dle různých hledisek. Jedním z dělení je klasifikace **podle iniciativy v rámci Lisabonské strategie** na:

1. zločiny porušující soukromí,
2. zločiny se vztahem k obsahu počítače,
3. ekonomické zločiny,
4. zločiny se vztahem k duševnímu vlastnictví.

Další možností je členění **podle Budapešťské Úmluvy** [(Úmluva Rady Evropy](https://cs.wikipedia.org/w/index.php?title=%C3%9Amluva_Rady_Evropy_o_kyberkriminalit%C4%9B&action=edit&redlink=1) [o kyberkriminalitě](https://cs.wikipedia.org/w/index.php?title=%C3%9Amluva_Rady_Evropy_o_kyberkriminalit%C4%9B&action=edit&redlink=1) - mezinárodní dohoda z roku 2001 pro harmonizaci národních právních systémů v oblasti počítačové a internetové kriminality) na:

1. trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů,
2. trestné činy související s počítači,
3. trestné činy související s obsahem, zejména s dětskou pornografií,
4. trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

Tento výčet v sobě zahrnuje pouze ta jednání, v nichž počítač vystupuje jako přímý či nepřímý prostředek páchání trestné činnosti. Zcela logicky sem nespadají jednání, při kterých sice bylo využito počítače nebo jemu podobných zařízení, avšak tato nebyla pro dokonání trestného činu nezbytná, nicméně přispěla určitou měrou k zefektivnění a ulehčení postupu pachatelů.

Závršník11 tuto klasifikaci velmi zdařile dále modifikuje pro účely kybernetické kriminality. Tímto způsobem vymezil tři kategorie kybernetické kriminality, a to:

1. kyberkriminalitu spojenou s integritou informačního systému a dat,
2. kyberkriminalitu spojenou s obsahem a
3. kyberkriminalitu spojenou s počítači.

Dalším v dostupné literatuře uváděným členěním je členění kyberkriminality **podle Samuela C. McQuade** (řídícího profesora a koordinátora programu pro bezpečnost podnikání RIT) na:

1. Zločin s využitím počítače - protiprávní jednání, pro jehož spáchání byl užitečný [[11]](#footnote-11)

jeden nebo více počítačů, avšak tyto počítače nebyly pro dokonání nezbytné.

1. Počítačový zločin - protiprávní jednání, pro jehož spáchání a dokonání bylo zapotřebí použít jednoho nebo více počítačů.
2. Zneužití počítače - použití počítače takovým způsobem, který je schopen přivodit újmu jednotlivci, skupině či organizaci, a který může současně narušovat zavedená pravidla nebo procedury. Při zneužití počítače nicméně nemusí nastat taková míra společenské škodlivosti, která by vedla k porušení trestních předpisů.
3. Počítač jako nástroj deviace - tím je myšleno takové chování, které využívá počítačová nebo telekomunikační zařízení jako nástroj k porušování sociálních norem, mnohdy až s trestněprávním přesahem.[[12]](#footnote-12)
4. **PRÁVNÍ ÚPRAVA KYBERKRIMINALITYY**

Příchod kybernetické kriminality vyžadoval právní změny. Trestněprávní úprava se však ukázala obtížnou, protože v případě kybernetické kriminality je třeba navíc vzít v úvahu, že ochrana tradičními právními prostředky nepostačuje, neboť

* nové jevy nejsou ve většině případů postižitelné starými normami,
* působnost trestněprávních norem je omezena, neboť trestní právo je projevem státní suverenity,
* dochází k překrývání jurisdikcí jednotlivých států.

V současné době není právní úprava v oblasti kybernetické kriminality koncepční ani v rámci evropské právní regulace, a jinak tomu není ani v České republice.

Nekoncepčnost je způsobena více příčinami, zejména však

1. **Problémy s vlastní definicí kybekriminality** - právní normy taxativně nevyjmenovávají všechny druhy nezákonného jednání.
2. **Nedostatkem vůle a kvalifikace zákonodárce -** problém, jak pojmenovat a definovat jednotlivá jednání, a jakým způsobem má být ta či ona problematika upravena. Nestačí jen vůle zákonodárců, ale je třeba i jejich odpovídající vzdělání a schopnost porozumět problému, který se zákonem snaží regulovat, což není v tak specifické oblasti jednoduché.
3. **Rychlostí legislativního procesu,** který nestačí dynamickému vývoji kyberkriminality. V takto dynamickém prostředí je aplikace trestněprávních předpisů přinejmenším obtížná.
	1. **Mezinárodní právní úprava**

První reakcí na kyberkriminalitu byl **Manuál OSN o prevenci a kontrole trestných činů spojených s počítači** z roku 1990**,** který upozornil na nepřipravenost států vůči novým technologiím v oblasti právní regulace a vyzval státy k mezinárodní spolupráci. Jako přední orgány zabývající se touto problematikou Manuál označil OECD[[13]](#footnote-13), Radu Evropy a právě OSN.

V oblasti mezinárodního práva souvisejícího s kybernetickou kriminalitou je v současné době stále nejvýznamnějším dokumentem **Úmluva o kybernetické kriminalitě**. Úmluva byla schválena Výborem ministrů Rady Evropy na jejím 109. zasedání 8. listopadu 2001 a otevřena k podpisu byla v Budapešti dne 23. listopadu 2001. V platnost vstoupila dne

1. července 2004.

Úmluva o kybernetické kriminalitě neboli Budapešťská úmluva se dělí na Preambuli a čtyři kapitoly, obsahující celkem čtyřicet osm článků. Po úvodních definicích následuje katalog kriminalizovaných činů, které Úmluva dělí do čtyř skupin:

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů

1. neoprávněný přístup (čl. 2)
2. neoprávněné zachycení informací (čl. 3)
3. zásah do dat (čl. 4)
4. zásah do systému (čl. 5)
5. zneužití zařízení (čl. 6)
6. Trestné činy související s počítači
7. falšování údajů souvisejících s počítači (čl. 7)
8. podvod související s počítači (čl. 8)
9. Trestné činy související s obsahem, zejména s dětskou pornografií (čl. 9)
10. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu (čl. 10)

Tyto skutkové podstaty se staly základem nových skutkových podstat v současném trestním zákoníku. Dále zakotvuje požadavek na úpravu trestní odpovědnosti právnických osob v rámci právních úprav jednotlivých států, které k Úmluvě přistoupily.

Úmluva představuje nejvýznamnější právní dokument týkající se kyberkriminality a jeho cílem je vytvořit mezinárodní právní rámec pro účinné potírání počítačové kriminality prostřednictvím harmonizace prvků skutkových podstat v oblasti počítačové kriminality za účelem zajištění adekvátního postihu pachatelů, stanovení nezbytných vnitrostátních vyšetřovacích pravomocí pro zajišťování důkazů v elektronické formě a vyšetřování počítačové kriminality, jakož i zavedení pohotového a efektivního režimu mezinárodní spolupráce ve vztahu k trestným činům souvisejícím s informačními.[[14]](#footnote-14) Tzn., že tato úmluva stanoví smluvním stranám povinnost zavést do národních právních řádů takové nástroje, pomocí kterých bude možné postihovat definované kybernetické trestné činy, jejichž taxativní výčet uvádí.

Dne 28. 1. 2003 byl přijat **Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě.**[[15]](#footnote-15)Tento dokument definuje okruh trestných činů, kterým se Úmluva o kyberkriminalitě nevěnuje, tj.

1. šíření rasistických a xenofobních materiálů,
2. rasisticky a xenofobně motivovaná pohrůžka,
3. rasisticky a xenofobně motivovaná urážka,
4. popření, hrubé snižování, schvalování nebo ospravedlnění genocidy nebo zločinů
5. proti lidskosti,
6. návod a pomoc k těmto jednáním.

Dodatkový protokol vstoupil pro Českou republiku v platnost dne 1. 12. 2014.

Dalším významným dokumentem v oblasti kyberkriminality je **tzv. Tallinnský manuál** mezinárodního práva použitelný na kybernetickou válku**.** Jedná se o dokument, který vydalo Centrum excelence pro spolupráci v oblasti kybernetické obrany NATO v estonském Tallinnu. Dokument byl publikován v dubnu 2013 a je primárně zaměřen na kybernetickou válku. Mj. řeší otázku uplatnitelnosti norem mezinárodního práva na oblast kybernetické války, když v pravidle č. 6 uvádí: *„stát nese odpovědnost za kybernetické operace, které jsou u přičitatelné, a které představují porušení závazku mezinárodního práva“.*[[16]](#footnote-16)

* 1. **Unijní právní úprava**

EU[[17]](#footnote-17) se snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možno účinněji postihovat kyberkriminalitu.

Již v roce 1999 na zasedání v Helsinkách vyhlásila Evropská komise celoevropskou strategickou iniciativu eEurope - Informační společnost pro všechny. Jejím hlavním cílem bylo poskytnutí výhod informační společnosti všem obyvatelům.

Nejširší rámec, kterým se od roku 2010 EU řídí, se pak nazývá Evropa 2020; jedná se o desetiletou strategii, jejímž cílem je dosáhnout hospodářského růstu. Klade si za cíl pět bodů, kterých chce dosáhnout prostřednictvím sedmi iniciativ, přičemž jednou z nich je tzv. Digitální agenda pro Evropu, která sama navrhuje sedm klíčových oblastí, ve kterých je třeba vhodnými nástroji dosáhnout následujících požadovaných cílů:[[18]](#footnote-18)

- vytvoření jednotného digitálního trhu,

- zlepšení rámcových podmínek pro interoperabilitu mezi výrobky a službami v oblasti ICT,

- posílení důvěry v Internet a jeho bezpečnost,

- záruka poskytování výrazně rychlejšího internetového připojení,

- podpora investic do výzkumu a vývoje,

- zvýšení digitální gramotnosti, dovedností a začlenění,

- zavádění IKT k řešení společenských úkolů, jako jsou změna klimatu, zvyšující se náklady na zdravotní péči a stárnoucí populace.

Prostředkem pro sbližování práva jednotlivých členských států jsou především rámcová rozhodnutí, směrnice a další dokumenty EU/ES. Z hlediska boje s kybernetickou kriminalitou se jeví jako nejvýznamnější následující dokumenty:

1. směrnice Rady 91/250/EHS o právní ochraně počítačových programů,
2. rozhodnutí rady 92/242/EHS o bezpečnosti informačních systémů,
3. rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu,
4. nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),
5. rámcové rozhodnutí rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi státy,
6. nařízení Evropského parlamentu a Rady (EU) 2016/794, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. 5. 2016 a další.

Jedná se pouze o demonstrativní výčet dokumentů.

* 1. **Právní úprava kyberkriminality v ČR**

Nejvýznamnějším vnitrostátním předpisem upravujícím hmotněprávní aspekty internetové kriminality je nepochybně **z. č. 40/2009 Sb., trestní zákoník.**

První trestné činy spojené s počítači se objevily již v 70. a 80. letech minulého století a byly nejčastěji kvalifikovány jako sabotáž podle § 97 zákona č. 140/1961 Sb. Trestní zákon platný v té době neobsahoval skutkovou podstatu, která by stanovila postih za neoprávněný přístup k počítačovému systému. Postupný nárůst trestné činnosti s využitím počítače s sebou přinesl naléhavou potřebu přijmout takovou trestněprávní úpravu, která by byla účinná a umožnila postihnout i tato protiprávní jednání.

První "počítačový" delikt u nás byl obsažen v zákoně č. 140/1961 Sb., trestním zákonu, do kterého byl včleněn od 1. ledna 1992 zákonem č. 557/1991 Sb. Jednalo se o trestný čin poškození a zneužití záznamu na nosiči informací podle § 257 a) trestního zákona, jehož se dopustil ten, kdo získal přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch

1. takových informací neoprávněně užil,
2. informace zničil, poškodil, změnil nebo učinil neupotřebitelnými, nebo
3. učinil zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,

za což mu hrozil trest odnětí svobody až na jeden rok nebo zákaz činnosti nebo peněžitý trest nebo propadnutí věci nebo jiné majetkové hodnoty.

Zákon č. 40/2009 Sb., trestní zákoník, zohlednil význam informačních technologií při páchání trestné činnosti a mezinárodní charakter kriminality. Právní úprava skutkových podstat počítačové kriminality v zákoně č. 40/2009 Sb. zahrnuje jednak klasické trestné činy, páchané v kyberprostoru, kterými jsou zejména:

- trestný čin neoprávněného nakládání s osobními údaji podle § 180 trestního zákoníku,

- trestný čin poškození cizích práv podle § 181 trestního zákoníku,

- trestný čin porušení tajemství dopravovaných zpráv podle § 182 trestního zákoníku,

- trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle § 183 trestního zákoníku,

- trestný čin pomluvy podle § 184 trestního zákoníku,

- trestný čin šíření pornografie podle § 191 trestního zákoníku,

- trestný čin výroby a jiného nakládání s dětskou pornografií podle § 192 tr. zákoníku,

- trestný čin krádeže podle § 205 trestního zákoníku,

- trestný čin zpronevěry podle § 206 trestního zákoníku,

- trestný čin neoprávněného užívání cizí věci podle § 207 trestního zákoníku,

- trestný čin podvodu podle § 209 trestního zákoníku,

- trestný čin provozování nepoctivých her a sázek podle § 213 trestního zákoníku.[[19]](#footnote-19)

V souvislosti s ratifikací Úmluvy[[20]](#footnote-20) byly do trestního zákoníku zařazeny skutkové podstaty nových trestných činů, a to:

1. trestného činu neoprávněného přístupu k počítačovému systému podle § 230 tr. zákoníku,
2. trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 trestního zákoníku,
3. trestného činu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 232 trestního zákoníku.

Trestné činy podle § 230 - § 232 trestního zákoníku jsou specifickou skupinou soudně trestných deliktů. Od ostatních trestných činů proti majetku, jejichž druhovým objektem jsou majetkové zájmy různorodé povahy, se odlišují právě svým primárním objektem, kterým je společenský, parciální či individuální zájem na důvěrnosti, integritě a dostupnosti počítačových systémů, sítí a počítačových dat, jakož i zájem na zamezení zneužití takových systémů, sítí a dat k páchání trestné činnosti různorodé povahy.[[21]](#footnote-21) Nepřímo jsou chráněny i další zájmy, obchodní tajemství, bankovní tajemství, autorská díla, údaje o pacientech, údaje o zaknihovaných cenných papírech, utajované informace, pokud je nosič informací obsahuje. Předmětem útoku je nosič informací, resp. jeho obsahové a technické vybavení.[[22]](#footnote-22)

Trestného činu **neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 trestního zákoníku** se dopustí ten, kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, přičemž mu hrozí trest odnětí svobody až na jeden rok, zákaz činnosti nebo propadnutí věci nebo jiné majetkové hodnoty. Pachatel, který získá přístup k počítačovému systému nebo k nosiči informací a

1. neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
2. data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
3. padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
4. neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, může být potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Ust. § 230 trestního zákoníku tedy obsahují 2 základní skutkové podstaty:

a) v odstavci 1 je chráněna důvěrnost počítačových dat a počítačového systému nebo jejich částí a

b) v odstavci 2 jsou chráněny integrita a dostupnost počítačových dat a systémů.

Podle ustanovení § 230 odst. 3 písm. b) je okolností podmiňující použití vyšší trestní sazby situace, kdy pachatel spáchá trestný čin podle odst. 1 nebo 2 téhož ustanovení v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Jelikož ustanovení § 230 odst. 1 kriminalizuje již pouhý neoprávněný přístup k počítačovému systému a nevyžaduje se, aby došlo k omezení funkčnosti (postačí, že k tomu směřoval úmysl pachatele), je úprava v trestním zákoníku nad rámec závazku vyplývajícího z Úmluvy o kybernetické kriminalitě. Z hlediska subjektivní stránky je k naplnění skutkových podstat definovaných v ustanovení § 230 trestního zákoníku vyžadováno zavinění ve formě úmyslu.

S cílem dostát závazkům plynoucím z Úmluvy o počítačové kriminalitě (čl. 6) byla do trestního zákoníku nově zařazena skutková podstata tr. činu **opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat** podle § 231 odst. 1 trestního zákoníku, která kriminalizuje jednání pachatele, jež spočívá již v pouhém držení, výrobě, zpřístupňování nebo jiném nakládání s prostředky, postupy nebo nástroji užívanými ke spáchání vlastních kybernetických útoků, tj. svou povahou přípravné jednání k trestným činům porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b). c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, odst. 2 (tzv. předčasně dokonaný trestný čin).

Objektem tohoto trestného činu je zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků, jež primárně slouží ke spáchání trestných činů porušení tajemství dopravovaných zpráv podle ustanovení § 182 odst. 1 písm. b), c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle ustanovení § 230 odst. 1, 2.[[23]](#footnote-23) Z hlediska subjektivní stránky je k naplnění skutkové podstaty definované v ustanovení § 231 trestního zákoníku vyžadováno zavinění ve formě úmyslu a to tak, že úmysl musí směřovat ke spáchání některého z uvedených trestných činů. To znamená, že opatření a přechovávání přístupového zařízení a hesla samo o sobě bez takového úmyslu trestné není. Neoznámení ani nepřekažení tohoto trestného činu nejsou trestné.

Trestného čin **poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 232 trestního zákoníku se dopustí ten, k**do z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

1. data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo
2. učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Úprava ustanovení § 232 trestního zákoníku jde nad rámec závazků vyplývajících z mezinárodních smluv nebo unijního práva. Objektem je v tomto případě ochrana dat a technického a programového vybavení počítače před nedbalostním poškozovacím jednáním, pokud je těmito zásahy způsobena značná škoda.

Z důvodu, že kriminalizace nedbalostního jednání je v tomto případě i s ohledem na zásadu subsidiarity trestněprávní represe (§ 12 odst. 2 trestního zákoníku) poněkud diskutabilní, tak byla trestní odpovědnost omezena na případy hrubé nedbalosti a zároveň způsobení škody značného rozsahu.

**Tabulka č. 1 - Nápad trestných činů podle § 230 - 232 trestního zákoníku**

|  |
| --- |
| **Tr. činy podle § 230 - 232 TZk** |
| rok | nápad |
| 2015 | 707 |
| 2016 | 635 |
| 2017 | 784 |

* **porušení autorského práva**, **práv souvisejících s právem autorským a práv k databázi podle § 270 tr. zákoníku**

Podle judikatury se za neoprávněný zásah do zákonem chráněných práv ve smyslu § 270 odst. 1 trestního zákoníku rozumí i takové jednání pachatele, který v prostoru vyhrazeném pro své internetové stránky umístí odkazy umožňující neoprávněný přístup k rozmnoženinám děl umístěným na externích serverech tak, že kdokoli k nim může mít prostřednictvím takové stránky přístup, aniž by k tomu měl souhlas nositelů autorských práv, a využije tzv. hostingu s možností uložení dat na serveru. Pachatel, který takovým jednáním umožní přístup k rozmnoženině díla, aniž by k tomu byl oprávněn, poruší autorská práva k jednotlivým dílům a poruší práva na sdělování díla veřejnosti ve smyslu § 18 odst. 1, 2 autorského zákona.**[[24]](#footnote-24)**

Na základě Úmluvy o kybernetické kriminalitě zavedl **zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim** trestní odpovědnost právnických osob, a tím **stíhat, odsoudit a potrestat právnickou osobu, která spáchala trestný čin.** Pokud zákon nestanoví jinak, použije se na trestní odpovědnost právnických osob trestní zákoník. Odpovědnost za trestný čin právnické osobě vzniká, pokud statutární orgán, jeho člen nebo jiná osoba ve vedoucím postavení, nebo s rozhodujícím vlivem na řízení, nebo zaměstnanec právnické osoby při plnění pracovních povinností páchá protiprávní čin v zájmu právnické osoby nebo v rámci její činnosti. Druhou podmínkou pro vznik trestní odpovědnosti právnické osoby za jednání jejího zaměstnance je, že se musí jednat o čin schválený nebo na pokyn některé z osob ve vedoucím postavení nebo s rozhodujícím vlivem.

Právní úprava, která se týká kybernetické bezpečnosti v ČR, je obsažena zejména v **zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů**. Přijetím tohoto předpisu došlo s účinností od 1. ledna 2015 ke zvýšení efektivity řešení kybernetických incidentů, a to stanovením podmínek spolupráce mezi veřejnou správou a soukromými osobami. Charakterizuje kybernetický bezpečnostní incident jako narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Základním cílem zákona o kybernetické bezpečnosti je zvýšit bezpečnost kybernetického prostoru a zejména se snažit ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky.**[[25]](#footnote-25)**

Na základě zákona o kybernetické bezpečnosti došlo ke zřízení **Národního úřadu pro kybernetickou a informační bezpečnost**, jehož činnost byla zahájena dne 1. srpna 2017. Tento úřad převzal činnost Národního centra kybernetické bezpečnosti, které spadalo pod Národní bezpečnostní úřad. Součástí úřadu je tzv. Vládní CERT (Computer Emergency Response Team), což je specializovaný tým pro prevenci a řešení bezpečnostních incidentů v počítačových sítích.

1. **TENDENCE VÝVOJE KYBERNETICKÉ KRIMINALITY**

Ve vývoji kybernetické kriminality lze předpokládat:

* že objektem útoku budou v převážné většině nehmotné informace, nikoliv hmotné prostředky informačních systémů a technologií,
* že útoky na technická zařízení se budou odehrávat zejména na mobilní zařízení a zařízení nedostatečně zabezpečená a připojená do sítě zaměstnavatele,
* možnost útoků na průmyslové řídicí systémy (ICS) a systémy dispečerského řízení a sběru dat (SCADA) v kritické infrastruktuře,
* využití všech druhů internetové komunikace, vč. sociálních sítí,
* tupý vandalismus,
* finanční podvody spojené s kyberprostorem,
* kriminální jednání vlastních zaměstnanců,
* masivní zneužívání Internetu k šíření nepravdivých údajů, a to nejen vůči fyzickým osobám, ale i vůči osobám právnickým,
* prohloubení střetu mezi anonymitou a ochranou soukromí na Internetu,
* porušování autorských práv,
* útoky na kritickou informační a komunikační infrastrukturu ze strany cizích států ale i malých skupin osob.**[[26]](#footnote-26)**

Aby byl boj s kyberkriminalitou opravdu úspěšný, je třeba řešit všechny problémy jak v oblasti zákonodárství, tak v oblasti organizační a technické současně. Zákony by měly zahrnovat všechny formy trestního jednání a stanovit dostatečné postihy.**[[27]](#footnote-27)**

Prevence je důležitější než represe. V případě bezpečnostního incidentu je Dle Václava Jirovského by měla prevence spočívat především v následujících činnostech:

1. přijetí opatření, která omezí možnost útoku na počítačový systém,
2. testování přijatých opatření,
3. detekci průniku nebo počátečních aktivit směřujících k průniku do systému a maximální využití nástrojů, které jsou k tomu určeny. Během detekce takové aktivity je možno ve smyslu prvního kroku přijmout okamžitá opatření vedoucí ke zvýšení bezpečnosti ohrožené části systému nebo eliminaci útočníka.
4. vyšetřování průniku, shromažďování důkazů a odstraňování vzniklých škod.**[[28]](#footnote-28)**

**ZÁVĚR**

Kybernetická kriminalita je neoddělitelnou součástí světa tak, jak je kyberprostor nedílnou a dnes již neoddělitelnou součástí našeho světa. Jeho ochrana proti nelegálním aktivitám (kyberkriminalitě) se musí stát rovněž nedílnou součástí ochrany nejen států, ale i fyzických a právnických osob. Proti kybernetickému nebezpečí lze stejně jako proti jakémukoliv jinému nebezpečí bojovat jednak prevencí a a dále represí. Do oblasti prevence zahrnujeme budování zabezpečených ICT, výchovu k bezpečnosti, základní i aplikovaný výzkum a mezinárodní spolupráci.

Trestní právo je sice podstatným nástrojem v boji proti kyberkriminalitě, ale nemělo by být primárním prostředkem ochrany. Podle zásady subsidiarity trestní represe, jak ji vymezila judikatura Ústavního soudu ČR, by měly být nejprve voleny prostředky obrany v řízení ve věcech občanskoprávních, dále v řízení správním a pouze v krajních případech by mělo být přistupováno k trestnímu stíhání. Právní úprava bohužel na kriminální jevy spojené s novými technologiemi reaguje s velkým zpožděním.

Pro lepší regulaci kyberprostoru je nutné:

1. pokračovat v harmonizaci právní úpravy kyberprostoru, a to nejen v rámci Evropy, ale celosvětově,
2. zlepšovat spolupráci při vyšetřování kybernetické kriminality mezi státy navzájem a tak zvýšit úspěšnost odhalení pachatelů trestné činnosti v oblasti kyberprostoru,
3. zefektivnit vymáhání práva v kyberprostoru.

*„Aby byl boj s počítačovou kriminalitou opravdu úspěšný, je třeba řešit všechny problémy jak v oblasti zákonodárství, tak v oblasti organizační a technické současně. Zákony by měly zahrnovat všechny formy trestního jednání a stanovit dostatečné postihy.“*[[29]](#footnote-29)

**Literatura**:

1. DRAŠTÍK, Antonín a kol., 2015. *Trestní zákoník: komentář*. Praha: Wolters Kluwer, 3264 s. ISBN 978-80-7478-790-4.
2. JELÍNEK, Jiří a kol., 2009. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 896 s. ISBN 978-80-87212-24-0.
3. JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 288 s. ISBN 978­80-247-1561-2.
4. GŘIVNA, Tomáš a kol., 2014. *Kriminologie*. Praha: Wolters Kluwer, 530 s. ISBN 97880-7478-614-3.
5. GŘIVNA, Tomáš a Radim POLČÁK, 2008. *Kyberkriminalita a právo*. Praha: nakladatelství Auditorium, 220 s. ISBN: 978-80-903786-7-4.
6. SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 220 s. ISBN 978-80-903786-7-4. Čeněk. 636 s. ISBN 978­80-7380-501-2.
7. ŠÁMAL, Pavel a kol., 2009. *Trestní zákoník. Edice velké komentáře*. Praha: C.H.Beck, 2084 s. ISBN 978-80-7380-501-2.
8. VLČEK, Martin, 1989. *Počítače a kriminalita (trestněprávní a kriminologické aspekty),* Praha, Academia, ISBN 978-80-2000-139-5.
9. ZAVRŠNIK, Aleš, 2017. *Kyberkriminalita.* Praha: Wolters Kluwer, 148 s. ISBN 97880-7552-755-5.
10. *Statistické přehledy kriminality za roky 2011 až 2017* [cit. 10. 09. 2018]. Dostupné: <http://www.policie.cz/clanek/archiv-statistiky-statisticke-prehledy-kriminality.aspx>
11. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: ASPI [právní informační systém]. Wolters Kluwer ČR
12. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. In: ASPI [právní informační systém]. Wolters Kluwer ČR
13. Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů. In: ASPI [právní informační systém]. Wolters Kluwer ČR
14. Zákon č. 418/2011 Sb, o trestní odpovědnosti právnických osob a řízení proti nim), ve znění pozdějších předpisů. In: ASPI [právní informační systém].Wolters Kluwer ČR
15. Manuál OSN pro prevenci a kontrolu počítačového zločinu. [online] OSN ©2001. [cit.

10.09.2018]. Dostupné z:

<http://216.55.97.163/wpcontent/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Gu> ide.pdf

1. Úmluva o počítačové kriminalitě. In: COE [právní informační systém]. Councilof Europe Treaty office. [cit. 16.07.2020]. Dostupné z: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>
2. Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: COE [právní informační systém]. Council of Europe Treaty office [cit. 16.07.2020]. Dostupné z: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f>
3. Talinský manuál mezinárodního práva použitelného na kybernetickou válku, [cit. 16.07.2020]. Dostupné z: http://issuu.com/nato\_ccd\_coe/docs/tallinnmanual?e=5903855/1802381
1. SMEJKAL, V. a kol. *Počítačové právo.* Praha: C.H.Beck,1995, 264 s. ISBN: 80-7049-101-9. s. 99. [↑](#footnote-ref-1)
2. VLČEK, M. *Počítače a kriminalita (trestněprávní a kriminologické aspekty),* Praha, Academia, 1989, ISBN 8020001395. [↑](#footnote-ref-2)
3. Viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 73. [↑](#footnote-ref-3)
4. Viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s.

ISBN 978-80-7380-501-2. s. 74-75. [↑](#footnote-ref-4)
5. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 15. [↑](#footnote-ref-5)
6. SMEJKAL, V. a kol. *Počítačové právo.* Praha: C.H.Beck,1995, 264 s. ISBN: 80-7049-101-9. s. 220. [↑](#footnote-ref-6)
7. Věcný záměr zákona o kybernetické bezpečnosti, 2012, s. 56. [↑](#footnote-ref-7)
8. ZAVRŠNIK, A. *Kyberkriminalita.* Praha: Wolters Kluwer, 2017, 148 s. ISBN 97880-7552-755-5. s. 4. [↑](#footnote-ref-8)
9. Viz ZAVRŠNIK, A. *Kyberkriminalita.* Praha: Wolters Kluwer, 2017, 148 s. ISBN 97880-7552-755-5. s. 4. [↑](#footnote-ref-9)
10. GŘIVNA, T. a kol. *Kriminologie*. Praha: Wolters Kluwer, 2014. 530 s. ISBN 97880-7478-614-3. s. 336. [↑](#footnote-ref-10)
11. ZÁVRŠNÍK. A. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017.148 s. ISBN 97880-7552-755-5. s. 16 [↑](#footnote-ref-11)
12. McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. ISBN 0313339740. s. 43. [↑](#footnote-ref-12)
13. Organizace pro hospodářskou spolupráci a rozvoj [↑](#footnote-ref-13)
14. Viz Úmluva o počítačové kriminalitě. In: COE [právní informační systém]. Council of Europe Tre-aty office. [cit. 10.09.2018]. Dostupné z: [https://www.coe.int/en/web/conventions/full-list/- /conventions/rms/0900001680081561](https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561) [↑](#footnote-ref-14)
15. Viz Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: COE [právní informační systém]. Council of Europe Treaty office [cit. 10.09.2018]. Dostupné z: [https://www.coe.int/en/web/conventions/full-list/- /conventions/rms/090000168008160f](https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f) [↑](#footnote-ref-15)
16. Talinský manuál mezinárodního práva použitelného na kybernetickou válku. [cit. 10.09.2018]. Dostupné z: http://issuu.com/nato\_ccd\_coe/docs/tallinnmanual?e=5903855/1802381 [↑](#footnote-ref-16)
17. ČR podala žádost o vstup 17. ledna 1996, žádosti bylo vyhověno k 1. květnu 2004. [↑](#footnote-ref-17)
18. European Commission. *Digitální agenda pro Evropu: klíčové iniciativy* (online) © European Union, 1995­2015. [cit. 10.09.2018]. Dostupné z: <http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm?locale=EN> [↑](#footnote-ref-18)
19. ŠÁMAL, P. a kol. *Trestní zákoník. Edice velké komentáře*. Praha: C.H.Beck, 2009, ISBN 978-80-7380-501-2. s. 2084. [↑](#footnote-ref-19)
20. Úmluva o počítačové kriminalitě. In: COE [právní informační systém]. Council of Europe Tre-aty office. [cit. 10.09.2018]. Dostupné z:

<https://www.coe.int/en/web/conventions/full-list/-conventions/rms/0900001680081561> [↑](#footnote-ref-20)
21. DRAŠTÍK, A. a kol. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015, ISBN 978-80-7478-790-4. s. 1476. [↑](#footnote-ref-21)
22. JELÍNEK, J. a kol. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 2009, 896 s., ISBN 978-80-87212-24-0. s. 626. [↑](#footnote-ref-22)
23. ŠÁMAL, P. a kol. *Trestní zákoník. Edice velké komentáře*. Praha: C.H.Beck 2009, ISBN 978-80-7380-501-2. s. 2097-98. [↑](#footnote-ref-23)
24. Viz Usnesení Nejvyššího soudu sp. zn. 8 Tdo 137/2013 ze dne 27. 2. 2013 [↑](#footnote-ref-24)
25. Viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 93. [↑](#footnote-ref-25)
26. Viz SMEJKAL, V. *Kybernetická kriminalita.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 571. [↑](#footnote-ref-26)
27. GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. Praha: nakladatelství Auditorium, 2008. 220 s. ISBN: 978-80-903786-7-4. s. 88. [↑](#footnote-ref-27)
28. Viz JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, 2007. [↑](#footnote-ref-28)
29. GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. Praha: nakladatelství Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4. s. 88. [↑](#footnote-ref-29)