
ZÁKLADY TRESTNÉHO PRÁVA V KONTEXTE INFORMAČNÝCH TECHNOLÓGIÍ A KYBERNETICKEJ BEZPEČNOSTI



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

- **Časť I: Trestnoprávny rámec kyberkriminality v SR**
 - Všeobecné základy trestného práva, hmotnoprávna úprava a procesné aspekty zaistovania digitálnych dôkazov.
- **Časť II: Inštitucionálny rámec boja proti kyberkriminalite**
 - Špecializované útvary Policajného zboru SR a úloha Europolu (EC3, J-CAT).
- **Časť III: Medzinárodný kontext a budúce výzvy**
 - Kľúčové medzinárodné nástroje, vplyv judikatúry EÚ a nové technologické výzvy (AI, IoT).

CIEĽ PREDNÁŠKY

- Poskytnúť komplexný a expertný prehľad trestnoprávnej regulácie v oblasti IT a kybernetickej bezpečnosti v Slovenskej republike.
- Systematicky analyzovať a prepojiť teoretickú (právnú) a praktickú (inštitucionálnu) rovinu.
- Detailne mapovať skutkové podstaty trestných činov, ako aj organizačné štruktúry a kompetencie špecializovaných zložiek Policajného zboru a Europolu.

ÚVOD

Tomu, čo je zakázané iba niekedy, alebo iba v niektorých kultúrach, hovoríme **malum prohibitum**. To sú previnenia proti spoločenským normám. Patria tam napríklad predpisy ktoré upravujú súboje či hry alebo autorské právo. Okrem toho sú tu aj činy, ktoré voláme **malum in se**, a sú považované za zlo takmer vždy a všade, napr. vražda, znásilnenie alebo krádež.

V každej spoločnosti prevláda určitý názor o tom, ako by sa ľudia mali normálne správať. Kriminálne sa potom chová človek, ktorý tieto obecne platné normy porušuje.

ÚVOD - METODOLÓGIA

- **Primárne pramene:** Analýza Zákona č. 300/2005 Z. z. Trestný zákon (TZ) a Zákona č. 301/2005 Z. z. Trestný poriadok (TP).
 - **Medzinárodné právo:** Budapeštiansky dohovor o počítačovej kriminalite.
 - **Právo EÚ:** Smernica 2013/40/EÚ o útokoch na informačné systémy a Smernica (EÚ) 2022/2555 (NIS2).
 - **Praktická rovina:** Oficiálne strategické a informačné materiály Ministerstva vnútra SR, Prezídia Policajného zboru a Europolu (najmä správa IOCTA).
-

ČASŤ I: TRESTNOPRÁVNÝ RÁMEC KYBERKRIMINALITY V SR

- Táto časť sa venuje právnym základom postihu kyberkriminality v Slovenskej republike, od všeobecných princípov až po konkrétne trestné činy.
- **Slovensko nemá jeden samostatný zákon s názvom „zákon o počítačovej kriminalite“, existujú ale jasné a špecifické právne normy, ktoré upravujú počítačové trestné činy v rámci Trestného zákona aj ďalších aktov**

ČASŤ I: TRESTNOPRÁVNÝ RÁMEC KYBERKRIMINALITY V SR

Zákony, ktorých ustanovenia sa týkajú počítačovej kriminality, boli prijaté vo viacerých oblastiach, a to:

- Zákon o ochrane osobných údajov (zákon č. 18/2018 Z. z.)
- Zákon o ochrane utajovaných skutočností (zákon č. 215/2004 Z.z.)
- Zákon o elektronických komunikáciách (zákon č. 452/2021 Z. z..)
- Zákon o elektronickom obchode (zákon č. 22/2004 Z.z.)
- Zákon o elektronickom podpise (zákon č. 215/2002 Z.z.)
- Zákon o dôveryhodných službách (Zákon č. 272/2016 Z.z.)

ČASŤ I: TRESTNOPRÁVNÝ RÁMEC KYBERKRIMINALITY V SR

Zákony, ktorých ustanovenia sa týkajú počítačovej kriminality, boli prijaté vo viacerých oblastiach, a to:

- Zákon o reklame (zákon č. 147/2001 Z.z.)
- Zákon o ochrane spotrebiteľa pri finančných službách na diaľku (Zákon č. 311/2025 Z. z.)
- Autorský zákon (zákon č. 185/2015 Z. z.)
- Trestný zákon (zákon č. 300/2005 Z.z.)

ČASŤ I: TRESTNOPRÁVNÝ RÁMEC KYBERKRIMINALITY V SR

Súvisiace právne predpisy ZZ SR

- [69/2018 Z. z.](#) Zákon o kybernetickej bezpečnosti
 - [165/2018 Z. z.](#) Vyhláška pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov
 - [166/2018 Z. z.](#) Vyhláška pre riešenie kybernetických bezpečnostných incidentov
 - [95/2019 Z. z.](#) Zákon o informačných technológiách vo verejnej správe
 - [179/2020 Z. z.](#) Vyhláška, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
 - [492/2022 Z. z.](#) Vyhláška, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti
 - [493/2022 Z. z.](#) Vyhláška o audite kybernetickej bezpečnosti
 - [367/2024 Z. z.](#) Zákon o kritickej infraštruktúre
 - [226/2025 Z. z.](#) Vyhláška, ktorou sa ustanovujú podrobnosti o hláseniach
 - [227/2025 Z. z.](#) Vyhláška o bezpečnostných opatreniach
-

ČASŤ I: TRESTNOPRÁVNÝ RÁMEC

- Úrad na ochranu osobných údajov SR predložil do medzirezortného pripomienkového konania návrh úplne **nového zákona o zabezpečení ochrany osobných údajov**, ktorý by mal nadobudnúť účinnosť 1. januára 2026.
- Nový zákon má za cieľ zosúladiť slovenskú právnu úpravu so zásadami európskej legislatívy tým, že sa vyhne duplicitnému preberaniu nariadenia GDPR do zákona. Namiesto toho sa sústreďí výlučne na tie oblasti, ktoré nariadenie výslovne ponecháva v kompetencii členských štátov.
- **Pre organizácie to bude znamenať potrebu revízie interných smerníc a dokumentácie** – najmä kvôli novému číslu zákona, ale aj možným vecným zmenám v povinnostiach a procesoch.

- <https://www.bezpecnostvpraxi.sk/aktuality/novy-zakon-o-ochrane-osobnych-udajov-od-roku-2026-aktbvp.htm>

ČASŤ I: TRESTNOPRÁVNÝ RÁMEC

- Úrad na ochranu osobných údajov SR predložil do medzirezortného pripomienkového konania návrh úplne **nového zákona o zabezpečení ochrany osobných údajov**, ktorý by mal nadobudnúť účinnosť 1. januára 2026.
- Nový zákon má za cieľ zosúladiť slovenskú právnu úpravu so zásadami európskej legislatívy tým, že sa vyhne duplicitnému preberaniu nariadenia GDPR do zákona. Namiesto toho sa sústreďí výlučne na tie oblasti, ktoré nariadenie výslovne ponecháva v kompetencii členských štátov.
- **Pre organizácie to bude znamenať potrebu revízie interných smerníc a dokumentácie** – najmä kvôli novému číslu zákona, ale aj možným vecným zmenám v povinnostiach a procesoch.

- <https://www.bezpecnostvpraxi.sk/aktuality/novy-zakon-o-ochrane-osobnych-udajov-od-roku-2026-aktbvp.htm>

PODSTATA A FUNKCIE TRESTNÉHO PRÁVA

- **Ochranná funkcia:** Trestné právo chráni najdôležitejšie spoločenské hodnoty a záujmy (život, zdravie, majetok, sloboda).
- **Zásada *ultima ratio* (posledný prostriedok):** Trestné právo nastupuje až vtedy, keď iné prostriedky právnej ochrany (občianske, správne právo) nie sú dostatočné.
- Štát disponuje najintenzívnejšími donucovacími prostriedkami – trestnými sankciami.

TRESTNÉ PRÁVO V DIGITÁLNO M PRIESTORE

- Aplikácia zásady *ultima ratio* je v digitálnom prostredí mimoriadne komplexná.
 - Hranica medzi protiprávnym konaním (napr. porušenie zmluvných podmienok) a trestným činom (napr. podvod) je často veľmi tenká.
 - Rozhodujúcim kritériom je **preukázanie úmyslu**, čo je v anonymnom online prostredí náročné.
 - To kladie vysoké nároky na odbornosť a technické kapacity orgánov činných v trestnom konaní.
-

ZLOŽKY TRESTNÉHO PRÁVA SR

- **Trestné právo hmotné (Trestný zákon):**
 - Vymedzuje, čo je trestný čin.
 - Stanovuje podmienky trestnej zodpovednosti.
 - Definuje druhy trestov a ochranných opatrení.
- **Trestné právo procesné (Trestný poriadok):**
 - Upravuje postup orgánov činných v trestnom konaní (policajt, prokurátor) a súdov.
 - Reguluje zisťovanie trestných činov a stíhanie páchatel'ov pri rešpektovaní základných práv.

ZÁKON Č. 300/2005 Z. Z. TRESTNÝ ZÁKON V ZNENÍ NESKORŠÍCH PREDPISOV - POJEM A DRUHY TRESTNÉHO ČINU

§ 8 Trestný čin je protiprávny čin, ktorého znaky sú uvedené v tomto zákone, ak tento zákon neustanovuje inak.

§ 9 Druhy trestných činov Trestný čin je prečin a zločin.

§ 10 Prečin

(1) Prečin je

- a) trestný čin spáchaný z nedbanlivosti alebo
- b) úmyselný trestný čin, za ktorý tento zákon v osobitnej časti ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby neprevyšujúcou päť rokov.

(2) Nejde o prečin, ak vzhľadom na spôsob vykonania činu a jeho následky, okolnosti, za ktorých bol čin spáchaný, mieru zavinenia a pohnútku páchatel'a je jeho závažnosť nepatrná.

ZÁKON Č. 300/2005 Z. Z. TRESTNÝ ZÁKON V ZNENÍ NESKORŠÍCH PREDPISOV

§ 11 Zločin

- (1) Zločin je úmyselný trestný čin, za ktorý tento zákon v osobitnej časti ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou päť rokov.
- (2) O zločin ide aj vtedy, ak v prísnejšej skutkovej podstate prečinu spáchaného úmyselne je ustanovená horná hranica trestnej sadzby prevyšujúca päť rokov.
- (3) Zločin, za ktorý tento zákon ustanovuje trest odňatia slobody s dolnou hranicou trestnej sadzby najmenej desať rokov, sa považuje za obzvlášť závažný.

ZÁKON Č. 300/2005 Z. Z. TRESTNÝ ZÁKON V ZNENÍ NESKORŠÍCH PREDPISOV

Zavinenie

§ 15 Trestný čin je spáchaný úmyselne, ak páchatel'

- a) chcel spôsobom uvedeným v tomto zákone porušiť alebo ohroziť záujem chránený týmto zákonom, alebo
- b) vedel, že svojím konaním môže také porušenie alebo ohrozenie spôsobiť, a pre prípad, že ho spôsobí, bol s tým uzrozumený.

§ 16 Trestný čin je spáchaný z nedbanlivosti, ak páchatel'

- a) vedel, že môže spôsobom uvedeným v tomto zákone porušiť alebo ohroziť záujem chránený týmto zákonom, ale bez primeraných dôvodov sa spoliehal, že také porušenie alebo ohrozenie nespôsobí, alebo
 - b) nevedel, že svojím konaním môže také porušenie alebo ohrozenie spôsobiť, hoci o tom vzhľadom na okolnosti a na svoje osobné pomery vedieť mal a mohol.
-

ZÁKON Č. 300/2005 Z. Z. TRESTNÝ ZÁKON V ZNENÍ NESKORŠÍCH PREDPISOV

PÁCHATEĽ, SPOLUPÁCHATEĽ A ÚČASTNÍK TRESTNÉHO ČINU

§ 19 Páchatel'

(1) Páchatel' trestného činu je ten, kto trestný čin spáchal sám.

§ 20 Spolupáchatel'

Ak bol trestný čin spáchaný spoločným konaním dvoch alebo viacerých páchatel'ov (spolupáchatelia), zodpovedá každý z nich, ako keby trestný čin spáchal sám.

ZÁKON Č. 300/2005 Z. Z. TRESTNÝ ZÁKON V ZNENÍ NESKORŠÍCH PREDPISOV

§ 21 Účastník

(1) Účastník na dokonanom trestnom čine alebo na jeho pokuse je ten, kto úmyselne

- a) zosnoval alebo riadil spáchanie trestného činu (organizátor),
- b) naviedol iného na spáchanie trestného činu (návodca),
- c) požiadal iného, aby spáchal trestný čin (objednávateľ), alebo
- d) poskytol inému pomoc na spáchanie trestného činu, najmä zadovážením prostriedkov, odstránením prekážok, radou, utvrdzovaním v predsavzatí, sľubom pomôcť po trestnom čine (pomocník).

(2) Na trestnú zodpovednosť účastníka sa použijú ustanovenia o trestnej zodpovednosti páchatel'a, ak tento zákon neustanovuje inak.

VYMEDZENIE POJMU "KYBERKRIMINALITA"

- Štáty EÚ sa dlhodobo zaoberali vymedzením pojmu počítačová kriminalita.
- Príslušné výbory EÚ sa dohodli na definícii počítačovej kriminality, podľa ktorej:

Počítačová kriminalita je nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu.

definícia podľa Dohovoru o počítačovej kriminalite

VYMEDZENIE POJMU "KYBERKRIMINALITA"

- Slovenský Trestný zákon neobsahuje legálnu definíciu tohto pojmu.
- Ide o pragmatický prístup, keďže akákoľvek pevne kodifikovaná definícia by mohla rýchlo zastarať a brániť postihu nových foriem kriminality.
- Právna prax a teória sa opierajú o medzinárodné dokumenty, najmä **Budapešťiansky dohovor.**

TEORETICKÉ DELENIE KYBERKRIMINALITY

- **Priama počítačová kriminalita (v užšom zmysle):**
 - Počítač, systém alebo dáta sú priamym **cieľom** útoku.
 - Jednoduché vyčíslenie škody, pretože poškodený vie presne koľko finančných prostriedkov vynaložil na kúpu počítača
- **Nepriama počítačová kriminalita (v širšom zmysle):**
 - Počítač alebo technika sú **nástrojom** na páchanie "tradičných" trestných činov.
 - Príklady: podvody, vydieranie, šírenie detskej pornografie, porušovanie autorských práv online.

TEORETICKÉ DELENIE KYBERKRIMINALITY

Druh počítačovej kriminality	Charakteristika	Príklady
Priama počítačová kriminalita	Trestné činy zamerané proti počítaču ako hmotnému majetku . Cieľom je poškodiť alebo zničiť samotné zariadenie. Škodu možno jednoducho vyčíslieť.	<ul style="list-style-type: none">• Krádež počítača alebo notebooku• Úmyselné zničenie hardvéru• Poškodenie dátového nosiča (napr. disku)• Fyzické napadnutie IT infraštruktúry (napr. rozbitie servera)
Nepriama počítačová kriminalita	Trestné činy páchané pomocou počítača , pričom útok smeruje proti nehmotnému majetku – údajom, informáciám, financiám alebo reputácii.	<ul style="list-style-type: none">• Hacking (neoprávnený prístup do systému)• Šírenie vírusov, ransomware, trojanov• Phishing a internetové podvody• Krádež identity a osobných údajov• Porušovanie autorských práv (pirátstvo)• Kyberšikana, vydieranie online• Kryptojacking (zneužitie cudzieho zariadenia na ťažbu kryptomien)• Priemyselná špionáž

KLÍČOVÉ POJMY TRESTNÉHO ZÁKONA V KONTEXTE IT

- Definície vychádzajú z Budapeštianskeho dohovoru a právnej doktríny.
- **Počítačový systém:** Zariadenie alebo skupina vzájomne prepojených zariadení, z ktorých jedno alebo viaceré automatizovane spracúvajú údaje.
 - Zahŕňa nielen PC a servery, ale aj smartfóny, tablety, sieťové prvky a zariadenia IoT.

KLÚČOVÉ POJMY (POKRAČOVANIE)

- **Počítačový údaj:** Záznam skutočností, informácií alebo pojmov vo forme vhodnej na spracovanie v počítačovom systéme.
 - Zahŕňa akékoľvek digitálne dáta, od dokumentov a obrázkov až po softvér a škodlivý kód (malvér).
- **Informačný systém:** Pojem definovaný v špecializovaných predpisoch (napr. zákon o IS verejnej správy) ako funkčný celok zabezpečujúci systematickú informačnú činnosť.

HMOTNOPRÁVNÁ ÚPRAVA - ÚVOD

- Osobitná časť Trestného zákona obsahuje viacero skutkových podstát, ktoré priamo alebo nepriamo postihujú kyberkriminalitu a dajú sa systematicky rozdeliť do niekoľkých kategórií.

TRESTNÉ ČINY PROTI DÔVERNOSTI, INTEGRITE A DOSTUPNOSTI (§ 247 - § 247D TZ)

Problematika útokov na informačné systémy

- neoprávnený prístup do počítačového systému podľa § 247 Trestného zákona,
- neoprávnený zásah do počítačového systému podľa § 247a Trestného zákona,
- neoprávnený zásah do počítačového údajov podľa § 247b Trestného zákona,
- neoprávnené zachytávanie počítačových údajov podľa § 247c Trestného zákona,
- výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov podľa § 247d Trestného zákona.

TRESTNÉ ČINY PROTI DÔVERNOSTI, INTEGRITE A DOSTUPNOSTI (§ 247 - § 247D TZ)

Tieto ustanovenia tvoria jadro postihu priamej počítačovej kriminality a sú v súlade s Budapeštianskym dohovorom.

- **§ 247 Neoprávnený prístup do počítačového systému:** Postihuje základný akt "hackingu", ak páchatel' prekoná bezpečnostné opatrenie.
- **§ 247a Neoprávnený zásah do počítačového systému:** Kriminalizuje konania narúšajúce fungovanie systému.

URČENIE HRANÍC A KRITÉRIÍ RIZIKA TRESTNÉ ČINY PROTI DÔVERNOSTI, INTEGRITE A DOSTUPNOSTI (POKRAČOVANIE)

- **§ 247b Neoprávnený zásah do počítačového údajá:** Postihuje neoprávnené vymazanie, poškodenie alebo zneprístupnenie údajov. Kľúčové pri útokoch ransomvérom.
- **§ 247c Neoprávnené zachytávanie počítačových údajov:** Postihuje neoprávnené odpočúvanie neverejného prenosu dát (tzv. *sniffing*).
- **§ 247d Výroba a držba prístupového zariadenia....:** Postihuje výrobu a distribúciu nástrojov pre kybernetické útoky (malvér, heslá).

TRESTNÉ ČINY SPÁCHANÉ CEZ POČÍTAČ: PODVODY

- § 221 - § 225 Trestného zákona

Podvod: Najčastejšie aplikovaná skutková podstata pri online podvodoch.

Páchateľ uvedie niekoho do omylu alebo využije omyl a obohatí sa na škodu cudzieho majetku.

- **Typické formy v online prostredí:**

- **Phishing, vishing, smishing:** Vylákanie citlivých údajov (heslá, čísla kariet).
 - **Podvodné e-shopy a inzertné podvody:** Tovar po zaplattení nie je nikdy dodaný.
 - **Investičné podvody (Scams):** Lákanie na fiktívne vysoko výnosné investície.
-

PODVODY A SÚVISIACA KRIMINALITA

- **§ 219 Neoprávnené vyrobenie a používanie platobného prostriedku:** Priamo postihuje tzv.

carding (zneužitie údajov z platobnej karty) a *skimming*.

- **Systematické prepojenie:** Útok podľa § 247 (neoprávnený prístup) je často len prvým krokom, ktorý páchatel'ovi umožní spáchať následný podvod podľa § 221 (napr. únik dát z e-shopu a následný phishing).

PODVODY A SÚVISIACA KRIMINALITA

- § 360b **Nebezpečné elektronické obťažovanie**
- (1) Kto úmyselne prostredníctvom elektronickej komunikačnej služby, počítačového systému alebo počítačovej siete podstatným spôsobom zhorší kvalitu života iného tým, že
 - a) ho dlhodobo poníža, zastráša, neoprávnene koná v jeho mene alebo dlhodobo inak obťažuje, alebo
 - b) neoprávnene zverejní alebo sprístupní tretej osobe obrazový, zvukový alebo obrazovo-zvukový záznam jeho prejavu osobnej povahy získaný s jeho súhlasom, spôsobilý značnou mierou ohroziť jeho vážnosť alebo privodiť mu inú vážnu ujmu na právach,
- potrestá sa odňatím slobody až na tri roky.

TRESTNÉ ČINY SÚVISIACE S NEZÁKONNÝM OBSAHOM

- Internet je hlavným kanálom na šírenie nezákonného obsahu.
- **Detská pornografia (§ 368 - § 370 TZ):**
 - Prísne sa postihuje výroba, rozširovanie a prechovávanie materiálov sexuálneho zneužívania detí (CSAM).
 - Kľúčová je legálna definícia v § 132 ods. 4 TZ.
 - Judikatúra potvrdzuje, že súhlas dieťaťa na vyhotovení materiálov je z hľadiska trestnej zodpovednosti irelevantný.

TRESTNÉ ČINY SÚVISIACE S NEZÁKONNÝM OBSAHOM

Problematika sexuálneho zneužívania detí online

- výroba detskej pornografie podľa § 368 Trestného zákona,
- rozširovanie detskej pornografie podľa § 369 Trestného zákona,
- prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení podľa § 370 Trestného zákona,
- sexuálne zneužívanie podľa § 201a Trestného zákona, tzv. Grooming.

TRESTNÉ ČINY SÚVISIACE S NEZÁKONNÝM OBSAHOM

Problematika porušovania autorských práv:

- trestný čin porušovania autorského práva podľa § 283 Trestného zákona.
- Autorský zákon (zákon č. 185/2015 Z. z.)

TRESTNÉ ČINY SÚVISIACE S NEZÁKONNÝM OBSAHO (POKRAČOVANIE)

- **Extrémistické trestné činy (§ 421 - § 422d TZ):**
 - Postihujú výrobu, rozširovanie a prechovávanie extrémistických materiálov a verejné prejavy sympatie k extrémistickým hnutiam.
- **Výzvy pri vyšetrovaní:**
 - Obrovský objem dát (P2P siete, cloud).
 - Anonymizačné nástroje a cezhraničný charakter si vyžadujú úzku medzinárodnú spoluprácu (Europol, EC3).

TRESTNÉ DOPADY APLIKOVATEĽNÉ PRE HACKING

Skutok

Právna kvalifikácia

Hacking

Porušovanie autorského práva – §283

Trestná sadzba: 6 mesiacov – 8 rokov

Porušovanie tajomstva prepravovaných správ – §196

Trestná sadzba: 1 – 10 rokov

Odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby – §198

Trestná sadzba: 1 – 5 rokov

Neoprávnené užívanie cudzej veci – §215

Trestná sadzba: 1 – 8 rokov

TRESTNÉ DOPADY APLIKOVATEĽNÉ PRE PHISHING

Skutok	Právna kvalifikácia
Phishing	<p>Neoprávnené nakladanie s osobnými údajmi - §374 <i>Trestná sadzba: 1 – 2 roky</i></p> <p>Neoprávnené obohatenie sa - §226 <i>Trestná sadzba: 6 mesiacov – 12 rokov</i></p> <p>Podvod - §221 -§226 <i>Trestná sadzba: 2 - 15 rokov</i></p> <p>Ohrozenie obchodného, bankového, poštového, telekomunikačného a daňového tajomstva - §264 <i>Trestná sadzba: 6 mesiacov - 12 rokov</i></p> <p>Neoprávnené užívanie cudzej veci - §215 <i>Trestná sadzba: 1 - 8 rokov</i></p>

TRESTNÉ DOPADY

Možné tresty:

Fyzická osoba je trestne zodpovedná od 14 rokov, za niektoré činy od 15 rokov (trestný čin sexuálneho zneužívania).

- Odňatie slobody (najčastejší pri kyberkriminalite)
- Peňažný trest
- Zákaz činnosti
- Prepadnutie veci alebo majetku
- Domáce väzenie, probačný dohľad, atď.

ŠÍRENIE DEZINFORMÁCIÍ

- Slovenský právny poriadok nepozná špecifický trestný čin „šírenia dezinformácií“.
- Postih je možný len prostredníctvom existujúcich skutkových podstát, najčastejšie **§ 361 Šírenie poplašnej správy.**
- Aplikácia je možná len v závažných prípadoch, kde je preukázateľné "vážne znepokojenie" obyvateľstva (napr. falošné správy o kontaminácii vody).
- Zavedenie nového trestného činu naráža na konflikt so slobodou prejavu a princípom právnej istoty.

TRESTNÁ ZODPOVEDNOSŤ PRÁVNICKÝCH OSÔB (ZOTZPO)

- Zákon č. 91/2016 Z. z. zaviedol tzv. pravú trestnú zodpovednosť právnických osôb.
- Trestný čin sa považuje za spáchaný právnickou osobou, ak ho v jej prospech, mene alebo rámci činnosti spáchal napr. štatutár, zamestnanec alebo osoba vykonávajúca kontrolnú činnosť.

Firma môže byť trestne zodpovedná, ak trestný čin:

- umožnila zlou organizáciou, dohľadom či kontrolou,
- bol vykonaný v prospech firmy.

ZOTZPO - APLIKÁCIA NA KYBERKRIMINALITU

- Zákon obsahuje katalóg trestných činov, za ktoré môže byť právnická osoba stíhaná.
- Tento katalóg zahŕňa všetky kľúčové kybernetické trestné činy:
 - § 247 až § 247d (Neoprávnený prístup a súvisiace činy)
 - § 221 (Podvod)
 - § 219 (Neoprávnené použitie platobného prostriedku)
 - § 369 (Rozširovanie detskej pornografie)
 - § 422b (Rozširovanie extrémistických materiálov)
- Tento inštitút je kľúčový pre presadzovanie kybernetickej bezpečnosti v korporátnom sektore.

ZOTZPO - APLIKÁCIA NA KYBERKRIMINALITU

Kyberkriminalita môže súvisieť s aktivitami ako:

- Účelové zneužitie IT prostriedkov firmy
- Podvody cez e-shopy
- Protiprávne nakladanie s databázami
- Sprístupňovanie pirátskeho softvéru
- Prevádzkovanie nelegálnych kryptoplatforiem
- Organizovanie DDoS alebo iných útokov cez vlastnú infraštruktúru

Pri právnickej osobe sa skúma:

- systém riadenia a kontroly vo firme,
- či vedenie firmy vedelo, malo vedieť, umožnilo alebo nariadilo čin.

ZOTZPO - APLIKÁCIA NA KYBERKRIMINALITU

Možné tresty pre právnickú osobu:

- Zrušenie právnickej osoby
 - Prepadnutie majetku
 - Peňažný trest (často veľmi vysoký)
 - Zákaz činnosti
 - Zákaz prijímania dotácií, verejných financií
 - Zákaz účasti vo verejnom obstarávaní
 - Zverejnenie odsudzujúceho rozsudku
 - Prepadnutie vec
-

PROCESNOPRÁVNE ASPEKTY - ŠPECIFIKÁ DOKAZOVANIA

Vyšetrovanie kyberkriminality je náročné pre:

- **Volatilita (prchavosť) dôkazov:** Digitálne stopy môžu byť ľahko a rýchlo zničené.
- **Anonymita a pseudonymita:** Páchatelia využívajú VPN, Tor a falošné identity.
- **Cezhraničný charakter:** Dáta sa často nachádzajú na serveroch v rôznych krajinách.
- **Objem dát:** Analýza enormného množstva dát je technicky a personálne náročná.

- **Charakter dokazovania v oblasti kybernetickej bezpečnosti** je špecifický v tom, že sa opiera o zaistenie, uchovanie a interpretáciu nehmotných stôp, existujúcich len v kybernetickom priestore, súhrne nazývaných „digitálne stopy“.

DIGITÁLNY DÔKAZ

- Trestný poriadok SR neobsahuje legálnu definíciu pojmu „digitálny dôkaz“.
- Táto absencia je **kritickou procesnou medzerou**: zákon kriminalizuje digitálne konania, no neposkytuje jasné pravidlá pre zaobchádzanie s digitálnymi dôkazmi.
- V praxi sa postupuje podľa všeobecných ustanovení, čo môže byť právne napadnuteľné.

INŠTITÚTY TRESTNÉHO PORIADKU NA ZAIŠŤOVANIE DÔKAZOV

- **§ 116 TP - Zisťovanie údajov o elektronickej komunikácii:** Umožňuje získať prevádzkové a lokalizačné údaje (metadáta), ale nie obsah komunikácie. Vyžaduje príkaz sudcu.
- **§ 90 TP - Uchovanie a vydanie počítačových údajov:** Príkaz na uchovanie konkrétnych údajov (max. 90 dní), po ktorom môže nasledovať príkaz na ich vydanie.
- **Klasické inštitúty:** Vydanie a odňatie veci alebo domová prehliadka na fyzické zaistenie nosičov dát (PC, telefóny, USB).

ČASŤ II: INŠTITUCIONÁLNY RÁMEC BOJA PROTI KYBERKRIMINALITE

- Táto časť mapuje špecializované zložky Policajného zboru SR a kľúčovú úlohu európskych agentúr.
- V rámci Slovenskej republiky je zástupcom pre riešenie počítačovej kriminality Špecializovaný útvar Policajného zboru. Odbor, ktorý sa priamo zaoberá problematikou počítačovej kriminality, je Odbor počítačovej kriminality Úradu kriminálnej polície Prezídia Policajného zboru.

ŠPECIALIZOVANÉ ÚTVARY PZ SR

- **1. júl 2013:** Vznikol **Odbor počítačovej kriminality** ako reakcia na nárast kybernetickej trestnej činnosti.
- **1. február 2022:** V rámci reformy bol odbor začlenený do novovzniknutej **Národnej centrály osobitných druhov kriminality (NCODK)** Prezídia PZ.
- Cieľom NCODK je zefektívniť boj proti najzávažnejším formám kriminality, vrátane tej počítačovej.

ODBOR POČÍTAČOVEJ KRIMINALITY (NCODK)

- Je ústredným a najvyšším špecializovaným pracoviskom PZ pre boj s kyberkriminalitou s celoslovenskou pôsobnosťou.
- **Dvojaká úloha:**
 - **Servisná a metodická činnosť:** Poskytuje technickú a metodickú pomoc ostatným útvarom PZ.
 - **Výkonná činnosť:** Priamo vyšetruje obzvlášť zložité a závažné prípady, najmä s medzinárodným prvkom.
- **Štruktúra:**
 - Oddelenie odhaľovania
 - Oddelenie objasňovania a odborných činností

EUROPOL A JEHO ÚLOHA

- Agentúra Európskej únie pre spoluprácu v oblasti presadzovania práva.
- **Hlavné poslanie:** Podporovať členské štáty v boji proti závažnej medzinárodnej trestnej činnosti, kyberkriminalite a terorizmu.
- **Nemá výkonné právomoci** (nemôže zatýkať ani vykonávať prehliadky).
- Pôsobí ako centrálny uzol pre
 - **výmenu informácií, operačnú analýzu, expertízu a koordináciu** cezhraničných operácií.

EURÓPSKE CENTRUM PRE BOJ PROTI POČÍTAČOVEJ KRIMINALITE (EC3)

- Špecializované centrum zriadené v rámci Europolu v januári 2013.
- Cieľom je posilniť reakciu orgánov presadzovania práva na kyberkriminalitu v EÚ.
- **Strategické priority:**
 1. **Kyberkriminalita závislá od technológií** (malvér, hacking, ransomvér).
 2. **Online sexuálne zneužívanie detí** (boj proti CSAM).
 3. **Platobné podvody** (phishing, podvody s kartami).

ŠTRUKTÚRA A ČINNOSŤ EC3

EC3 uplatňuje trojpilierový prístup:

- 1. Operations (Operácie):** Poskytuje analytickú a koordinačnú podporu pri vyšetrovaniach členských štátov.
- 2. Forensics (Forezná činnosť):** Poskytuje vysokošpecializovanú technickú a digitálnu forenznú podporu (analýza malvéru, dešifrovanie, analýza kryptomien).
- 3. Strategy & Partnerships (Stratégia a partnerstvá):** Buduje partnerstvá so súkromným sektorom a akademickou obcou, vypracúva strategické analýzy (IOCTA).

SPOLOČNÁ OPERAČNÁ SKUPINA (J-CAT)

- **Joint Cybercrime Action Taskforce (J-CAT)** zriadená v septembri 2014 v rámci EC3.
- Operačný tím zložený zo styčných dôstojníkov z členských a kľúčových partnerských krajín, ktorí pracujú spoločne v sídle Europolu.
- **Hlavný cieľ:** Riadiť spravodajsky podložené a koordinované akcie proti najvýznamnejším kyberkriminálnym hrozbám a páchatelom.

STRATEGICKÁ ANALÝZA - SPRÁVA IOCTA

- **Internet Organised Crime Threat Assessment (IOCTA)** je jedným z najdôležitejších strategických produktov EC3.
- Poskytuje komplexný prehľad najnovších trendov a hrozieb v oblasti kyberkriminality z pohľadu orgánov presadzovania práva.

<https://www.europol.europa.eu/publications-events/main-reports/iocta-report>

KLÚČOVÉ TRENDY PODĽA IOCTA

- **Zločin ako služba (Crime-as-a-Service):** Profesionalizovaný ekosystém, kde si páchatelia môžu na darknete kúpiť alebo prenajať nástroje a služby (napr. Ransomware-as-a-Service).
- **Dominancia sociálneho inžinierstva a phishingu:** Ľudský faktor zostáva najslabším článkom. Phishing je hlavným počítačným vektorom väčšiny útokov.
- **Ukradnuté dáta ako centrálna komodita:** Osobné a finančné údaje sú hlavnou komoditou, s ktorou sa obchoduje v kyberkriminálnom podsvetí.

ČASŤ III: MEDZINÁRODNÝ KONTEXT A BUDÚCE VÝZVY

- Táto časť zasadzuje problematiku do širšieho medzinárodného kontextu a analyzuje budúce výzvy.

BUDAPEŠŤIANSKY DOHOVOR O POČÍTAČOVEJ KRIMINALITE

- Dohovor Rady Európy z roku 2001 je prvým a najdôležitejším medzinárodným zmluvným nástrojom v tejto oblasti.
- **Jeho význam spočíva v 3 pilieroch:**
 1. **Harmonizácia hmotného trestného práva** (kriminalizácia činov ako nelegálny prístup, počítačový podvod, detská pornografia).
 2. **Harmonizácia procesného práva** (nástroje na efektívne vyšetovanie).
 3. **Vytvorenie rámca pre rýchlu medzinárodnú spoluprácu** (sieť kontaktných bodov 24/7).

PRÁVNÝ RÁMEC EÚ

- **Smernica 2013/40/EÚ (o útokoch na IS):** Trestnoprávny nástroj, ktorý harmonizuje trestné právo členských štátov a stanovuje minimálne úrovne sankcií za hacking, DDoS útoky atď. (represívny prístup).
- **Smernica (EÚ) 2022/2555 (NIS2):** Regulačno-preventívny nástroj, ktorý ukladá povinnosti širokému spektru subjektov (prevádzkovatelia základných služieb) prijať bezpečnostné opatrenia a hlásiť incidenty.

BUDÚCE VÝZVY - UMELÁ INTELIGENCIA (AI)

- **Zneužitie AI páchatel'mi:** Automatizácia a zvyšovanie efektivity útokov (tvorba malvéru, generovanie presvedčivých phishingových e-mailov, vytváranie *deepfakes*).
- **Problém trestnej zodpovednosti:**
 - Systémy AI nemajú právnu subjektivitu a nemôžu byť trestne zodpovedné.
 - Zodpovednosť sa musí pričítať fyzickej alebo právnickej osobe (programátor, používateľ, prevádzkovateľ).
 - S rastúcou autonómiou AI hrozí vznik "**medzery v zodpovednosti**" (*responsibility gap*), keď je ťažké aplikovať tradičné koncepty zavinenia.

BUDÚCE VÝZVY - INTERNET VECÍ (IOT)

- Exponenciálny nárast pripojených zariadení vytvára **masívnu novú útočnú plochu**.
- Mnohé IoT zariadenia majú slabé alebo žiadne bezpečnostné zabezpečenie.
- **Trestnoprávne riziká:**
 - **Tvorba botnetov** na páchanie masívnych DDoS útokov (napr. botnet Mirai).
 - **Špionáž a narušenie súkromia** prostredníctvom kompromitovaných kamier a mikrofónov.
 - **Útoky s následkami vo fyzickom svete** (útoky na medicínske prístroje, dopravné systémy).

BUDÚCE VÝZVY – DEEP FAKE

Vyzliekacie aplikácie (tzv. deep nudes, AI deep nude, AI fake nude) sú softvérové nástroje poháňané umelou inteligenciou, ktoré dokážu z fotografií či videí odstrániť oblečenie, vygenerovať nahé ľudské telo a vytvoriť tak realistickú ilúziu nahoty.

Nástroje, ktoré toto umožňujú, sú pritom voľne k dispozícii, zneužiť ich tak môže doslova ktokoľvek. Táto technológia navyše nie je nijako regulovaná, v praxi ju môže využívať v podstate ktokoľvek, mnoho aplikácií tohto typu je úplne zadarmo.

BUDÚCE VÝZVY – DEEP FAKE

- **OHOVÁRANIE (§ 373)** Vytvorenie a šírenie deepfaku, ktorý zobrazuje osobu nahú alebo sexuálne, môže vážne poškodiť jej česť a vážnosť.
- **POŠKODZOVANIE CUDZÍCH PRÁV (§ 375)** Ak deepfake spôsobí osobe vážnu ujmu (súkromná, pracovná, spoločenská).
- **NEOPRÁVNENÉ NAKLADANIE S OSOBNÝMI ÚDAJMI (§ 374)**
- Použitie tváre osoby alebo jej identifikátorov **bez súhlasu** môže byť považované za porušenie práv.

BUDÚCE VÝZVY – DEEP FAKE

V Národnej rade SR prebieha legislatívne konanie, ktoré má:

- **zakotviť nové skutkové podstaty týkajúce sa zlomyselného tvorenia a šírenia deepfake obsahu,**
- **posilniť právo na ochranu digitálnej identity a**
- **doplniť aj rýchle súdne opatrenia proti šíreniu deepfake materiálu.**

ODPORÚČANIA - *DE LEGE FERENDA* (PRE LEGISLATÍVU)

- Je žiaduce zvážiť **zavedenie legálnej definície „digitálneho dôkazu“** a špecifických procesných pravidiel pre jeho zaistovanie a uchovávanie do Trestného poriadku.
- Cieľom je **zvýšiť právnu istotu** a znížiť riziko spochybňovania zákonnosti dôkazov v súdnom konaní.

ODPORÚČANIA - PRE PRAX A SPOLUPRÁCU

- **Aplikačná prax:** Pokračovať v neustálom vzdelávaní a špecializácii policajtov, prokurátorov a sudcov. Posilňovať personálne a technické kapacity Odboru počítačovej kriminality NCODK.
- **Medzinárodná spolupráca:** Prehĺbenie a zrýchlenie spolupráce, najmä prostredníctvom platforiem Europolu (EC3, J-CAT), je absolútnou nevyhnutnosťou.
- **Prevencia a partnerstvo:** Budovať silné partnerstvá so súkromným sektorom a akademickou obcou a investovať do osvetových kampaní pre verejnosť.

ĎAKUJEM ZA POZORNOST

- Otázky a odpověde