ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLIV
1/2025

VÝZVY TRESTNÉHO PRÁVA V DIGITÁLNOM VEKU: NEOPRÁVNENÝ PRÍSTUP DO POČÍTAČOVÉHO SYSTÉMU A KYBERŠIKANA

JUDr. Michal Minárik, PhD.

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra trestného práva, kriminológie a kriminalistiky
michal.minarik@flaw.uniba.sk

JUDr. Lenka Miklóssyová

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra trestného práva, kriminológie a kriminalistiky
lenka.miklossyova@flaw.uniba.sk

Výzvy trestného práva v digitálnom veku: neoprávnený prístup do počítačového systému a kyberšikana

Rozmach digitálnych technológií priniesol nielen nové možnosti komunikácie a prístupu k informáciám, ale zároveň aj nové formy kriminality, ktoré predstavujú významnú výzvu pre trestné právo. Tento článok sa zameriava na analýzu skutkovej podstaty trestného činu neoprávneného prístupu do počítačového systému podľa § 247 zákona č. 300/2005 Z. z. Trestného zákona (ďalej len „**TZ**“) a jeho príbuzných skutkových podstát, pričom reflektuje aj ich systematické zaradenie, teoretické základy a aplikačné ťažkosti. Autori sa venujú aj relevantnej európskej úprave, a upozorňujú na nedostatky v aplikačnej praxi, vrátane nízkej objasnenosti skutkov. Okrajovo je analyzovaná aj problematika kyberšikany ako forma kriminality úzko spätá s digitálnym prostredím, s dôrazom na novozavedený trestný čin nebezpečného elektronického obťažovania podľa § 360b TZ. Cieľom príspevku je prispieť k odbornej diskusii o efektívnosti trestnoprávnej reakcie na kybernetickú kriminalitu v kontexte súčasných výziev digitálneho veku.

Criminal law challenges in the digital age: unauthorised access to a computer system and cyberbullying

The expansion of digital technologies has brought not only new opportunities for communication and access to information but also new forms of criminality that pose a significant challenge for criminal law. This article focuses on the analysis of the elements of the criminal offence of unauthorized access to a computer system under Section 247 of Act No. 300/2005 Coll., the Criminal Code (hereinafter referred to as the "**Criminal Code**") along with related offences, while also reflecting on their systematic classification, theoretical foundations, and practical difficulties in application. The authors also address relevant European legislation and highlight deficiencies in practical enforcement, including the low clearance rate of such offences. The article also briefly examines the issue of cyberbullying as a form of crime closely linked to the digital environment, with particular emphasis on the newly introduced criminal offence of dangerous electronic harassment under Section 360b of the Criminal Code. The aim of the article is to contribute to the professional discourse on the effectiveness of the criminal law response to cybercrime in the context of the current challenges of the digital age.

Kľúčové slová: kyberkriminalita, neoprávnený prístup, počítačový systém, kyberšikana, Trestný zákon, elektronické obťažovanie, trestné právo

Keywords: cybercrime, unauthorized access, computer system, cyberbullying, Criminal Code, electronic harassment, criminal law

https://doi.org/10.62874/afi.2025.1.08

Úvod

Digitalizácia spoločnosti a prudký rozvoj informačných technológií viedli k vzniku nových foriem kriminality, ktoré si vyžadujú osobitnú trestnoprávnu reakciu. Slovenský právny poriadok reagoval na tieto výzvy zakotvením skupiny tzv. **„anti-hackerských“ trestných činov** do TZ, medzi ktorými zohráva kľúčovú úlohu skutková podstata neoprávneného prístupu do počítačového systému podľa § 247 TZ.

Príspevok sa zameriava na analýzu tohto trestného činu z hľadiska jeho znakov, systematického zaradenia a aplikačných problémov, pričom reflektuje aj relevantnú európsku úpravu a štatistické údaje o objasnenosti. Okrajovo je venovaná pozornosť aj **fenoménu kyberšikany** a jeho trestnoprávnemu postihu, najmä v kontexte novozavedeného

trestného činu **nebezpečného elektronického obťažovania**. Cieľom príspevku je prispieť k odbornej diskusii o efektívnosti a praktickej uplatniteľnosti právnych nástrojov na boj proti kyberkriminalite.

1 Právny rámec kyberkriminality na Slovensku

Vo všeobecnosti sa kyberkriminalita delí na dva základné typy: **cyber-dependent** a **cyber-enabled kriminalitu**, ktoré sa líšia podľa miery závislosti na informačných a komunikačných technológiách.[1] **Cyber-dependent kriminalita** predstavuje trestnú činnosť, ktorá je úplne závislá od technológií. Ide o trestné činy, ktoré môžu byť páchané výlučne prostredníctvom počítačov, počítačových sietí alebo iných druhov informačných a komunikačných technológií. V rámci tohto typu kriminality sú technológie nielen nástrojom, ale aj samotným cieľom útoku.[2] Typickými príkladmi sú nelegálny prienik do informačných systémov (hacking) či šírenie škodlivého softvéru (malware). Tento typ kyberkriminality sa označuje aj ako kyberkriminalita v užšom zmysle. Naopak, **cyber-enabled kriminalita** označuje trestnú činnosť, ktorá je technológiami iba „umožnená". Ide o také trestné činy, ktoré síce môžu byť spáchané aj bez využitia moderných technológií, avšak ich použitie zvyšuje ich účinnosť, dosah alebo rozsah. Informačné a komunikačné technológie teda nie sú nevyhnutným predpokladom na ich spáchanie, no zásadne ovplyvňujú ich závažnosť.[3] Príkladom sú prípady rozširovania detskej pornografie alebo nebezpečného prenasledovania (tzv. stalking), pri ktorých technológie slúžia ako prostriedok na vykonanie skutku. Tento typ kriminality sa označuje ako kyberkriminalita v širšom zmysle.

Slovenský TZ explicitne upravuje vyššie popísanú **cyber-dependent kriminalitu** vo svojej osobitnej časti. Ide najmä o skupinu trestných činov zaradených do štvrtej hlavy TZ medzi **trestné činy proti majetku**, neoficiálne nazývané aj „*počítačové trestné činy*". Tieto ustanovenia boli do TZ pridané novelou účinnou od 1. januára 2016 (zákon

[1] CROWN PROSECUTION SERVICE. Cybercrime – prosecution guidance. In: CPS.gov.uk [online]. [cit. 27.05.2025]. Dostupné na: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

[2] DRAŽOVÁ, P. Kyberkriminalita [online]. Bratislava: Právnická fakulta Univerzity Komenského, [cit. 29.05.2025]. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/Prednasky/Kyberkriminalita.pdf.

[3] DRAŽOVÁ, P. Kyberkriminalita [online]. Bratislava: Právnická fakulta Univerzity Komenského, [cit. 29.05.2025]. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/Prednasky/Kyberkriminalita.pdf.

č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, ďalej len „**zákon č. 398/2015 Z. z.**“), ktorá do právnej úpravy zaviedla ucelený systém tzv. **„anti-hackerských“ trestných činov**.[4] Táto zmena predstavovala transpozíciu požiadaviek **smernice Európskeho parlamentu a Rady 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV** (ďalej len „Smernica 2013/40/EÚ“), ktorá stanovila minimálne pravidlá na vymedzenie trestných činov, akými sú napríklad nezákonné vniknutie do informačných systémov, neoprávnené zasahovanie do údajov a pod. Slovenský zákonodarca na to reagoval zrušením pôvodného trestného činu *poškodenia a zneužitia záznamu na nosiči informácií* (§ 247 TZ v starom znení) a jeho nahradením piatimi novými skutkovými podstatami: **§ 247 neoprávnený prístup do počítačového systému, § 247a neoprávnený zásah do počítačového systému, § 247b neoprávnený zásah do počítačového údaja, § 247c neoprávnené zachytávanie počítačových údajov a § 247d výroba a držba prístupového zariadenia alebo hesla do počítačového systému**.

Neoprávneného prístupu do počítačového systému podľa § 247 TZ sa dopustí ten, kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti, a to buď neoprávneným vkladaním, prenášaním, poškodzovaním, vymazávaním, či iným neoprávneným zaobchádzaním s počítačovými údajmi, alebo neoprávneným zásahom do technického či programového vybavenia počítača, pričom takto získané informácie následne neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu.[5] Ide teda o postih **neoprávneného vniknutia** do cudzieho informačného systému (napr. počítača, servera, siete) tým, že páchateľ zdolá nejakú formu ochrany, ktorou bol systém zabezpečený. Takéto konanie je trestné bez ohľadu na ostatné okolnosti prípadu, to znamená, že zákon nevyžaduje pre trestnosť činu vznik určitej výšky škody alebo spôsobenie určitej ujmy na právach.

Podľa dôvodovej správy k zákonu č. 398/2015 Z. z. je individuálnym objektom u týchto novo zavedených počítačových trestných činov *„najmä ochrana počítačového systému ako celku alebo časti a ochrana počítačového údaju ako citlivej a zneužiteľnej informácie, do ktorej*

[4] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY. Dôvodová správa k návrhu zákona o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov. [online]. [cit. 21.5.2025]. Dostupné na: https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=417320.

[5] Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, § 247.

neoprávnený zásah je vzhľadom na široké spektrum možných negatívnych aspektov neakceptovateľný.“[6]

Z pohľadu **systematiky** ide síce o majetkové trestné činy, avšak trestný čin neoprávneného prístupu do počítačového systému má presah do viacerých sfér vrátane ochrany súkromia a údajov. Páchateľom býva najčastejšie **„hacker“** útočiaci zvonka na cudzí systém, ale teoreticky možno neoprávnený prístup spáchať aj **„insiderom“**, teda napríklad zamestnancom prekračujúcim svoje oprávnenia prístupu v rámci firemnej siete. V tomto kontexte považujeme za potrebné poznamenať, že pre účely dokazovania je relevantné, že z hľadiska trestného práva je **vecou** v zmysle § 130 ods. 2 TZ aj nehmotná informácia, dáta výpočtovej techniky alebo obrazový záznam na technickom nosiči. Táto skutočnosť má význam pri dokazovaní počítačových trestných činov preto, že nám napr. umožňuje **zaistiť digitálne dáta pri domovej prehliadke ako vec dôležitú pre dokazovanie**. *„Z uvedenej zákonnej definície pojmu „vec“ je zrejmé, že pri domovej prehliadke môžu byť predmetom zaistenia aj počítačové údaje, ktoré majú právnu povahu veci a ktoré sú zachytené na technickom nosiči, t. j. ktoré sú zachytené najmä na CD, DVD, USB kľúči, harddisku počítača, harddisku mobilného telefónu a podobne. Na tomto mieste je potrebné zdôrazniť, že počítačové údaje (ako nehmotný objekt) sú spravidla uložené na nejakom nosiči, ktorý je spôsobilý na ich trvalý alebo dočasný záznam.“*[7]

Skutková podstata trestného činu neoprávneného prístupu do počítačového systému je definovaná viacerými **typovými znakmi**, ktoré musia byť naplnené, aby mohlo byť konanie posúdené ako tento trestný čin. **Objektívna stránka** spočíva v *prekonaní bezpečnostného opatrenia* a získaní neoprávneného prístupu do systému.[8] Pojem *„bezpečnostné opatrenie“* právna úprava bližšie nedefinuje, ale v praxi pôjde o akúkoľvek bariéru brániacu voľnému vstupu do systému: typicky **heslo, prístupový kód, firewall, bezpečnostný softvér** a pod. Podmienkou trestnosti je, že páchateľ toto opatrenie *prekoná*, to znamená, že **dobrovoľné poskytnutie hesla** oprávnenou osobou (napr. ak používateľ sám útočníkovi prezradí svoje prihlasovacie údaje) zapríčiňuje, že

[6] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY. Dôvodová správa k návrhu zákona o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov. [online]. [cit. 21.5.2025]. Dostupné na: https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=417320.

[7] ŠAMKO, P. K zaisťovaniu počítačových údajov v trestnom konaní. Právne listy [online]. 21.1.2018 [cit. 21.5.2025]. Dostupné na: https://www.pravnelisty.sk/clanky/a626-k-zaistovaniu-pocitacovych-udajov-v-trestnom-konani.

[8] Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, § 247.

absentuje znak prekonania ochrany a v takom prípade páchateľ **nenaplní objektívnu stránku** tohto trestného činu, hoci by fakticky mohlo ísť o neautorizovaný vstup. Výnimočne by však mohlo prichádzať do úvahy posúdenie tohto konania ako **iného trestného činu** (napr. podvodu, ak páchateľ vyláka heslo podvodným konaním a získa tak prístup). Ak systém **žiadnu ochranu nemal** (bol voľne prístupný), nemožno hovoriť o trestnom čine podľa § 247 TZ.

Za zmienku stojí, že pri skúmaní spoločenskej škodlivosti konania prichádza do úvahy aj uplatnenie **materiálneho korektívu**. V kontexte neoprávneného prístupu do počítačového systému to znamená posúdiť napr. **motív a cieľ konania**, **rozsah zásahu** a rovnako jeho **následky**.[9]

Subjektívna stránka neoprávneného prístupu do počítačového systému vyžaduje úmyselné zavinenie. Páchateľ si teda musí byť vedomý, že preniká do cudzieho systému bez oprávnenia a vedome prelomiť alebo obísť jeho bezpečnostné prvky. Neopatrnosť či nedbanlivosť nestačí, čo znamená, že ak by napríklad niekto omylom vstúpil do cudzej databázy lebo systém nevyžadoval heslo a on sa domnieval, že ide o verejný prístup, chýbal by úmysel spáchať tento trestný čin. Naopak, v praxi častejšie nastávajú situácie, že páchateľ koná *s* priamym úmyslom, motivovaný napríklad snahou získať tajné informácie, spôsobiť škodu alebo **získať osobné údaje inej osoby s cieľom ich zneužitia**. Práve posledný menovaný motív zákon výslovne spomína pri príbuzných skutkových podstatách (§ 247a, 247b TZ uvádzajú zneužitie osobných údajov na získanie dôvery tretej strany ako okolnosť podmieňujúcu použitie vyššej trestnej sadzby). To naznačuje, že spojenie **kybernetického útoku s neoprávneným nakladaním s osobnými údajmi** sa považuje za obzvlášť nebezpečné (typicky ide o krádež identity či phishing, kedy páchateľ použije cudzie údaje na oklamanie ďalších osôb).

2 Odhaľovanie a stíhanie „anti-hackerských“ trestných činov

Napriek komplexnej právnej úprave zostáva odhaľovanie a stíhanie „anti-hackerských“ trestných činov výzvou. **Štatistiky kriminality** dostupné z Ministerstva vnútra SR vykazujú nasledovné údaje:

[9] Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, § 10 ods. 2.

Rok	Trestný čin	Zistené	Objasnené	Objasnené (v %)
2016	§ 247 (1)	16	-	-
	§ 247 (2)	1	-	-
2017	§ 247 (1)	26	-	-
2018	§ 247 (1)	23	-	-
2019	§ 247 (1)	29	4	14 %
2020	§ 247	27	-	-
	§ 247a	19	-	-
	§ 247b	11	1	9 %
	§ 247c	5	-	-
2021	§ 247	37	1	3 %
	§ 247a	14	-	-
	§ 247b	19	-	-
	§ 247c	1	-	-
	§ 247d	1	-	-
2022	§ 247	28	-	-
	§ 247a	10	-	-
	§ 247b	4	-	-
	§ 247c	2	-	-
2023	§ 247	28	-	-
	§ 247a	10	-	-
	§ 247b	4	-	-
	§ 247c	2	1	50 %
2024	§ 247	25	1	4 %
	§ 247a	11	-	-
	§ 247b	9	1	11 %

Tabuľka 1: Štatistika „anti-hackerských" trestných činov v rokoch 2016 – 2024[10]

[10] MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY. Štatistika kriminality v Slovenskej republike. [online]. [cit. 21.5.2025]. Dostupné na: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml.

Vo vyššie uvedenej tabuľke môžeme vidieť štatistické údaje týkajúce sa „anti-hackerských“ trestných činov na Slovensku v rokoch 2016-2024. Rok 2016 sme si vybrali ako začiatok skúmaného obdobia práve z toho dôvodu, že ako už bolo vyššie spomínané, trestné činy podľa § 247 až § 247d v novom znení vošli do účinnosti od januára 2016. Avšak v počiatočných rokoch v zbieraných údajoch sú pravdepodobne evidované aj trestné činy podľa starej právnej úpravy, kedy § 247 TZ upravoval trestný čin *poškodenia a zneužitia záznamu na nosiči informácií*. Tento trestný čin tiež môžeme zaradiť do kategórie „anti-hackerských“ trestných činov. Na základe údajov z tabuľky možno konštatovať, že ich **objasňovanie sa ukazuje ako problematické**. Už od roku 2016, kedy nadobudla účinnosť novela č. 398/2015 Z. z. implementujúca do právneho poriadku SR osobitné skutkové podstaty zamerané na ochranu počítačových systémov a údajov, je evidovaný výskyt viacerých skutkov kvalifikovateľných ako trestné činy v oblasti kyberkriminality podľa novozavedených § 247 a § 247a až § 247d. Napriek tomu však štatistické údaje svedčia o tom, že objasňovanie tejto formy kriminality je nízke a bez zreteľného trendu zlepšovania.

V počiatočných rokoch sledovaného obdobia (2016 – 2018) dominoval výskyt skutkov podľa § 247 TZ, avšak údaje o objasnenosti v tomto období absentujú. Prvé dostupné údaje o objasnení sa objavujú až v roku 2019, kedy bolo zo 29 zaznamenaných skutkov objasnených len 4, čo predstavuje objasnenosť 14 %. Následne sa objasnenosť výrazne znížila: v roku 2021 boli pri 37 skutkoch podľa § 247 objasnený len 1 (3 %) a podobne nízke hodnoty sa opakovali aj v rokoch 2023 a 2024 (4 %). Pri skutkových podstatách zavedených novelou z roku 2015 je situácia obdobná – výskyt skutkov podľa § 247a až § 247d je pravidelný, ale v nízkych absolútnych číslach a s minimálnymi objasnenými prípadmi. V roku 2020 bolo napríklad zistených 11 skutkov podľa § 247b, z ktorých bol objasnený iba jeden (9 %). Výnimočný je údaj z roku 2023, kedy boli zaznamenané dva skutky podľa § 247c a jeden z nich bol objasnený, čo predstavuje objasnenosť 50 %. Ide však o štatisticky málo významný údaj vzhľadom na nízky počet prípadov. Podobne aj § 247b vykazuje v roku 2024 objasnenosť 11 %, keď bol z objasnených deviatich skutkov objasnený jeden.

Podobné údaje evidujeme aj zo štatistík Ministerstva spravodlivosti SR, kde napríklad za rok 2023 boli celkovo za trestné činy podľa § 247

až § 247d **odsúdené iba 3 osoby**[11], čo samozrejme samé o sebe **neznamená neefektívnosť právnej úpravy**, avšak v komplexnom zhodnotení spolu so štatistickými údajmi Ministerstva vnútra SR značí o nízkej miere objasnenosti v tejto oblasti, čo môže naznačovať nedostatočné odhaľovanie páchateľov.

Skutočnosť, že objasnenosť skutkov sa dlhodobo pohybuje na úrovni jednotiek percent, poukazuje na **problémy v oblasti vyšetrovania týchto deliktov**. Tieto nedostatky môžu vyplývať jednak z technickej a personálnej nepripravenosti orgánov činných v trestnom konaní, ako aj z povahy samotných skutkov, ktoré si často vyžadujú špecifické odborné znalosti a medzinárodnú spoluprácu. S ohľadom na technologický vývoj a rastúci význam digitálnej bezpečnosti je nevyhnutné posilniť kapacity orgánov činných v trestnom konaní v tejto oblasti, vrátane zlepšenia analytických nástrojov, odborného a pravidelného vzdelávania a aktívnej kooperácie s odbornou verejnosťou. Bez týchto opatrení ostane právny rámec boja proti kybernetickej kriminalite len formálnym a jeho praktická účinnosť bude aj naďalej limitovaná.

Okrem toho je však potrebné poznamenať, že tieto tzv. „antihackerské" trestné činy netvoria gro počítačovej kriminality. Podľa JUDr. Srholca, vyšetrovateľa Policajného zboru SR, najrozšírenejším trestným činom v oblasti počítačovej kriminality sú trestné činy súvisiace s **detskou pornografiou**. Na základe jeho výskumu, ktorý vyhodnocoval štatistické údaje za rok 2018, viac než polovicu počítačovej kriminality predstavoval **trestný čin šírenia detskej pornografie**, ďalších 14 % tvorilo prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení, 11 % porušovanie autorského práva a 8 % výroba detskej pornografie, pričom zvyšok tvorili iné skutkové podstaty.[12] *„V roku 2018 by sa dalo povedať, že počítačová trestná činnosť je viac menej záležitosťou týkajúcou sa detskej pornografie (až na 87,7 %) a nie „antihackerských trestných činov". „Kladivo" na počítačových kriminálnikov, ustanovenia § 247 – § 247dTZ, teda spomenuté „antihackerské trestné činy", majú podiel 0,75 % z nápadu počítačovej*

[11] MINISTERSTVO SPRAVODLIVOSTI SLOVENSKEJ REPUBLIKY. Trestná agenda – štatistický prehľad za rok 2023 [online]. Bratislava: Ministerstvo spravodlivosti SR, 2024 [cit. 01.06.2025]. Dostupné na: http://justice.gov.sk/dokumenty/2025/03/I.-Trestna-agenda_2023.pdf.

[12] SRHOLEC, M. Kriminalistické avízo – časť IV. Počítačová kriminalita. Právne listy [online]. 18.6.2019 [cit. 21.5.2025]. Dostupné na: https://www.pravnelisty.sk/clanky/a753-kriminalisticke-avizo-cast-iv-pocitacova-kriminalita.

trestnej činnosti."[13] Tieto informácie naznačujú, že tzv. „anti-hackerské" trestné činy (§ 247 – 247d TZ) tvoria len **zanedbateľný zlomok celkovej kriminality v tejto oblasti**.

3 Problematika kyberšikany

Ďalšou problematikou, ktorá spadá do kategórie počítačových trestných činov, resp. do kategórie kyberkriminality, je kyberšikana. Kyberšikanovanie je nelegálna činnosť, pri ktorej sa obete, najmä deti a mladiství, stávajú cieľom šikanovania cez internet alebo mobilné zariadenia. Môže napr. zahŕňať urážky, vyhrážky, ohováranie, alebo sexuálne orientované útoky prostredníctvom online platforiem.

„Kyberšikana (z anglického pojmu „cyberbullying") je forma šikanovania, ktorá prebieha v online prostredí prostredníctvom digitálnych komunikačných nástrojov, ako sú napríklad sociálne siete. Hlavnou črtou kyberšikany je jej anonymita, ktorá páchateľom umožňuje konať bez fyzického kontaktu s obeťou. Tento druh šikany je často nepretržitý, pretože internet je neustále dostupný, čo znamená, že obeť je potenciálne vystavená neustálym útokom. Pri kyberšikane obete nemajú kontrolu nad tým, kedy a kde sa útoky udejú. Okrem toho môže byť kyberšikana zdieľaná s veľkým počtom ľudí, čo zvyšuje psychickú záťaž pre obeť."[14]

Kyberšikana predstavuje rastúcu výzvu aj na Slovensku. Výskum realizovaný Výskumným ústavom detskej psychológie a patopsychológie (VÚDPaP) v spolupráci s organizáciou eSlovensko už v roku 2011 identifikoval najčastejšie formy kyberšikany medzi mladými ľuďmi. Medzi najrozšírenejšie patrí nadávanie, zosmiešňovanie a šírenie nepravdivých informácií. Takmer polovica respondentov (49,8 %) sa stretla s nadávaním a vysmievaním, 42,6 % zaznamenalo šírenie nepravdivých informácií a 30 % čelilo sexuálnym narážkam. Výskum tiež poukázal na rozdiely medzi mestskými a vidieckymi oblasťami. Mladí ľudia z vidieka častejšie zažívali nadávanie a zosmiešňovanie (58,3 % oproti 38,6 % v mestách), stretávali sa s podvodnou identitou (21,1 % oproti 9,4 %) a boli vystavení nechcenej pornografii (19,4 % oproti

[13] SRHOLEC, M. Kriminalistické avízo – časť IV. Počítačová kriminalita. Právne listy [online]. 18.6.2019 [cit. 21.5.2025]. Dostupné na: https://www.pravnelisty.sk/clanky/a753-kriminalisticke-avizo-cast-iv-pocitacova-kriminalita.

[14] MIKLÓSSYOVÁ, L.; DAŇKO, M. *Problematika kyberšikany a využitie umelej inteligencie v boji proti nej*. In: Nehmotné statky interdisciplinárne [online]. [cit. 06.03.2025]. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta UK, 2024. ISBN 978-80-7160-735-9. s. 141-156. Dostupné na: https://dspace.uniba.sk/bitstream/handle/123456789/237/Nehmotne_statky_inerdiscplinarne_2024.pdf?sequence=3&isAllowed=y.

9,4 %). Štatisticky významné rozdiely boli zaznamenané aj medzi pohlaviami – dievčatá sa častejšie zapájali do žartovania a lákania na falošné stretnutia, zatiaľ čo chlapci viac natáčali a zverejňovali trápne situácie týkajúce sa iných osôb.[15]

Hoci sú mladí ľudia často obeťami kyberšikany, zároveň sú aj jej aktérmi. Viac ako polovica (59 %) priznala, že si na internete robí žarty z iných, 49,8 % sa dopustilo nadávok či zosmiešňovania a 16,5 % zverejnilo fotografie alebo videá iných osôb v trápnych situáciách. Väčšina obetí kyberšikany o incidente neinformuje dospelých, čo komplikuje riešenie situácie. Len 21,1 % tínedžerov sa zdôverilo kamarátovi, pričom rodičom sa zverilo iba 6,9 % a učiteľovi len 2 % mladých ľudí.[16]

Kyberšikana teda predstavuje závažnú výzvu, ktorá ovplyvňuje psychické zdravie a sociálne fungovanie mladých ľudí. Výskumné údaje poukazujú na jej vysoký výskyt, pričom obzvlášť znepokojujúce je, že mnohí mladí ľudia sa o skúsenostiach s kyberšikanou nikomu nezdôveria, čím sa znižuje možnosť včasnej pomoci a nápravy. Vzhľadom na psychické a sociálne dôsledky kyberšikany je nevyhnutné, aby sa tejto problematike venovala zvýšená pozornosť nielen zo strany škôl alebo rodičov, ale aj zo strany legislatívnych orgánov.

Čo sa týka trestnoprávnej úpravy kyberšikany, hoci samotné *„šikanovanie“* dlho nebolo v slovenskom trestnom práve explicitne upravené, jeho digitálne formy mohli napĺňať znaky viacerých trestných činov (napr. **nebezpečné vyhrážanie**, **vydieranie**, **ohováranie**, **nebezpečné prenasledovanie** atď.). Zákonodarca však napokon reagoval na rastúci výskyt kyberšikany a od 1. júla 2021 zaviedol nový trestný čin **nebezpečné elektronické obťažovanie (§ 360b TZ)** špecificky pokrývajúce prípady kyberšikany. Skutková podstata tohto trestného činu vyžaduje úmyselné konanie, ktoré spočíva v obťažovaní prostredníctvom elektronickej komunikačnej služby, počítačového systému alebo siete a vedie k podstatnému zhoršeniu kvality života obete, a to napríklad **ponižovaním, vyhrážaním, zverejnením fotografie alebo videa**

[15] MIKLÓSSYOVÁ, L.; DAŇKO, M. *Problematika kyberšikany a využitie umelej inteligencie v boji proti nej*. In: Nehmotné statky interdisciplinárne [online]. [cit. 06.03.2025]. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta UK, 2024. ISBN 978-80-7160-735-9. s. 141-156. Dostupné na: https://dspace.uniba.sk/bitstream/handle/123456789/237/Nehmotne_statky_inerdiscplinarne_2024.pdf?sequence=3&isAllowed=y.

[16] MIKLÓSSYOVÁ, L.; DAŇKO, M. *Problematika kyberšikany a využitie umelej inteligencie v boji proti nej*. In: Nehmotné statky interdisciplinárne [online]. [cit. 06.03.2025]. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta UK, 2024. ISBN 978-80-7160-735-9. s. 141-156. Dostupné na: https://dspace.uniba.sk/bitstream/handle/123456789/237/Nehmotne_statky_inerdiscplinarne_2024.pdf?sequence=3&isAllowed=y.

osobnej povahy, alebo tým, že páchateľ **neoprávnene koná v mene inej osoby**.[17] Tým sú pokryté najtypickejšie formy kyberšikany, ako je vytváranie falošných profilov, zverejňovanie intímnych záberov či tzv. **doxing** – cielené zisťovanie a zverejňovanie osobných údajov obete na internete. Doxing ilustruje prienik kyberšikany s témou **neoprávneného nakladania s osobnými údajmi** (keďže páchateľ bez súhlasu zverejní údaje obete s cieľom uškodiť jej); v praxi môže viesť až k ohrozeniu bezpečnosti obete či eskalácii ďalšej trestnej činnosti voči nej.[18]

Popri tom však v TZ existujú aj ďalšie ustanovenia chrániace **súkromie a osobné údaje** pred zneužitím v digitálnom prostredí. Za zmienku stojí napr. trestný čin podľa **§ 374 TZ – neoprávnené nakladanie s osobnými údajmi**, ktorý postihuje napr. situácie, keď osoba **bez zákonného dôvodu poskytne či zverejní osobné údaje**, ku ktorým sa dostala v súvislosti s výkonom verejnej moci alebo svojho zamestnania. TZ považuje ochranu osobných údajov za dôležitý spoločenský záujem, o čom svedčí aj existencia tohto samostatného trestného činu. Hoci § 374 TZ cieli skôr na **neoprávnené úniky dát „zvnútra“** (napr. úradník, ktorý zneužije údaje z databázy občanov), jeho existencia dopĺňa mozaiku nástrojov na boj proti kybernetickým deliktom, ktoré sú spojené s porušovaním súkromia.

Celkovo možno povedať, že slovenské trestné právo už v súčasnosti poskytuje rámec na postih väčšiny foriem škodlivého konania na internete, od neoprávnených prienikov do systémov, cez ničenie dát, až po online obťažovanie či zneužívanie osobných údajov. Výzvou zostáva **presadzovanie práva** v prostredí internetu a udržanie kroku legislatívy s rýchlo napredujúcim technologickým vývojom.

Záver

Trestnoprávna úprava kyberkriminality v Slovenskej republike prešla v uplynulých rokoch výrazným vývojom, najmä pod vplyvom medzinárodných záväzkov a práva Európskej únie. Konkrétne **trestný čin neoprávneného prístupu do počítačového systému a jemu príbuzné trestné činy** dnes predstavujú kľúčový nástroj postihu tzv. hackerských útokov, čím chránia nielen majetkové hodnoty, ale aj súkromie a informačnú bezpečnosť. V článku sme vysvetlili zákonné znaky trestného

[17] Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, § 360b.

[18] ŠKUBLA, M. Nebezpečné elektronické obťažovanie – nový trestný čin. Škubla & Partneri [online]. 1.7.2021 [cit. 21.5.2025]. Dostupné na: https://www.skubla.sk/clanky/nebezpecne-elektronicke-obtazovanie-novy-trestny-cin.

činu neoprávneného prístupu do počítačového systému a poukázali na súvisiace aspekty spojené s objasňovaním počítačových trestných činov.

Praktická aplikácia ukazuje, že hoci právny rámec existuje, **odhalenie a trestanie páchateľov minimálne v oblasti „anti-hackerských" trestných činov je náročné**. Štatistiky evidujú len minimum stíhaných prípadov, čo naznačuje latentnosť tejto kriminality a ťažkosti pri jej objasňovaní.

Okrajovo sme poukázali na fenomén kyberšikany a súvisiace trestné činy (ako nebezpečné elektronické obťažovanie či neoprávnené nakladanie s osobnými údajmi), ktoré dopĺňajú obraz trestnoprávnej ochrany v online priestore. Tieto ustanovenia reagujú na to, že internet môže byť prostriedkom nielen technických útokov na systémy, ale aj psychologických útokov na jednotlivcov.

Záverom možno konštatovať, že Slovenská republika má v súčasnosti pomerne robustný zákonný rámec na stíhanie kyberkriminality, založený na aktualizovanom TZ a podporený špecializovanými nástrojmi trestného práva procesného. Kľúčové bude tento rámec naďalej **udržiavať aktuálny**, t. j. pružne reagovať na nové formy útokov (napr. kriminalita spojená s umelou inteligenciou, útoky na kritickú infraštruktúru či masové úniky dát) a zároveň **efektívne aplikovať** existujúce normy v praxi. Len kombinácia kvalitnej legislatívy a jej dôsledného presadzovania môže naplniť cieľ trestného práva v kybernetickej oblasti, ktorým je ochrana spoločnosti a práv jednotlivcov pred novodobými hrozbami digitálneho veku.

Zoznam bibliografie

1. CROWN PROSECUTION SERVICE. Cybercrime – prosecution guidance. In: CPS.gov.uk [online]. Dostupné na: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
2. DRAŽOVÁ, P. Kyberkriminalita [online]. Bratislava: Právnická fakulta Univerzity Komenského. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/Prednasky/Kyberkriminalita.pdf
3. MIKLÓSSYOVÁ, L.; DAŇKO, M. Problematika kyberšikany a využitie umelej inteligencie v boji proti nej. In: Nehmotné statky interdisciplinárne [online]. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta UK, 2024. ISBN 978-80-7160-735-9. s. 141-156. Dostupné na: https://dspace.uniba.sk/bitstream/handle/

123456789/237/Nehmotne_statky_inerdiscplinarne_2024.pdf?sequence=3&isAllowed=y
4. MINISTERSTVO SPRAVODLIVOSTI SLOVENSKEJ REPUBLIKY. Trestná agenda – štatistický prehľad za rok 2023 [online]. Bratislava: Ministerstvo spravodlivosti SR, 2024. Dostupné na: http://justice.gov.sk/dokumenty/2025/03/I.-Trestna-agenda_2023.pdf
5. MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY. Štatistika kriminality v Slovenskej republike. [online]. Dostupné na: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml
6. NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY. Dôvodová správa k návrhu zákona o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov. [online]. Dostupné na: https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=417320
7. SRHOLEC, M. Kriminalistické avízo – časť IV. Počítačová kriminalita. Právne listy [online]. 18.6.2019. Dostupné na: https://www.pravnelisty.sk/clanky/a753-kriminalisticke-avizo-cast-iv-pocitacova-kriminalita
8. ŠAMKO, P. K. zaisťovaniu počítačových údajov v trestnom konaní. Právne listy [online]. 21.1.2018. Dostupné na: https://www.pravnelisty.sk/clanky/a626-k-zaistovaniu-pocitacovych-udajov-v-trestnom-konani
9. ŠKUBLA, M. Nebezpečné elektronické obťažovanie – nový trestný čin. Škubla & Partneri [online]. 1.7.2021. Dostupné na: https://www.skubla.sk/clanky/nebezpecne-elektronicke-obtazovanie-novy-trestny-cin
10. Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.