Vyučovanie informatiky ako súčasť prevencie počítačovej kriminality

Informatics education as a part of cybercrime prevention

Ivan Bacigál
Prezídium Policajného zboru MV SR
Pribinova 2
812 72 Bratislava
Slovenská republika
ivan.bacigal@minv.sk

Tatiana Hajdúková
Katedra informatiky a manažmentu
Sklabinská 1
835 17 Bratislava
Slovenská republika
tatiana.hajdukova@minv.sk

ABSTRACT

One of the main goals achieved through teaching computer science and information and communication technology education, is a task to gain practical knowledge which allows for effective work with information using computer-assisted techniques. Side by side with education, which starts from tender age, goes learning of how to use this newly acquired knowledge according to social conventions and social development. It is required that compulsory education of information and communication technology leads to understanding of potential risks of using modern technology and necessity of protecting oneself and their privacy from threats, especially among young children. Study describes current trends of cyber criminality, which negatively affects functioning of society and lives of individuals. The study also contains information concerning development and current state of International Cyber Law Enforcement, which is dictated by the International Convention on Cybercrime (Budapest Convention on Cybercrime).

Keywords

Cyber crime. Internet. Information technologies. Anonymity. Digital reality.

ABSTRAKT

Medzi hlavné ciele vyučovania informatiky a informatickej výchovy na základných školách patrí nadobúdanie praktických zručností umožňujúcich efektívnu prácu s informáciami s podporou výpočtovej techniky. Na strednej škole sa informatická gramotnosť žiakov rozvíja o teoretické a technické poznatky súvisiace s vývojom technológií, ktoré si moderná doba vyžaduje. Súčasne s výchovou a vzdelávaním od najútlejšieho veku však musí prebiehať aj predávanie informácií, ako tieto nadobudnuté znalosti a zručnosti využívať v súlade so spoločenskými pravidlami a pre spoločenský rozvoj. Je potrebné, aby formálna výučba v rámci vzdelávacej oblasti IKT viedla ku správnym návykom a uvedomeniu si potenciálnych rizík a potrieb chrániť seba a svoje súkromie pred nebezpečenstvami, ktoré použitie moderných technológií umožňuje. Príspevok, ktorý vnikol v rámci riešenia vedecko-výskumnej úlohy výsk. 161 Metódy spracovania policajne relevantných informácií na Akadémii Policajného zboru v Bratislave, popisuje súčasné trendy zneužívania informačných technológií, ktoré majú negatívne vplyvy na fungovanie spoločnosti a životy jednotlivcov a aktuálne trendy v oblasti počítačovej kriminality. Obsahom príspevku je aj vývoj a aktuálny stav medzinárodného práva v oblasti boja proti počítačovej kriminalite v zmysle medzinárodného Dohovoru o počítačovej kriminalite (Budapeštianskeho dohovoru).

Kľúčové slová

Počítačová kriminalita. Internet. Informačné technológie. Anonymita. Digitálna realita.

1. ÚVOD

Počítač je zariadenie slúžiace na realizáciu výpočtov alebo riadenie operácií, ktoré sú vyjadriteľné číselnými alebo logickými výrazmi. Vzhľadom na prudký vývoj v oblasti informačných technológií sú počítače stále viac implementované do rôznych inteligentných systémov využívaných v domácnostiach, motorizovaných dopravných prostriedkoch, riadení všetkých druhov dopravy, pri prevádzke budov a mnohých ďalších, pretože prispievajú k ich automatizácii, spoľahlivosti, presnosti a zvyšujú bezpečnosť a komfort. Objavovanie nových poznatkov alebo skutočností s pridanou hodnotou obvykle znamená preveriť veľké množstvo kombinácií známych informácií, ktoré počítač sprostredkováva a veľmi urýchľuje. Progres vývoja počítačov je tak prudký, že tvorba a aktualizácia súvisiacich právnych noriem často nestíha reagovať na nové technológie a súvisiace hrozby. Podľa Dohovoru o počítačovej kriminalite zverejneného v Zbierke zákonov pod č. 137/2008 je počítačový systém, zariadenie, alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno zariadenie, alebo viaceré zariadenia vykonávajú automatizované spracúvanie údajov na základe programu. Bez ohľadu na kritérium klasifikácie počítačov, vo všetkých prípadoch zostáva ich charakterizujúcou vlastnosťou programovateľnosť. V dnešnej dobe už poznáme aj samoučiace sa systémy, ktoré smerujú k vývoju umelej inteligencie. Programovateľnosť samoučiacich systémov je len vlastnosť podmieňujúca ich hlavnú funkciu a to schopnosť učiť sa. Používanie a rozvoj informačných technológií neustále napreduje, čo okrem pozitívnych zmien v prospech zbližovania a rozvoja spoločnosti prináša aj možnosti zneužívania ich funkcií na páchanie kriminality sofistikovanejšími spôsobmi. Súčasné problémy sveta spojené so zavádzaním nových technológií do života spoločnosti s možnosťami ich zneužívania proti obyvateľom, ako aj mnoho ďalších a ďalších udalostí, procesov a javov vo svete nevytvárajú bezpečné prostredie pre život ľudí, pre sociálnu sféru[1, s. 45]. Pre veľkú rôznorodosť informačných technológií formy páchania počítačovej kriminality nie je možné

definovať krátkym textom, ktorý by ju súčasne vystihoval v plnom význame.

2. POČÍTAČOVÁ KRIMINALITA

Pri páchaní počítačovej kriminality sa často vyskytuje záujem o obsah počítača, t. j. o údaje v ňom uložené. Krádež nehmotných elektronických údajov zvykne byť spozorovaná s časovým oneskorením, alebo dokonca nemusí byť spozorovaná vôbec, pretože po vytvorení elektronickej kópie nič nezmizne. Počítačové siete a elektronické informácie môžu byť zneužité ako prostriedok na páchanie trestnej činnosti a stopy o tejto činnosti sa môžu uchovávať na akomkoľvek mieste počítačovej infraštruktúry obsahujúcej pamäťové médium. V mnohých prípadoch jedine expertná znalosť technických možností zariadení ako aj spôsobov použitia týchto technológií v sieťach umožňuje odhaliť trestnú činnosť. Odhaľovanie a objasňovanie sa povahou svojho predmetu a svojím zázemím, v konkrétnom systéme policajného konania, podstatne odlišujú od iných policajno-bezpečnostných činností. [2, s. 14]. Nedodržanie správnych postupov môže mať za následok nenávratné znehodnotenie dôkazov potrebných na usvedčenie páchateľa a jeho prepustenie. [3, s. 222]. Navyše ani samotné zistenie nežiadúceho protispoločenského správania nemusí stačiť na potrestanie jeho páchateľov, nakoľko platná legislatíva musí byť aktuálne schopná reflektovať a akceptovať relevantnosť a informačnú hodnotu predložených digitálnych stôp. Odhaľovanie, dokumentovanie a vyšetrovanie počítačovej trestnej činnosti je postavené na štandardizovaných postupoch, ktoré aby mohli byť akceptované v trestnom konaní, musia spĺňať definované kritéria zákonnosti. Ak má mať právny systém schopnosť eliminovať a postihovať nové formy nežiadúceho protispoločenského konania, musí zmenou legislatívy dynamicky reagovať na novovznikajúce formy kriminality. Jedným z problémov je koordinované prijímanie zákonov na ochranu kybernetickej bezpečnosti, nakoľko zákony sa prijímajú na národnej úrovni v každej krajine samostatne, ale vďaka internetu páchatelia počítačovej kriminality pôsobia globálne na celom svete. [4, s. 369]. V tomto prípade máme na mysli najmä elektronické komunikačné služby, na ktorých je vyspelá spoločnosť súčasnosti vybudovaná, pretože nie sú limitované vzdialenosťou ani dlhými časovými stratami pri prenose signálu.

Rozsah problematiky počítačovej kriminality presahuje možnosti tohto príspevku, preto pohľad na ňu zúžime na oblasť dotýkajúcu sa výchovy detí a mládeže. Prevencia počítačovej kriminality a inej protispoločenskej činnosti nespočíva len vo vzdelávaní mládeže o potenciály využitia technológií vo svoj prospech, ale v cieľavedomom poskytovaní informácií o možnostiach ich zneužitia. Prostredníctvom Internetu je možné rozširovať škodlivú aktivitu nielen zo slovenských domén a IP adries, ale celého zahraničného kybernetického priestoru. Meniace sa medzinárodné, ale aj európske bezpečnostné prostredie si vyžaduje zdokonaľovanie charakteru prípravných opatrení k ochrane obyvateľstva. [5, s. 111] Nezávisí odkiaľ hrozba prichádza, v každom prípade je potrebné naučiť sa brániť. Prevencia na školách by mala spočívať aj v poskytovaní konkrétnych informácií, vrátane trestnej zodpovednosti za svoje konanie. V prípade adolescentov sa prejavuje ich nedostatočné právne povedomie, pretože si neuvedomujú dôsledky svojho konania, respektíve často ho nesprávne považujú za formu zábavy a spôsob verejného prezentovania, ktoré môže byť v skutočnosti protizákonné. Pekným príkladom môže byť komunikácia na sociálnych sieťach, ktorú považujú mnohí, nielen mladí, za anonymnú. Širokej verejnosti používateľov informačných technológií je potrebné poskytovať rady, ako sa nestať obeťou trestného činu, respektíve ako sa brániť pred počítačovými útokmi legitímnymi prostriedkami, nakoľko represívne prostriedky sú obvykle nasadzované v situáciách, pri ktorých už reálne nastali negatívne následky protizákonného konania.

2.1 Digitálna realita verzus skutočnosť

Tak ako už bolo naznačené v úvodnej časti, jednou z dôležitých úloh učiteľov súčasnosti je nielen skvalitniť vzdelávanie a výchovu detí a mládeže využívaním moderných technológií, ale aj učiť ich rozlišovať realitu od počítačového sveta. Mladí ľudia môžu moderné technológie využívať pre obohatenie zážitkov a zjednodušenie svojho života, alebo sa môžu modernými technológiami nechať spútať alebo ich dokonca zneužívať na páchanie trestnej činnosti. Minulý rok boli zverejnené informácie, že istý poskytovateľ služieb na internete svojich používateľov nepovažuje za klientov využívajúcich svoje služby, ale za tovar, s ktorým môže obchodovať (najmä za účelom poskytovania marketingových informácií používateľom). Túto filozofiu diktovania pravidiel zo vzťahu poskytovateľ služieb a používateľ je cítiť čoraz viac.

Ďalším negatívnym faktorom je, že mladí ľudia každodenne ovplyvnení informáciami (je jedno či v audiovizuálnej podobe alebo v podobe počítačových hier) si nedostatočne uvedomujú rozdiel medzi skutočným a digitálne predstieraným prostredím. Kým sa dôsledky konania hráčov v digitálnom svete a digitálnej komunite môžu zdať „cool“[1] alebo bez dôsledkov, v reálnom svete podobné konanie môže skončiť tragicky. Ale platí to aj naopak. Pocit nesmrteľnosti prežitý v digitálnom svete sa transformuje v reálnom svete do „ľahkovážneho správania“, čím sa deti stávajú obeťou v podstate dvakrát. Jedenkrát ako dôsledok konania v reálnom svete a druhýkrát ako reálna bytosť oklamaná virtuálnym svetom, v ktorom sa jej nemôže nič bolestivé stať (sled udalostí sa nedá stlačením klávesy spustiť odznovu). Alarmujúce je, že v súčasnosti vyššie uvedené neplatí iba o mladej generácii, ale čoraz viac postihuje celé spektrum ľudskej spoločnosti.

2.2 Počítačová kriminalita ako dôsledok technologického pokroku

Ako reakcia na nárast protispoločenského konania spojeného s rozvojom počítačových a komunikačných technológii, nadnárodný charakter tejto trestnej činnosti a aplikačné problémy v oblasti vymožiteľnosti práva bol 23. novembra 2001 v Budapešti otvorený na podpis medzinárodný Dohovor o počítačovej kriminalite (ďalej len dohovor). Národná rada Slovenskej republiky s dohovorom vyslovila súhlas svojím uznesením č. 583 z 23. októbra 2007, prezident Slovenskej republiky dohovor ratifikoval 12. decembra 2007. Dohovor nadobudol platnosť 1. júla 2004 v súlade s článkom 36 ods. 3[2] a 1. mája 2008 v Slovenskej republike v súlade s článkom 36 ods. 4.

[1] anglický slangový výraz – vtipný, dômyselný, úžasný

[2] Tento dohovor nadobudne platnosť prvý deň mesiaca nasledujúceho po uplynutí troch mesiacov odo dňa, keď päť

Dohovor zaviazal signatárske krajiny vrátane Slovenska definovať nasledovné protispoločenské konania ako trestné činy:

„Nezákonný prístup„ – neoprávnený prístup do počítačového systému ako celku alebo do jeho časti spáchaný porušením bezpečnostných opatrení s úmyslom získať počítačové údaje alebo s iným nečestným úmyslom, alebo vo vzťahu k počítačovému systému prepojenému s iným počítačovým systémom.

„Nezákonné zachytenie údajov“ – zachytávanie neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v rámci tohto systému vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje také počítačové údaje vykonané technickými prostriedkami.

„Zasahovanie do údajov“ – neoprávnené poškodenie, vymazanie, zhoršenie kvality, pozmenenie počítačových údajov alebo zamedzenie prístupu.

„Zasahovanie do systému“ – neoprávnené závažné marenie funkčnosti počítačového systému vkladaním, prenášaním, poškodením, vymazaním, zhoršením, pozmenením počítačových údajov alebo zamedzením prístupu k nim.

„Zneužitie zariadení“ čím rozumieme:

a) výroba, predaj, obstarávanie na účely použitia, dovoz, distribúciu alebo iné sprístupnenie:

- zariadenia vrátane počítačového programu vytvoreného alebo upraveného predovšetkým s cieľom spáchať niektorý z vymedzených trestných činov,
- počítačového hesla, prístupového kódu alebo podobných údajov, ktorých pomocou je možný prístup do počítačového systému ako celku alebo do niektorej jeho časti, s úmyslom ich použiť na spáchanie niektorého z vymedzených trestných činov,
- držba veci uvedenej v odseku 1 písm. a) bode i. alebo s úmyslom ju použiť na spáchanie niektorého z trestných činov vymedzených v článkoch 2 až 5.

„Falšovanie počítačových údajov“ – vloženie, pozmenenie, vymazanie počítačových údajov alebo zamedzenie prístupu k nim, v ktorých dôsledku stratia údaje autentickosť, s úmyslom považovať ich za autentické alebo aby sa na základe nich ako autentických údajov konalo, na právne účely, bez ohľadu na to, či tieto údaje sú alebo nie sú priamo čitateľné alebo zrozumiteľné

„Počítačový podvod“ – spôsobenie majetkovej ujmy inému:

- vložením, pozmenením, vymazaním počítačových údajov alebo zamedzením prístupu k nim,
- zásahom do fungovania počítačového systému s podvodným alebo nečestným úmyslom neoprávnene získať pre seba alebo pre iného majetkový prospech.

„Trestné činy týkajúce sa detskej pornografie“. Detská pornografia“ zahŕňa pornografický materiál, ktorý zobrazuje:

a) maloletú osobu zúčastnenú na zjavnom sexuálnom správaní,
b) osobu, ktorá sa zdá byť maloletá a ktorá sa zúčastňuje na zjavnom sexuálnom správaní,
c) realistické zobrazenia maloletej osoby zúčastnenej na zjavnom sexuálnom správaní.

štátov vrátane najmenej troch členských štátov Rady Európy vyjadrí súhlas byť viazané dohovorom v súlade s ustanoveniami odsekov 1 a 2.

„Trestné činy týkajúce sa porušenia autorských a príbuzných práv“ – porušenie autorského práva vymedzeného právnym poriadkom v súlade so záväzkami, ktoré prijali signatárske štáty podľa Parížskeho aktu z 24. júla 1971, ktorým sa mení Bernský dohovor o ochrane literárnych a umeleckých diel; Dohody o obchodných aspektoch práv na duševné vlastníctvo a Zmluvy Svetovej organizácie duševného vlastníctva (WIPO) o autorskom práve, okrem osobnostných práv priznaných týmito dohovormi a v súlade so záväzkami, ktoré prijala podľa Medzinárodného dohovoru o ochrane výkonných umelcov, výrobcov zvukových záznamov a rozhlasových organizácií (Rímsky dohovor); Dohody o obchodných aspektoch práv na duševné vlastníctvo a Zmluvy Svetovej organizácie duševného vlastníctva (WIPO) o výkonoch a zvukových záznamoch, okrem osobnostných práv priznaných týmito dohovorom.

Okrem definície konkrétneho protiprávneho konania dohovor definoval aj spôsob spolupráce v trestnom konaní, akým sú napríklad vzájomná právna pomoc týkajúca sa prístupu k uloženým počítačovým údajom, postup pri výmene digitálnych stôp, či zabezpečenie vytvorenia medzinárodnej siete kontaktných miest, ktoré sú v signatárskych krajinách k dispozícii 24 hodín 7 dní v týždni, za účelom zabezpečenia poskytovania okamžitej pomoci za účelom vyšetrovania alebo konania v prípade trestných činov spojených s počítačovými systémami a dátami, alebo za účelom zhromažďovania dôkazov o trestnom čine v elektronickej forme. Účelom Dohovoru je podporiť efektívnu medzinárodnú spoluprácu, zlepšiť globálne podmienky pre dôveru a bezpečnosť medzi členskými krajinami, nakoľko v online prostredí nemajú opodstatnenosť hraničné kontroly [6, s. 59].

2.3 Trestno-právne dôsledky páchania počítačovej trestnej činnosti

V slovenskom právnom systéme boli požiadavky a záväzky dohovoru implementované hlavne do Trestného zákona , kde v zmluve uvedené protiprávne konania nájdeme implementované naprieč celým zákonom. Počítačová trestná činnosť je už v súčasnosti stanovená širšie ako bolo definované v požiadavkách dohovoru z roku 2001. Počítačovú kriminalitu dnes rozdeľujeme na počítačovú kriminalitu (computer crime) v užšom zmysle a počítačovú kriminalitu v širšom zmysle, kam býva zaradená aj kriminalita súvisiaca s počítačovými technológiami tzv. computer related crime. Medzi počítačovú kriminalitu dnes zaraďujeme najmä nasledovné:

§ 201a Sexuálne zneužívanie
Trestný čin spácha ten, kto prostredníctvom elektronickej komunikačnej služby navrhne dieťaťu mladšiemu ako pätnásť rokov osobné stretnutie v úmysle spáchať na ňom trestný čin sexuálneho zneužívania alebo trestný čin výroby detskej pornografie, pričom sám nie je dieťaťom.

§ 219 Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty

Trestný čin spácha ten, kto neoprávnene vyrobí, pozmení, napodobní, falšuje alebo si obstará platobný prostriedok alebo elektronické peniaze alebo inú platobnú kartu vrátane telefónnej

karty alebo predmet spôsobilý plniť takú funkciu na účel použiť ho ako pravý alebo na taký účel ho prechováva, prepravuje, použije alebo poskytne inému a ten, kto neoprávnene vyrobí, prechováva, obstará si alebo inak zadováži alebo poskytne inému nástroj, počítačový program alebo iný prostriedok špeciálne prispôsobený na spáchanie činu tohto trestného činu.

§ 226 Neoprávnené obohatenie
Trestný čin spácha ten, kto na škodu cudzieho majetku seba alebo iného obohatí tým, že neoprávneným zásahom do technického alebo programového vybavenia počítača, automatu alebo iného podobného prístroja alebo technického zariadenia slúžiaceho na automatizované uskutočňovanie predaja tovaru, zmenu alebo výber peňazí alebo na poskytovanie platených výkonov, služieb, informácií či iných plnení dosiahne, že tovar, služby alebo informácie získa bez požadovanej úhrady alebo peniaze získa neoprávnene, a spôsobí tým na cudzom majetku škodu.

§ 247 Neoprávnený prístup do počítačového systému
Trestný čin spácha ten, kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časť.

§ 247a Neoprávnený zásah do počítačového systému
Trestný čin spácha ten, kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu.

§ 247b Neoprávnený zásah do počítačového údaja
Trestný čin spácha ten, kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti.

§ 247c Neoprávnené zachytávanie počítačových údajov
Trestný čin spácha ten, kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje alebo kto ako zamestnanec poskytovateľa elektronickej komunikačnej služby spácha tento čin alebo inému úmyselne umožní spáchať taký čin, alebo pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby.

§ 247d Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov

Trestný čin spácha ten, kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údaja podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti.

§ 283 Porušovanie autorského práva
Trestný čin spácha ten, kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze.

§ 368 Výroba detskej pornografie
Trestný čin spácha ten, kto využije, získa, ponúkne alebo inak zneužije dieťa na výrobu detskej pornografie alebo detského pornografického predstavenia alebo umožní také jeho zneužitie, alebo sa inak podieľa na takejto výrobe, potrestá sa odňatím slobody na štyri roky až desať rokov.

§ 369 Rozširovanie detskej pornografie
Trestný čin spácha ten, kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje alebo inak rozširuje detskú pornografiu.

§ 370 Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení
Trestný čin spácha ten, kto prechováva detskú pornografiu alebo kto koná v úmysle získať prístup k detskej pornografii prostredníctvom elektronickej komunikačnej služby alebo sa úmyselne zúčastní detského pornografického predstavenia.

§ 376 Poškodzovanie cudzích práv
Trestný čin spácha ten kto neoprávnene poruší tajomstvo listiny alebo inej písomnosti, zvukového záznamu, obrazového záznamu alebo iného záznamu, počítačových dát alebo iného dokumentu uchovávaného v súkromí iného tým, že ich zverejní alebo sprístupní tretej osobe alebo iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach.

2.4 Vývoj počítačovej trestnej činnosti

Okrem Dohovoru o počítačovej kriminalite boli pod vplyvom ďalšieho vývoja počítačovej kriminality, a to najmä znepokojujúcich rozmerov vývoja na vnútroštátnej aj medzinárodnej úrovni v oblasti sexuálneho vykorisťovania a sexuálneho zneužívania detí (vrátane trestnej činnosti súvisiacej s detskou pornografiou) prijaté aj ďalšie medzinárodné právne normy. Patria k nim napríklad smernica Európskeho parlamentu a rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii a dohovor Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním v Lanzarote 25. 10. 2007, ktorý pre Slovenskú republiku nadobudol platnosť len 1. júla 2016. Hlavným účelom ich prijatia bolo zintenzívnenie vnútroštátneho a medzinárodného boja proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii.

Potrebné je zdôrazniť, že tieto činy majú zničujúci vplyv na zdravie a psychosociálny vývoj detí a pokiaľ sa tento vývoj nepodarí zastaviť a zvrátiť, tento problém môže mať vážny vplyv aj na vývoj celej spoločnosti.

V oblasti počítačových útokov bola prijatá smernice Európskeho parlamentu a Rady Európy 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy. Smernica zohľadnila nové metódy páchania počítačových trestných činov a významne rozšírila komplex protiprávnych konaní v súvislosti s neoprávneným prístupom do počítačových systémov, neoprávneným zásahom do počítačových systémov a počítačových údajov, neoprávneným zachytávaním počítačových údajov a manipuláciou s nástrojmi určenými na spáchanie týchto trestných

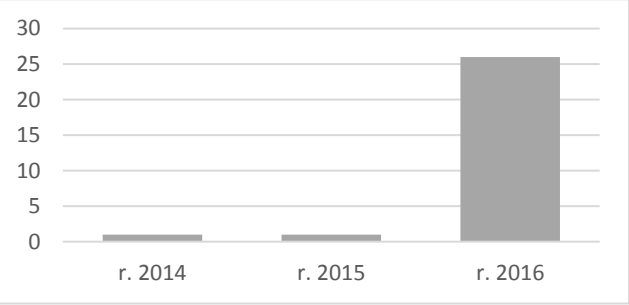
činov. Na tento účel boli vytvorené nové individuálne skutkové podstaty trestných činov definujúce jednotlivé typy nových foriem protiprávnych konaní[3].

2.5 Aktuálny stav registrovanej počítačovej kriminality v slovenskom kybernetic-priestore

Na Slovensku už vyše 30 rokov funguje Evidenčno-štatistický systém kriminality (EŠSK), ktorý je využívaný v policajnej praxi na umožnenie sledovania miery registrovanej trestnej činnosti v minulosti na území Československa, po osamostatnení len na území Slovenska. V EŠSK sa sústreďujú oznámenia o podozrení zo spáchania trestných činov, údaje o trestných činoch a údaje o známych páchateľoch. Od jeho zavedenia do praxe až do súčasnej doby bola dodržiavaná zásada, aby do systému boli zavádzané údaje len na základe procesných úkonov, ktoré sú zdrojom dát a podliehajú posudzovaniu orgánmi prokuratúry. Výstupy z EŠSK sa prostredníctvom Štatistického úradu SR poskytujú najvyšším štátnym orgánom a prostredníctvom INTERPOLU aj do zahraničia.

Na základe evidencie EŠSK za posledné tri roky je viditeľný výrazný nárast zaznamenaný v roku 2016 v počte neoprávnených zásahov do technického alebo programového vybavenie počítača podľa § 226 Neoprávnené obohatenie, zobrazené na grafe 1[4].

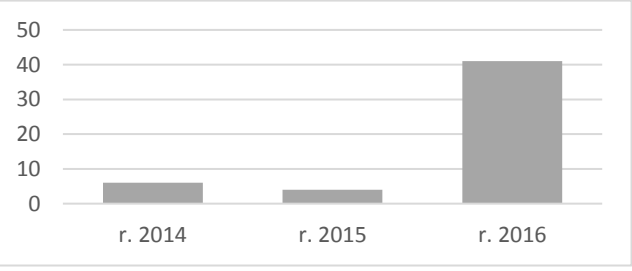
Graf 1 § 226 Neoprávnené obohatenie v SR, 2014-2016



Zdroj: Spracované podľa údajov EŠSK

Podobný vzostup za rok 2016 možno vidieť aj v prípade § 283 Porušovanie autorského práva na grafe 2, pričom objasnenosť týchto trestných činov nedosahovala ani 20%.

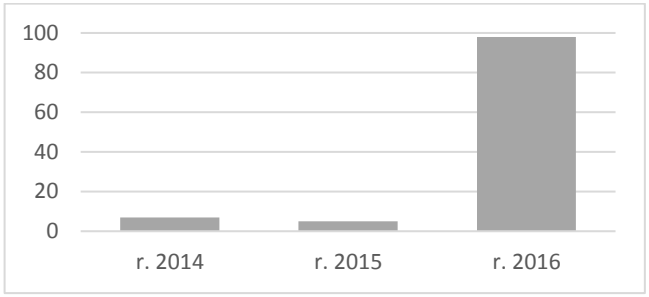
Graf 2 § 283 Porušovanie autorského práva v SR, 2014-2016



Zdroj: Spracované podľa údajov EŠSK

V takmer 100 prípadov počas roka 2016 bolo zaregistrovaných a vyšetrovaných podľa § 369 Rozširovanie detskej pornografie. Nárast evidovaných prípadov je podobne dramaticky zvýšený ako pri vyššie spomenutej počítačovej kriminalite, avšak s podstatne vyššou frekvenciou výskytu. Navyše sa v týchto prípadoch jedná výlučne o detské obete.

Graf 3 § 369 Rozširovanie detskej pornografie v SR, 2014-2016



Zdroj: Spracované podľa údajov EŠSK

Na základe vlastných skúseností však zvýšené počty v policajných štatistikách nie sú len indikátorom zvýšenia nápadu tejto trestnej činnosti, ale aj viditeľným presúvaním kapacít kriminálnej polície na oblasť odhaľovania a objasňovania počítačovej kriminality, ako reakcie vyvolanej jej nárastom a závažnosťou. Nezanedbateľným faktorom je určite aj zníženie ľahostajnosti obetí a ich zákonných zástupcov, zvyšovanie informovanosti občianskej verejnosti ako i prijatie dlho očakávaných zmien v legislatívnej oblasti, ku ktorým prišlo k 1. januáru 2016.

3. POZITÍVNY VÝVOJ PREVENCIE NA SLOVENSKU A VAROVNÉ SIGNÁLY ZO ZAHRANIČIA

Okrem smerovania policajnej štatistiky do reálnych čísel považujeme za ďalší a veľmi dôležitý pozitívny vývoj aj akceleráciu intenzity preventívnych aktivít a záujem médií o problematiku osvety v oblasti ochrany používateľov internetu a moderných počítačových a telekomunikačných technológií pred počítačovou kriminalitou a to nielen detí, ale aj dospelých.

Tu treba zdôrazniť, že prevencia formou osvety, hlavne preventívne akcie cielene zamerané na určité špecifické skupiny potencionálnych obetí (napr. diferencovane podľa veku – žiaci prvého stupňa, žiaci druhého stupňa, stredoškoláci, vysokoškoláci a mladí dospelí, dospelí a seniori) sú najúčinnejším a pritom aj najlacnejším spôsobom boja proti počítačovej kriminalite. Kým polícia nastupuje do boja proti počítačovej kriminalite vo väčšine prípadov až v momente odhaľovania, objasňovania a vyšetrovania tejto špecifickej trestnej činnosti, pracovníci a často aj nadšenci bezodplatne pracujúci na poli prevencie vedia zachrániť obete ešte pred týmto momentom, ktorý už znamená istým spôsobom aj ďalšiu prehru spoločnosti.

[3] Dôvodovú správu k smernici Európskeho parlamentu a Rady Európy 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy prerokovala a schválila vláda Slovenskej republiky na svojom rokovaní dňa 1. júla 2015

[4] Objasnenosť týchto trestných činov nedosiahla ani 50%

Slovensko svojím neskorším vstupom do sféry informatizácie má obrovskú príležitosť poučiť sa z chýb vývoja informatizácie v zahraničí. Vývoj možno v mnohých oblastiach označiť za alarmujúci a preto je potrebné na varovné signály upozorňovať a tým vytvárať predpoklady na to, aby sa naša spoločnosť pokúsila týmto negatívnym trendom zabrániť alebo ich aspoň minimalizovať. Z posledného obdobia môžeme upozorniť aspoň na niektoré z nich.

V marci 2017 priniesli slovenské média[5] *správy o nemeckom 19 ročnom mužovi Marcelovi Hessovi, ktorý na internete zverejnil informácie a fotografie z brutálnej vraždy 9 ročného chlapca. Na mieste činu si spravil ešte zakrvavený trendovú selfie fotografiu, ktorú tiež zverejnil. Počas vyšetrovania bolo preukázané, že zavraždil aj inú osobu, ktorú poznal z internetu. Mladý muž sa ku skutku bez emócii priznal a ako dôvod uviedol, že ho k tomu viedla frustrácia. Napriek tomu, že v internetovej komunikácii bol aktívny, psychológ uviedol, že u neho absentovali sociálne kontakty, mal nulovú emocionálnu inteligenciu a označil ho za extrémne nebezpečného. Marcel Hess bol závislí od počítačov a počítačových hier.*

Ďalšou šokujúcou správou zverejnenou v médiách[6] *v marci 2017 je článok o znepokojení nórskej polície, menovite Národného úradu pre boj proti organizovanej kriminalite a inej závažnej trestnej činnosti Kripos o veľkom počte mužov vo veku 18 až 60 rokov, ktorí si cez počítačovú sieť z Hongkongu objednávajú nafukovacie panny s podobou detí. Časť z týchto prípadov bola priamo spojená s prípadmi súvisiacimi s detskou pornografiou.*

Alarmujúce prepojenie medzi internetom a šírením terorizmu v Európe nemožno spochybniť. Už v roku 2015 vydala Európskej komisia znepokojujúcu správu o šírení islamského radikalizmu prostredníctvom internetu, ktorá je do dnes stále aktuálnou a boj proti jeho šíreniu naďalej pokračuje[7]. Tak ako bolo v správach uvedené, nebezpečenstvo terorizmu, nie je spojené len s nelegálnou migráciou, ale rizikovými osobami sú často vlastní sfanatizovaní občania Európskej únie (často veľmi mladí), ktorí sú vďaka slepému preberaniu informácií z internetových zdrojov ľahko verbovaní do teroristických zoskupení alebo manipulovaní k páchaniu závažnej násilnej trestnej činnosti v mene rôznych ideológií.

Smutné je, že sa k radikálnym skupinám pridávajú často aj nadpriemerne inteligentní ľudia.

Príkladom môže byť napríklad 20 ročný mladík odsúdený v USA, ktorý sa k Islamskému štátu pridal ako hacker[8]*. Anglický hacker Junaid Hussain zabitý v Sýrii americkým dronom pôsobil ako šéf kybernetickej jednotky Islamského štátu.*

Najsmutnejším prípadom, z tejto skupiny bola vražda kňaza vo francúzskom meste Saint-Étienne-du-Rouvray, kde mladí muži v mene Islamského štátu podrezali tamojšieho kňaza[9]*. V tomto prípade už pred týmto skutkom sami rodičia upozornili na radikalizáciu mladíka, pričom mladík pochádzal zo vzdelanej rodiny. Matka 19 ročného francúzskeho občana Adela Kermicha je profesorka a sestra je lekárka.*

Toto riziko v plnom rozsahu platí aj o šírení extrémizmu a náboru do rôznych vojenských konfliktov, nakoľko metódy šírenia propagandy sú veľmi podobné.

Na začiatku roka 2017 boli zaznamenané aj iné alarmujúce udalosti ako sú krádeže vozidiel deťmi (často svojim rodičom) a následné dopravné nehody s následkom usmrtenia alebo ťažkého zranenia účastníkov cestnej premávky. Napriek tomu, že priamu súvislosť s využívaním moderných technológií ťažko dokázať, skreslené vnímanie reality hroziaceho nebezpečenstva v narastajúcom rozsahu v týchto prípadoch je viditeľné.

Negatívnych príkladov z posledného obdobia je naozaj niekoľko. Cieľom nie je poukázať na závažnosť kriminality mladých v spojení počítačovými a inými modernými komunikačnými technológiami, ale na ich nepripravenosť čeliť týmto lákadlám, či hrozbám, ktoré na nich v internetovom svete číhajú.

Dôležitosť úlohy zavedenia určitej regulácie audiovizuálneho obsahu dostupného mladým bolo aj jednou z priorít slovenského predsedníctva SK PRES v oblasti kultúry a audiovízie, pričom výsledkom bol návrh revízie smernice o audiovizuálnych mediálnych službách[10] pod predsedníckym vedením ministra kultúry SR.

Aktualizácia a praktické plnenie smernice o audiovizuálnych mediálnych službách môže byť dobrým začiatkom zastavenia nebezpečných trendov, ktoré vplývajú na mladú generáciu.

4. PSEUDOANONYMNÁ BUDÚCNOSŤ ĽUDSTVA

Technologický pokrok v dnešnej dobe priniesol dva základné technologicko-filozofické smery. Nekontrolované zverejňovanie informácií zo súkromného života (vo väčšine prípadov pravdepodobne neuvedomelé a vynútené poskytovateľmi služieb) a na druhej strane snaha o zachovanie anonymity, ktoré niekedy

[5] https://www.aktuality.sk/clanok/422996/nemecky-tinedzer-sa-priznal-k-dvom-vrazdam/
https://svet.sme.sk/c/20480403/devatnastrocny-nemecky-mladik-sa-priznal-k-dvom-vrazdam.html

[6] http://www.topky.sk/cl/11/1613283/Norska-policia-je-znepokojena--Coraz-viac-muzov-si-dovaza-nafukovacie-panny-v-podobe-deti
https://svet.sme.sk/c/20474460/norsko-znepokojuje-narast-dovozu-nafukovacich-panien-s-podobou-deti.html

[7] http://spravy.pravda.sk/svet/clanok/374053-teroristicke-utoky-nie-su-dielom-utecencov-upozornuje-europska-komisia/
https://svet.sme.sk/c/20289595/eu-vypoveda-vojnu-islamskemu-statu-na-internete-ziada-o-pomoc-it-firmy.html

[8] http://www.zive.sk/clanok/118218/v-usa-odsudili-hackera-na-20-rokov-za-pomahanie-islamskemu-statu
https://svet.sme.sk/c/7982776/dron-zabil-hlavneho-hackera-islamskeho-statu-kradol-data-aj-blairovi.html

[9] http://www.ta3.com/clanok/1088129/vrahom-knaza-bol-tinedzer-ktoreho-zmenil-utok-na-charlie-hebdo.html

[10] http://www.eu2016.sk/sk/politicke-a-expertne-podujatia/konferencia-ochrana-maloletych-regulacne-konvergencie

hraničia až s pokusmi o nastolenie právnej anarchie. Málokto si však uvedomuje, že čokoľvek, považované za anonymné, sa ľahko môže stať verejným. Preto pri moderných technológiách musíme slovo anonymita vždy chápať vo význame pseudoanonymita. Toto platí nielen pri rôznych technológiách tzv. anonymného pripojenia na verejnú sieť internet, ale aj pri digitálnych kryptomenách, či ďalších technológiách, ktoré ešte len čakajú za rohom budúcnosti. Každý jednotlivec využívaním nových technológií fungujúcich na globálnych komunikačných sieťach stráca časť súkromia a delí sa o svoje súkromie s veľkými technologickými spoločnosťami, ktorých obchodný plán je založený na zhromažďovaní a obchodovaní s týmito informáciami. Každý jednotlivec si musí sám vybrať medzi ľahšou cestou zdieľania svojho súkromia, nepoužívania týchto technológií alebo sa vzdelávať, ako technológie používať tak, aby zásah do jeho súkromia dokázal minimalizovať. Schopnosť orientovať sa v bezpečnostnom prostredí, už nie je iba otázkou dobrej vôle, ale stáva sa čoraz viac nevyhnutnosťou a elementárnym predpokladom prežitia. [7, s. 188] Je dôležité, aby si toto mladá generácia uvedomila a osvojila. Pri vzdelávaní získavajú kľúčové postavenie osoby s odbornými poznatkami v oblasti informatiky a srdcom pedagóga.

5. ZÁVER

Keď zlyháva rodina natoľko, že je ohrozený život, zdravie a zdravý fyzický a duševný vývoj dieťaťa, je úlohou spoločnosti nahradiť tieto kľúčové výchovné funkcie a postarať sa o deti, ktoré sú budúcnosťou spoločnosti. V takýchto núdzových prípadoch musí aj poznatky, ako prežiť v digitálnom veku a ako využívať nové technológie bezpečne, sprostredkovať deťom samotná spoločnosť. Podobný princíp funguje aj v prírode a je nevyhnutným predpokladom prežitia rodu či druhu. Problémom súčasných rodín je, že sa začína strácať záujem o budovanie budúcnosti detí, nakoľko riešia existenčné problémy. Pomerne často sa obmedzuje konanie rodičov len na akési prežívanie (tzv. „život z práce do práce“). Navyše mnohí z týchto rodičov majú problém, hlavne technického charakteru, ako sa s modernými technológiami vysporiadať. Záchranným kolesom sa tak môže stať v tomto búrlivom čase rýchleho vývoja nových informačných technológií informácia ako prežiť bezpečne, ktorá príde k dieťaťu včas.

BIBLIOGRAFICKÉ ODKAZY

[1] VÁŇA, J. *Environmentálna bezpečnosť – podmienka bezpečnosti sociálnej sféry.* In *SECURITY – THE KEY REQUIREMENT OF THE PRESENT: SELECTED ISSUES OF SECURITY SCIENCE.* Bratislava : Akadémia PZ v Bratislave, 2016. s. 45-57. ISBN 978-80-8054-675-5.

[2] LISOŇ, M. *Odhaľovanie a objasňovanie trestných činov všeobecnej kriminality*. Akadémia PZ v Bratislave, 2016. s. 248. ISBN 978-80-8054-673-1.

[3] HAJDÚKOVÁ, T., BACIGÁL, I. *Využitie virtuálnej komunikácie cez internet ako prostriedok ku sexuálnemu zneužívaniu detí.* In *Mravnostná kriminalita ako spoločenský fenomén a možnosti jej kontroly*. Bratislava : Akadémia PZ v Bratislave, 2015. s. 242. 978-80-8054-646-5.

[4] KURILOVSKÁ, L., ŠIŠULÁK, S. *Internetový marketing ako metóda páchania trestnej činnosti* In *Aktuálne otázky tretsného práva v teórii a praxi*. [Online] 2015, 3. ročník. [Dátum: 12. 9. 2015.] Dostupné tiež na: http://www.akademiapz.sk/sites/default/files/KVPV/KTP/Aktu%C3%A1lne%20ot%C3%A1zky%20TP%20v%20T%20a%20P%20-%203.ro%C4%8D. %20e-verzia.pdf. ISBN 978-80-8054-637-3.

[5] METEŇKO, J., BINDEROVÁ, M. *Koordinovanie národného výskumu a politiky na zaistenie bezpečnosti pri významných udalostiach v Európe* EU SEC II : Záverečná správa medzinárodnej vedeckovýskumnej úlohy : FP7 Grant Agreement (2008-2011). Bratislava : Akadémia PZ v Bratislave, 2012. s. 34. EAN 9788080546762.

[6] ODLER, R. *Schengenský priestor verzus obchodovanie s ľuďmi.* In *Sborník příspěvků z 6. ročníku mezinárodní vědecké konference "Bezpečná Evropa 2013.* Karlovy Vary : Vysoká škola Karlovy Vary, 2013. S 110121.

[7] MURDZA, K. *Bezpečnostná dezorientácia občana a jej negatívne dôsledky* In *SECURITY – THE KEY REQUIREMENT OF THE PRESENT: SELECTED ISSUES OF SECURITY SCIENCE*. Bratislava : Akadémia PZ, 2016. s. 188-197. ISBN 978-80-8054-675-5.

[8] Stratégia prevencie kriminality a inej protispoločenskej činnosti zákona č. 583/2008 Z. z. o prevencii kriminality a inej protispoločenskej činnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 403/2010 Z. z.,

[9] Dohovor o počítačovej kriminalite publikovaný pod č. 137/2008 Z.z.

[10] Smernica Európskeho parlamentu a rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii

[11] Dohovor Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním publikovaný pod č. 164/2016 Z. z

[12] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy

[13] SMAHEL, D., HELSPER, E., GREEN, L., KALMUS, V., BLINKA, L., ÓLAFSSON, K. 2012. *Excessive Internet Use Among European Children* [online] [vytvorené november 2012] dostupné na internete http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ExcessiveUse.pdf. 9 p. ISSN 2045 – 256X.

[14] GREGUSSOVA, M., DROBNÝ, M. 2012. *Deti v sieti, Ako chrániť seba a naše deti na internete.* Bratislava : eSlovensko, 2013. 108 s. ISBN 978-80-970676-6-3.

[15] ÓLAFSSON, K., LIVINGSTONE, S., HADDON, L. et al. 2013. *Children´s Use of Online technologies in Europe, A review of the European evidence base.* London : LSE The school of economics and political science, [online] [vytvorené máj 2013] dostupné na internete

[16] SAKAŘ, P.: *Sexuální reviktimizace,* In Česká a slovenská psychiatrie. č. 7, ročník 103, Brno: ČSL JEP, 2007, s. 346-352, ISSN 1212-0383.

[17] VELIČKOVÁ HULANOVÁ, L. *Kybergrooming a kyberstalking*. In: KRČMÁŘOVÁ, Barbora et al. Děti a online rizika: Sborník studií. 1. vyd. Praha: Sdružení Linka bezpečí, 2012, s. 87 - 107. ISBN 978-80-904920-2-8. Dostupné z: http://www.linkabezpeci.cz/webmagazine/kategorie.asp?idk=239

[18] QUAYLE, E., TAYLOR, M. *Model of Problematic Internet Use in People with a Sexual Interest in Children*, CYBERPSYCHOLOGY & BEHAVIOR, Volume 6, Number 1, 2003, Mary Ann Liebert, Inc.

[19] Tlačový servis INHOPE. Statistiky horkých linek varují – v prostředí online roste výskyt materiálů se sexuálně zneužívanými dětmi [online]. [vytvorené 16. 6. 2014]. [cit. 2015-3-25]. Dostupné na internete: http://www.saferinternet.cz/aktuality/337-statistiky-horkych-linek-varuji-%E2%80%93-v-prostredi-online-roste-vyskyt-materialu-se-sexualne-zneuzivanymi-detmi.html.

[20] http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/D2.2ReviewEvidenceDatabase.pdf . ISSN 2045 - 256X.