Informačná bezpečnosť občana ako špecifický aspekt bezpečnosti

Peter Lošonczi[1]

Abstrakt
Príspevok uvádza čitateľa do problematiky týkajúcej sa informačnej bezpečnosti občana v oblasti ochrany osobných údajov, autorských práv a iných oblastiach života jednotlivca žijúceho vo výrazne štandardizovanom prostredí SR ako integrálnej súčasti EÚ. Poukazuje na bežné oblasti života občana v konfrontácii s aplikáciou trendov v predmetnej téme smerujúcich z rozhodnutia EÚ až k občanovi SR. Spracovanie poukazuje na možné riziká, ale aj na možnosti riešenia všeobecného zachovania bezpečnosti občana pred nástrahami ako je zneužitie osobných údajov, profilovanie jednotlivca alebo až krádež identity, a to pri triezvom narábaní s nástrojmi ako je napr. GDPR (General Data Protection Regulation).

Kľúčové slová
informačná bezpečnosť, osobný udaj, riziko, legislatíva

Abstract
The article familiarizes the reader with issues related to information security of a citizen in the area of personal data protection, copyright and other areas of life of an individual living in a highly standardized environment of the Slovak Republic being an integrated part of the European Union. It points to the common areas of citizens' life in confrontation with the application of trends in the subject from the EU decision to the citizen of the Slovak Republic. The processing shows the possible risks as well as options of addressing the issue of the general security of citizens and its maintenance. This maintenance protects the citizens against such dangers as personal data misuse, individual profiling or identity theft, while cleverly using the tools such as GDPR (General Data Protection Regulation).

Key words
information security, personal data, risk, legislation

JEL classification
K36, K38, K24

1 Úvod

Podľa medzinárodného štandardu ISO/IEC 27001 je informačná bezpečnosť ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je zaistenie kontinuity nielen obchodných procesov. Informácia je obsahom údajov a vyskytuje sa v rozličných formách - písomnej ústnej, obrazovej, elektronickej (digitálnej) a na jej spracovávanie (získavanie, prenos, spracovávanie, uchovávanie, archiváciu a ničenie) sa používajú rôzne prostriedky. Nakoľko je informácia kľúčovým aktívom, jej ohrozenie je problém, ktorý treba rýchle a efektívne riešiť. Adekvátna ochrana informácie vychádza z toho, na aký účel sa informácia používa a čo ju a akým spôsobom ohrozuje. Informácia sa v čoraz väčšej miere spracováva v digitálnej/elektronickej forme pomocou počítačov a iných IKT (informačné a komunikačné technológie) systémov. Získať neoprávnený prístup k informáciám, narušiť ich dôvernosť,

[1] Ing. Peter Lošonczi, PhD. MBA MSc., Vysoká škola bezpečnostného manažérstva v Košiciach, Ústav bezpečnostného manažérstva, Kukučínova 17, 04001 Košice, peter.losonczi@vsbm.sk.

dostupnosť, integritu alebo autentickosť možno aj prostredníctvom útoku na IKT zariadenia, v ktorých sa informácia spracováva. Potenciálna možnosť narušenia informácií (priamo alebo prostredníctvom útoku na technické zariadenie alebo prostredie v ktorom sa informácia spracováva) sa nazýva hrozba.

Hrozba (Threat) je pojem používaný v riadení rizík pre označenie zdroja nejakej negatívnej udalosti, sily, osoby alebo aktivity, ktorá chce alebo môže poškodiť nejakú hodnotu. Niekedy sa tiež používa pojem nebezpečenstvo. Hrozba má nežiaduci vplyv na bezpečnosť alebo môže spôsobiť škodu, stratu, nežiaducu zmenu, či iný nežiaduci jav. Hrozbou môžu byť živelné pohromy (napr. povodeň, požiar, kalamita atď.), havárie (napr. dopravná nehoda, kontaminácia vody, výbuch, radiácia, atď.), spoločenské javy (napr. vojnový konflikt, zločin, atď.) , ekonomické javy (napríklad finančná kríza, pohyb menového kurzu, nedostupnosť úveru, atď.) alebo správanie jednotlivcov (napríklad chyba obsluhy, krádež, neoprávnené užívanie, zneužitie právomoci, atď.).

Podstatu informačnej bezpečnosti dobre vystihujú smernice Guidelines for the Security of Information Systems, vydané OECD (Organisation for Economic Co-operation and Development - Organizácia pre hospodársku spoluprácu a rozvoj) v júli 2002, ktoré zdôraznili, že je potrebné podporovať vývoj bezpečnostnej kultúry, t. j. sústrediť sa na bezpečnosť pri vývoji informačných systémov a sietí a osvojiť si nové spôsoby myslenia a správania pri používaní informačných systémov a sietí. Smernice postulujú 9 základných princípov, z ktorých je potrebné vychádzať pri riešení informačnej bezpečnosti systémov. (Z týchto princípov vychádza a podrobnejšie ich rozpracováva medzinárodný štandard ISO/IEC 27001)

Bezpečnosť informačného systému je tiež často chápaná ako hraničný technologický problém s jasne definovanými okrajovými podmienkami. To však v reálnom svete neplatí.

Vo výklade terminológie bezpečnosti informačných technológií je informačná bezpečnosť definovaná ako bezpečnosť pri manipulácii s informáciami, predovšetkým vzhľadom na požiadavky, čo sa týka dôvernosti, integrity a dostupnosti informácií. Niektorí autori pridávajú aj požiadavky na zodpovednosť, autentickosť a užitočnosť informácií, ktoré majú vplyv na hodnotenie bezpečnosti systému. V súlade s informačnou bezpečnosťou by mali služby, požadujúce bezpečný informačný systém, zabezpečiť: Dostupnosť, Dôvernosť, Zodpovednosť, Autentickosť, Užitočnosť.

Samozrejme ochrana informácií nie je jediným problémom pri zabezpečení IS (informačný systém). Rovnako ako cenné informácie je potrebné chrániť všetky zdroje, aktíva IS, informačné technológie, dokumenty a ľudské zdroje. (Janošcová, 2014)

2 Špecifické atribúty informačnej bezpečnosti vo vzťahu k jednotlivcovi

2.1 Informačná hygiena a ekológia

Vo vzťahu k informačnej bezpečnosti sa v terminológii objavujú inovatívne pojmy ako je informačná hygiena a informačná ekológia. V krátkosti sa im budeme venovať.

Informačná hygiena

Dôležitou súčasťou práce s informáciami, počítačom a internetom je uvedomenie si toho, že výsledok alebo očakávané riešenie pomocou rýchleho vyhľadávania informácií, respektíve záujmového obsahu, nemusia byť vždy smerodajné, pravdivé alebo také podľa ktorých by sme sa mali stoj čo stoj riadiť. Je treba sa naučiť pracovať s informáciami z viacerých zdrojov, ktoré by sa mali overovať a taktiež by sme sa mali vysporiadať s prebytkom informácií, ktoré je treba filtrovať vhodnou selekciou. Dôležitým faktorom je takisto doba, ktorú sme ochotní denne takýmto aktivitám venovať a kladenie si otázky, či nie sú na úkor dôležitejších vecí.

Vo všeobecnosti by sa dalo povedať, že je informačná hygiena nástroj, ktorý umožňuje dosahovať prostredníctvom vhodného usporiadania informačného a pracovného režimu vyššiu efektivitu pri získavaní informácií.

V danej súvislosti sa často poukazuje na súčasný stav spoločnosti, kde sa stretávame s nadbytkom informácií a z toho vychádzajúceho problému informačného preťaženia. Je preto potrebné postupne meniť naše informačné návyky. Informačnú hygienu je možné chápať aj ako súčasť duševnej hygieny. Existujú preto niektoré všeobecné zásady pri práci s internetom, ktoré môžu dopomôcť k lepšiemu usporiadaniu pracovného režimu.

Informačná ekológia

Ďalším pojmom s ktorým sa informačná hygiena spája je informačná ekológia. Ako odozva na zvyšujúci sa podiel informácií nielen na rýchlo sa rozvíjajúcom internete, ale aj v každodenných médiách sa okolo roku 2000 do oblasti informačnej vedy začal čoraz častejšie dostávať pojem informačná ekológia. Pojem nemá svoju vlastnú definíciu, ktorá by presne vystihovala samotnú podstatu informačnej ekológie ako takej. Je mnoho autorov, ktorí sa ňou zaoberajú z rôznych pohľadov. Informačnú ekológiu možno definovať ako vzťahy človeka a informačného prostredia. Obsahuje tvorbu, komunikovanie, rozširovanie a využívanie informácií s cieľom regulovať informačné procesy a vzájomné prispôsobovanie človeka a informačného prostredia. Pojem ekológie ako vedy o vzťahoch organizmov a prostredia a ich vzťahov navzájom sa preniesol do informačného prostredia organizácií. Vzťahy človeka a informačného prostredia môžu ovplyvňovať aktivity človeka, hodnoty, komunita a nástroje komunikovania a organizovania odborných informácií. K cieľom informačnej ekológie informačných systémov a služieb patrí „čistota" informačného prostredia ako zmysluplné regulovanie procesov využívania informácií. Informačné prostredie je často „znečistené" rozmanitosťou zdrojov a ich neorganizovanosťou. Informačná ekológia preto môže pomôcť minimalizovať informačné preťaženie človeka a riziká využívania informácií v elektronickom prostredí.

2.2 Vývoj v oblasti ľudských práv

Pre chápanie súvislosti a koreňov informačnej bezpečnosti je často potrebné nahliadnuť aj do minulosti. Zároveň treba informačnú bezpečnosť chápať ako súčasť ľudských práv, ktoré v histórii ľudstva mali svoj špecifický vývoj.

Z historického hľadiska mali pre formovanie ľudských práv význam viaceré dokumenty, medzi ktoré patrí najmä anglická Magna Charta Libertatum z roku 1215, uhorská Zlatá bula z roku 1222, anglický Habeas Corpus Act z roku 1679 a anglická Listina práv (Bill of Rights) z roku 1689. Ideál ľudských práv univerzálneho charakteru, ktorý má svoj pôvod v prirodzenej právnej náuke, sa však dostal do popredia až v období osvietenstva. Rozhodujúci význam pre zakotvenie ľudských práv mala Deklarácia práv človeka a občana bola prijatá francúzskym Ústavodarným národným zhromaždením v roku 1789 počas Veľkej francúzskej revolúcie. Táto deklarácia odmietla stavovské rozdelenie spoločnosti a deklarovala rovnosť všetkých ľudí pred zákonom, čím otvorila cestu k zrušeniu privilégií viažucich sa k stavovskej príslušnosti a zamedzeniu diskriminácie. prekážkou zakotvenia týchto práv v medzinárodných zmluvách. Preto sú práva tretej generácie obsiahnuté iba v nezáväzných dokumentoch, ako je Deklarácia Konferencie Organizácie spojených národov o životnom prostredí človeka (Štokholmská deklarácia) z roku 1972 a Deklarácia z Ria de Janeira o životnom prostredí a rozvoji z roku 1992. (Ľudské práva, 2018)

Pre zakotvenie ľudských práv a slobôd v povojnovej Európe mala rozhodujúci význam Všeobecná deklarácia ľudských práv prijatá Valným zhromaždením Organizácie spojených národov 10. decembra 1948, ktorá je všeobecným katalógom ľudských práv. Pre ochranu

ľudských práv v európskom priestore má rozhodujúci význam Európsky dohovor o ochrane ľudských práv a základných slobôd podpísaný pod záštitou Rady Európy v roku 1950 v Ríme.

Význam ľudských práv pre Európsku úniu zdôraznilo prijatie Charty základných práv Európskej únie v roku 2000.

Právnu úpravu ľudských práv v Slovenskej republike rieši Ústava Slovenskej republiky č. 460/1992 Zb., ktorá vo svojej druhej hlave zakotvuje základné práva a slobody a ústavný zákon č. 23/1991 Zb., ktorým sa uvádza Listina základných práv a slobôd ako ústavný zákon Federálneho zhromaždenia Českej a Slovenskej federatívnej republiky.

Ľudské práva sa zvyčajne členia na tri generácie. Toto členenie vyjadruje nielen podstatu a znaky jednotlivých typov ľudských práv, ale aj historickú genézu ich vzniku. Prvá generácia ľudských práv zahŕňa občianske a politické práva, kde patrí aj právo na informácie a právo na súkromie, ktoré úzko súvisia s ďalšími právami patriacimi práve do tejto skupiny - právo na nedotknuteľnosť osoby a jej súkromia, právo na ochranu ľudskej dôstojnosti, osobnej cti, dobrej povesti, na ochranu mena, právo na vlastníctvo, slobodu prejavu a podobne.

Druhú generáciu práv tvoria hospodárske, sociálne a kultúrne práva kde radíme právo na slobodnú voľbu povolania, právo podnikať a uskutočňovať inú zárobkovú činnosť, právo na prácu, na spravodlivé a uspokojujúce pracovné podmienky, právo slobodne sa združovať, právo na štrajk, práva žien, mladistvých a osôb zdravotne postihnutých, právo na primerané hmotné zabezpečenie v starobe, pri nespôsobilosti v práci, na ochranu zdravia, právo na vzdelanie, či právo na slobodu vedeckého bádania a umenia, aj právo na zákonnú ochranu tvorivej duševnej činnosti.

Tretiu generáciu ľudských práv tvoria práva, ktoré prekračujú rámec prvej a druhej generácie, a zahŕňa pomerne široký okruh práv, ktoré možno charakterizovať ako práva solidarity. Zabezpečenie dodržiavania týchto práv si vyžaduje určitú formu účasti a spolupráce viacerých jednotlivcov a štátov. Realizácia týchto práv presahuje štátne hranice a mnohokrát aj hranice regiónov či kontinentov. Suverenita štátov, kontroverzná povaha týchto práv a rozdielne ekonomické podmienky v rôznych štátoch sú však prekážkou zakotvenia týchto práv v medzinárodných zmluvách. Preto sú práva tretej generácie obsiahnuté iba v nezáväzných dokumentoch, ako je Deklarácia Konferencie Organizácie spojených národov o životnom prostredí človeka (Štokholmská deklarácia) z roku 1972 a Deklarácia z Ria de Janeira o životnom prostredí a rozvoji z roku 1992. (Ľudské práva, 2018)

Všetky spomenuté práva sa dotýkajú aj informačnej spoločnosti v ktorej práve žijeme.

3 Ochrana občana

Ako z kontextu predošlého vyplýva majú ľudské práva priamu nadväznosť na ochranu jednotlivca a to v rôznych špecifických rovinách. Ochrana občana alebo jednotlivca sa spája so základnými ľudskými právami a slobodami, kam patrí spôsobilosť každého na práva, teda na právo na život, na nedotknuteľnosť osoby a jej súkromia, na osobnú slobodu, na právo zachovania ľudskej dôstojnosti, osobnej cti, dobrej povesti, na ochranu mena, na ochranu pred neoprávneným zasahovaním do rodinného a súkromného života. Nájdeme tu taktiež právo vlastniť a tiež právo na nedotknuteľnosť obydlia. Samozrejmosťou by malo byť listové tajomstvo, tajomstvo dopravovaných správ, iných písomností, ochrana osobných údajov, sloboda pohybu a pobytu, sloboda myslenia, svedomia, náboženského vyznania a viery, právo zmeniť náboženské vyznanie a vieru, verejne prejavovať svoje zmýšľanie, právo slobody náboženstva, viery, zúčastňovania sa náboženských obradov, vyučovania náboženstva, organizácií cirkví, brannej povinnosti a vojenskej služby. Patrí tu tiež zákaz vyhostenia vlastného občana, zákaz mučenia, krutého zaobchádzania, neľudského či ponižujúceho zaobchádzania alebo trestu a takisto zákaz nútených prác alebo služieb.

V informačnej spoločnosti je jedným z jej hlavných problémov aj kybernetická bezpečnosť, ktorej narušenie môže spôsobiť veľké škody a oslabiť dôveru občanov v digitálnu

spoločnosť. Kladie sa preto veľký dôraz na právo, čo sa týka súkromia v informačnej spoločnosti. Aj toto právo predstavuje v súčasnosti základné ľudské právo, ktoré je ako také chránené rôznymi legislatívnymi prostriedkami. Hranica medzi súkromným a verejným je však veľmi tenká a aj vďaka postupne prebiehajúcim sociálnym či technologickým zmenám je problematické presne definovať obsah a rozsah súkromia jednotlivca.

Vzhľadom na značnú dynamiku a rozsah vývoja internetu, webových služieb a viacerých alternatív k tradičným spôsobom komunikácie informácií sa však legislatívne opatrenia javia ako nedostatočne flexibilné a neschopné vyrovnať krok s tempom vzniku nových bezpečnostných rizík. To kladie významný podiel zodpovednosti za ochranu súkromia na plecia samotného používateľa. Okrem iného by sa za jeden zo základných problémov v rámci otázok súkromia na internete mohla považovať aj absencia primeranej informačnej gramotnosti, čo môže mať za následok nedostatočnú informovanosť používateľa o rizikách, ktoré mu hrozia pri práci v kyberpriestore. (Právo na súkromie v informačnej spoločnosti, 2011)

3.1 Ochrana občana v praxi

Dalo by sa povedať, že snáď všetky oblasti ľudskej činnosti sú čoraz viac závislé od informácií a informačných technológií podporujúcich spracovanie informácií.

Informačné súkromie: Daná problematika sa takisto spája s informačným súkromím, ktoré môže označovať iba súkromie osobných údajov, ale vzhľadom na súčasnú spätosť komunikácie s výpočtovou technikou sa často využíva na spoločné pomenovanie komunikačného a dátového súkromia.

Internetové súkromie: Toto označenie odkazuje najmä na právo jednotlivca pokojne užívať súkromný život na internetovej sieti a právo na ochranu súkromných informácií podľa zákona, ale jeho obsahom je aj zákaz nezákonného odhaľovania či poskytovania určitých osobných a citlivých informácií na internete vrátane faktov a fotografií. Užívateľ má právo vedieť, aké informácie o ňom sú zhromažďované na webových stránkach, na aký účel budú použité a komu budú poskytnuté. Právo si vybrať. Klienti majú právo rozhodnúť o použití svojich osobných údajov. Primeraný prístup. Užívatelia by mali mať prístup k osobným údajom a opraviť či zmazať chybné informácie prostredníctvom primeraných prístupov kvôli kontrole správnosti a úplnosti týchto údajov. Poskytovateľ siete by mal garantovať bezpečnosť informácií a predchádzať neautorizovaným a nelegálnym prístupom. Používatelia by mali mať právo vyžadovať, aby stránka poskytovala nevyhnutné a primerané opatrenia na ochranu ich údajov. Internetové súkromie by navyše malo obsahovať právo užívateľa mať nad informáciami kontrolu a v prípade potreby podať žalobu na súde.

Duševné vlastníctvo: Je „majetok" nehmotnej povahy, ktorý je výsledkom tvorivého myslenia alebo tvorivej duševnej činnosti. Je predmetom právnej ochrany a jeho používanie je preto viazané na súhlas autora, či tvorcu. Právo duševného vlastníctva obsahuje dve oblasti. Prvou je autorské právo a práva súvisiace s autorským právom, ktoré súvisia skôr s umeleckou, kultúrnu oblasťou a druhou oblasťou je právo priemyselného vlastníctva súvisiace skôr s hospodárskou, technickou oblasťou.

Osobné údaje : Osobné údaje sú vstupnou bránou do súkromia každého z nás. S osobnými údajmi sa stretávame v každodennom živote pri uplatňovaní rôznych spoločenských vzťahov pričom nie vždy je jasné, čo všetko možno považovať za osobné údaje. Podľa článku 4 odsek 1 nariadenia GDPR (Nariadenie Európskeho parlamentu a Rady EÚ o ochrane osobných údajov - General Data Protection Regulation) sú osobné údaje akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby ("dotknutej osoby"). Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Nariadenie GDPR

dopĺňa, že osobným údajom je aj emailová adresa, dokonca podľa nového nariadenia GDPR osobné údaje sú aj cookies. Definícia pojmu osobné údaje je pomerne zložitá. Po obsahovej stránke je tvorená z niekoľkých základných bodov, ktoré spoločne vystupujú v pozícii identifikátorov patriacich konkrétnej fyzickej osobe a vytárajú jej identitu. Tá ale v rovine základných ľudských práv a slobôd prislúcha výlučne fyzickej osobe, teda jednotlivcovi, ktorému zákon poskytuje ochranu pri spracúvaní jeho osobných údajov. Pokiaľ ide o údaje určujúce právnickú osobu alebo fyzickú osobu - podnikateľa, ktoré budú spracúvané v informačnom systéme prevádzkovateľa, nie sú osobnými údajmi a nebudú spadať do pôsobnosti zákona. Osobnými údajmi sú údaje, ktoré sa týkajú konkrétnej fyzickej osoby. Vo všeobecnosti sa dá povedať, že osobnými údajmi môžu byť akékoľvek údaje týkajúce sa konkrétnej osoby, a preto aj zákon v sebe neobsahuje presný výpočet údajov, ktoré možno považovať za osobné údaje. Poskytuje tzv. demonštratívny výpočet charakteristík, ktoré určujú alebo sú spôsobilé určiť jej osobu, pričom môže byť k dispozícii v akejkoľvek forme, a to v grafickej, fotografickej, zvukovej alebo papierovej podobe ako aj v pamäti počítača. Zvukové a obrazové údaje je potrebné pokladať za osobné údaje, pretože taktiež môžu poskytovať informácie o jednotlivcovi. Za osobné údaje sa môžu pokladať aj informácie obsiahnuté vo voľnom texte v elektronickom dokumente za predpokladu, že sú splnené ostatné kritéria definície osobných údajov. To, či je nejaký údaj osobným, je potrebné posudzovať v danej situácii, na základe dostupných údajov, ktoré možno k fyzickej osobe priradiť.

Bežne spracovávanými osobnými údajmi sú napríklad titul, meno, priezvisko, adresa trvalého alebo prechodného pobytu, dátum narodenia, e-mail, či telefónne číslo. Okrem toho poznáme tzv. osobitnú kategóriu, ktorých spracovanie je povolené iba v zákonom stanovených výnimkách. Jedná sa najmä o údaje týkajúce sa rasy, náboženstva, politického príslušenstva, ďalej údaje, ktoré sa týkajú zdravia, prípadne pohlavného života osôb. Za osobitnú kategóriu v súčasnosti platný zákon o ochrane osobných údajov považuje aj fotografiu alebo videozáznam ale len v prípade, ak sa spracúvajú osobitnými technickými prostredkiami určenými ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu osoby.

Za osobné údaje už budú podľa GDPR považované aj online identifikátory osôb, napríklad IP adresa, cookies, identifikátory mobilných zariadení. Ak sa napríklad IP adresa dá použiť na zistenie, kde sa jednotlivec nachádza, ide o osobné údaje. Takisto aj elektronické identifikátory, napríklad RFID technológie. Lokalizačné údaje sa klasifikujú ako osobné, pretože sa dajú použiť na identifikáciu toho, kde jednotlivec žije, kde pracuje.

Nariadenie považuje za spracovanie osobných údajov aj sledovanie správania fyzických osôb na internete s využitím technológií, ktoré vytvárajú profily týchto osôb za účelom prijatia rozhodnutia týkajúceho sa týchto osôb alebo analýzy či predvídania ich osobných preferencií, správania a postojov. Profilovanie je v súčasnosti bežne používaný marketingový nástroj pri maloobchodnom predaji cez internet, GDPR stanovuje prevádzkovateľom podmienky, pri ktorých môžu tento nástroj využívať.

Genetické údaje podľa GDPR sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby. Genetické údaje sa používajú na účely lekárskej a výskumnej činnosti.

Biometrické údaje GDPR charakterizuje ako osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad daktyloskopické údaje. Typickým biometrickým údajom je napríklad rozpoznanie sietnice či odtlačok prsta.

Spracovanie fotografie alebo grafického zobrazenia podpisu bez získavania biometrických údajov osobitnými technickými prostriedkami sa nebude považovať za spracovanie osobitných kategórií osobných údajov. (Riško, 2018)

4 Rizika spojene s informačnou bezpečnosťou občana

Na základe uvedených chránených záujmov vo vzťahu k občanovi môžeme zadefinovať niektoré základné rizika.

Zneužitie osobných údajov

V trestnom zákone môžeme nájsť skutkové podstaty trestných činov, ktoré majú predchádzať a chrániť zneužitie osobných údajov. V trestnom zákone je možné nájsť trestný čin podľa § 374 a to Neoprávnené nakladanie s osobnými údajmi. Pri naplnení skutkovej podstaty tohto trestného činu sa páchateľ potrestá odňatím slobody až na jeden rok. Odňatím slobody až na dva roky sa páchateľ potrestá, ak spácha takýto čin a spôsobí ním vážnu ujmu na právach dotknutej osoby, alebo ak ho spácha verejne alebo ak ho spácha závažnejším spôsobom konania. Ak orgány činné v trestnom konaní odhalia zneužitie osobných údajov na internete, môže tiež dôjsť k naplneniu skutkovej podstaty trestného činu. (Zneužitie osobných údajov, 2018)

Počítačová kriminalita

Ako sme už viackrát spomenuli, informačné technológie sú fenomén, ktoré okrem praktických prínosov prináša aj negatívne javy. Tak ako mnohé iné nástroje, je aj počítačová technika použiteľná na účely, ktoré nie sú vždy v súlade so spoločenskými požiadavkami, ba častokrát idú za hranice stanovených noriem. Sprievodným javom internetových technológií je aj nárast aktivít, ktoré sú často klasifikované ako protizákonné a v informatickom a právnom slangu dostali pomenovanie počítačová kriminalita alebo IT kriminalita.

Dohovor o počítačovej kriminalite zaviedol zaujímavú kategorizáciu činov, ktoré sú namierené proti dôvernosti, dostupnosti a integrite počítačových systémov, sietí a počítačových údajov. Sú to trestné činy proti dôvernosti, hodnovernosti a dostupnosti počítačových údajov a systémov. Radíme sem: nezákonný prístup do počítačového systému, nezákonné zachytávanie údajov, zasahovanie do údajov, zasahovanie do systému, počítačové trestné činy (falšovanie počítačových údajov a počítačové podvody), trestné činy týkajúce sa obsahu - trestné činy týkajúce sa detskej pornografie. Trestné činy týkajúce sa porušenia autorských a príbuzenských práv.

IT kriminalitu je možné rozdeliť na dve základné oblasti:

1) oblasť kde IT (počítače, softvérové vybavenie) sú prostriedkom, to znamená, že práve pomocou výpočtovej techniky je páchaná trestná činnosť a teda počítač je len nástrojom na dosiahnutie iného cieľa. Ide napríklad o:

- pozmeňovanie a falšovanie peňazí a cenín
- ohováranie, zastrašovanie, vydieranie
- úverové podvody (fiktívne doklady)
- prechovávanie a šírenie dát v rozpore so zákonom

2) oblasť kde aktíva sú cieľom aktivít považovaných za trestnú činnosť. Patrí sem:

- porušovanie autorského práva
- cielené útoky zamerané voči dôvernosti, dostupnosti, integrite informačných systémov a dát, ktoré sú v nich spracované

- zneužívanie a poškodzovanie dát na nosiči informácií
- neoprávnené nakladanie s údajmi dôverného charakteru (napríklad osobné údaje)

Hrozbou nie je iba internet

Pripájanie sa na internet cez tablet alebo telefón je v dnešnej dobe už úplne bežné. Avšak aj tu by mali byť užívatelia opatrní. Takisto si treba dávať pozor pri rôznych mobilných aplikáciách. Telefón so sebou taktiež prináša napríklad riziko nevyžiadaných, marketingových telefonátov. Je preto správne byť opatrný a nezverejňovať svoje telefónne číslo na internete.

Odborníci považujú za nebezpečné hlavne zadávanie osobných dát, ktoré sú však nevyhnutné pri registrácii na rôznych webových stránkach. Málokto číta aj zmluvné podmienky, takže užívateľ nemá istotu, u koho citlivé informácie nakoniec skončia. Tieto riziká nie sú ani tak vecou verejných vyhľadávačov, ale hovoríme skôr o tzv. šedej zóne internetu.

Zákon o ochrane osobných údajov uvádza, že každý človek má právo sa rozhodnúť, ako so svojimi osobnými údajmi bude nakladať a komu ich sprístupní. Zneužité môžu byť osobné údaje, bankové údaje, zdravotné správy, fotografie, či videá, prípadne informácie o sociálno-ekonomických pomeroch.

5 Národne a európske legislatívne prostredie rizika spojene s informačnou bezpečnosťou občana

5.1 Národne a európske legislatívne prostredie

Pre štandardizáciu pravidiel ochrany a záujmov občana popísaných v predošlých častiach je vytvorená rada legislatívnych nástrojov, ktorých synergia doma aj v zahraničí ma snahu zjednotiť nové chápanie ochrany občana voči nástrahách 21. storočia.

Zákon č. 18/2018 Z. z. - Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov - Zákonom sa slovenský právny poriadok harmonizuje s nariadením (GDPR) a do jeho tretej časti je transponovaná Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV.

Medzi právne normy a predpisy týkajúce sa informačnej bezpečnosti patria:

- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností,
- vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti,
- vyhláška NBÚ č. 91/2002 Z. z. ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií,
- zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov,
- zákon 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

5.2 Európske systémové nástroje týkajúce sa informačnej bezpečnosti občana

Organizačné zabezpečenie úloh štátu v oblasti informačnej bezpečnosti prešlo vo vybraných krajinách z pôsobnosti jedného rezortného orgánu na viaceré štátne inštitúcie. Aby sa zabezpečila vzájomná koordinácia jednotlivých aktivít, boli určené koordinujúce inštitúcie. Na tento účel boli v niektorých prípadoch využité existujúce orgány a inštitúcie (USA - NIST), ale v iných prípadoch vznikli nové inštitúcie (napr. v Nemecku - Federálnych úrade pre informačnú bezpečnosť - BSI) špeciálne pre riešenie otázok informačnej bezpečnosti.

Európska komisia prijala počas svojej existencie rad dokumentov právneho/regulačného charakteru, priamo súvisiacich s informačnou bezpečnosťou.

Pravdepodobne závažnosť informačnej bezpečnosti pre informatizáciu spoločnosti a množstvo úloh s tým súvisiacich viedlo k tomu, že EÚ 15. marca 2004 vytvorila agentúru ENISA (European Network and Information Security Agency), ktorá má slúžiť ako centrum excelencie pre sieťovú a informačnú bezpečnosť a má zabezpečiť v EÚ potrebnú vysokú úroveň bezpečnosti sietí a prenášaných údajov. V roku 2006 ENISA ustanovila ad hoc pracovnú skupinu Working Group on "Regulatory Aspects of Network and Information Security" (WG RANIS), ktorá spracovala prehľad legislatívnych a regulačných aktivít EU v oblasti informačnej bezpečnosti.

Dohovor Rady Európy o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov, známy pod názvom Dohovor 108, sa považuje za základný kameň vzťahujúci sa na súkromný život a ochranu osobných údajov v Európe. Podpísaný bol 28. januára 1981 v Štrasburgu. Deň jeho podpisu, 28. január, je Dňom ochrany osobných údajov, ktorý je dobrou príležitosťou pre nás všetkých sa zamyslieť nad ochranou svojho súkromia a osobných dát. V súčasnosti ochrana osobných údajov prechádza v Európskej únii zásadnou zmenou, ktorá vyvrcholila tento rok v máji, odkedy (25.5.2018) sa začalo v praxi uplatňovať Všeobecné nariadenie o ochrane osobných údajov (General Data Protection Regulation - GDPR).

Okrem spomenutých nadnárodných nástrojov na ochranu osobných údajov a všeobecne práva na súkromie má väčšina štátnych zriadení platné individuálne legislatívne opatrenia, ktoré riešia túto problematiku v súlade s týmito medzinárodnými odporúčaniami.

Aj keď EÚ prijala rad dokumentov buď priamo venovaných informačnej bezpečnosti alebo s ňou súvisiacich, dlho nemala výkonné orgány, ktoré by sa zaoberali informačnou bezpečnosťou. Na vytváranie analytických dokumentov využívala/využíva akademické alebo súkromné organizácie, resp. vytvára pracovné skupiny z existujúcich odborných orgánov a národných inštitúcií. Svoje zámery v oblasti informačnej bezpečnosti EÚ presadzuje najmä prostredníctvom európskej legislatívy. Jej úlohou je teda pomáhať EÚ, jej členským štátom aj komerčnej sfére predchádzať, riešiť a odpovedať na sieťové a informačno-bezpečnostné problémy.

6 Konkrétne situácie, ktoré môžu vzniknúť pri zneužití údajov

Potenciálne nebezpečenstvo spočívajúce v zneužití osobných údajov hrozí prakticky vo všetkých oblastiach nášho súkromného aj spoločenského života. Osobné údaje sú zapisované už pri našom narodení do zdravotnej dokumentácie. Počas školskej dochádzky sa naše údaje priebežne poskytujú takisto. Predkladáme ich pri každom prijímacom pohovore a tiež v styku s rôznymi inštitúciami na ktoré narazíme, či už pri sobáši, kúpe auta, zariaďovaní bývania alebo pri vybavovaní pôžičiek, respektíve pri kúpach väčšieho charakteru, prípadne v knižnici, pri registrácii na rôznych záujmových portáloch, aj pri vybavovaní poistenia, či dokladov potrebných na cestovanie. Čo sa týka bezpečnosti našich údajov, nie je zväčša možné vystopovať kto s nimi prišiel do styku a či ich neoprávnene nevyužil.

Údaje, ktoré môžu byť zneužité:

Osobné údaje - meno, bydlisko, telefónne číslo, škola, pracovisko, vek, rodné číslo, pohlavie, informácie o zdravotnom stave, príslušnosť k náboženskej skupine, sexuálna orientácia, emailová adresa, prístupové heslá k emailovej schránke, k internetovým profilom. (Metodické usmernenie č. 1/2013)

- Bankové údaje - číslo účtu, heslo, informácie ku kreditným kartám.
- Fotografie a videá - predovšetkým také, ktoré vás zachytávajú v nepríjemných alebo trápnych situáciách, tiež aj fotografie, ktoré poskytujú informácie o vašom životnom štýle, trávení voľného času (napríklad fotografie z dovoleniek). Informácie o sociálno-ekonomických pomeroch - informácie o tom, kde a ako žijete, aké sú vaše príjmy (v

prípade detí príjmy rodičov), čo vlastníte (elektronika, dopravné prostriedky, nehnuteľnosti), akým záľubám sa venujete.

Tieto údaje sa dostávajú k „nechceným“ adresátom prostredníctvom emailov, SMS správ, zverejnením na chatoch a internetových fórach, zadaním na webových stránkach, zverejnením v profiloch, na sociálnych sieťach, na stránkach na zverejňovanie fotografií a videí. Naše údaje sa k nepovolaným ľuďom môžu dostať aj sprostredkovane, napr. ak našu fotografiu uverejní náš kamarát, prípadne sa našimi majetkovými pomermi niekto cez internet pochváli. (Kozáriková, 2014)

Osobné informácie

Akékoľvek zverejnené osobné informácie (napr. informácie o rasovej alebo národnostnej príslušnosti, o zdravotnom stave, či intímnom živote) sa v rukách nepovolanej osoby môžu stať príčinou posmechu, vyhrážok alebo nástrojom na vydieranie. Aj ďalšími informáciami, ktoré zverejňujeme na internete (komentáre v diskusiách, členstvo v internetových skupinách, fotografie z akcií) o sebe vytvárame určitý obraz, ktorý môže ovplyvniť mienku nášho okolia, prípadne potenciálneho zamestnávateľa.

Existuje veľa možností ako, kde, alebo kým sa dajú osobné údaje zneužiť. Vzhľadom na nespočetné množstvo situácií, ktoré v bežnom živote môžu vzniknúť, uvádzame pár príkladov s ktorými sa môže stretnúť veľká skupina bežných užívateľov informačných technológií.

„Nabúranie" do profilu, zneužitie profilu, e-mailovej schránky: Ak dávame k dispozícii svoje prístupové meno a heslo alebo ak si volíme ľahko zistiteľné heslo, môže sa niekto „nabúrať" do nášho profilu alebo e-mailovej schránky a následne vystupovať v našom mene - napr. posielať e-maily, komunikovať na chate a pod.

Pozor na rodné číslo: Rodné číslo je jedinečný identifikátor osôb v Slovenskej republike. Slúži na identifikáciu osoby, jej pohlavia a veku. Rodné číslo sa považuje za kľúč k všetkým ostatným údajom. Odborníci preto upozorňujú, že by mali občania uvádzať svoje rodné číslo iba na miestach, kde je to nevyhnutné a ktoré sú vierohodné.

Kontakt: Ak dávame verejne k dispozícii svoju e-mailovú adresu alebo mobilné číslo, musíme rátať s tým, že nás môže ktokoľvek kontaktovať. Rôzne firmy a spoločnosti využívajú možnosť osloviť nás cielenou reklamou podľa veku, záujmov, spotrebiteľského správania. Okrem zasielania rôznych reklamných správ a spam-u sa však môže stať, že nás bude prostredníctvom emailov, telefonátov alebo SMS správ kontaktovať niekto, kým kontaktovaný byť nechceme, môže vás opakovane obťažovať, až prenasledovať.

Krádeže: Informácie o sociálno-ekonomických pomeroch môžu byť dobrým návodom pre zlodejov, ktorí si takto vytipujú vhodnú obeť. Podľa toho, že zverejníme termín nášho odchodu na dovolenku, resp. fotografie z dovolenky; alebo naše denné zvyklosti, ľahko zistia vhodnú dobu, kedy nebudeme doma. Pre šikovného podvodníka nie je problém vydávať sa napríklad za kamaráta príbuzného a tieto informácie od neho postupne vysondovať.

Zneužitie fotografií: Fotografie sa na internet dostávajú tak, že ich tam zverejníme sami (v profiloch, na sociálnych sieťach, na stránkach na zverejňovanie fotografií), prípadne naše fotografie zverejní niekto iný alebo ich nechránené posielame sami prostredníctvom e-mailu.
Fotografie, ktoré nás zachytávajú v nepríjemných alebo trápnych situáciách (napr. pod vplyvom alkoholu), fotografie v spodnej bielizni alebo s odhalenými časťami tela, v erotických pózach, sa môžu dostať k niekomu, komu nechcete (napríklad k našim rodičom, kolegom, deťom) a môžu byť použité na vydieranie alebo na zosmiešnenie. Fotografie môžu byť zneužité aj na vytvorenie falošného profilu na rôznych sociálnych aplikáciách, je z nich možné vytvoriť fotomontáž a môžu byť informáciou pre zlodejov a podvodníkov.

Vydieranie, pomsta, šikanovanie: Nepodceňujme takisto fakt, že hociktorý z uvedených spôsobov zneužitia osobných údajov môže byť cestou pre vydieranie, pomstu alebo

šikanovanie. Po zverejnení emailovej adresy alebo telefónneho čísla môžeme byť opakovane obťažovaní prezváňaním, zastrašovaní vyhrážkami, napádaní agresívnymi správami. Naše telefónne číslo môže byť zverejnené v rôznych inzerátoch, napr. aj v ponuke erotických služieb. Nabúranie do profilu a vystupovanie v našom mene býva často práve aktom pomsty. Informácie o nás, našej rodine, majetkových pomeroch sa môžu stať podkladom pre vydieranie alebo šikanovanie, či kyberšikanu.
Sexuálne obťažovanie, zneužitie: Aj keď sa obeťou sexuálneho obťažovania (prípadne následne až sexuálneho zneužitia) na internete môže stať ktokoľvek, špeciálne ohrozenou skupinou sú deti. Citlivými údajmi sú v tomto prípade predovšetkým vek, pohlavie, fotografie zverejnené v internetových profiloch. Čím viac osobných údajov o sebe zverejníme, tým viac priestoru vytvárame pre agresora, jednak upútaním pozornosti, ale aj možnosťou nadviazania kontaktu.
Online nakupovanie: Viaceré internetové obchody vyžadujú pred nákupom registráciu, či už kvôli samotnému nákupu alebo na marketingový prieskum. Tieto údaje môžu byť posunuté ďalej iným spoločnostiam a môžu byť taktiež zneužité.
Škodlivé vírusy: Môžeme tu spomenúť aj rôzne vírusy, ktoré patria do skupiny škodlivého softvéru. Vírusy sú zrejme najrozšírenejšie pomenovanie, aj keď nie celkom presné. Vírusy sú totiž len jedno z nebezpečenstiev, ktoré ohrozujú náš počítač a naše osobné údaje uložené v počítači, respektíve na sieti.

Podľa charakteru uvedených príkladov je zrejmé, že znalosť o daných formách zneužitia osobných údajov je cestou ako potláčať túto formu kriminality. Vzdelávanie v danej oblasti na rôznych úrovniach školstva v kombinácii s modernými inovatívnymi formami vzdelávania je tou správnou formou, ako nenútene zvyšovať bezpečnostné povedomie u širokej verejnosti. (Kováčová, Vacková, 2015)

7 Záver

Na bezpečnosť občana v dobe moderných technológií, kde sú informácie základným artiklom, sa kladie čoraz väčší dôraz. Existuje mnoho možností ako informácie vyhľadávať, spracovávať a následne aj správnym spôsobom využívať. Túto aktivitu však sprevádzajú aj niektoré negatívne javy. Nielen odborníci sa neustále boria s problémom ako pri daných činnostiach, napríklad pri poskytovaní osobných údajov, či už fyzickom alebo prostredníctvom internetu, sa dá zabrániť ich zneužitiu.

Pozitívnym javom je, že si spoločnosť stále viac uvedomuje dôležitosť danej témy, keďže v čase globalizačných procesov je prakticky spätá s každou oblasťou, nielen pracovného, ale aj súkromného života.

Literatúra

[1] Janošcová, R. (2014). Princípy informačnej bezpečnosti. Retrieved from http://ics.upjs.sk/~jirasek/ops/Janoscova.pdf
[2] Kazanský, R. (2013). *Súčasné problémy výskumu medzinárodných konfliktov a kríz a ich riešenia*. Banská Bystrica, SR: Belianum.
[3] Kováčová, L., & Vacková, M. (2015). Applying Innovative Trends in the Process of Higher Education Security Personnel in Order to Increase Efficiency. *Procedia - Social and Behavioral Sciences*.
[4] Kozáriková, M. (2014). Dobrovoľne o sebe zverejňujeme citlivé informácie. Existuje ešte vôbec ochrana osobných údajov? Retrieved October 14, 2018, from https://www.aktuality.sk/clanok/259947/dobrovolne-o-sebe-zverejnujeme-citlive-informacie-existuje-este-vobec-ochrana-osobnych-udajov/
[5] Ľudské práva. (2018). Retrieved from http://ludskeprava.euroiuris.sk/index.php?link=vseob_lud_prava

[6] Metodické usmernenie č. 1/2013 k pojmu osobné údaje. (2013). Retrieved October 14, 2018, from https://marekstrba.sk/tag/metodicke-usmernenie-c-12013-k-pojmu-osobne-udaje/
[7] Právo na súkromie v informačnej spoločnosti. (2011). Retrieved October 14, 2018, from http://itlib.cvtisr.sk/archiv/2011/1/pravo-na-sukromie-v-informacnej-spolocnosti.html?page_id=815
[8] Zákon o ochrane osobných údajov 18/2018 Z.z. - (2018). Retrieved October 14, 2018, from https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525
[9] Zneužitie osobných údajov. (2018). Retrieved October 14, 2018, from http://www.banos.sk/sluzby/ochrana-osobnych-udajov/zneuzitie-osobnych-udajov