POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Informační etika a negativní jevy související s jejím porušováním

Diplomová práce

Information ethics and negative phenomena related to its violation

Master thesis

VEDOUCÍ PRÁCE

RNDr. Václav HNÍK, CSc.

AUTORKA PRÁCE

Bc. Olga PEŠKOVÁ

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 25. 8. 2022

Bc. Pešková Olga

Poděkování

Mé poděkování patří RNDr. Václavu Hníkovi, CSc. za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování diplomové práce věnoval.

ANOTACE

Tato diplomová práce se zabývá informační etikou a negativními jevy souvisejícími s jejím porušováním. Cílem této práce je tedy poukázat na současné negativní jevy, které jsou spojeny s informační etikou v kyberprostoru, dodržování, resp. nedodržování etického rámce v praktickém měřítku. Konkrétně je řešena otázka informační etiky v jednotlivých oblastech internetu. První část je teoretická, vysvětlení základních pojmů, důležitých pro toto téma či představení legislativy a kodexů provázaných s problematikou a také představuji mnou vybrané závažné negativní jevy, rozdělila jsem je z důvodu přehlednosti do samostatných kapitol. V následující praktické části je uveden konkrétní případ - negativní jev, který je uveden do současné četnosti a kategorizován jako trestný čin. Třetí část obsahuje mnou vybraný případ, ve kterém rozebírám porušení informační etiky.

KLÍČOVÁ SLOVA

etika * informace * kodex * bezpečnost * internet * kyberprostor * dezinformace

ANNOTATION

This diploma thesis deals with information ethics and negative phenomena related to its violation. The aim of this work is therefore to point out the current negative phenomena that are associated with information ethics in cyberspace. compliance, respectively non-compliance with the ethical framework on a practical scale, specifically the question of information ethics in individual areas of the Internet is addressed. The first part is theoretical, so the explanation of the basic concepts important for this topic or the introduction of legislation and codes related to the issue, and it is also focused on selected negative phenomena, which are divided into separate chapters. In the following practical part, a certain negative phenomenon is presented, which is included in the current frequency, as well as one criminal act. The third part contains a case chosen by me, in which I analyze a violation of information ethics.

KEYWORDS

ethics * information * codes * safety * internet * cyberspace * desinformation

Obsah

Úvod

Téma mé diplomové je informační etika a negativní jevy související s jejím porušováním. Ráda bych zopakovala cíl této práce. Ten spočívá hlavně v tom, poukázat na současné nejčastější negativní jevy, které jsou spojeny s informační etikou kyberprostoru, dodržování, resp. nedodržování etického rámce v praktickém měřítku, konkrétně je řešena otázka informační etiky v jednotlivých oblastech internetu, a přednést tak komplexní shrnutí problematiky etického chování v internetovém prostředí, a to nejen v procentuálním vyčíslení současné četnosti, ale i na případech spojených s trestnou činností, které jsou vždy představeny v samostatných kapitolách. Toto téma jsem si vybrala z několika důvodů. Prvním z důvodů je, že toto téma je v současnosti více než aktuální. V koronavirové době probíhalo veškeré dění ve společnosti přes internet. Například práce, školní výuka, zkoušky, schůzky, nakupování i výběrová řízení, protože jinak se v podstatě žít nedalo. Dalším a neméně důležitým důvodem je přemíra informací. Znovu musím zmínit současnou situaci a to, jak se na nás valí každou minutu nové informace, se stává někdy až nesnesitelné. Proto jsem si v tom sama chtěla udělat jasno. Zjistit, jaké problémy jsou nejčastější, jaký je vlastě rozdíl mezi pojmem dezinformace a tzv. fake news, jak se jim vyvarovat či jak je rozpoznat. Prozkoumat nakolik lidé ještě rozlišují dobré a špatné a jak tuto hranici posunul online svět.

V tomto fenoménu spatřuji dva zásadní problémy. První se týká obrovského světa internetu. Vzhledem k rozsahu, který internetové prostředí v dnešní době zaujímá, není lehké ho korigovat, ať už odkázáním na naše morální či etické cítění, tak legislativou, která se snaží podchytit hrozby, kontrolovat a popřípadě uvalit trest jedinci za porušení určitých zásad. Dnešní doba a internet zvlášť je hrozně rychlý a neustále se vyvíjí, což je pro legislativu nebo pro všeobecné nástroje k ochraně jedince/společnosti velice těžké a všeobecně vládne neustálý pocit, že zákon je vždy o krok pozadu. Druhým problémem je vzdělání. Na to jak velkou roli hraje online svět v našich životech, víme o něm děsivě málo. Jak se bránit před útoky, jak si ověřovat informace, jak vůbec v kyberprostoru fungovat.

To, obzvláště u mladých lidí, kteří v něm tráví už i většinu volného času, může být obrovský problém.

V mé diplomové práci se tedy budu v první části věnovat vysvětlení základních pojmů, které jsou důležité pro pochopení, dále uvádím platnou legislativu spojenou s informační etikou a také vybrané etické kodexy. Poté vždy představím určitý negativní jev spojený s informační etikou a v další části (praktické) uvedu negativní jev do souvislosti dnešní doby a také příklad trestného činu, který se v České republice v nedaleké době stal. Následuje případová studie, ve které je představen případ, který je dle mého názoru velmi důležitý a který si získal velkou pozornost světa a právě ukázal, jak nebezpečné místo může internet být.

Teoretická část

1 Definice základních pojmů

1.1. Etika

Etika, disciplína zabývající se tím, co je dobré a špatné a morálně správné a špatné. Termín je také aplikován na jakýkoli systém nebo teorii morálních hodnot nebo principů.

Jak máme žít? Zaměříme se na štěstí nebo na poznání, ctnost nebo vytváření krásných předmětů? Pokud si zvolíme štěstí, bude to naše vlastní nebo štěstí všech? A co konkrétnější otázky, které před námi stojí: je správné být v dobré věci nepoctivý? Můžeme ospravedlnit život v přepychu, zatímco jinde na světě lidé hladoví? Je odchod do války oprávněný v případech, kdy je pravděpodobné, že budou zabiti nevinní lidé? Je špatné klonovat lidskou bytost nebo ničit lidská embrya v lékařském výzkumu? Jaké jsou naše závazky, pokud vůbec nějaké, vůči generacím lidí, kteří přijdou po nás, a vůči nelidským zvířatům, se kterými sdílíme planetu?

Etika se těmito otázkami zabývá na všech úrovních. Jejím předmětem jsou základní otázky praktického rozhodování a mezi její hlavní zájmy patří povaha konečné hodnoty a standardy, podle nichž lze lidské jednání posuzovat jako správné nebo nesprávné.

Pojmy etika a morálka spolu úzce souvisí. Nyní je běžné odvolávat se na etické soudy nebo etické zásady tam, kde by dříve bylo přesnější mluvit o morálních soudech nebo morálních zásadách. Tyto aplikace jsou rozšířením významu etiky. V dřívějším použití se tento termín nevztahoval na samotnou morálku, ale na studijní obor nebo obor zkoumání, jehož předmětem je morálka. V tomto smyslu je etika ekvivalentem morální filozofie.[1]

Ačkoli etika byla vždy považována za odvětví filozofie, její všeobjímající praktická povaha ji spojuje s mnoha dalšími oblastmi studia, včetně antropologie,

[1] Janoš, Karel. Informační etika. Praha: Česká informační společnost, 1993

biologie, ekonomie, historie, politiky, sociologie a teologie. Přesto zůstává etika odlišná od těchto disciplín, protože nejde o věcné znalosti tak, jako jsou vědy a další obory zkoumání. Spíše to souvisí s určením povahy normativních teorií a aplikací těchto souborů principů na praktické morální problémy.

1.1.1. Počátky etiky

Pokud má člověk na mysli vlastní etiku – tedy systematické studium toho, co je morálně správné a co špatné – je jasné, že etika mohla vzniknout teprve tehdy, když lidské bytosti začaly přemýšlet o tom, jak nejlépe žít. Tato reflexivní fáze se objevila dlouho poté, co si lidské společnosti vyvinuly nějaký druh morálky, obvykle ve formě obvyklých norem správného a nesprávného chování. Proces reflexe měl tendenci vycházet z takových zvyků, i když nakonec mohl shledat nedostatek. V souladu s tím etika začala zavedením prvních morálních kodexů.

Prakticky každá lidská společnost má nějakou formu mýtu, která vysvětluje původ morálky. V pařížském Louvru je černý babylónský sloup s reliéfem zobrazujícím boha slunce Šamaše, který Chamurappimu (zemřel kolem roku 1750 př. n. l.) předkládá zákoník zákonů, známý jako Chamurappiho zákoník. Hebrejská Bible (Starý zákon) o tom, že Bůh dal Mojžíšovi deset přikázání (vzkvétala ve 14. – 13. století př. n. l.) na hoře Sinaj, lze považovat za další příklad. V dialogu Protagoras od Platóna (428/427–348/347 př. n. l.) je zjevně mýtický popis toho, jak se Zeus smiloval nad nešťastnými lidmi, kteří se fyzicky nevyrovnali ostatním zvířatům. Aby Zeus napravil tyto nedostatky, dal lidem morální smysl a schopnost práva a spravedlnosti, aby mohli žít ve větších společenstvích a vzájemně spolupracovat.

Není překvapivé, že morálka by měla být vybavena veškerým tajemstvím a silou božského původu. Nic jiného by nemohlo poskytnout tak silné důvody pro přijetí mravního zákona. Tím, že kněžství přisoudilo morálce božský původ, stalo se jejím vykladačem a strážcem, a tím si zajistilo moc, které se jen tak nevzdá. Toto spojení mezi morálkou a náboženstvím bylo tak pevně vytvořeno, že se stále někdy tvrdí, že bez náboženství nemůže existovat žádná morálka.

Podle tohoto názoru není etika samostatným studijním oborem, ale spíše oborem teologie.[2]

S názorem, že morálku stvořila božská moc, existuje určitá obtíž, již Platónovi známá. Platón ve svém dialogu Euthyphro zvažoval návrh, že je to božské schválení, co dělá akci dobrou. Platón poukázal na to, že pokud by tomu tak bylo, nebylo by možné říci, že bohové takové činy schvalují, protože jsou dobré. Proč je tedy schvalují? Je jejich schválení zcela libovolné? Platón to považoval za nemožné, a tak se domníval, že musí existovat nějaká měřítka dobra nebo zla, která jsou nezávislá na tom, co mají a nemají rádi bohové. Moderní filozofové obecně přijali Platonův argument, protože alternativa implikuje, že pokud by například bohové náhodou schvalovali mučení dětí a neschvalovali pomoc bližním, pak by mučení bylo dobré a sousedství špatné.

1.1.1.1 Starověké Řecko

Starověké Řecko bylo kolébkou západní filozofické etiky. Myšlenky Sokrata (asi 470–399 př. n. l.), Platóna a Aristotela (384–322 př. n. l.) budou diskutovány v další části. Náhlý rozkvět filozofie v tomto období měl kořeny v etickém myšlení dřívějších staletí. V básnické literatuře 7. a 6. století př. n. l. existovaly, stejně jako v jiných kulturách, morální předpisy, ale žádné skutečné pokusy formulovat koherentní celkový etický postoj. Řekové později označovali nejvýznamnější z těchto básníků a raných filozofů jako sedm mudrců a často je s úctou citují Platón a Aristoteles. Znalost myšlenky tohoto období je omezená, protože často zůstávají pouze fragmenty původních spisů spolu s pozdějšími zprávami o pochybné přesnosti.[3]

Pythagoras (asi 580 – asi 500 př. n. l.), jehož jméno je známé díky geometrické větě, která nese jeho jméno, je jedním z raných řeckých myslitelů, o nichž se ví jen málo. Zdá se, že nenapsal vůbec nic, ale byl zakladatelem myšlenkové školy, která se dotýkala všech aspektů života a která mohla být

---

[2] VANĚK, Jiří. Obecná, ekonomická a informační etika. 1. vydání. Praha: Wolters Kluwer ČR, 2010. ISBN 978-80-7357-504-5.
[3] SINGER, Peter. Moral philosophy. *Britannica* [online]. Velká británie: Encyclopædia Britannica, 2016 [cit. 2022-08-15]. Dostupné z: https://www.britannica.com/topic/ethics-philosophy

jakýmsi filozofickým a náboženským řádem. Ve starověku byla škola nejlépe známá pro svou obhajobu vegetariánství, které bylo stejně jako u džinistů spojeno s vírou, že po smrti těla se lidská duše může usadit v těle zvířete (viz. reinkarnace). Pythagorejci pokračovali v zastávání tohoto názoru po mnoho staletí a klasické pasáže v dílech spisovatelů jako Ovidius (43 př. n. l. – 17 n. l.) a Porfyrij (234–305), kteří se postavili proti krveprolití a zabíjení zvířat, lze vysledovat až k Pythagorovi.[4]

Je ironií, že důležitý podnět pro rozvoj mravní filozofie přišel od skupiny učitelů, k nimž se pozdější řečtí filozofové – Sokrates, Platón a Aristoteles – chovali důsledně nepřátelsky: sofisté. Tento termín byl používán v 5. století k označení třídy profesionálních učitelů rétoriky a argumentace. Sofisté slibovali svým žákům úspěch v politické debatě a zvýšený vliv na záležitosti města. Byli obviněni, že jsou žoldáci, kteří učí své studenty vyhrávat argumenty spravedlivými prostředky nebo faulem. Aristoteles řekl, že Prótagoras (asi 490 – asi 420 př. n. l.), snad nejslavnější ze sofistů, tvrdil, že učí, jak „učinit slabší argument silnějším“.

Sofisté však byli víc než jen učitelé rétorických triků. Považovali se za nositele kulturních a intelektuálních kvalit nezbytných pro úspěch a jejich zapojení do argumentů o praktických záležitostech je přirozeně vedlo k rozvoji názorů na etiku. Opakujícím se tématem v názorech známějších sofistů, jako byli Protagoras, Antiphon (asi 480–411 př. n. l.) a Thrasymachus (rozkvetl koncem 5. století př. n. l.), je to, co se běžně nazývá dobré a špatné nebo spravedlivé a nespravedlivé neodráží žádný objektivní fakt přírody, ale je spíše záležitostí společenské konvence. Protagoras je zjevným autorem slavného epigramu shrnujícího toto téma: „Člověk je mírou všech věcí“. Platón ho představuje slovy: „Cokoli se každému městu zdá spravedlivé a v pořádku, je spravedlivé a v pořádku pro toto město, pokud si to tak myslí. Protagoras, stejně jako Hérodotos, vyvodil ze svého etického relativismu umírněný závěr. Tvrdil, že i když se konkrétní obsah morálních pravidel může lišit, musí existovat určitá pravidla, má-li být život snesitelný. Protagoras tedy prohlásil, že základy etického systému nepotřebují nic od bohů ani od žádné zvláštní metafyzické říše mimo běžný svět smyslů.

[4] Janoš, Karel. Informační etika. Praha: Česká informační společnost, 1993

Zdá se, že Thrasymachos zvolil radikálnější přístup – pokud je Platónovo zobrazení jeho názorů historicky přesné. Vysvětlil, že pojem spravedlnost neznamená nic jiného než poslušnost zákonů společnosti, a protože tyto zákony vytváří nejsilnější politická skupina ve vlastním zájmu, spravedlnost nepředstavuje nic jiného než zájem silnějšího. Thrasymachos však pravděpodobně netvrdil, že cokoli dělají ti nejmocnější, je správné; pravděpodobněji popíral, že by rozlišení mezi správným a špatným mělo nějaký objektivní základ. Pravděpodobně by pak povzbudil své žáky, aby sledovali své vlastní zájmy, jak nejlépe dovedli. Je tedy raným představitelem morálního skepticismu a možná i etického egoismu, názoru, že správné je sledovat vlastní zájmy.

Není divu, že s myšlenkami tohoto druhu v oběhu by ostatní myslitelé měli reagovat hlouběji do etiky, aby zjistili, zda lze odolat potenciálně destruktivním závěrům některých sofistů. Tato reakce vytvořila díla, která od té doby slouží jako základní kámen celé stavby západní etiky.

1.1.2 Aplikovaná etika

Nejvýraznějším vývojem ve studiu etiky od poloviny 60. let 20. století byl růst zájmu mezi filozofy o praktickou nebo aplikovanou etiku – tedy aplikaci normativních etických teorií na praktické problémy. Nejedná se, pravda, o úplně nový odchod. Od Platóna dále se morální filozofové zabývali praktickými otázkami, včetně sebevražd, odhalení dětí, zacházení se ženami a správného chování veřejných činitelů. Křesťanští filozofové, jmenovitě Augustin a Akvinský, s velkou pečlivostí zkoumali takové záležitosti, jako kdy je válka spravedlivá, zda je někdy správné lhát a zda křesťanská žena dělá něco špatného, když spáchá sebevraždu, aby se zachránila před znásilněním. Hobbes měl při psaní svého Leviatana eminentně praktický účel a Hume psal o etice sebevraždy. Britští utilitáři se velmi zabývali praktickými problémy; skutečně považovali sociální reformu za cíl své filozofie. Bentham tedy psal o volební a vězeňské reformě a právech zvířat a Mill diskutoval o moci státu zasahovat do svobody svých občanů,

postavení žen, trestu smrti a právu jednoho státu napadnout jiný, aby tomu zabránil, z páchání zvěrstev na vlastním lidu.[5]

Nicméně během prvních šesti desetiletí 20. století morální filozofové do značné míry zanedbávali aplikovanou etiku – něco, co se nyní zdá téměř neuvěřitelné, vezmeme-li v úvahu traumatické události, kterými většina z nich prožila. Zdá se, že nejpozoruhodnější výjimka, Bertrand Russell (1872–1970), považoval své spisy o etických tématech za značně oddělené od své filozofické práce a nepokoušel se rozvíjet své etické názory nějakým systematickým nebo přísným způsobem.

V této době převládal názor, že morální filozofie je zcela oddělena od „moralizování“, což je úkol, který je lepší přenechat kazatelům. Co se obecně nezvažovalo, bylo, zda mohou morální filozofové, aniž by pouze kázali, účinně přispívat k diskusím o praktických otázkách zahrnujících obtížné etické otázky. Hodnota takové práce začala být široce uznávána až během 60. let, kdy nejprve americké hnutí za občanská práva a následně válka ve Vietnamu a růst studentského politického aktivismu začaly vtahovat filozofy do diskusí o etických otázkách rovnosti, spravedlnosti, války a občanské neposlušnosti.

Aplikovaná etika se brzy stala součástí filozofických osnov většiny univerzit v mnoha různých zemích. Zde nelze více než stručně zmínit některé z hlavních oblastí aplikované etiky a poukázat na problémy, které vyvolávají.

Rovnoprávnost (rovnost, lidská práva a spravedlnost), zvířata (etické chování i ke zvířatům – chov, testování, hlavně zásluhou publikací - Animals, Men and Morals: An Inquiry into the Maltreatment of Non-humans z roku 1972, kterou vydali Roslind a Stanley Godlovitch a John Harris, a o tři roky později následovala kniha Petera Singera Animal Liberation.), enviromentální etika, válka a mír, potrat, eutanazie a hodnota lidského života a bioetika (hlavně nový vývoj v medicíně a biologických vědách).[6]

---

[5] SINGER, Peter. Moral philosophy. Britannica [online]. Velká británie: Encyclopædia Britannica, 2016 [cit. 2022-08-15]. Dostupné z: https://www.britannica.com/topic/ethics-philosophy

[6] SINGER, Peter. Moral philosophy. *Britannica* [online]. Velká británie: Encyclopædia Britannica, 2016 [cit. 2022-08-15]. Dostupné z: https://www.britannica.com/topic/ethics-philosophy

1.2. Informace

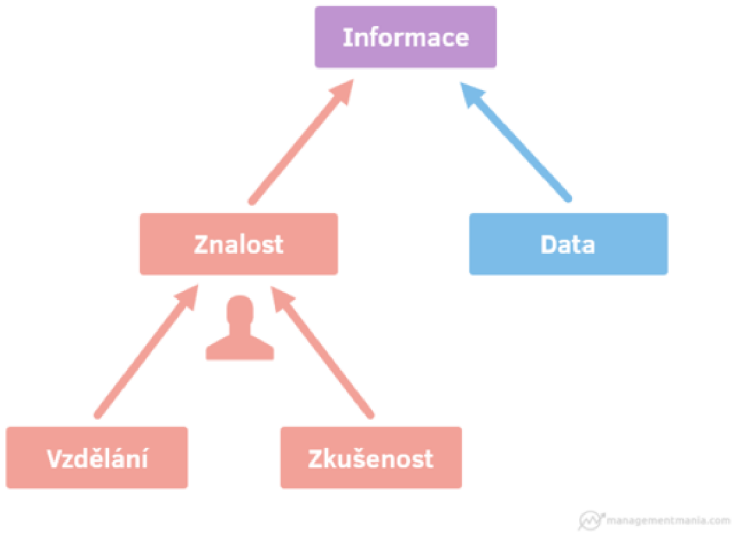
Informace rovná se data, která jsou konkrétním člověkem interpretována díky jeho znalostem. Jinými slovy co je pro jednoho člověka informace, pro jiného mohou být jen prázdná slova. Jsou to tedy relevantní údaje nebo data obsahující hodnotu, které svému adresátovi nějak pomáhá či snižuje jeho neznalost.

Slovníková definice pojmu informace je *„Sdělení snižující míru neurčitosti na straně adresáta*“. V praxi se používá slovo informace zjednodušeně i pro data. Například: *Všechny informace v naší firmě ukládáme do jednoho informačního systému.*

- informace rychle zastarávají (v čase se jejich význam nebo důležitost mění)
- v čase se může měnit i hodnota informací (cenná informace se může změnit v bezcennou a naopak)
- informace jsou relativní a subjektivní, závislé na interpretaci a situaci
- informace má nehmotný charakter, je vždy spojena s nějakým interpretem – člověkem
- hodnota informací se liší podle toho, kdo je jejich příjemcem
- informaci nelze skladovat
- informace nezávislá na formátu či médiu (přestože může být uložena)
- informace samy o sobě nejsou nositeli znalosti
- informace jsou data, kterým přiřazuje důležitost a význam jejich uživatel při interpretaci[7]

[7] Informace. *Www.managementmania.com* [online]. Praha: ManagementMania's Series of Management, 2018 [cit. 2022-01-25]. Dostupné z: https://managementmania.com/cs/informace

Grafické znázornění informace je zobrazeno v grafu číslo 1.



Graf 1 – Informace

(zdroj: https://managementmania.com/cs/informace)

1.3. Informační etika

Informační etika je obor aplikované etiky, který se zabývá využíváním a zneužíváním informací, informačních technologií a informačních systémů pro osobní, profesní a veřejné rozhodování. Je například v pořádku stahovat duševní vlastnictví někoho jiného, jako jsou obrázky nebo hudba? Měli by někdy knihovníci odstranit kontroverzní knihy z regálů nebo sledovat vyhledávání uživatelů na internetu? Měl by vědec zveřejnit genom viru Ebola na internetu?

Informační etika poskytuje rámec pro kritické úvahy o vytváření, kontrole a používání informací. Vyvolává otázky týkající se vlastnictví informací a přístupu k duševnímu vlastnictví, práv lidí číst a prozkoumávat World Wide Web, jak se rozhodnou. Informační etikové zkoumají a hodnotí vývoj morálních hodnot, vytváření nových mocenských struktur, informační mýty a řešení etických konfliktů v informační společnosti (Capurro 2001). Jestliže bioetika řeší živé systémy, pak informační etika obdobně pokrývá informační systémy. Tam, kde se bioetika vyvinula z lékařské etiky po druhé světové válce a zapojila se do širších důsledků společenských změn, jako je informovaný souhlas a reprodukční práva, informační etika vyrostla z tradic profesionální etiky knihovníků a raných

informačních profesionálů, aby popsala a vyhodnotila konkurenční zájmy, která se snažila ovládnout informační aktiva high-tech společnosti (Smith 1997). Stejně jako jiné oblasti aplikované etiky ve vědě a technice se informační etika zaměřuje na společenskou odpovědnost a význam lidskosti ve vztahu ke strojům.

Informační etika, postavená na základě kodexů a závazků profesionálních knihovníků chránit právo na čtení, bojovat proti cenzuře, chránit soukromí patronů, zajistit důvěrnost knihovních záznamů a poskytovat služby všem, rozšířila tyto tradice do kyberprostoru. Pojem informační etika se poprvé objevil v literatuře knihovnictví a informační vědy koncem 80. let (Hauptman) vedle dalších pojmů, jako je etika informačních technologií, katalogizační etika a archivní etika. V několika příštích letech se informační etika rozrostla tak, aby zahrnovala dilemata, kterým čelí knihovníci a informační profesionálové (Mason, Mason a Culnan 1995), když zaváděli nové informační a komunikační technologie (ICT) do veřejných, akademických a speciálních knihoven a také do publikací, zdravotnictví a nového informačního průmyslu.

Dnešní informační etika zahrnuje širokou škálu problémů zahrnujících tvorbu, získávání, organizaci, správu, překlad, duplikaci, ukládání, vyhledávání a jakékoli další procesy zahrnující tištěné nebo digitální texty, grafiku, hlas a video. Informační etika může řešit jakýkoli problém týkající se informační společnosti nebo znalostní ekonomiky. Jako oblast aplikované etiky čerpá z historických a filozofických vhledů (Floridi 1999) s cílem popsat současné problémy, jako je překlenutí digitální propasti a vytvoření normativních řešení pro osobní a profesionální chování a pro veřejnou politiku.[8]

1.4. Počítačová etika

Počítačová etika je proto souborem morálních zásad, které upravují používání počítačů. Mezi běžné problémy počítačové etiky patří práva duševního vlastnictví (například elektronický obsah chráněný autorskými právy), obavy o soukromí a vliv počítačů na společnost.

[8] INFORMATION ETHICS. *Encyclopedia.com* [online]. AN ELITE CAFEMEDIA PUBLISHER, 2019 [cit. 2022-08-15]. Dostupné z: https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/information-ethics

Například je snadné duplikovat elektronický (nebo digitální) obsah, počítačová etika by naznačovala, že je špatné to dělat bez souhlasu autora. Ačkoliv je možné získat přístup k osobním informacím někoho v počítačovém systému, počítačová etika by poukázala na neetičnost této akce.

Jak technologie postupuje, mají počítače stále větší dopad na společnost. Počítačová etika proto podporuje diskusi o tom, jaký velký vliv by měly mít počítače v oblastech, jako je umělá inteligence a lidská komunikace. Jak se svět počítačů vyvíjí, počítačová etika nadále vytváří etické standardy, které řeší nové problémy vyvolané novými technologiemi.[9]

1.5. Internet

Internet, architektura systému, která způsobila revoluci v komunikacích a způsobech obchodování tím, že umožnila propojení různých počítačových sítí po celém světě. Internet, někdy označovaný jako „síť sítí“, se objevil ve Spojených státech v 70. letech 20. století, ale pro širokou veřejnost se stal viditelným až na počátku 90. let. Odhaduje se, že do roku 2020 bude mít přístup k internetu přibližně 4,5 miliardy lidí, tedy více než polovina světové populace.

Internet poskytuje schopnost tak výkonnou a obecnou, že ji lze použít téměř pro jakýkoli účel, který závisí na informacích, a je přístupná každému jednotlivci, který se připojí k jedné z jeho základních sítí. Podporuje lidskou komunikaci přes sociální média, elektronickou poštu (e-mail), „chatovací místnosti“, diskusní skupiny a přenos zvuku a videa a umožňuje lidem spolupracovat na mnoha různých místech. Podporuje přístup k digitálním informacím mnoha aplikací, včetně World Wide Web. Ukázalo se, že internet je živnou půdou pro velký a rostoucí počet „elektronických podniků“ (včetně dceřiných společností tradičních „kamenných“ společností), které většinu svých prodejů a služeb provádějí přes internet.

V současnosti se objevilo to, co se nazývalo „Web 2.0“, internet s důrazem na sociální sítě a obsah vytvářený uživateli. Služby sociálních médií, jako je Facebook, Twitter a Instagram, se staly jedněmi z nejoblíbenějších internetových

[9] Počítačová etika. *Www.tech-lib.eu* [online]. Praha: Sharpened Productions, 2020 [cit. 2022-01-25]. Dostupné z: https://tech-lib.eu/definition/computerethics.html

stránek, protože uživatelům umožňovaly sdílet svůj vlastní obsah se svými přáteli a širším světem. Mobilní telefony získaly přístup k webu a s uvedením chytrých telefonů, jako je iPhone od společnosti Apple (představen v roce 2007), počet uživatelů internetu na celém světě explodoval z přibližně jedné šestiny světové populace v roce 2005 na více než polovinu v roce 2020.

Zvýšená dostupnost bezdrátového přístupu umožnila aplikace, které byly dříve neekonomické. Například globální polohovací systémy (GPS) v kombinaci s bezdrátovým přístupem k internetu pomáhají mobilním uživatelům lokalizovat alternativní trasy, generovat přesné zprávy o nehodách a spouštět záchranné služby a zlepšit řízení dopravy a kontrolu přetížení.

To, co začalo jako převážně technický a omezený vesmír designérů a uživatelů, se stalo jedním z nejdůležitějších médií konce 20. a počátku 21. století. Jak Pew Charitable Trust poznamenal v roce 2004, trvalo 46 let, než se podařilo zajistit elektřinu ve 30 procentech Spojených států; trvalo pouhých 7 let, než internet dosáhl stejné úrovně připojení k americkým domácnostem. V roce 2005 použilo internet 68 procent dospělých Američanů a 90 procent amerických teenagerů. Evropa a Asie byly propojeny přinejmenším stejně dobře jako Spojené státy. Téměř polovina občanů Evropské unie je online a ve skandinávských zemích jsou ještě vyšší. V asijských zemích jsou velké rozdíly; například v roce 2005 měly Tchaj-wan, Hongkong a Japonsko nejméně polovinu své populace online, zatímco Indie, Pákistán a Vietnam méně než 10 procent. Jižní Korea byla světovým lídrem v připojení své populace k internetu prostřednictvím vysokorychlostního širokopásmového připojení.

Takové statistiky mohou mapovat růst internetu, ale nabízejí jen málo vhledů do změn, k nimž došlo, když uživatelé – jednotlivci, skupiny, korporace a vlády – začlenili technologii do každodenního života. Internet je nyní stejně živou zkušeností jako nástrojem pro provádění konkrétních úkolů, který nabízí možnost vytvořit prostředí nebo virtuální realitu, ve které by jednotlivci mohli pracovat, společensky komunikovat s ostatními a možná i žít svůj život.

2. Související legislativa v oblasti práce s informacemi v ČR

Protože etika reprezentuje ve společnosti pouze doporučení, jak se chovat a nemá žádné zákonem dané sankce a tresty za porušení etického chování (samozřejmě ne vždy je to takhle jednoduché, v nějakých situacích je jedinec vázán povinností směrnice či vnitřního nařízení organizace), přicházejí na řadu zákony.

Právní předpisy týkající se světa počítačových sítí, zejména internetu. S rostoucím provozem na internetu roste i počet a druh právních problémů souvisejících s touto technologií. Mezi vášnivě diskutované problémy patří obscénnost některých online stránek, právo na soukromí, svoboda slova, regulace elektronického obchodování a použitelnost zákonů o autorských právech.

V této kapitole jsou uvedeny zákony, které jsou nejdůležitější pro řešenou problematiku.

2.1. Listina základních práv a svobod

V dnešní době, kdy mají informace velkou cenu, a kdy nám technologie umožňují vyhledávat informace rychleji než kdykoli dříve, je ochrana dat (zejména těch osobních), obzvláště důležitá. Shromažďování osobních údajů může být totiž snadno zneužitelné. Tuto oblast pokrývá celá řada legislativních předpisů, přičemž jedním z nejdůležitějších je *Listina základní práv a svobod*, která ukládá:

- nedotknutelnost osoby a jejího soukromí,
- ochranu lidské důstojnosti, osobní cti, dobré pověsti a jména, soukromého a rodinného života,
- ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.[10]

[10] HEMEROVÁ - HÁJKOVÁ, Kateřina. Etické principy v informační činnosti. Praha, 2004. Diplomová práce. Univerzita Karlova v Praze. Str. 47

Ochrana soukromých dat a údajů je paradoxně v konfliktu s ochranou bezpečnosti obyvatel. Vyvstává tu otázka, co je důležitější. Naše soukromí nebo bezpečnost? Řada států, ze strachu z teroristických útoků, monitoruje soukromé údaje lidí, např. v Austrálii má stát právo číst všechny e-maily australských občanů.[11] Teroristické útoky jako události z 11. září 2001 přispěly k tomu, že monitoring osob i jejich činností na internetu a přístup státu k těmto informacím je nyní běžný.

2.2. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Zákon o svobodném přístupu k informacím upravuje pravidla pro poskytování informací a rovněž upravuje podmínky práva svobodného přístupu k daným informacím. Dále jsou zde stanovena pravidla, při kterých povinné subjekty, jimiž jsou státní orgány, územní samosprávní celky a veřejné instituce, musejí poskytnout informace upínající se k jejich působnosti. V zákoně také nalezneme mimo jiné ochranu utajovaných informací a ochranu obchodního tajemství.[12]

2.3. Zákon č. 121/2000 Sb., o právu autorském

V této podkapitole si povíme něco k autorskému právu. Je to odvětví práva, které se věnuje vztahům mezi tvůrci díla a jejich uživateli. Předmětem tohoto práva je již zmíněné dílo, které může být literární nebo vědecké či umělecké. Tvůrci tudíž mohou býti spisovateli, filmaři, hudebníci nebo v současné době i programátoři. Je také nutné zmínit, že autorské právo náleží k dílu hned od momentu, co bylo stvořeno a dá se vnímat.

Zákon rovněž obsahuje výlučná práva osobnostní a výlučná práva majetková. Práva osobnostní jsou nepřevoditelná a zanikají smrtí autora, to

[11] ČINČERA, Jan. Informační etika: Sylabus k bakalářskému studiu informační vědy. 1. vyd. Brno: Masarykova universita, 2002, 81 s. ISBN 80-210-2981-1. str. 29
[12] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. [Online] [Citace: 3. listopad 2021.] Dostupné z: http://www.zakonyprolidi.cz/cs/1999-106.

znamená, že se jich osoba nemůže vzdát, patří mezi ně například právo rozhodnout o zveřejnění díla nebo právo na nedotknutelnost díla, což znamená, že autor musí dát svolení k změně nebo zásahu do díla. Na druhou stranu s majetkovými právy lze nakládat volně. To pokrývá i právo dílo užít (tzn. rozšiřování originálu nebo rozmnoženiny díla, rozmnožování, vystavování originálu, půjčování díla aj.).[13] Poskytnutím oprávnění dílo užít jiné osobě však majetkové právo autora nezaniká, autor je pouze povinen strpět užití díla jinou osobou v rozsahu stanoveném v licenční smlouvě.

2.4. Zákon č. 110/2019 Sb. o zpracování osobních údajů

Zákon o zpracování osobních údajů je zákon, který upravuje zavedení nařízení (EU) GDPR, zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelné předpisy Evropské unie a k naplnění práva každého na ochranu osobních údajů, upravuje práva a povinnosti při zpracování osobních údajů. Zpracováním je myšlena operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je uskutečňován pomocí či bez automatizovaných postupů, jako je shromáždění, zaznamenání, atd.

Tento zákon zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelné předpisy Evropské unie:

- Směrnice 2016/680[14]
- Nařízení 2016/679 (též nařízení GDPR)[15]

Struktura zákona:

- Základní ustanovení
- Zvláštní ustanovení o ochraně osobních údajů podle přímo použitelného předpisu EU

[13] Zákon č. 121/2000 Sb., o právu autorském. [Online] [Citace: 3. listopad 2021.] Dostupné z: http://www.zakonyprolidi.cz/cs/2000-121.

[14] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

[15] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

- Ochrana osobních údajů při zpracování za účelem předcházení, vyhledávání nebo odhalování trestných činů
- Ochrana osobních údajů při zajišťování obrany a bezpečnosti ČR
- Úřad pro ochranu osobních údajů
- Přestupky

3. Kodexy informační etiky

Jedná se o soubor obecných, ale i konkrétních norem a předpisů. Tento dokument vymezuje vztahy mezi členy určité komunity.

Rozlišujeme etický kodex závazný, který může zaměstnanec dostat k pracovní smlouvě k podepsání a na základě jeho porušení mu hrozí sankce nebo výpověď. Dodržování etického kodexu nezávazného je dobrovolné.

Etické kodexy a podobné dokumenty slouží ke kultivaci podnikového prostředí a podnikové kultury. Svůj etický kodex může mít jakákoliv profese, nejčastěji však slýcháme o etickém kodexu lékařů (Hippokratova přísaha), právníků a policistů.

Etický kodex neřeší nečestné chování, stanovuje však pravidla, která vymezují hranice těm, kteří se k nim dobrovolně přihlásili. Tudíž fakt, že etické kodexy nabývají své platnosti a účinnosti, ještě neznamená, že se jimi budou lidé (jednoznačně) řídit a také že budou vědět o jejich podstatě a přínosu pro společnost.[16]

3.1. Počítačový kodex

Jak bylo zmíněno výše, oblast informační etiky je neodmyslitelně propojena s národním, tak i mezinárodním právem. V této kapitole si přiblížíme počítačovou etiku. Tato pravidla formuloval Patrick Sullivan z institutu pro počítačovou etiku ve Washingtonu. Podnět daný křesťanským Desaterem je zde nepřehlédnutelný.

Desatero počítačové etiky:

1. *Počítač nevyužiješ ke škodě jiného.*
2. *Nebudeš se vměšovat do práce druhých lidí se zlým úmyslem.*
3. *Nebudeš pátrat v souborech jiných lidí se zlým úmyslem.*
4. *Nevyužiješ počítače ke krádeži.*
5. *Pro křivé svědectví nepoužiješ počítač.*
6. *Nevyužiješ kopii softwaru, za který jsi nezaplatil.*

[16] LIBOR, Marek. Informační etika a její dodržování v online prostředí. Praha, 2014. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Mgr. Ing. Tomáš Sigmund, Ph.D.

7. *Nevyužiješ bez povolení počítačový zdroj jiných lidí.*
8. *Za své nevezmeš dílo jiného.*
9. *Vezmeš v potaz společenské následky programu, který jsi stvořil.*
10. *Budeš užívat počítač ohleduplně a s úctou.*[17]

3.2. Kodex žurnalistický

Tento kodex je úplné pojmenování psaných i nepsaných norem, které lze použít v žurnalistice a měl by vytyčovat meze, jak by se měly novináři rozhodovat v každodenních etických otázkách

Tisk byl v Československu dlouhou dobu cenzurován. Před rokem 1989 mohla žurnalistika jako taková existovat pouze a jen v určité podobě, která byla politicky schválená, ale po roce 1989 se tisk konečně osvobodil a novináři začali mít v této oblasti neomezené možnosti.

Jako první Česká televize kodifikovala dne 27. září 1995 Status ČT, jehož prvkem je i kodex ČT.[18]

Roku 1998 dne 18. června Syndikát novinářů České republiky dle mezinárodních i národních dokumentů vypracoval etický kodex novináře, který zavazuje jeho členy a k jehož dobrovolnému respektování vyzval všechny české a moravské novináře bez ohledu na to, zda jsou nebo nejsou členy syndikátu.

Tento kodex má tři části:

1. Právo občanů na pravdivé, včasné a nezkreslené informace. Novináři přebírají proto plnou odpovědnost za to, že informace, které prezentují veřejnosti, jsou včasné, pravdivé, úplné a nezkreslené. Novinář je zavázán publikovat jen informace, jejichž počátek je znám, nebo v opačném případě je doplnit o všechny podrobnosti. Uznávat pravdu bez zřetele na důsledky,

[17] *TEXTOVÁ OPORA PRO E-LEARNINGOVÝ KURZ INFORMAČNÍ VÝCHOVY F*** VUT* [online]. 2007. Brno: pracovní skupina pro informační vzdělávání [cit. 2022-01-31]. Dostupné z: http://w18.fme.vutbr.cz/studium/zavprace/etika/kapitola_8_a.pdf
[18] Co je etický kodex. Www.eticky-kodex.cz [online]. Praha: worldPress, 2019 [cit. 2022-01-26]. Dostupné z: http://www.eticky-kodex.cz/co-je-eticky-kodex/

které to pro něj může mít, hledat informace, které slouží veřejnému zájmu, i přes překážky. Samozřejmě odmítat jakýkoli nátlak na uveřejnění nepravdivé/falešné, nebo jen polopravdivé informace, nepřipustit jakékoli zásahy státních orgánů, které by mohly ovlivnit pravdivost sdělení. Nepravost prostředků je při tom třeba hodnotit v souvislosti s veřejným zájmem na zveřejňování příslušné informace.

2. Požadavky na profesionalitu v nejvyšším stupni. Charakterem novinářské profese je odpovědnost k veřejnosti. Z toho důvodu základní předpoklad pro tuto činnost je vysoká profesionalita a proto je novinář povinen přijímat osobní odpovědnost za veškeré publikované materiály a snažit se vyhnout všem činnostem, které by jej mohli dostat do kompromitující situace a vést ke střetu zájmů. Novinář by také neměl využít výsad, které by vedly z jeho povolání, ke zveřejňování svých osobních postojů či výhod plynoucích z členství v Syndikátu novinářů.[19]
3. Autoritu medií v žurnalistice zvyšuje hlavně důvěryhodnost, seriózност a slušnost. Nepřesné a neověřené publikované informace nic neomlouvá. Pokud si zdroj přeje zůstat v anonymitě, je novinář povinen zachovat profesionální tajemství, i pokud by mu z toho měly vzniknout nepříjemnosti. Ctít soukromí, hlavně dětí a osob, které nemají kapacitu na to pochopit následky svých činů – výpovědí.[20] Hlavně problematika dětí a jejich pochopení světa internetu se řeší v dalších kapitolách.

3.3. Kodex sociálních sítí

Při neuváženém jednání nám mohou sociální sítě pěkně zkomplikovat život. Pokud se naopak naučíte využívat potenciál sociálních sítí naplno, mohou vám pomoci budovat obchodní příležitosti, najít životního partnera nebo načerpat nějakou inspiraci. Každá síť má svá specifika, zaměření, a i další možnosti využití.

[19] Etický kodex. Www.syndikat-novinaru.cz [online]. Praha: SYNDIKÁT NOVINÁŘŮ ČESKÉ REPUBLIKY, 2022 [cit. 2022-01-26]. Dostupné z: https://www.syndikat-novinaru.cz/o-nas/etika/eticky-kodex/
[20] Etický kodex. Www.syndikat-novinaru.cz [online]. Praha: SYNDIKÁT NOVINÁŘŮ ČESKÉ REPUBLIKY, 2022 [cit. 2022-01-26]. Dostupné z: https://www.syndikat-novinaru.cz/o-nas/etika/eticky-kodex/

Vzhledem k tomu, že když byly stanovovány etické kodexy pro práci ve veřejnoprávních médiích a schvalovány parlamentem, neboť jsou nedílnou součástí zákonného rámce, které veškeré fungování v rámci veřejné služby upravuje, ještě nebyly sociální sítě, nemohlo být pamatováno na tento aspekt novinářské práce. I proto v říjnu 2019 vydala česká televize, a to přímo ředitel divize Zpravodajství a Sport Zdeněk Šámal, tento ´interní pokyn´, podle něhož by se redaktoři a moderátoři Zpravodajství ČT měly chovat, dle Desatera pro práci novinářů České televize na sociálních sítích, doposud.

Pro kvalitní výkon novinářské profese je používání všech typů médií jednou z podmínek. Samozřejmě v tomto kontextu Česká televize chápe i současný trend sociálních médií jako důležitý prvek pro dolování informací, komunikaci s veřejností, ale také pro získávání informací o postoji jedince, ale i celé společnosti. Povzbuzuje proto aktivní přístup svých zaměstnanců k sociálním sítím, a to zejména Twitteru, Facebooku a Instagramu.

Z pohledu nestrannosti a zachování důvěry je nutné dodržovat při používání veřejných sítí určité body, které uveřejnila webová stránka www.otevrenamedia.cz a jsou to tyto:

1. *„Veškeré aktivity novinářů České televize na sociálních médiích jsou vždy veřejnými projevy. Platí pro ně proto pravidla týkající se veřejného projevu zaměstnanců České televize vyplývající z Kodexu České televize a dalších předpisů. Cokoli, co publikujeme, lajkujeme nebo sdílíme na sociálních sítích, nesmí ohrozit důvěru v naši vlastní nestrannost, ani v objektivitu, nezávislost a vyváženost vysílání České televize.*
2. *Máme na paměti, že pro veřejnost je obtížné rozlišit osobní postoje novináře prezentované na veřejné síti od oficiálního vyjádření téže osoby ve vysílání.*
3. *Cokoli, co publikujeme, včetně fotografií, nesmí ohrozit důstojnost novináře ani dobrou pověst České televize.*
4. *V diskusích reagujeme vždy s rozmyslem. Dodržujeme standardy, pravidla a zásady slušné komunikace, věcnost a úctu k faktům. Jsou nám cizí zbytečné spory nebo vulgární způsob diskuse.*

5. *Ručíme svou osobní pověstí za to, že informace námi zveřejněná je ověřená a že splňuje základní formální parametry, které bychom uplatnili i v naší novinářské práci. Při zacházení s cizími texty na sítích dodržujeme autorský zákon a pravidla pro práci se zdroji platná ve zpravodajství a publicistice České televize.*
6. *Informace, které získáme při práci, nesmíme zveřejnit na sítích dříve, než jsou publikovány ve vysílání nebo na webu České televize.*
7. *Jsme obezřetní při používání vtipu, ironie, sarkasmu nebo nadsázky. V psané komunikaci nemáme k dispozici řadu výrazových prostředků, a naše vyjádření tak nemusí být správně pochopena.*
8. *Na sítích nediskutujeme interní agendu České televize a nezneužíváme informace, které jsme získali při výkonu povolání v České televizi, a informace, které nejsou určené pro zveřejnění.*
9. *Zdržíme se čehokoli, co by mohlo být vykládáno jako podpora stanovisek politických stran a hnutí nebo obchodních zájmů firem a produktů či celebrit a podobně.*
10. *Snažíme se kultivovaně používat mateřský jazyk.“*[21]

Sociální sítě samozřejmě nevyužívají pouze novináři, jak to tedy funguje pro ostatní? Po přihlášení, například na sociální síti Facebook, je formulář, který odsouhlasíte. Je zde uvedeno, jak se v prostředí sítě chovat a na co si dát pozor. Není tu vysloveně kontrola, pouze forma hlášení, kde si sami uživatelé hodnotí, co už je na ně moc. To znamená, že když je v příspěvku například ukázáno hodně násilí či nahoty, může uživatel osobu, co tento příspěvek přidala nahlásit a pokud bude tento uživatel nahlášen vícekrát, Facebook ho smaže. Velkou nevýhodou je, že nikdo nekontroluje, zda je hlášení pravdivé či není, tudíž zde vznikají i problémy se šikanou na internetu a to takové, že jsou nahlašovány i příspěvky, které problematické nejsou, a jen někdo chce uškodit jinému uživateli.

Nicméně etický kodex sociální sítě definuje pravidla komunikace v sociálních médiích, jejichž dodržování je sice dobrovolné, ale pro úspěšné a bezproblémové užívání je považováno za závazné.

---

[21] Etické kodexy veřejnoprávních médií. *Www.otevrenamedia.cz* [online]. Praha: SeeMedia, 2022 [cit. 2022-01-26]. Dostupné z: http://otevrenamedia.cz/eticke-kodexy-verejnopravnich-medii/

Jako v reálném světě chápeme nutnost slušného chování, tak na sociálních sítích jsou na něj uživatelé snad ještě citlivější.

- Necenzurovat.
- Nelhat.
- Nebojovat s ostatními uživateli ani konkurencí.
- Nepoužívat vulgarismy.
- Chovat se podle nejlepšího vědomí a svědomí.
- Umět přiznat chybu, omluvit se a sjednat nápravu.

3.3.1. Kodex influencera

Tento kodex patří do kategorie kodexu reklamy i sociálních sítí, které jsou v současné době hodně populární, a mladší generace je používá každý den. Tento fenomén jde rychlým tempem kupředu, proto regulace či podchycení problémů je dost obtížné.

Kodex vychází z návrhu *Doporučených pravidel spolupráce zadavatele a* influencera, který vznikl v rámci samoregulačního působení SPIR v reakci na potřebu standardizace chování trhu a vyjasnění norem v oblasti mladého a rychle se rozvíjejícího influencer marketingu. Reklama bývá nedostatečně označena, někdy není označená vůbec. Ke zpřehlednění situace na trhu SPIR vytvořil *Doporučená pravidla*, jejichž cílem je kultivace trhu. Pravidla vycházejí ze Zákona o regulaci reklamy č. 40/1995 Sb.

Všechna tato protiplnění naplňují znaky placené obchodní spolupráce a zavazují dle webu www.samoregulace.cz influencera k následujícím pravidlům.

1. *„Informace o obchodní spolupráci označená (#)[22] "placenepartnerstvi" musí být vizuálně či slovně uvedena na začátku zveřejňovaného obsahu, a to jednoznačně a srozumitelně tak, aby byl každý schopen poznat, zda se jedná*

[22] použití # není nutné, řídí se zvyklostmi platformy

o placenou reklamu. Odběratelům musí být zřejmé, že sponzoring byl poskytnut výměnou za vytvoření příspěvku a propagaci značky.

2. *Influencer musí přizpůsobit formu sdělení předpokládané cílové skupině, tzn. například, je-li alespoň 25 % předpokládaného publika mladší osmnác-ti let, musí být sdělení pochopitelné i jim. Nad rámec uvedení informace o obchodní spolupráci označené (#)"placenepartnerstvi" použije autor navíc nástroje jednotlivých platforem, které umožňují označení placené spolupráce. Neznamená to ale, že mohou být použita pouze tato označení, protože ta jsou spotřebitelům málo srozumitelná a zavádějící.*
3. *Influencer nesmí o svých zkušenostech se službou či produktem lhát či je zamlčovat. Nesmí například předstírat, že si produkt sám koupil, když mu byl poskytnut firmou.*
4. *Influencer zajistí, že způsob, jakým je označena informace o obchodní spolupráci, odpovídá podmínkám platformy, na které je sdělení umístěno. V případě video platforem (např. YouTube) ponechá influencer informaci o obchodní spolupráci v obraze dostatečně dlouho, aby ji mohl každý zaznamenat, tedy přečíst.*
5. *Influencer či zadavatel vyslyší upozornění samoregulátora na případné porušování těchto pravidel a zjedná doporučenou nápravu.*
6. *Influencer a zadavatel vezmou v úvahu inzerování cílovým skupinám, jejichž předpokládané publikum tvoří z jedné čtvrtiny a více osoby mladší 18 let, nebo inzerování produktů či služeb, které jsou vyjmenovány v Zákoně o regulaci reklamy (např. reklama na tabákové výrobky, alkohol, humánní léčivé přípravky apod.). Budou se v tomto případě řídit regulací dle platných zákonů, zejména Zákona o regulaci reklamy 40/1995 Sb. Pokud influencer předpokládá, že více než čtvrtina jeho sledujících jsou mladší osmnácti let, nebude zejména inzerovat tabákové výrobky, alkohol, léky či hazardní hry apod."*[23]

[23] Kodex influencera. *Www.samoregulace.cz* [online]. Praha: SPIR z. s. p. o. [cit. 2022-01-31]. Dostupné z: https://www.samoregulace.cz/kodex-influencera

4. Negativní jevy

4.1. Dezinformace

Čínský vojevůdce a stratég Sun-c‘ je autorem dodnes často citovaného díla *Umění války.* Mezi méně často zmiňovanými pasážemi jeho díla najdeme i myšlenku dokládající význam psychologického podmanění či obelstění nepřítele: „Získat sto vítězství ve stovce bitev není znakem vynikajícího vojevůdce. Pravým znakem vynikajícího vojevůdce je podrobení si nepřítele bez boje.“ Těžko si představit, že by metody bez boje nezahrnovaly kromě diplomacie i jeho demoralizaci propagandou[24] a různými způsoby psychologické války.[25]

Přestože byli nacisté již ve 30. letech obviňováni z používání dezinformací, podstatné jméno a praxe jsou nejčastěji spojovány se sovětskou KGB. Mnoho lidí si myslí, že „dezinformace“ je doslovný překlad ruského „dezinformatsiya“, což znamená „dezinformace“, je to termín, který KGB údajně používala v 50. letech 20. století k označení oddělení vytvořeného k šíření propagandy.

Dezinformace je pojem, kterým se v poslední době začaly označovat veškeré chybné, mylné či falešné zprávy. Často je také používán jako synonymum pro pojmy fake news a hoax.

Fake news jsou zprávy, které mohou být vnímány jako zpravodajství, ale v realitě může jít například o PR článek. V překladu do českého jazyka by to mohlo doslovně znamenat falešné zpravodajství. Jako fake news můžou být označeny i celé weby, které se vydávají za korektní, ale nedosahují určených zpravodajských standardů.

[24] Pokus přimět lidi myslet a chovat se požadovaným způsobem
[25] TÁBORSKÝ, Jiří. *V síti dezinformací: Proč věříme alternativním faktům*. 1 vydání. Praha: Grada Publishing, 2020. ISBN 978-80-271-1066-4.

Hoax je falešná (chybná, lživá) zpráva, která by měla mít poplašný charakter. Nejlepší přirovnání je k úmyslnému spuštění požárního poplachu, i když se žádný požár ve skutečnosti nekoná.

Pojem dezinformace je složitější. Nejdřív si musíme slovo rozdělit na předponu dez- a slovo informace. Informace je dost široký pojem, který jsme si již v předchozích kapitolách vysvětlili, ale v tomto kontextu ho budeme vnímat jako synonymum slov fakt či údaj. Informace mohou ale mít i předpony mis- a mal-.

- Misinformace – je chybná, ale neúmyslná. Někdo vydal nepravdivý údaj, ale nešlo o úmysl. Například překlep v desetinné čárce, chybné místo či čas apod. Pokud jde skutečně o omyl, autor se omluví a informaci opraví.
- Malinformace – je pravdivá, ale je vypuštěna za účelem někoho poškodit. Může jít například o zveřejnění něčích osobních údajů nebo různých citlivých informací ze zákulisí podniku.

Dezinformace je vesměs kombinací obojího. Je chybná (jako misinformace), je úmyslná (jako malinformace) a jejím cílem je někoho poškodit a/nebo obelhat.[26]

Dezinformace jsou jedním z hlavních problémů demokratických zemí. Za fake news jsou často artikulovány strategie, které mají manipulovat veřejným míněním a narušovat stabilitu států a jejich důležitých institucí.

Hoaxy a dezinformace jsou již dlouho globální hrozbou pro svobodu a demokracii. Rozvoj a rozšiřující se používání digitálních médií umožňuje rychlé šíření kampaní, takže dezinformace se stávají čím dál palčivějším problémem. V posledních letech se tok informací i dezinformací mnohonásobně zrychlil, jak se ukázalo na sítích v souvislosti s pandemií COVID-19.

Protisměrné dezinformační kampaně jsou jako horečka nízkého stupně, která nahlodává kolektivní národní vůli, pokud nebudou zavedena silnější zmírňující opatření. Neexistuje žádná obrazná vakcína, která by poskytla ochranu v případě dezinformací. Poučení ze studia marketingu kolem teorie očkování a soubor úsilí

[26] PAMMENT, James. *RESIST - Příručka pro boj s dezinformacemi* [online]. Praha: Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra, 2020 [cit. 2021-12-19]. Dostupné z: https://gcs.civilservice.gov.uk/guidance/resist-counter-disinformation-toolkit/.

od vzdělávání po větší průmyslovou regulaci technologických společností však nabízí naději na odolnost vůči vyvíjejícím se nepřátelským informačním operacím.

Evropská rada na svém zasedání v červnu 2018 pověřila vysokou představitelku Unie pro zahraniční věci a bezpečnostní politiku a Evropskou komisi, aby do prosince 2018 ve spolupráci s členskými státy a v souladu se závěry Evropské rady z března 2015 předložily akční plán pro koordinované reakce na dezinformace. Tento akční plán byl předložen a schválen Evropskou radou ve dnech 13. a 14. prosince 2018.[27]

Facebook, Google, Twitter a další globální platformy se zavázaly důsledněji postupovat proti šíření dezinformací či propagandy. Evropská komise zveřejnila nová pravidla, na jejichž základě mají provozovatelé webů spolupracovat s ověřovateli faktů.

Zaměřovat by se měly například na falešné účty a pokročilé manipulační praktiky. Mají také odříznout strůjce cílených dezinformací od reklamních příjmů. Nový kodex dnes již podepsalo 34 firem a organizací. Vedle zmíněné trojice je mezi nimi například TikTok, Microsoft či český Seznam.[28]

Komise nyní v době ovlivněné ruskou válečnou propagandou pravidla rozšířila, aby zahrnovala například i rozmáhající se využívání automatických technik či cíleně manipulativní videa označovaná jako deepfake.[29]

4.2. Kyberšikana

Kyberšikana je formou psychické šikany. Jde o opakované násilné chování prostřednictvím moderních komunikačních technologií, především mobilního telefonu, internetu a sociálních sítí. Nejčastějším způsobem je zasílání textových

---

[27] Ministerio de Asuntos Exteriores. The fight against disinformation. *Www.exteriores.gob.es* [online]. Spain: Directorate-General for Communications, 2022, 2020 [cit. 2022-08-15]. Dostupné z: https://www.exteriores.gob.es/en/PoliticaExterior/Paginas/LaLuchaContraLaDesinformacion.aspx

[28] Ověřovatelé faktů a přísnější kontrola. Boj proti dezinformacím bude důslednější. Forbes [online]. Česko: MediaRey, SE, 2022, 16. června 2022 [cit. 2022-08-15]. Dostupné z: https://forbes.cz/overovatele-faktu-a-prisnejsi-kontrola-boj-proti-dezinformacim-bude-duslednejsi/

[29] Ověřovatelé faktů a přísnější kontrola. Boj proti dezinformacím bude důslednější. *Forbes* [online]. Česko: MediaRey, SE, 2022, 16. června 2022 [cit. 2022-08-15]. Dostupné z: https://forbes.cz/overovatele-faktu-a-prisnejsi-kontrola-boj-proti-dezinformacim-bude-duslednejsi/

zpráv, vytváření webových stránek, kde jsou oběti uráženy, „chatování“ na sociálních sítích a následné zneužívání a zveřejňování konverzací či fotek.[30]

Cílem útočníka je oběť vyvést z rovnováhy, zesměšnit ji, ponížit, snížit jí sebevědomí, zkrátka jí jakýmkoli způsobem ublížit.

Většinou je provozována záměrně a úmyslně, musíme si ale uvědomit, že tomu tak nemusí být vždy. Stačí, aby si někdo udělal z druhého legraci, dotyčný to nepochopí nebo si to vezme příliš osobně, jde-li o citlivou osobu a kyberšikana je na světě.

Kyberšikana je velmi snadno uskutečnitelnou formou šikany. Především v dnešním světě, kdy jsou děti a dospívající na internetu a sociálních sítích závislí. Píší si s kde kým, zakládají „přátelství“ s kýmkoli, kdo je o něj požádá, píší si bezprostředně o všem. A když se někdo cítí sám, na internetu okamžitě najde spoustu lidí, kteří budou ochotni si s ním psát a „kamarádit se“. Posílají si fotky (i choulostivé), ani dotyčnému nemusí hned dojít, že se v daném případě o kyberšikanu už jedná.

Nejvíce ohroženou skupinou, která by se mohla stát obětí podvodníka nebo násilníka jsou dle průzkumů děti, především pak dívky ve věku od 12 do 15 let.

4.2.1. Kyberšikana versus klasická šikana

I přesto, že se kyberšikana a klasická šikana v základu slova shodují, jsou úplně jiné. Mají jiné dopady, jiné uskutečnění.

- Anonymita - je hlavním znakem kyberšikany. U klasické šikany útočníka známe, vidíme ho, víme, o koho se jedná. Je to často spolužák ze školy či bývalý kamarád, zkrátka někdo, s kým jsme se už dostali do kontaktu. Kyberšikana je v tomto ohledu velice záhadná a zrádná, útočníka nevidíme. Používá falešná jména, fotografie, e-mailové adresy, neznámá telefonní čísla. Často se také jedná o někoho, koho ve skutečnosti dobře známe, a chce nám tímto způsobem ublížit. Ale není to podmínkou, útočníka jsme nemuseli v životě vůbec nikdy vidět. Kvůli anonymitě je těžké útočníka

[30] ROGERS, Vanessa. Kyberšikana: pracovní materiály pro učitele a žáky i studenty. Praha: Portál, 2011. ISBN 978-80-7367-984-2. (zadní strana)

odhalit. Tímto faktorem je velmi posílen, dovolí si na oběť naléhat víc než při klasické šikaně, použít drsnější metody. Díky vhodně zvolené technologii útočníka v některých případech ale není odhalení jednoduché.

- Útočník - u klasické šikany platí fakt, že útočníkem je fyzicky zdatnější jedinec, obvykle staršího věku než jeho oběti, spíše mužského pohlaví a rovněž jsou to lidé, obklopeni partou, ve které mají úspěch. U kyberšikany toto ale neplatí. Útočníkem může být kdokoli. Na věku, pohlaví a jeho síle nezáleží. Stačí jen, má-li potřebné znalosti v oblasti komunikačních technologií a ty má dnes už kdekdo. Podle výzkumů bývají kyberútočníci sami často oběťmi kyberšikany nebo jejími pozorovateli. Chtějí útok oplatit, i když to bude jen další nevinný člověk.[31]
- Místo a čas útoku - klasická šikana je předvídatelná. Většinou se odehrává ve stejný čas, například každý den po škole. Často i na stejném místě. To nám dává možnost se před útočníkem/útočníky krýt, utéct, popřípadě útok oddálit. Kyberútočník si nás ale může najít kdykoli, když se připojíme na internet, anebo, mám-li u sebe mobilní telefon. Není proto předvídatelná. Může přijít kdykoli a kdekoli. I když se zdá, že jsme v bezpečí domova, nemusí tomu tak být.
- Publikum - při šikaně, ať už je jakákoli, zvyšuje útočníkovi sebevědomí publikum. U klasické šikany, jak již bylo zmíněno, má útočník často podporu své party, od jiných lidí se mu jí většinou nedostává. Kyberšikana může mít díky velikosti internetového prostoru podporu velikou. A to ani nemusí oběť napadat opakovaně. Stačí jedno video či citlivé zprávy nahrané na internet a o další šíření a rozesílání se už postarají jiní. Ta tzv. podpora ani nemusí být podpora v pozitivním slova smyslu. Ale i když příspěvek uživatelé pošlou jen znechuceně někomu dalšímu, podílí se na šíření rovněž. Pro oběť to pak může mít fatální následky.
- Důsledky - při jakékoli šikaně jsou na oběti zanechány stopy. Klasická šikana je spojována s fyzickými dopady, modřinami, škrábanci, krví atd. Kyberšikana zanechá na oběti důsledky psychické. O to horší je člověku

[31] Co je kyberšikana?. *E-bezpečí* [online]. Praha: Pedagogická fakulta Univerzity Palackého v Olomouci [cit. 2022-01-31]. Dostupné z: https://www.e-bezpeci.cz/index.php/temat/kyberikana/17-cojekybersikana

nějak pomoci, protože to na něm často ani nepoznáme. Dotyčný se se svými problémy uzavírá, nechce o nich mluvit. Má strach, stydí se to přiznat. Často pak své problémy nezvládnou.[32]

4.3. Kybergrooming

Tento typ kyberšikany je považován za nejvíce nebezpečný. Kybergrooming je proces „spřátelení se“ s mladým člověkem online „za účelem usnadnění online sexuálního kontaktu a/nebo fyzického setkání s ním s cílem spáchat sexuální zneužití“.

Kybernetický grooming je, když se někdo (často dospělý) spřátelí s dítětem online a vybuduje si emocionální spojení s budoucími záměry sexuálního zneužívání, sexuálního vykořisťování nebo obchodování s lidmi.[33]

Hlavní cíle jsou:

- Získat důvěru dítěte
- Podplácení dárky či různými službami, budování kamarádského vztahu
- Získat od dítěte intimní a osobní údaje (často sexuální povahy – jako jsou sexuální rozhovory, obrázky nebo videa)
- Vyvolání emoční závislosti oběti na osobě útočníka
- Osobní setkání
- Sexuální obtěžování, vyhrožování, vydírání či zneužití dítěte

Pachatelé často přebírají falešnou identitu dítěte nebo dospívajícího a oslovují své oběti na webových stránkách vhodných pro děti, takže děti zůstávají

[32] Co je kyberšikana?. *E-bezpečí* [online]. Praha: Pedagogická fakulta Univerzity Palackého v Olomouci [cit. 2022-01-31]. Dostupné z: https://www.e-bezpeci.cz/index.php/temat/kyberikana/17-cojekybersikana

[33] Cyber grooming. *Www.childsafenet.org* [online]. Nepal: CENTRAL DEVELOPMENT REGIO, 2018 [cit. 2022-08-16]. Dostupné z: https://www.childsafenet.org/new-page-15

zranitelné a netuší, že je někdo oslovil se špatným úmyslem. Konverzace často začínají nenápadnými a obecnými otázkami o věku, zálibách, škole, rodině a přecházejí v otázky týkající se sexuálních zkušeností, přičemž oběti přesvědčují k výměně erotického materiálu.

Anonymita a dostupnost digitální technologie umožňuje pachatelům přistupovat k více dětem najednou, čímž se exponenciálně množí případy kybergroomingu. Průzkum z roku 2012 ve Spojeném království odhalil, že 42 procent dětí (ve věku 11–16 let) obdrželo online přílohy e-mailem od cizích lidí. Podobně v jiné studii sestávající z 264 případů groomingu bylo uvedeno: „podezřelí žádali sexuální obrázky v 93,4 procentech případů, ve 24 procentech případů bylo mladé osobě vyhrožováno distribucí existujících obrázků nebo jinou újmou; mladý člověk ve 30 procentech případů skutečně poslal sexuální obrázky; a ve 35,5 procentech případů podezřelý poslal oběti své sexuální obrázky nebo požádal mladého člověka o interakci prostřednictvím webové kamery“ (ICMEC).[34] Ostatně nemusíme koukat ani přes hranice, ale dokumentární film V síti z roku 2020 skvěle ukázal atmosféru, která panuje na internetu v České republice, výsledky nejsou vůbec dobré. Naopak, globálně existuje jen několik případů, kdy proběhlo odsouzení za trestný čin kybernetického groomingu, protože dvě třetiny zemí světa nemají žádné specifické zákony týkající se kybergroomingu u dětí.

Existují alespoň tři odlišné typy pachatelů[35]:

1. Pachatel se zkreslenou představou
2. Adaptabilní pachatel
3. Hypersexuální

Pachatel se zkreslenou představou – ten, který věří, že je v romantickém a souhlasném vztahu s mladým člověkem. Na rozdíl od toho, co si většina lidí myslí, tento konkrétní pachatel odhaluje svou totožnost oběti a nepoužívá žádné

[34] Cyber grooming. *Www.childsafenet.org* [online]. Nepal: CENTRAL DEVELOPMENT REGIO, 2018 [cit. 2022-08-16]. Dostupné z: https://www.childsafenet.org/new-page-15

[35] Cyber grooming. *Www.childsafenet.org* [online]. Nepal: CENTRAL DEVELOPMENT REGIO, 2018 [cit. 2022-08-16]. Dostupné z: https://www.childsafenet.org/new-page-15

neslušné obrázky dětí. Než se setkají tváří v tvář, tráví spoustu času spřátelením se se svou obětí.

Adaptabilní pachatel - používá mnoho identit online a přizpůsobuje svůj styl péče tak, aby vyhovoval jeho účelům. Tento pachatel může nebo nemusí používat neslušné obrázky, ale na osobu, kterou kontaktuje, bude pohlížet jako na sexuálně zralou. Není jeho cílem setkat se vždy s mladým člověkem v reálném životě.

Hypersexuální delikvent - zaměřuje se na sdílení a zabezpečení velkého množství neslušných obrázků dětí. Tento pachatel bude součástí online sítě sexuálních delikventů. Výzkumníci říkají, že tento typ pachatelů bude pravděpodobně používat různé identity, aby navázal rychlý kontakt s mladým člověkem.

4.4. Elektronická korespondence

V populární kultuře 90. let se kyberprostor jako termín bral k popisu „místa“, ve kterém lidé vzájemně komunikovali při používání internetu. Toto je místo, kde se odehrávají online hry, země chatovacích místností a domov konverzací prostřednictvím rychlých zpráv. Klasická korespondence v listové podobě pomalu ztrácí své kouzlo s neustálým rozvojem elektronické korespondence a právě tento moderní elektronický způsob komunikace je dnes hojně využíván.

Následuje představení konkrétních (vybraných) problémů v souvislosti s elektronickou korespondencí.

4.4.1. Phishing

K phishingu dochází, když útočníci posílají škodlivé e-maily, jejichž cílem je přimět lidi, aby se stali obětí podvodu. Obvykle je záměrem přimět uživatele, aby odhalili finanční informace, systémové přihlašovací údaje nebo jiná citlivá data.

Tento termín se objevil v polovině 90. let, kdy hackeři začali používat podvodné e-maily k odchytu informací od nic netušících uživatelů. Protože tito první hackeři byli často označováni jako „phreakové“, tento termín se stal známým

jako „phishing“ s „ph“. Phishingové e-maily lákají lidi dovnitř a přimějí je vzít návnadu. A jakmile se zapojí, uživatel i organizace mají potíže.[36]

V roce 2000 se útočníci obrátili na bankovní účty. Phishingové e-maily byly používány k oklamání uživatelů, aby vyzradili své přihlašovací údaje k bankovnímu účtu. E-maily obsahovaly odkaz na škodlivou stránku, která zrcadlila oficiální bankovní stránky, ale doména byla nepatrnou variací oficiálního názvu domény (např. paypai.com místo paypal.com). Později útočníci pronásledovali další účty, jako je eBay a Google, aby ukradli přihlašovací údaje, peníze, dopustili se podvodu nebo spamovali ostatní uživatele.

Phishing je příkladem sociálního inženýrství: soubor technik, které podvodní umělci používají k manipulaci s lidskou psychologií. Techniky sociálního inženýrství zahrnují padělání, nesprávné nasměrování a lhaní – to vše může hrát roli při phishingových útocích. Na základní úrovni využívají phishingové e-maily sociální inženýrství k povzbuzení uživatelů, aby jednali bez přemýšlení.

Ať už je phishingová kampaň zacílena nebo zaslána co největšímu počtu obětí, začíná škodlivou e-mailovou zprávou. Útok je maskován jako zpráva od legitimní společnosti. Čím více aspektů zprávy napodobuje skutečnou společnost, tím pravděpodobněji bude útočník úspěšný.

Cíle útočníka se liší, ale obvykle je cílem ukrást osobní údaje nebo přihlašovací údaje. Útok je usnadněn sdělením pocitu naléhavosti ve zprávě, který by mohl ohrozit pozastavení účtu, ztrátu peněz nebo ztrátu práce cílového uživatele. Uživatelé, kteří byli oklamáni požadavky útočníka, nemají čas zastavit se a přemýšlet, zda se požadavky zdají rozumné. Teprve později poznají varovné signály a nepřiměřené požadavky.[37]

Phishing se neustále vyvíjí, aby obcházel zabezpečení a detekci lidí, takže organizace musí neustále školit zaměstnance, aby poznali nejnovější strategie phishingu. Stačí pouze jedna osoba, která se stane obětí phishingu a podnítí vážné porušení zabezpečení dat. To je důvod, proč je to jedna z nejkritičtějších hrozeb ke zmírnění a nejobtížnější, protože vyžaduje lidskou obranu.

---

[36] What is phishing?. *Www.proofpoint.com* [online]. United Kingdom: Proofpoint Trust, 2021 [cit. 2022-08-16]. Dostupné z: https://www.proofpoint.com/us/threat-reference/phishing

[37] What is phishing?. *Www.proofpoint.com* [online]. United Kingdom: Proofpoint Trust, 2021 [cit. 2022-08-16]. Dostupné z: https://www.proofpoint.com/us/threat-reference/phishing

4.4.2. Spam

Spam je v českém právním řádu nazýván „nevyžádané obchodní sdělení“.[38] Spam je jakýkoli druh nechtěné, nevyžádané digitální komunikace, která se rozesílá hromadně. Spam je nejčastěji zasílán prostřednictvím e-mailu, ale může být také distribuován prostřednictvím textových zpráv, telefonních hovorů nebo sociálních médií.

První příklad nevyžádaného e-mailu pochází z roku 1978, kde se nevyžádaná zpráva objevila u 15 % uživatelů ARPANET – předchůdce internetu. Tento proto-internetový spam byl reklamou na nový model počítače od společnosti Digital Equipment Corporation. Fungovalo to – lidé kupovali počítače, avšak celková negativní zpětná vazba byla tak velká, že se tato forma marketingu vytratila.[39]

V 80. letech se lidé scházeli v regionálních online komunitách, nazývaných BBS (BBS), provozovaných fandy na jejich domovských serverech. Na typické BBS mohli uživatelé sdílet soubory, posílat oznámení a vyměňovat si zprávy. Během vášnivých online výměn uživatelé zadávali slovo „spam“ znovu a znovu, aby se navzájem „utopili“.

Spam začal vážně až s nástupem internetu a okamžité e-mailové komunikace na počátku 90. let. Spam dosáhl epidemických rozměrů se stovkami miliard spamových e-mailů, které zaplavily naše e-mailové schránky.

V případě obrany proti spamování jsou důležité dva body. Za prvé je vhodné mít více mailových schránek (pracovní, soukromý, pro online nakupování či pro přihlášení na sociální sítě a účasti v diskuzních fórech), zabrání se tím míchání spamu s důležitými například pracovními e-maily. Druhý bod je antivirová ochrana, není to obrana, na kterou se lze spolehnout na 100%, ale její účinnost je vysoká a stojí za to jí věnovat zvýšenou pozornost, stále lepší než zjistit, že nám celý počítač ochromil malware.

---

[38] VALÁŠEK, Michal. Spam a Úřad pro ochranu osobních údajů. [Online] 2011. [Citace: 3. listopad 2021.] Dostupné z: http://www.lupa.cz/clanky/spam-a-urad-pro-ochranu-osobnich-udaju/.

[39] Spam. Www.eset.com [online]. Praha: ESET, spol. s r.o. nebo ESET North America, 2021 [cit. 2022-01-25]. Dostupné z: https://www.eset.com/cz/spam/

Praktická část

5. Negativní jevy související s informační etikou

5.1. Dezinformace

Masivní rozšíření sociotechnických systémů a mikroblogovacích platforem na World Wide Web (WWW) vytváří přímou cestu od producentů ke spotřebitelům obsahu, to znamená, že umožňuje zprostředkování a mění způsob, jakým uživatelé získávají informace, debatují a vytvářejí si názory. Toto nezprostředkované prostředí může podporovat zmatek ohledně příčinných souvislostí, a tak podněcovat spekulace, fámy a nedůvěru. V roce 2011 jeden blogger tvrdil, že globální oteplování je podvod, jehož cílem je omezit svobodu a oslabit demokracii. Dezinformace o epidemii Eboly způsobily zmatek mezi zdravotníky a takových případů je v současnosti neuvěřitelné množství, vraťme se ovšem na začátek.

Jak už jsme mohli pochopit, rozvoj médií proměnil zásadním způsobem charakter společnosti i charakter vedení válek. Tato část mé diplomové práce tedy bude o světě bez hranic, který média/internet představuje a o mediální válce, která v kapitole dezinformací musí zaznít.

První tzv. mediální válkou se stala první válka v Perském zálivu, tedy ozbrojený konflikt mezi Irákem a koalicí 28 států, k němuž došlo v roce 1991 po útoku tehdejšího prezidenta Iráku Saddáma Husajna na Kuvajt. V oblasti působilo velké množství novinářů, kteří své reportáže posílali do celého světa v reálném čase. Ostatně i Saddám Husajn si moc médií uvědomoval a dovolil novinářům zůstat v bombardovaném Bagdádu, aby celý svět viděl dopady války, trosky města. Sliboval si od toho narušení soudržnosti spojenců a snížení veřejné podpory této válce.[40]

[40] TÁBORSKÝ, Jiří. V síti dezinformací: Proč věříme alternativním faktům. 1 vydání. Praha: Grada Publishing, 2020. ISBN 978-80-271-1066-4.

To se příliš nezdařilo. Západ totiž nasazoval vlastní propagandu, která byla jednoduše účinnější než úsilí Husajna. Často se promítali záběry například z kamer umístěných na hlavě tzv. chytrých bomb naváděných laserem, které s maximální přesností našly svůj cíl a zničily je víceméně bez dopadu na civilní obyvatelstvo. Tyto záběry se považují za propagandistické, protože se později ukázalo, že tyto tzv. chytré bomby představovaly jen asi osm procent zbraňových systémů použitých proti Iráčanům. Drtivá většina byly obyčejné bomby, které měly katastrofální účinky.

Samozřejmě ještě větší rozmach propagandy přinesl internet. První válkou, v níž sehrál internet větší roli, byl konflikt v Kosovu. Kosovská osvobozenecká armáda si vytvořila vlastní webové stránky a po přerušení rozhlasového vysílání šířila svůj pohled na konflikt prostřednictvím internetu. To samé dělali i Srbové, kteří kyberprostor využívali k útokům proti Severoatlantické alianci.[41]

5.1.2. Dezinformace v procentech

Tento průzkum provedla politická a sociální síť TNS ve 28 členských státech EU mezi 7. a 9. únorem 2018. Celkem bylo telefonicky ve svém mateřském jazyce dotazováno 26 576 respondentů z různých sociálních a demografických skupin. S pověřením Evropské komise - generálního ředitelství pro komunikační sítě. Použitá metodika je metodikou průzkumu Eurobarometr, který provedlo generální ředitelství pro komunikaci - monitorování médií, analýza médií a jednotka eurobarometru.[42] V následující tabulce je zobrazeno, v jakých zemích byl průzkum proveden.

[41] TÁBORSKÝ, Jiří. *V síti dezinformací: Proč věříme alternativním faktům*. Praha: Grada Publishing, 2020 [cit. 2022-08-15]. ISBN 978-80-271-1066-4.
[42] Directorate-General for Communications Networks a Content and Technology. *Fake news and disinformation online* [online]. Publications Office: European Commission, 2018 [cit. 2022-08-11]. ISBN 978-92-79-81900-1. Dostupné z: https://data.europa.eu/doi/10.2759/559993

Polsko	PL	Lotyšsko	LV
Česká republika	CZ	Lucembursko	LU
Bulharsko	BG	Itálie	IT
Dánsko	DK	Malta	MT
Německo	DE	Nizozemsko	NL
Estonsko	EE	Rakousko	AT
Řecko	EL	Belgie	BE
Španělsko	ES	Portugalsko	PT
Francie	FR	Rumunsko	RO
Chorvatsko	HR	Slovensko	SK
Irsko	IE	Slovinsko	SI
Maďarsko	HU	Finsko	FI
Kypr	CY	Švédsko	SE
Litva	LT	Spojené království	UK

Tabulka 1 – Státy
(zdroj: vlastní zpracování)

Prvním zásadním zjištěním, které je z dotazníku zřejmé, je skutečnost, že dotázaní věří více tradičním formám sdělování informací než těm „novějším“ z online světa. Většina respondentů (70%) věří informacím, které jsou sdělovány rozhlasem, další v pořadí se umístila televize (66%), tištěná media (63%) v závěsu jsou zprávy z online světa (47%) a na konci sestaveného žebříčku jsou podcasty a sociální sítě s méně než 30%. Tato čísla jsou výsledkem šetření napříč dotazovanými státy.

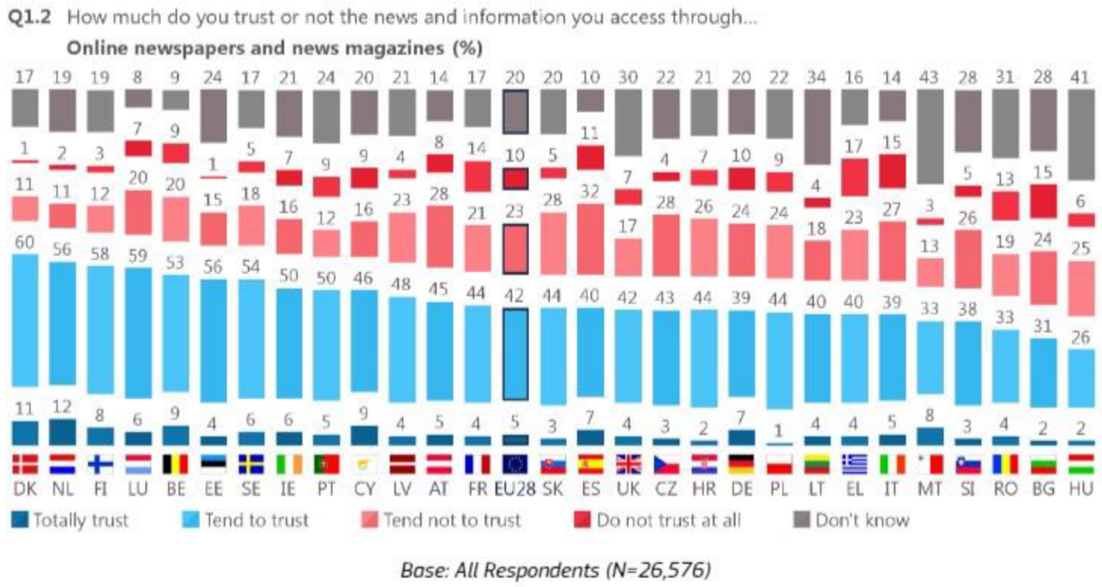
Druhým zjištěním plynoucím z dotazníku je, že většina dotázaných tvrdí, že se s tzv. fake news setkávají minimálně jednou týdně.

Více než třetina respondentů (37%) uvádí, že se s falešnými zprávami setkává každý den nebo téměř každý den, a dalších 31% uvádí, že se tak děje alespoň jednou týdně.

Sedm z deseti respondentů (71%) je zcela nebo do určité míry přesvědčeno, že jsou schopni identifikovat zprávy nebo informace, které zkreslují realitu nebo jsou nepravdivé, zatímco 26% si není jistých.

Posledním důležitým zjištěním, které vyplývá z tohoto výzkumu, je informace, že většina respondentů si myslí, že existence fake news je problémem pro jejich stát a pro demokracii – zhruba 85%. V každém dotazovaném státě je to minimálně 70%.[43]

Pro zajímavost uvádím ještě graf 2, který detailně rozepisuje, jakou důvěru mají dotazovaní v konkrétní zemi, v online zprávy. Jak si můžeme všimnout, nejlépe je na tom Dánsko a nejhůře Maďarsko. Česká republika je v druhé polovině spektra.



Graf 2 – Online média

(zdroj: https://data.europa.eu/doi/10.2759/559993)

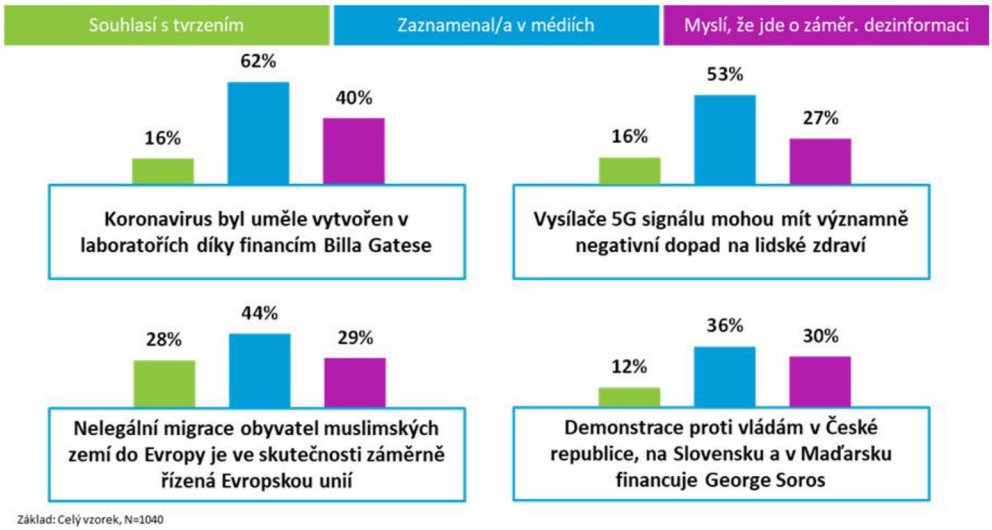
Graf číslo 3 znázorňuje, jak dotazovaní respondenti věří čtyřem rozšířeným konspiračním teoriím. „*Na základě úspěšnosti těchto 4 konspiračních příběhů lze odhadnout, že v české internetové veřejnosti existuje jádro přibližně 12–16 % lidí, kteří takovýmto dezinformacím a konspiracím věří. Mezi nimi převažují především příslušníci starší generace, lidé z menších a středních měst a lidé s nižšími příjmy,*“ komentuje výsledky Josef Šlerka z NFNZ[44]. Dle dotazníku se v české

[43] Directorate-General for Communications Networks a Content and Technology. *Fake news and disinformation online* [online]. Publications Office: European Commission, 2018 [cit. 2022-08-11]. ISBN 978-92-79-81900-1. Dostupné z: https://data.europa.eu/doi/10.2759/559993

[44] Nadační fond nezávislé žurnalistiky

společnosti nejvíce rozšířila informace, že „koronavir byl uměle vytvořený v laboratořích díky financím Billa Gatese“.

Analýza dat byla uskutečněna na vzorku 1 040 respondentů internetové populace 15+, v roce 2020.[45]



Zdroj: NFNZ / Nielsen Admosphere, N=1040, internetová populace ČR 15+, ČNP, říjen-listopad 2020

Graf 3 – Konspirační teorie

(zdroj: https://simar.cz/cerstve-namleto/cesi-a-dezinformace.html)

5.1.3. Případ v České republice související s dezinformacemi

Dříve novinářka Jana Peterková, která se blíže seznámila s miliardářem Tomášem Pitrem a kvůli tomuto vztahu skončila před soudem, který ji ale v roce 2011 zprostil obžaloby, bude ústřední postavou reálného příběhu spojeným s dezinformacemi. Paní Peterková se poslední době “proslavila” zejména jako politická aktivistka.

Byla to ona, kdo pořádal demonstrace proti vládním opatřením. Odmítá očkování proti coronaviru, šíří často už vyvrácené lži. Pro svoji činnost využívá sociální sítě, má svůj facebookový profil a na něm živě vysílá, má cca 14 000

[45] Češi a dezinformace. *Simar - Sdružení agentur pro výzkum trhu a veřejného mínění* [online]. Praha: SIMAR, 2020 [cit. 2022-01-31]. Dostupné z: https://simar.cz/cerstve-namleto/cesi-a-dezinformace.html

sledujících. Často své sledující zve a bere také s sebou na protivládní demonstrace. Dopad její činnosti je relativně značný. Začátkem února roku 2021 se celá kauza začala řešit veřejně, nepodložené informace se dostávaly i do klasických médií, mezi nimi byl dokonce Český Rozhlas.

Byl 29. leden 2021, kdy paní Peterková zrovna živě natáčela další demonstraci před Úřadem vlády. Paní Václava Vondráčková vstoupila do živého vysílání a začala paní Peterkové tvrdit, že pomáhá v pečovatelském domě v Měšicích. Povídala, že se tam očkovali senioři a ti senioři po očkování vakcínou proti coronaviru zemřeli. Jana Peterková jí v tomto živém vysílání věnovala několik minut času a poté se dále zabývala demonstrací. Ale ještě se stihli v probíhajícím živém vysílání domluvit, že se po ukončení demonstrace sejdou a popovídají si více o tomto závažném tvrzení.

Paní Václava Vondráčková a Jana Peterková informaci zveřejnily, přestože žádné očkování v pečovatelském domě neprobíhalo. Vakcína se tam totiž ještě vůbec nedostala a s určitostí v předchozích, či v tu dobu současném měsíci, nikdo v pečovatelském domě nezemřel.

Pečovatelský dům v Měšicích podal žalobu. „*České právo nezná pojem dezinformace,*“ uvedl právník pečovatelského domu Robert Falbr, „ *proto žaloba byla podána na šíření nepravdivých a dehonestujících informací. Je možné podat žalobu na ochranu dobré pověsti, když se jedná o společnost, o firmu, anebo na ochranu osobnosti, pokud se jedná o konkrétní osobu.“*[46]

Soud proběhl 13. ledna roku 2022, u soudu nebyla Jana Peterková přítomna, neměla ani svého právního zástupce. Soud jednoznačně rozhodl o tom, že šířila dezinformace a určil také trest. Jana Peterková musí stáhnout ze svého facebookového profilu veškerá videa, která se týkají této kauzy. Musí se veřejně omluvit a navíc musí zaplatit pečovatelskému domu pokutu ve výši 250.000 korun.[47]

---

[46] MAGDOŇOVÁ, Jana. První rozsudek za dezinformace o covidu. IRozhlas [online]. Praha: Český rozhlas [cit. 2022-01-31]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/podcast-vinohradska-12-koronavirus-dezinformace-soud-trest-jana-peterkova_2201180600_miz

[47] MAGDOŇOVÁ, Jana. První rozsudek za dezinformace o covidu. *IRozhlas* [online]. Praha: Český rozhlas [cit. 2022-01-31]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/podcast-vinohradska-12-koronavirus-dezinformace-soud-trest-jana-peterkova_2201180600_miz

5.1.4. Návrhy a řešení

V této podkapitole bych se ráda věnovala tomu, jak se vlastně dezinformacím můžeme bránit, jaké jsou možnosti a jejich výhody a nevýhody. V první řadě zmíním, že je, dle mého názoru, zásadní posílit nejen preventivní, ale i represivní stránku v rámci této problematiky. S návrhem nové legislativy přišlo ministerstvo vnitra v tomto roce (2022), měla by mimo jiné umožnit v krajním případě blokaci určitých webů.

O návrhu legislativních opatření byla česká veřejnost informovaná v červnu tohoto roku a měla by podle mých informací proběhnout široká diskuze mezi odbornou veřejností na téma dezinformace a jak jim zabránit či je alespoň maximálně omezit. Krajním řešením, které by v tomto návrhu mělo být, je i již zmíněná blokace určitých zdrojů. Ministr vnitra Vít Rakušan se vyjádřil takto „„*Musela by to být jasně doložená fakta, že se jedná nejen o nějaký názor nebo lež, ale i o strategicky nebezpečnou informaci. Což musí potvrdit orgány, které se věnují bezpečnosti České republiky,"*[48]. Návrh je zatím v plenkách a povedou se ještě pravděpodobně dlouhé debaty na toto téma. Určitou výhodou by bez pochyby bylo, že společensky závažné dezinformace by mohly vymizet či by mohl být zřejmý jejich úbytek i z toho důvodu, že by původci měli větší obavy přijít vůbec s něčím takovým na „trh". Na druhou stranu je zde jasný i opačný problém a to je cenzura, jak i zdůraznila vládní opozice. Kdo by kontroloval pravdivost a zdroje? Kde by byla hranice, že tato informace je strategicky nebezpečná? Jak jsem uvedla v ukázkovém případu v předchozí kapitole, může se jednat o jedno živé vysílání na sociální síti, nikomu kvůli tomu nejde přímo o život a stejně tato zpráva mohla ovlivnit stovky ne-li tisíce životů a to tak, že na základě zhlédnutí rozhovoru, občané změnili názor na vakcinaci proti Covid-19, přestože se jasně následně prokázalo, že to byla lež.

Vzhledem k tomu, že situace na českém internetu je z hlediska dezinformačních kampaní už dlouhou dobu nedostatečně řešená, vznikají i různá

[48] Vnitro chce omezit dezinformace. Připravilo návrh zákona. *Www.ceskatelevize.cz* [online]. Praha: Česká televize, 1996–2022 [cit. 2022-08-24]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3499030-vnitro-chce-omezit-dezinformace-pripravilo-navrh-zakona

občanská uskupení a hnutí. Jedná se o občany, kterým není tato situace lhostejná, bojovníci proti cizím dezinformačním kampaním na českém internetu. Jednou z těchto skupin jsou i Čeští elfové. Možná jste o nich ještě neslyšeli, ale tahle skupina samozvaných strážců českého internetu stále roste. Obyčejní lidé se k této skupině mohou dobrovolně přidat a po svém zaměstnání nebo studijních povinnostech přijít domů a vyhledávat dezinformace, k tomu ještě z pochopitelných důvodů anonymně. Zformovali se kolem roku 2018 po vzoru ostatních států, kde už takové skupiny fungovali a také si říkali „elfové". Náplní jejich činnosti je tedy monitoring a rozbor cizích dezinformačních kampaní a následné sledování, jak se tyto informace šíří prostřednictvím webů, e-mailů či sociálních sítí. Informace poté dávají na svůj web, kde se může každý kdo má pochybnosti ujistit, zda je např. poplašná zpráva pravdivá. Je sympatické, že se o to tito lidé dobrovolně snaží a mnohdy zabraňují, ze své vlastní iniciativy a bez jakéhokoliv prospěchu, zveřejňování lží. Říkají, že jsou tam, kam zákon zatím nedosáhne, proto vyvracejí lživé informace, kterým důvěřivý a zranitelní občané můžou uvěřit. Bohužel se o nich zatím moc neví, nejsou veřejně známí, což jsem si i sama osobně ověřila mezi známými a sousedy, ani moje rodina nevěděla, že taková platforma na internetu docela úspěšně funguje. Tudíž mohu tvrdit, že se jejich informace zatím k „obyčejným" lidem ve velkém měřítku nedostávají. V rámci prevence by dle mého názoru mohli pomoci osvětové preventivní kampaně, např. prostřednictvím činnosti neziskových organizací.

Cenzura, odvěké téma. Ano či ne? Je cenzura v menším měřítku omezení práva na svobodné vyjadřování nebo je to jediná cesta jak bezpečně fungovat? Na tyto otázky není snadné odpovědět, v neposlední řadě proto, že jednou z otázek je, kdo a jak by cenzuru informací prováděl. Globální povaha a dosah internetu představují potíže při kontrole obsahu. Některé země již cenzurují části internetu, blokují webové stránky a v době nepokojů vypínají služby sociálních médií, jako je Twitter. Dle mého názoru internet může být cenzurován takovým způsobem, že zůstane dobrým zdrojem informací a živým společenským prostorem a zároveň ochrání ty, kteří jsou nejvíce ohroženi internetovým vykořisťováním. V reálném světě jsme si také našli cestu, jak fungovat s určitou cenzurou, s určitými pravidly chování, s určitou legislativou, která nás také ve spoustě případů omezuje, ať už si to připouštíme nebo ne a to i v demokratické

společnosti, tak proč by takto nemohl fungovat i kyberprostor? V reálném světě, také člověk nemůže jít na Václavské náměstí a prodávat dětskou pornografii, zvolávat nacistická hesla či nabízet za pár korun knihy či filmy někoho jiného. Nejde, protože by za to byl sankcionován či jinak potrestán. Je mi jasné, že nastává mnoho otázek, ale vše se dá postupně realizovat. Mohl by se upravit způsob, jakým lidé mohou vstupovat do virtuálního prostředí, označují příspěvky/weby/zdroje, které nesou něco „alarmujícího" či společensky závažného. Mohla by být systémově upravována zejména činnost policejních orgánů, vytvářena specializovaná pracoviště na všech jejích úrovních. Napadá mě, že mladí lidé, kteří jsou nabíráni k policii, několik let tzv. „šlapou chodník", to znamená, že jsou nasazováni k pochůzkové nebo pořádkové službě, přitom jejich znalosti a dovednosti ve virtuálním prostředí mohou být mnohonásobně větší, oproti jejich starším kolegům, kteří se věnují bezpečnostním otázkám v internetovém prostředí. Zároveň by mohl fungovat státní orgán na způsob činnosti ombudsmana, pro občany, kteří potřebují radu, zastání, či byly nějakým způsobem v kyberprostoru postiženi a nevědí, jak se bránit. Samozřejmě všechny tyto způsoby ochrany jsou složité na funkčnost a nejen finančně nákladné, dle mého názoru je však nejvyšší čas tuto problematiku ve větším měřítku řešit. Internet je ve společnosti obrovskou rychle se rozvíjející platformou s nepředstavitelnými možnostmi a právě proto nemůže zůstat zcela nehlídán a nekontrolován.

Na závěr této kapitoly bych chtěla uvést, že samozřejmě i teď jsou určité možnosti, jak dezinformace rozpoznat a bránit se před nimi, bohužel ale nemáme šanci před nimi utéct a jejich počet má vzrůstající tendenci. Na selský rozum se v této problematice spoléhat nedá. Existují skupiny či weby, které se snaží o změnu, ale bohužel v záplavě informací či dezinformací je to dle mého názoru zatím jenom kapka v moři.

5.2. Kyberšikana a kybergrooming

5.2.1. Kyberšikana

5.2.1.1. Kyberšikana v procentech

Zatímco se školy, vlády a nezávislé organizace pokoušejí zvýšit povědomí o kyberšikaně a online stalkingu – statistiky kyberšikany v prováděném dotazníkovém šetření ukazují, že problém v dohledné době nezmizí. Ve skutečnosti nedávné studie odhalily, že během pandemie Covid-19 se hrozba dokonce zvýšila.

Níže jsou uvedeny výsledky mezinárodního průzkumu Ipsos, respondenty byli dospělé osoby ve 28 zemích světa. Odhaluje, že stále větší počet rodičů uvádí, že jejich děti zažily nějakou formu kyberšikany.[49]

V období od 23. března do 6. dubna 2018 bylo provedeno celkem 20 793 rozhovorů mezi dospělými ve věku 18-64 let v USA a Kanadě a dospělými ve věku 16-64 v ostatních zemích.

Zvláště zajímavé výsledky uvádí Rusko a Japonsko. V obou zemích rodiče vyjádřili extrémně vysokou míru důvěry, že jejich děti nikdy nezažily žádnou kyberšikanu.

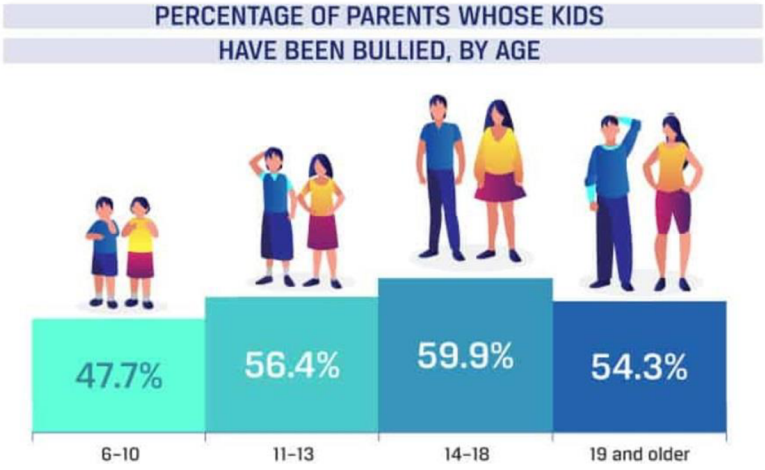
Indičtí rodiče patří mezi ty, jež v nejvyšší míře vyjádřily důvěru svým dětem názorem, že jejich děti byly alespoň někdy obětí kyberšikany, vzrůst je zaznamenán od roku 2011 do roku 2018. V Evropě a Americe se také zdá, že si více rodičů uvědomuje negativní zkušenosti svých dětí s kyberšikanou nebo jejich děti stále častěji zažívají podobné útoky online.

V obrázku 1 můžeme vidět porovnání:

- 47,7 % rodičů s dětmi ve věku 6-10 let uvedlo, že jejich děti byly šikanovány

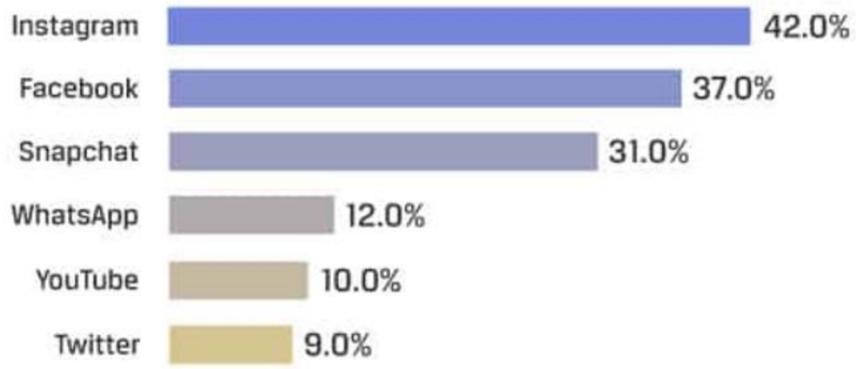
[49] BISCHOFF, PAUL. Almost 60 percent of parents with children aged 14 to 18 reported them being bullied. *Comparitech* [online]. united kingdom: Comparitech Limited, 2019, 8. května, 2019 [cit. 2022-08-11]. Dostupné z: https://www.comparitech.com/blog/vpn-privacy/boundless-bullies/

- 56,4 % rodičů s dětmi ve věku 11-13 let uvedlo, že jejich děti byly šikanovány
- 59,9 % rodičů s dětmi ve věku 14-18 let uvedlo, že jejich děti byly šikanovány
- 54,3 % rodičů s dětmi ve věku 19 let a více uvedlo, že jejich děti byly šikanovány



Obrázek 1 – Kyberšikana
(zdroj: https://www.comparitech.com/blog/vpn-privacy/boundless-bullies/)

Téměř 83 procent rodičů v průzkumu uvedlo, že k šikaně došlo ve škole a 32 procent uvedlo, že k šikaně došlo v autobuse. Zatímco většina šikany se vyskytovala na fyzických místech, k šikaně na digitálních platformách docházelo v širší škále. Devatenáct procent šikany bylo prostřednictvím sociálních sítí (v grafu číslo 4 můžeme vidět, na jakých platformách skutečně nejvíce dochází ke kyberšikaně) a 11 procent prostřednictvím zasílání textových zpráv.



Graf 4 – Rozdělení sociálních sítí
(zdroj: https://www.comparitech.com/blog/vpn-privacy/boundless-bullies/)

Online videohry, internetové stránky, jiná než sociální média, telefonní hovory a e-maily jsou samozřejmě také využívány k šikaně. Zrádnost digitálního světa spočívá v tom, že člověk ani nemusí mít žádný účet na sociálních sítích, aby se stal obětí kyberšikany.

Téměř 66 procent rodičů si myslí, že školy by měly vést děti k odpovědnosti za kyberšikanu i mimo školní areál – a jejich přání je podpořeno výzkumem. Studie ukázaly, že kyberšikana obvykle není úplně mimo školní areál, přičemž sociální média a internetové obtěžování jsou často indikátorem šikany i ve škole. I když škola neudělá nic, aby zasáhla, 35 procent rodičů uvedlo, že informovali školu o incidentu s kyberšikanou.[50]

5.2.1.2 *Případ v České republice související s kyberšikanou*

Pan Jaroslav Pulpán je hlavním aktérem v případu v České republice, který souvisí s kyberšikanou. Pulpán se vydával za vrstevnici neznámých dívek, které oslovoval přes skype nebo messenger. Poté, co z nich vymámil nahé fotografie, je nutil vydíráním k sexuálním praktikám před webkamerou.

Tento mladý pán obtěžoval a zneužíval dívky od roku 2012 do roku 2015. Vytvořil si smyšlené profily na sociálních sítích a chatoval v již zmíněných aplikacích, kde navazoval kontakty zejména s dívkami mezi 10 a 12 lety. Některé

[50] BISCHOFF, PAUL. Almost 60 percent of parents with children aged 14 to 18 reported them being bullied. Comparitech [online]. united kingdom: Comparitech Limited, 2019, 8. května, 2019 [cit. 2022-08-11]. Dostupné z: https://www.comparitech.com/blog/vpn-privacy/boundless-bullies/

dívky na jeho přání masturbovaly nebo močily, když jim začal hrozit zveřejněním jejich erotických snímků, které na nich vymámil. Jeho nejmladší oběti bylo sedm let.

Pulpán trpí podle znalců osobnostní poruchou a je zcela nevyzrálý a závislý na internetové erotice, avšak u mladíka nezjistili žádnou deviaci. V době skutků měl kvůli své nevyzrálosti prý podstatně snížené ovládací schopnosti. Kontakt s velmi mladými dívkami zvolil podle expertů proto, že se mu s nimi snáze komunikovalo.

Dvaadvacetiletý Jaroslav Pulpán sexuálně útočil přes internet na více než 160 převážně nezletilých dívek a byl za to pravomocně odsouzen pražským vrchním soudem na 6,5 roku vězení.

Rozsudek uznal Pulpána vinným z celé řady trestných činů, konkrétně ze sexuálního nátlaku, z vydírání, šíření pornografie, výroby dětské pornografie, zneužití dítěte k výrobě pornografie a z ohrožování výchovy dítěte.[51]

5.2.2. Kybergrooming

5.2.2.1. *Případ v České republice související s kybergroomingem*

Pavel Hovorka, vrátný v pražských tiskárnách, byl v roce 2008 odsouzen za pohlavní zneužívání, vydírání, svádění k pohlavnímu styku a ohrožování mravní výchovy dítěte. Byl odsouzen na 6,5 roku odnětí svobody (původní trest 8 let mu byl zmírněn u odvolacího soudu). Tento případ patří k nejtragičtějším mediálně známým případům kybergroomingu.

Hovorka se podle rozsudku dopustil v sedmi případech pohlavního zneužívání, šestnáctkrát ohrozil mravní výchovu mládeže, ve 13 případech chlapce vydíral a několikrát nezletilé sváděl k pohlavnímu styku. Hovorka vinu odmítá. Celkem podle žalobců zneužil 20 chlapců, jeden z nich dokonce utrpěl

[51] Jaroslav Pulpán. Česká televize [online]. Praha: Česká televize [cit. 2022-01-31]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/2606459-na-internetu-sexualne-obtezoval-160-prevazne-nezletilych-divek-ve-vezeni-stravi-65

těžkou újmu na zdraví. Všichni chlapci Hovorku usvědčili, soud měl navíc k dispozici jejich nahé fotografie a e-maily, kterými Hovorka disponoval.

Soudkyně upozornila, že selhaly veškeré mechanismy půjčování dětí z dětského domova. V jednom případě si odtud Hovorka půjčil desetiletého chlapce, aniž by si vedení domova ověřilo, kde muž vůbec bydlí, trvalé bydliště má totiž Hovorka hlášené na městském úřadě a žil na vrátnici. „*Pan Hovorka se s námi kontaktoval, měl s námi určité společné projekty, navštěvoval děti. Nebyl víceméně důvod, proč nepustit chlapce do Prahy*.“ uvedla ředitelka Dětského domova v Uherském Ostrohu Jana Frühaufová.[52]

Soud vrátného Hovorku uznal vinným, že od roku 2005 do svého zatčení v roce 2007 zneužil dvě desítky nezletilých chlapců, které si vybíral z řad dětí z dětských domovů anebo je kontaktoval přes internetové seznamky (zejména na serveru Lide.cz), s některými také chatoval. Oběti lákal na fiktivní soutěž „Dítě VIP“, v rámci které vítězům sliboval, že stráví dva týdny v Praze a získají zajímavé soutěžní ceny.

Řadu obětí, které dorazily na osobní schůzku, přiměl k pohlavnímu styku. Za pohlavní styk dětem nabízel peníze, některé také vydíral. Zneužité chlapce si fotografoval a natáčel videokamerou. Chlapcům pak hrozil, že vyzradí jejich homosexuální orientaci a zveřejní jejich nahé fotografie (některé mu za úplatu posílali, některé pořídil sám), pokud jej nebudou dále navštěvovat. Někteří se bránili, a tak je podle obžaloby znásilnil.[53]

5.2.3. Návrhy a řešení

Vzhledem k tomu, že kyberšikana a kybergrooming spadají do stejné kategorie, budu se zabývat těmito problémy dohromady. Ráda bych se zaměřila hlavně na vzdělávání dětí, ale také dospělých a také na generační propast, která je v současné internetové době veliká.

---

[52] Pavel Hovorka. *Česká televize* [online]. Praha: Česká televize [cit. 2022-01-31]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/1422179-soud-poslal-muze-za-zneuzivani-chlapcu-na-osm-let-do-vezeni

[53] Pavel Hovorka. E-bezpečí [online]. Praha: Pedagogická fakulta Univerzity Palackého v Olomouci [cit. 2022-01-31]. Dostupné z: https://www.e-bezpeci.cz/index.php/temat/kyberikana/pavel-hovorka

Jak už jsem v této práci zmínila a ještě s určitostí zmíním, obrovským problémem je vzdělávání, ať už mladých nebo starších lidí. Internet je s námi už několik desetiletí a kupodivu se ve školních osnovách ve velkém nauka o tomto fenoménu neobjevuje. Vyučuje se sice na základních i středních školách předmět informatika, ten se však věnuje tvoření v aplikacích word či excel nebo se žáci učí sami vytvořit web, ale není tu dostatečně kladen důraz na etickou/informační část internetu. Jinak řečeno na mediální výchovu, která by měla rozvíjet u dětí kritické myšlení. Je formálně zavedena v rámcových vzdělávacích programech, ale pouze jako doplněk k dalším předmětům, ne jako samostatný celek pro výuku, což je určitě velkou nevýhodou. Žáci se učí nejstarší historii, o tom, co se stalo v Babylonu (což samozřejmě není špatně), ale neví, jak si mohou ověřit informace například v současném zpravodajství. Netuší, jak nakládat s jejich osobními citlivými informacemi a jak se bránit v případě, že už takovou chybu udělali.

S touto problematikou určitě souvisí i vzdělávání rodičů. Hodně se mluví o tom, že rodiče by měly kontrolovat, co dítě dělá na sociálních sítích a existují i možnosti, jak dětem určité stránky zablokovat, bohužel ale rodiče i se snahou něco takového dělat neví, jak to udělat, neví co je aktuálně tzv. IN, kde a co všechno je ke kontrole třeba. Zde bych ráda zmínila internetovou stránku www.e-bezpeci.cz, kde se tyto informace člověk dozví, ale jak jsem si opět ověřila na svém okolí, málokdo tuto stránku zná a navštěvuje. Je možné se vzdělávat v případě zájmu bezplatně či formou kurzu, který je sice placený, ale cena je nízká. Moc se mi líbí, že je zde možnost zakoupit kurz třeba pro více rodičů najednou. Dejme tomu, že by škola na třídních schůzkách nabízela rodičům tuto variantu a zprostředkovala tak tuto službu pro všechny za ještě výhodnější cenu. Bohužel dle mých informací, toto moc neprobíhá a přijde mi to jako velká škoda. Mohli by pomoci letáky či články v klasických novinách, aby o této možnosti věděli i starší rodiče, kteří na počítači třeba moc neumí.

Ráda bych ještě zmínila, že ani učitelé to nemají jednoduché. Vrátila bych se k odstavci, kde mluvím o zavedení mediální výchovy do školních osnov. Z mnou prováděného šetření není velké procento pedagogů proškoleno, aby takovou výuku mohli provádět. Nemluvě o tom, že pokud se na ně děti obrátí, sami nevědí, co a jak. To je dle mého názoru velké pochybení státu a státních organizací, protože znova se vracíme k tomu, jak velkou část našich životů

vedeme online a nikdo, ani lidé, kteří mají velký vliv na děti, jsou s nimi podstatnou část dne, neví, jak zacházet s online informacemi, co aktuálně děti na internetu provádí. Od mé sestřenice vím, že se v současné době děti baví tím, že si zalepují na noc ústa lepicí páskou a sdělují si on-line jaké to je.

5.3. Elektronická korespondence

5.3.1 Phishing

Útočníci se živí strachem a pocitem naléhavosti. Je běžné, že útočníci uživatelům sdělují, že jejich účet je omezen nebo bude pozastaven, pokud na e-mail neodpoví. Strach nutí uživatele ignorovat běžné varovné signály a zapomínat na své phishingové vzdělání. Dokonce i administrátoři a bezpečnostní experti občas podlehnou phishingu.

Obvykle se phishingový e-mail posílá co největšímu počtu lidí, takže pozdrav je obecný. Následující příklad ukazuje běžný příklad phishingového e-mailu.

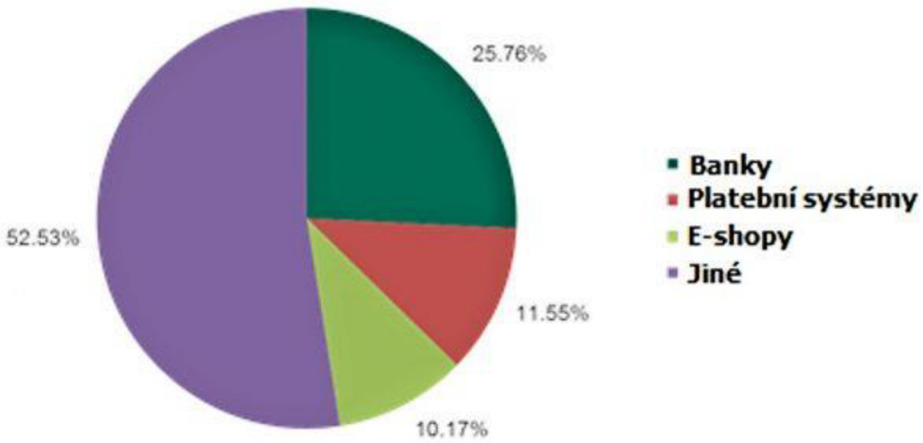
Obrázek 2 – Phishing

(zdroj: https://www.idnes.cz/zpravy/domaci/intenre-hackeri-kyberkriminalita-e-maily-phishing-podvody.A190531_151308_domaci_onkr)

5.3.1.1. Phishing v procentech

Dle internetové stránky www.proofpoint.com bylo v roce 2020 nahlášeno 241 324 případů, to je o 110% více než v roce 2019, kdy bylo nahlášeno „pouze“ 114 702 incidentů. Dále je uvedeno, že 96% útoků je vedeno přes e-mailovou adresu.[54]

V grafu číslo 5 vidíme rozložení finančního phishingu z roku 2016. Nejvíce tohoto podvodného jednání vidíme pod záštitou banky.



Rozložení finančního phishingu v roce 2016

Graf 5 – Phishing
(zdroj: https://ictrevue.hn.cz/c3-65637740-0ICT00_d-65637740-temer-50-phishingovych-utoku-cililo-v-lonskem-roce-na-finance)

5.3.1.2. Případ v České republice související s Phishingem

Případ, který v této kapitole uvádím, se stal v České republice v roce 2016. Jedná se o malware Nemucod, který se dříve šířil skrze infikované přílohy e-mailových zpráv. Ty byly označeny jako nezaplacená faktura nebo předvolání k soudu. No kdo z nás by takový e-mail neotevřel, že? Pokud se uživatel nachytal a otevřel infikovanou zprávu, pak se do počítače instaloval již zmíněný Nemucod,

[54] What is phishing?. Www.proofpoint.com [online]. United Kingdom: Proofpoint Trust, 2021 [cit. 2022-08-16]. Dostupné z: https://www.proofpoint.com/us/threat-reference/phishing

který umožňoval útočníkovi na infikované počítače posílat další škodlivé kódy. V případě Nemucodu šlo o ransomware[55]. Došlo tedy k zašifrování dat na počítači a požadavku na výpalné.[56]

5.3.2. Spam

Kontrola e-mailu v poslední době je jako vejít do obřího nákupního centra, kde všichni chtějí, abyste si koupili jejich produkty, najali jejich služby nebo si vzali nigerijského prince. Tisíce a tisíce e-mailů, všechny pod společným jmenovatelem. Spam.

5.3.2.1. Spam v procentech

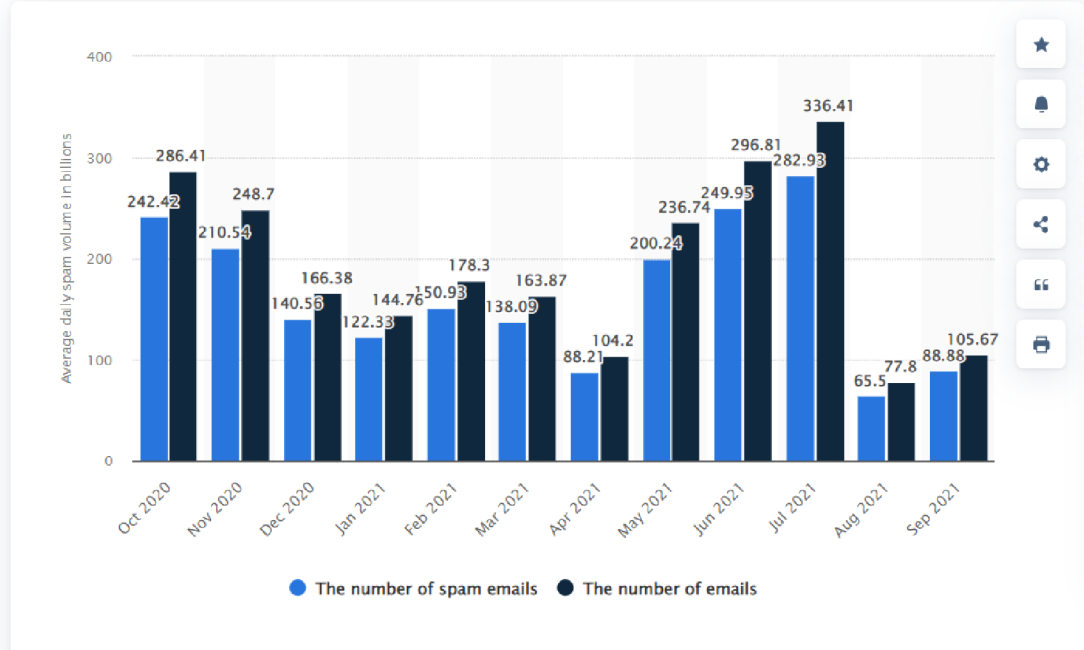
Spam je pro většinu uživatelů internetu obrovský problém – ve skutečnosti 52 % účastníků průzkumu nedávno uvedlo, že hlavním problémem je spam.[57] A navzdory vývoji antispamového softwaru, jako jsou spamové filtry a blokátory spamu, jednotlivci i podniky stále pociťují negativní účinky spamu.

Průměrný denní objem spamu na celém světě od října 2020 do září 2021.

Jak můžeme vidět na grafu 6, mezi říjnem 2020 a zářím 2021 dosáhl globální denní objem spamu nejvyšší úrovně v červenci 2021, s téměř 283 miliardami spamových e-mailů z celkového počtu 336,41 miliard odeslaných e-mailů. Od srpna 2021 toto číslo kleslo na 65,50 miliardy. K září průměrný objem spamu opět vzrostl o 36 procent a dosáhl 88,88 miliardy z celkového počtu 105,67 miliardy e-mailů odeslaných po celém světě.

---

[55] Ransomware je škodlivý kód, který zamyká přístup k infikovanému zařízení nebo šifruje jeho obsah. Po uživateli požaduje výpalné s příslibem (samozřejmě negarantovaným), že po zaplacení dojde k zpřístupnění zařízení a/ nebo odšifrování dat.
[56] Phishing. Www.eset.com [online]. Praha: ESET, spol. s r.o. nebo ESET North America, 2021 [cit. 2022-01-25]. Dostupné z: https://www.eset.com/cz/phishing/
[57] Spam Statistics and Facts. *Spamlaws* [online]. USA: Spamlaws.com, 2021 [cit. 2022-08-15]. Dostupné z: https://www.spamlaws.com/spam-stats.html



Graf 6 – Spam

(zdroj: https://www.statista.com/statistics/1270424/daily-spam-volume-global/)

Reklama tvoří 36 % veškerého světového spamu. Nejběžnější spamové e-maily jsou reklamní zprávy. V některých případech mají tyto reklamy svůj účel. Většinou však může být jejich přítomnost interpretována jako neuctivá a obtěžující. Obsah související s dospělými je druhou největší kategorií spamu a tvoří zhruba 31,7 % všech spamových zpráv. Internet se hemží obsahem pro dospělé a všechny statistiky o phishingu se shodují, že je to místo, kde se skrývá většina jeho malwaru. Toto je nebezpečný spam ve své nejčistší podobě. Podle statistik je spam na seznamce neúprosný a pro spammery ziskový. Jako poslední s 26,5 % všech nevyžádaných e-mailů jsou finanční záležitosti, což je třetí největší kategorie nevyžádaných e-mailů. Finanční zprávy, softwarové reklamy a služby zaujímají třetí místo mezi nejlepšími světovými spammery.[58]

5.3.2.1 *Případ v České republice související se spamem*

Tento příběh související s fenoménem spam poukáže na SCAM419 nebo také případ známý jako Nigerijské dopisy.

[58] What's On the Other Side of Your Inbox - 20 SPAM Statistics for 2022. *Www.dataprot.net* [online]. New York: DATAPROT, 2016, 20. července 2022 [cit. 2022-08-16]. Dostupné z: https://dataprot.net/statistics/spam-statistics/

Jistý Patrik Chan se představil jako zaměstnanec banky v Hongkongu a poslal ženě z Jindřichova Hradce typický podvodný e-mail, kterým žádal o to, aby se žena vydávala za dědičku jistého Musa Omary Numary. Na údajném účtu po zemřelém se měla nacházet částka 22.500.000 USD, peníze se měly ženě převést a pak dle informací v e-mailu se o tuto částku rozdělí.

Žena si tento e-mail přečetla, s vidinou spousty peněz na základě instrukcí kontaktovala dalšího komplice Pietra Rodolfa. Ten ji jakoby zřídil ve fiktivní bance v Nizozemí účet. Vše vypadalo reálně, protože muži vytvořili falešné webové stránky se všemi informacemi, proto žena neměla žádné podezření a ochotně jim posílala peníze, o které si řekli. Například za zřízení účtu a za převod velké částky, v první části podvodu se jednalo celkem o 3.900 USD.

Následně došlo k údajnému převodu částky 22.500.000 USD na onen fiktivní účet. Na falešných webových stránkách si dokonce žena mohla „ověřit" i jejich přijetí. Avšak když je chtěla převést do jiné banky, bylo jí sděleno, že musí uhradit tzv. osvobození od daně ve výši 29.250 USD. Na základě toho jí byl zaslán číselný kód potřebný pro převod. Jenže po jeho zadání systém požadoval další kód. Pieter Rodolf jí sdělil, že v případě tak velké částky je nutné zadat ještě další tzv. antiteroristický kód. Za něj požadoval finanční částku ve výši 49.550,60 USD. Tuto částku naštěstí již žena neodeslala a oznámila vše patřičným úřadům.[59]

5.3.3. Návrhy a řešení

Elektronická pošta nebo e-mail je jedním z nejjednodušších a nejpohodlnějších kanálů, kde můžeme přenášet informace a sdílet data s ostatními. Je však také běžné přijímat informace nebo e-maily, které obsahují škodlivé přílohy nebo pochybné zprávy. Někteří poskytovatelé e-mailových služeb filtrují a označují takové pochybné e-maily slovem „SPAM" v předmětu e-mailu, čímž příjemci označují, že se jedná buď o nevyžádaný e-mail, nebo o nevyžádaný e-mail s pochybným obsahem, který odesílatel odeslal mnoha příjemcům.

[59] Spam. *Www.internetembezpecne.cz* [online]. Praha: Czech Th!s, 2018 [cit. 2022-01-25]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/spam/

Mohou nastat případy, kdy automatický e-mailový filtr vašeho poskytovatele e-mailových služeb omylem označí legitimní e-maily jako spam kvůli jejich obsahu (např. e-mail obsahuje hypertextový odkaz). Ve většině případů však e-maily označené jako „SPAM“ nebo přesměrované do složky nevyžádané pošty ve vaší poštovní schránce odesílají spammeři. Předmětem spamových zpráv je obvykle nabídka levných léků na předpis, reklamy na nové léky a stav balíků od přepravních společností. Před otevřením jakýchkoli příloh (i když to vypadá jako nevinný textový nebo obrázkový soubor) nebo kliknutím na hypertextové odkazy se ujistěte, že jste důkladně prozkoumali obsah spamových e-mailů. Nestahujte v takových e-mailech obsah blokovaný vašimi poskytovateli e-mailových služeb.

U elektronické korespondence bych ráda řekla, že e-mail je nejčastěji používaný ke komunikaci starší populací, která se dokázala naučit základním způsobem fungovat na internetu. Důchodci většinou nemají sociální sítě jako mladší generace, ale naučili se používat e-mail, kde si mezi sebou posílají fotky vnoučat nebo svých domácích mazlíčků. Důchodci jsou možná v tomto ohledu ještě zranitelnější než děti, protože s tímto fenoménem nazvaným internet, nemají velkou zkušenost a většina z nich už bohužel nemá ani kapacitu na to, aby se to dalo zásadním způsobem změnit. Zde bych apelovala na jejich rodinu, dcery a syny, aby kontrolovali, co na internetu dělají. Musím konstatovat, že o tomto se mluví často i ve zprávách například na televizním kanálu Nova nebo Prima, které většinou tato ohrožená část obyvatelstva sleduje. Byli by určitě účinné i letáky, například na úřadech, s informacemi na co si dávat v kyberprostoru pozor, a s odkazy na důvěryhodné informační stránky.

6 Případová studie

Amanda Todd – případ, který hnul zákony

„Bojuji, abych zůstala na tomto světě, protože všechno se mě tak hluboce dotýká. Nedělám to pro pozornost. Dělám to proto, abych byla inspirací a ukázala, že mohu být silná. Ubližovala jsem sama sobě, aby bolest zmizela, protože bych raději ublížila sobě než někomu jinému. Doufám, že vám mohu ukázat, že každý má svůj příběh a budoucnost každého bude jednoho dne zářivější, musíte to prostě zvládnout. Já jsem taky pořád tady, ne?“

Amanda Todd, 7. září 2012.

Tato kanadská dívka čelila kyberšikaně dlouhé 3 roky. Bohužel v 15 letech (10. října 2012) již déle nevydržela tlak snášet a spáchala sebevraždu.

Vše začalo v Amandiných 12 ti letech, v sedmé třídě základní školy. Pomocí chatu se seznámila s mužem, který předstíral, že je stejného věku jako Amanda. Nějakou dobu si psali, a když muž získal její důvěru, přemluvil ji v konverzaci ve více lidech (jejich domnělých přátelích), aby před webkamerou ukázala svá ňadra. Amanda po nějaké době souhlasila, ale nevěděla, že muž si z tohoto okamžiku učinil fotografii. Konverzace mezi ní a mužem na nějakou dobu utichla. Po roce se jí ozval znovu. Vyhrožoval, že zveřejnění fotku, kterou měl, pokud mu nepošle ještě další. To však Amanda odmítla. Přes noc vznikla na internetu webová stránka s jejími fotkami, osobními informacemi i zmíněnou fotografií ňader. Dále muž přímo rozeslal fotku všem jejím kamarádům dokonce i rodinným příslušníkům.

Toto byl pro Amandu začátek pekla. Ve škole začala být kvůli fotce vysmívána a šikanována. Začala trpět depresemi a sebepoškozovala se. To vedlo k tomu, že se poprvé pokusila o sebevraždu tak, že vypila bělidlo a skončila v nemocnici na jednotce intenzivní péče. Na zprávu o jejím nepovedené sebevraždě reagovali lidé podáváním návrhů na to, jak nejlépe odejít z tohoto světa. Ať už oni, či zoufalství a bezmoc, které dívka prožívala, vyprovokovaly nakonec Amandu k druhému, tentokrát úspěšnému pokusu o zabití, k tomu se

dostaneme později. Nicméně ani její viditelné psychické problémy, nedonutili její spolužáky přestat. Nutno dodat, že Amanda žila pouze se svým otcem, který několikrát inicioval změnu školy, ale pokaždé se našel někdo, kdo fotku našel a zesměšňování začalo nanovo. Tomuto psychickému tlaku odolávala zhruba 2 roky, než se její matka rozhodla zasáhnout a vzít si ji k sobě. Do jiného města, jiné školy.

Zde se Amanda snažila začít nový život, vše se zlepšilo, přesto nebyla u ostatních oblíbená. To bylo pravděpodobně způsobeno tím, že už trpěla depresemi, se kterými se léčila, i úzkostnou poruchou. Nicméně nebyla šikanována, ani novými spolužáky zesměšňována na internetu, ale stále byla sama.

Po nějakém čase si ji ale muž znovu našel a vše začalo nanovo. Opět její fotka kolovala mezi jejími spolužáky, přáteli a dokonce i mezi učiteli. Změnilo se jen místo a čas.

Zhruba měsíc před smrtí umístila Amanda na webovou stránku YouTube 8 minutové video (některé záběry jsou ukázány na obrázku č. 2), kde vypráví celý svůj příběh a popisuje své utrpení, prosí, aby ji ostatní nechali na pokoji. Bohužel její video způsobilo, že si dívka kvůli němu odnesla jen další posměch. Život této dívky končí 10. října roku 2012, kdy ji matka našla doma oběšenou.

Obrázek 3 – Amanda Todd

(zdroj: https://cyberbullying.org/amanda-todd-cyberbullying-and-suicide)

Do Amandiny smrti v Kanadě neexistoval zákon definující kyberšikanu jako trestný čin. Kriminalisté nejprve uzavřeli případ jako sebevraždu bez cizího přičinění. To ve veřejnosti zvedlo vlnu nevole. Případem se začala zabývat i známá hackerská skupina Anonymous[60], zobrazeno v obrázku číslo 4. Povedlo se jim na internetu najít muže, jež stál za utrpením mladé slečny. Zveřejnili jeho adresu, jméno i osobní informace. Hrozilo, že bude veřejně lynčován. Jednalo se o 32letého muže z Nizozemska. Ten tímto způsobem znepříjemňoval život dalším dívkám z různých zemí světa.

[60] Hnutí Anonymous jsou rozšíření po celém světě. Jeho představitelé se účastnili několika veřejných protestů s jasným poselstvím – šířit informace a podporovat svobodu projevu. Neustále se diskutuje o tom, zda je tato hackerská skupina prospěšná, nebo spíše škodlivá.

Obrázek 4 – Zapojení Anonymous do případu
(zdroj: https://www.digitaltrends.com/social-media/anonymous-kody-maxson-amanda-todd-bully/)

Aydin Coban, jehož podobizna je zobrazena na obrázku číslo 5, v té době už 38letý nizozemský občan, čelil 72 obviněním, včetně přechovávání dětské pornografie, vydírání, podvodu a držení tvrdých drog.

Obrázek 5 - Aydin Coban
(zdroj: https://bc.ctvnews.ca/outrage-grows-over-book-published-by-alleged-amanda-todd-tormentor-1.3730593)

Soud vyslechl, jak se Coban na internetu spřátelil s mladými dívkami, tak že předstíral, že je dospívajícím chlapcem, a donutil je, aby mu poskytly explicitní obrázky, které pak použil k vydírání. Vyšetřovatelé soudu řekli,

že některé z jeho obětí byly roky týrány, stejně jako Amanda. V roce 2017 byl Coban odsouzen soudem v Nizozemsku k téměř 11 letům vězení za online podvody a vydírání 34 mladých žen a pěti mužů.[61]

Vydal prohlášení, v němž popírá, že by mučil Amandu Toddovou. Nicméně důkazy byly nevyvratitelné a proto v prosinci roku 2020 byl konečně 42letý Nizozemec Aydin Coban vydán do Kanady, aby čelil obvinění z vydírání, kriminálního obtěžování, komunikace s mladým člověkem za účelem spáchání sexuálního trestného činu a dvou případů držení dětské pornografie.

Expertka na kyberšikanu Barbara Coloroso řekla, že Cobanovo vydání do Kanady je známkou pokroku v této problematice. "*Vydání se děje stále častěji*," řekla Coloroso. "*Amandina matka Carol udržovala tento případ v centru pozornosti, což je velmi důležité. Podporuje povědomí dospívajících a jejich rodičů o tom, že se to může stát komukoli.“*[62] Od smrti své dcery se Carol Todd stala obhájkyní a řečnicí na téma online obtěžování a věří, že ačkoli zákonodárci mají svou roli, vzdělání je při řešení kyberšikany zásadní.

Jak již bylo nastíněno, tento případ otevřel diskuzi ohledně šikany i kyberšikany. Pár dní po Amandině nešťastném odchodu ze světa, Cristy Clark (bývalá politička) podala do sněmovny návrh na debatu ohledně kyberšikany. Pomohla také Amandině matce založit první neziskovou organizaci na pomoc obětem kyberšikany.

Tento případ lze rozdělit do tří částí.

1. Začnu situací, kdy se Amanda svlékla před kamerou. V tomto bodě bych ráda upozornila na vzdělání, které se mladým lidem dostává, lépe řečeno nedostává ohledně kyberprostoru. V této chvíli si Amanda evidentně neuvědomila anonymitu prostředí, že to s kým komunikuje, nemusí být její kamarád, za kterého se uvedený pachatel vydával a ani pachatel si na začátku nutně nemusel

[61] AMANDA TODD CYBERBULLY JAILED FOR ALMOST ELEVEN YEARS. *Cybersmile* [online]. london: The Cybersmile Foundation, 2021 [cit. 2022-01-31]. Dostupné z: https://www.cybersmile.org/news/amanda-todd-cyberbully-jailed-for-almost-eleven-years
[62] For the mother of Amanda Todd, it's been a long quest for justice. *Global News* [online]. Praha: Corus Entertainment, 2021 [cit. 2022-01-31]. Dostupné z: https://globalnews.ca/news/7628542/amanda-todd-bullying-case/

uvědomit závažnost celé situace. Zvlášť děti si ve svém věku nedokáží rozumově zpracovat, co se může stát ani co mohou způsobit. Amanda byla kyberšikanována i šikanována od svých vrstevníků a v tomto bodě, dle mého názoru, mohlo hodně pomoci, kdyby její spolužáci a kamarádi věděli, co mohou a co ne, kdyby jí někdo z nich pomohl situaci řešit. Vzdělání o bezpečnosti na internetu už by mělo patřit do osnov základního vzdělání. Do této problematiky samozřejmě spadá i etika, morálka a výchova jedince. V dnešní době je i pro rodiče mnohdy jednodušší, když jejich dítě je na internetu a mají chvilku „klid“.

2. Řešení situace rodiči dívky a škol, do kterých Amanda chodila, se jeví také jako laxní a problematické. Ráda bych navázala na první bod a to, když jsem zmínila, že pro rodiče je mnohdy jednodušší nechat dítě na internetu bez dozoru. Dle mého názoru je to do určitého věku dítěte nevhodné. Kontrola na internetu je dost kontroverzní téma, ale určitě není od věci. Děti nejsou mravně ještě vyspělé, nepřemýšlí tolik o tom, co by daná věc mohla znamenat do budoucnosti a proto by zde kontrola od rodičů měla fungovat. Je jen správné, aby rodič věděl, co dítě v kyberprostoru dělá a s kým a jak se takto baví. Je určitě důležitá i výchova a důraz na to být vzorem pro své syny a dcery. V případě Amandy si myslím, že to bylo hrubě podceněno, samozřejmě nevím, jaké vztahy byly v rodině, ale určitě rodiče měli zasáhnout dříve, silněji a hlasitěji. Bylo jasně zřejmé volání o pomoc od Amandy ať už slovně nebo činy, sebepoškozování i první pokus o sebevraždu.

   Učitel na základní škole je ve styku s dětmi skoro celý den a určitě by si měl všímat náznaků a vztahů, které jsou ve třídě a podle toho také včas jednat.

3. Poslední bod bude pohled na řešení této situace po smrti dívky. Vlastně mi připadá, že celý tento případ se začal řešit až po smrti Amandy. Začnu-li od rodičů, kdy se matka najednou zajímala o to, jak škola celý tento problém řešila, přitom ho sama roky neřešila. Orgány činné v trestním řízení neměli velkou snahu o dopadení

muže, který Amandě dělal ze života peklo. V tomto případu mi přijde zajímavé, že se do toho vložila již zmíněná skupina Anonymous a pachatele vypátrala a vlastně udělala práci za státní činitele. Jediná světlá věc na této tragédii je, že se posléze začala tato problematika více řešit, ukázalo se, že to je problém enormních rozměrů a začala se dle toho upravovat i legislativa.

Závěr

V první kapitole této práce jsou představeny základní pojmy a především etické teorie, které v přímé konfrontaci s aktuálními trendy internetového prostředí stále nacházejí své uplatnění, resp. dokazují svou aktuálnost, i když její míra je ovlivněna zejména postojem dnešní společnosti a prostorem, který virtuální svět představuje. Ve druhé kapitole se věnuji základní legislativě, která je s touto problematikou spjatá a určitě ji nelze vynechat. Následující kapitola obsahuje kodexy, které by měly směřovat uživatele k etickému chování na internetu. Uvádím tři kodexy s tím, že jeden je ještě vložen jako podkapitola u sociálních sítí. V mé práci nalezneme vysvětlení vybraných negativních jevů souvisejících s informační etikou. Praktickou částí jsem se snažila ke každému jevu najít procentuální vyjádření výskytu v současnosti. Také zde najdeme vybrané trestné činy, které se staly v České republice. V závěrečné části mé práce je zpracována případová studie. Jako případ jsem si vybrala tragický příběh dívky Amandy a to z několika důvodů. Prvním je, že tento případ byl hodně medializován a upoutal pozornost mnoha lidí. Druhý důvod je ten, že v tomto případě je děj rozvinutý do mnoha rovin, tudíž je mnoho úhlů pohledu – dívka si najde přátele přes internet, které nikdy neviděla a začne jim důvěřovat, Amanda je zmanipulovaná ke svléknutí se před kamerou a následně kvůli tomu vydírána starším mužem. Kyberšikana i klasická šikana, která kvůli tomu přijde, je nevídaného rozměru. Následně po dívčině sebevraždě se do toho vloží hackerská skupina Anonymous a najde pachatele. Nakonec se zjistí, že zákony, které by měly chránit uživatele, nejsou dostatečné a díky tomuto případu se o nich znovu jedná.

Vzhledem k neustálému rozvoji informačních a komunikačních technologií je těžké pokrýt všechny oblasti, jež souvisí s informacemi a jejich šířením. Je zde určitě důležitá zmíněná legislativa, která ale nemůže pokrýt vše a mnohdy je, jak jsem již uváděla, nejméně krok pozadu za současnými trendy a proto je nutné, aby fungovala etika a etické zásady, jak v osobním měřítku, tak celospolečenském. Internetové médium v dnešní době zásadně ovlivňuje život značné části populace napříč celým světem.

Největším problémem, co se týče informační etiky a negativních jevů s ní spojenými, je vzdělávání. Dle mého názoru je hrubě nedostatečné vzhledem k míře, v jaké je dnes celý kyberprostor a zvlášť internet používán. V osnovách na základních školách stále chybí informace o tom, jak pracovat s dezinformacemi, jak se zachovat v případě kyberšikany, ale i například jak se jí vyvarovat, což je alarmující. Mladí lidé nejsou tolik mravně vyspělí na to, aby pochopili, co můžou způsobit, proto je určitě více než vhodné jim to neustále a dokola vhodně předkládat a vysvětlovat.

Cílem této práce bylo poukázat na současné negativní jevy, které jsou spojeny s informační etikou v kyberprostoru. Dodržování, resp. nedodržování etického rámce v praktickém měřítku, konkrétně jsou řešeny otázky informační etiky v jednotlivých oblastech internetu. Cíl práce jsem, dle mého názoru, splnila.

Seznam použité literatury

Monografie

[1] ČINČERA, Jan. Informační etika: sylabus k bakalářskému studiu informační vědy. Brno: Masarykova univerzita, Filozofická fakulta, 2002. ISBN 80-210-2981-1

[2] HEMEROVÁ - HÁJKOVÁ, Kateřina. Etické principy v informační činnosti. Praha, 2004. Diplomová práce. Univerzita Karlova v Praze.

[3] Janoš, Karel. Informační etika. Praha: Česká informační společnost, 1993

[4] KARLÍČEK, M., KRÁL, P. Marketingová komunikace: Jak komunikovat na našem trhu. 1. vydání. Praha: Grada, 2011. 224 s. ISBN 978-80-247-3541-2.

[5] LIBOR, Marek. *Informační etika a její dodržování v online prostředí*. Praha, 2014. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Mgr. Ing. Tomáš Sigmund, Ph.D.

[6] ROGERS, Vanessa. Kyberšikana: pracovní materiály pro učitele a žáky i studenty. Praha: Portál, 2011. ISBN 978-80-7367-984-2.

[7] TÁBORSKÝ, Jiří. *V síti dezinformací: Proč věříme alternativním faktům*. 1 vydání. Praha: Grada Publishing, 2020. ISBN 978-80-271-1066-4.

[8] VANĚK, Jiří. Obecná, ekonomická a informační etika. 1. vydání. Praha: Wolters Kluwer ČR, 2010. ISBN 978-80-7357-504-5.

Zákonná úprava

[1] Zákon č. 106/1999 Sb. o svobodném přístupu k informacím. [Online] [Citace: 3. listopad 2021.] Dostupné z: http://www.zakonyprolidi.cz/cs/1999-106.

[2] Zákon č. 121/2000 Sb. o právu autorském. [Online] [Citace: 3. listopad 2021.] Dostupné z: http://www.zakonyprolidi.cz/cs/2000-121.

[3] Zákon č. 250/2016 Sb. o odpovědnosti za přestupky a řízení o nich. § 21 a § 23

Webové stránky a elektronické zdroje

[01] AMANDA TODD CYBERBULLY JAILED FOR ALMOST ELEVEN YEARS. Cybersmile [online]. london: The Cybersmile Foundation, 2021 [cit. 2022-01-31]. Dostupné z: https://www.cybersmile.org/news/amanda-todd-cyberbully-jailed-for-almost-eleven-years

[02] BISCHOFF, PAUL. Almost 60 percent of parents with children aged 14 to 18 reported them being bullied. *Comparitech* [online]. united kingdom: Comparitech Limited, 2019, 8. května, 2019 [cit. 2022-08-11]. Dostupné z: https://www.comparitech.com/blog/vpn-privacy/boundless-bullies/

[03] Co je kyberšikana?. E-bezpečí [online]. Praha: Pedagogická fakulta Univerzity Palackého v Olomouci [cit. 2022-01-31]. Dostupné z: https://www.e-bezpeci.cz/index.php/temat/kyberikana/17-cojekybersikana

[04] Cyber grooming. *Www.childsafenet.org* [online]. Nepal: CENTRAL DEVELOPMENT REGIO, 2018 [cit. 2022-08-16]. Dostupné z: https://www.childsafenet.org/new-page-15

[05] Češi a dezinformace. Simar - Sdružení agentur pro výzkum trhu a veřejného mínění [online]. Praha: SIMAR, 2020 [cit. 2022-01-31]. Dostupné z: https://simar.cz/cerstve-namleto/cesi-a-dezinformace.html

[06] Directorate-General for Communications Networks a Content and Technology. *Fake news and disinformation online* [online]. Publications Office: European Commission, 2018 [cit. 2022-08-11]. ISBN 978-92-79-81900-1. Dostupné z: https://data.europa.eu/doi/10.2759/559993

[07] Etické kodexy veřejnoprávních médií. Www.otevrenamedia.cz [online]. Praha: SeeMedia, 2022 [cit. 2022-01-26]. Dostupné z: http://otevrenamedia.cz/eticke-kodexy-verejnopravnich-medii/

[08] Etický kodex. Www.syndikat-novinaru.cz [online]. Praha: SYNDIKÁT NOVINÁŘŮ ČESKÉ REPUBLIKY, 2022 [cit. 2022-01-26]. Dostupné z: https://www.syndikat-novinaru.cz/o-nas/etika/eticky-kodex/

[09] Informace. Www.managementmania.com [online]. Praha: ManagementMania's Series of Management, 2018 [cit. 2022-01-25]. Dostupné z: https://managementmania.com/cs/informace

[10] INFORMATION ETHICS. *Encyclopedia.com* [online]. AN ELITE CAFEMEDIA PUBLISHER, 2019 [cit. 2022-08-15]. Dostupné z: https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/information-ethics

[11] Jaroslav Pulpán. Česká televize [online]. Praha: Česká televize [cit. 2022-01-31]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/2606459-na-internetu-sexualne-obtezoval-160-prevazne-nezletilych-divek-ve-vezeni-stravi-65

[12] Kodex influencera. Www.samoregulace.cz [online]. Praha: SPIR z. s. p. o. [cit. 2022-01-31]. Dostupné z: https://www.samoregulace.cz/kodex-influencera

[13] MAGDOŇOVÁ, Jana. První rozsudek za dezinformace o covidu. IRozhlas [online]. Praha: Český rozhlas [cit. 2022-01-31]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/podcast-vinohradska-12-koronavirus-dezinformace-soud-trest-jana-peterkova_2201180600_miz

[14] Ministerio de Asuntos Exteriores. The fight against disinformation. Www.exteriores.gob.es [online]. Spain: Directorate-General for Communications, 2022, 2020 [cit. 2022-08-15]. Dostupné z: https://www.exteriores.gob.es/en/PoliticaExterior/Paginas/LaLuchaContraLaDesinformacion.aspx

[15] Ověřovatelé faktů a přísnější kontrola. Boj proti dezinformacím bude důslednější. Forbes [online]. Česko: MediaRey, SE, 2022, 16.června 2022 [cit. 2022-08-15]. Dostupné z: https://forbes.cz/overovatele-faktu-a-prisnejsi-kontrola-boj-proti-dezinformacim-bude-duslednejsi/

[16] Pavel Hovorka. Česká televize [online]. Praha: Česká televize [cit. 2022-01-31]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/1422179-soud-poslal-muze-za-zneuzivani-chlapcu-na-osm-let-do-vezeni

[17] Pavel Hovorka. E-bezpečí [online]. Praha: Pedagogická fakulta Univerzity Palackého v Olomouci [cit. 2022-01-31]. Dostupné z: https://www.e-bezpeci.cz/index.php/temat/kyberikana/pavel-hovorka

[18] PAMMENT, James. *RESIST - Příručka pro boj s dezinformacemi* [online]. Praha: Centrum proti terorismu a hybridním hrozbám Ministerstva vnitra, 2020 [cit. 2021-12-19]. Dostupné z: https://gcs.civilservice.gov.uk/guidance/resist-counter-disinformation-toolkit/.

[19] Phishing. Www.eset.com [online]. Praha: ESET, spol. s r.o. nebo ESET North America, 2021 [cit. 2022-01-25]. Dostupné z: https://www.eset.com/cz/phishing/

[20] Počítačová etika. Www.tech-lib.eu [online]. Praha: Sharpened Productions, 2020 [cit. 2022-01-25]. Dostupné z: https://tech-lib.eu/definition/computerethics.html

[21] Spam. Www.eset.com [online]. Praha: ESET, spol. s r.o. nebo ESET North America, 2021 [cit. 2022-01-25]. Dostupné z: https://www.eset.com/cz/spam/

[22] SINGER, Peter. Moral philosophy. *Britannica* [online]. Velká británie: Encyclopædia Britannica, 2016 [cit. 2022-08-15]. Dostupné z: https://www.britannica.com/topic/ethics-philosophy

[23] Spam Statistics and Facts. *Spamlaws* [online]. USA: Spamlaws.com, 2021 [cit. 2022-08-15]. Dostupné z: https://www.spamlaws.com/spam-stats.html

[24] Svaz knihovníků a informačních pracovníků ČR. Kodex etiky českých knihovníků. [Online] 2004. [Citace: 3. Listopad 2021.] Dostupné z: http://www.skipcr.cz/co-je-skip/kodex-etiky.

[25] TEXTOVÁ OPORA PRO E-LEARNINGOVÝ KURZ INFORMAČNÍ VÝCHOVY F*** VUT [online]. 2007. Brno: pracovní skupina pro informační vzdělávání [cit. 2022-01-31]. Dostupné z: http://w18.fme.vutbr.cz/studium/zavprace/etika/kapitola_8_a.pdf

[26] VALÁŠEK, Michal. Spam a Úřad pro ochranu osobních údajů. [Online] 2011. [Citace: 3. listopad 2021.] Dostupné z: http://www.lupa.cz/clanky/spam-a-urad-pro-ochranu-osobnich-udaju/.

[27] Víte co je KYBERŠIKANA?. Policie [online]. Praha: Policie ČR [cit. 2022-01-31]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[28] Vnitro chce omezit dezinformace. Připravilo návrh zákona. *Www.ceskatelevize.cz* [online]. Praha: Česká televize, 1996–2022 [cit. 2022-08-24]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3499030-vnitro-chce-omezit-dezinformace-pripravilo-navrh-zakona

[29] What is phishing?. *Www.proofpoint.com* [online]. United Kingdom: Proofpoint Trust, 2021 [cit. 2022-08-16]. Dostupné z: https://www.proofpoint.com/us/threat-reference/phishing

[30] What's On the Other Side of Your Inbox - 20 SPAM Statistics for 2022. *Www.dataprot.net* [online]. New York: DATAPROT, 2016, 20. července 2022 [cit. 2022-08-16]. Dostupné z: https://dataprot.net/statistics/spam-statistics/

Seznam obrázků

Seznam tabulek

Seznam grafů