Scénář hrozby Deep fakes v ochraně obyvatelstva

Bc. Aleš Hrubý

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Aleš Hrubý**
Osobní číslo:	**L20445**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Scénář hrozby Deep fakes v ochraně obyvatelstva**

Zásady pro vypracování

1. Proveďte rešerši soušasného stavu předmětné oblasti.
2. Analyzujte Deep fakes v kontextu informační bezpečnosti z hlediska legislativy České republiky.
3. Analyzujte možnosti zneužití Deep fakes v ochraně obyvatelstva.
4. Navrhněte scénář hrozby Deep fakes v ochraně obyvatelstva.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ADAMS, Maurice. *Deepfake technology & 2020 u.s. electrions: a threat to democracy and how to spot deepfakes*. Independently published. Dallas, 2019. ISBN 978-1705466322.
2. SHICK, Nina. *Deep Fakes and the Infocalypse: What You Urgently Need To Know*. Monoray, 2020. ISBN 978-1913183523.
3. YOUNG, Norbert. *Deepfake technology: Complete Guide to Deepfakes, Politics and Social Media*. Independently published, 2019. ISBN 978-1078494694.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2021**
Termín odevzdání diplomové práce: **6. května 2022**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 1. prosince 2021

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 5. 8. 2022

Jméno a příjmení studenta: Bc. Aleš Hrubý

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá problematikou Deep fakes a s ní úzce souvisejícím jevem Fake news. Cílem práce je analyzovat hrozbu Deep fakes v prostředí ochrany obyvatelstva. Součástí navrhovaného scénáře je tvorba vlastního Deep fake videa včetně klonování hlasu. Závěr diplomové práce tvoří dotazník pro obyvatele České republiky, který má za úkol zjistit povědomí veřejnosti o výše zmíněných jevech. Následně jsou navržena opatření pro snížení vlivu Deep fakes a Fake news na obyvatelstvo.

Klíčová slova: Deep fakes, Fake news, informační bezpečnost, umělá inteligence

ABSTRACT

The diploma thesis deals with Deep fakes and the closely related Fake news phenomenon. The aim of the work is to analyse the threat of Deep fakes in the protection of the population. The proposed scenario includes the creation of its own Deep fake video, including voice cloning. The conclusion of the thesis consists of a questionnaire for the Czech people, which is tasked with finding out about Fake news and Deep fakes. Subsequently, measures are proposed to reduce the influence of Deep fakes and Fake News on the population.

Keywords: artificial intelligence, Deep fakes, Fake news, information security

Poděkování

Rád bych poděkoval za vedení diplomové práce Ing. Petru Svobodovi, Ph.D. za jeho vedení a pomoc při zpracování závěrečné práce. Děkuji také své rodině, která mi byla oporou během studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Problematika Deep fakes je relativně nový pojem, avšak s postupně rostoucím technologickým pokrokem začíná představovat nebezpečnou hrozbu pro obyvatelstvo. S dokonalejší umělou inteligencí se vytváří stále kvalitnější Deep fakes za pomoci speciálních aplikací, které jsou nenáročná na použití a jsou snadno dostupná široké veřejnosti. Téměř každý je potom schopen vytvořit Deep fakes, a proto se s ním stále častěji setkáváme např. v médiích nebo na sociálních sítích.

V dnešní moderní době vlastní většina populace mobilní telefon disponujícím kvalitním fotoaparátem, díky kterému lze pořídit potřebný snímek nebo videozáznam obličeje, jež je klíčový pro tvorbu Deep fakes. Falešné zprávy stále více a více na vzestupu, rychle se šíří a s využitím syntetických médií můžou mít bohužel větší dopad a vliv.

Diplomová práce je rozdělena na teoretickou a praktickou část. V teoretické části práce je vypracována literární rešerše zabývající se jevem Deep fakes a Fake news. Jsou uvedeny druhy falešných zpráv a je vysvětleno, proč je Fake news důležitou součástí Deep fakes. K vytvoření přesvědčivé Fake news se může využít právě Deep fakes. Dále je charakterizována informační bezpečnost a problematika Deep fakes a Fake news v kontextu informační bezpečnosti z hlediska legislativy.

V praktické části je vytvořen scénář hrozby Deep fakes v ochraně obyvatelstva. Součástí scénáře je zhotoveno vlastní Deep fake video s využitím klonování hlasu, které slouží pro dokreslení této problematiky. Cílem vytvořeného krátkého videa bylo ukázat snadnou tvorbu, kterou zvládne i běžný uživatel internetu. Závěrem diplomové práce je dotazník pro obyvatele České republiky, který má za úkol zjistit povědomí veřejnosti o Fake news a Deep fakes a potvrdit či vyvrátit stanovené hypotézy. V práci je uvedena jedna z metod odhalení Deep fakes a to DeepFake-Detect, což je on-line metoda běžně dostupná, a která byla použita na otázky v dotazníku č. 16, 17 a 18. Na závěr jsou navrhnuta opatření pro snížení vlivu Deep fakes a Fake news na obyvatelstvo.

CÍLE PRÁCE A POUŽITÉ METODY

Tato kapitola vytyčuje hlavní cíl a dílčí cíle diplomové práce. Dále kapitola obsahuje výčet a popis metod, které byly použity při jejím zpracování.

Hlavní cíl diplomové práce

- Analyzovat hrozbu Deep fakes v prostředí ochrany obyvatelstva.

Dílčí cíle diplomové práce

- Seznámit se s teoretickými základy dané problematiky.
- Provést dotazníkové šetření pro určení závažnosti Deep fakes.
- Zpracovat scénář zneužití Deep fakes v ochraně obyvatelstva.
- Analyzovat tvorbu Deep fakes a vytvořit vlastní video.
- Navrhnout opatření pro snížení vlivu Deep fakes.

Použité metody

K dosažení výše zmíněných cílů diplomové práce bylo využito několik metod vědeckého zkoumání. První z nich byla metoda literární rešerše, která sloužila pro sběr informací a dat z literárních a elektronických zdrojů za účelem zpracování teoretické části diplomové práce. Syntéza byla využita pro sestavení návrhu scénáře hrozby Deep fakes v ochraně obyvatelstva napříč různými odvětvími, kde může představovat zmíněný jev hrozbu. Metoda dedukce byla využita při tvorbě hypotéz, které sloužily jako opora pro sestavení dotazníku. Další zvolenou metodou je dotazníkové šetření, které sloužilo k potvrzení či vyvrácení hypotéz a mělo za úkol zjistit povědomí obyvatelstva o dané problematice. Metoda indukce byla využita při vyhodnocení hypotéz a dotazníku prostřednictvím statistického zpracování dat do grafů a tabulek, které znázorňují výsledky jednotlivých otázek získaných od respondentů. Následně byla použita metoda komparace, kdy došlo k porovnání výsledků z dotazníkového šetření o znalosti jevů Fake news a Deep fakes u obyvatel.

I. TEORETICKÁ ČÁST

1 FAKE NEWS

Specifikem problematiky Fake news bylo již od samotného počátku neschopnost ověřit pravdivost faktů a následné chyby. Již od druhé poloviny 18. století řešil tento problém král Jiří III., protože se kolem jeho královské rodiny šířily nepravdivé zprávy, a proto tehdy založil Dvorní oběžník. Jedná se o oficiální záznam dění na královském dvoře, které vychází ve vybraných britských novinách i v dnešní době (Jackson, Guitan a Pelíšek, 2020).

Fake news je podle Gregora a Vejvodové (2018) nové pojmenování pro staré známé dezinformace. Jedná se o záměrně nepravdivé nebo zavádějící informace, vyskytují se v médiích a na sociálních sítích. Jejich cílem je ovlivňování a manipulace příjemce. S dezinformacemi (Fake news) se setkáváme téměř každý den, jedná se často o podvody, senzace a různé jiné skandály. Platí zde pravidlo, že potenciál má vše, co lze podat emotivně.

Nejděsivějším problémem Fake news je skutečnost, že se o nich ve velkém měřítku mluví a dochází tak ke snadnému šíření falešných informací. Fake news mohou být také využity pro získávání peněz. Využívá se tzv. clickbaitů, tedy zpráv na internetu, učené výhradně k tomu, abychom na ně chtěli kliknout. Další cílená forma šíření je zamířena na specifickou část obyvatelstva, která nesouhlasí s vládou nebo odlišnou částí společnosti. Následně vzniká větší neshoda přiživovaná dalšími Fake news, která se sdílí ve filtračních bublinách obdobně smýšlejících lidí, což u mnohých z nich vyvolává strach a předsudky (Jackson, Guitan a Pelíšek, 2020).

Jedním znakem dezinformace je částečně věrohodná informace. Jejím dalším faktorem je přizpůsobení se kulturnímu kontextu a schopnosti dostat se k lidem prostřednictvím velkého počtu kanálů – noviny, televize, sociální sítě (Gregor a Vejvodová, 2018).

Zvláštní případy výskytu Fake news se staly např. v roce 2019 během britských voleb, kdy jedna facebooková skupina vymyslela trik, že všichni její členové vedoucímu politikovi okomentovali příspěvek komentářem, který obsahoval pouze jedno slovo „výborně“. Následně si jeho konkurenti stěžovali, že zmíněný politik dostává falešnou podporu podvodem pomocí botů, ovšem se jednalo pouze o fígl, protože to byly skutečné osoby. Samozřejmě se ozvali odpůrci daného politika a začali přidávat pod jeho příspěvky komentáře typu „"Výborně"&name="Martine"syntax/error“, aby to vypadalo jako příspěvek od bota. Kuriózní případ se udál, když falešní falešníci zfalšovali falešné komentáře, což byla vážně pravda (Jackson, Guitan a Pelíšek 2020).

1.1 Propaganda

Již od 17. století nám novináři sdělují informace o událostech ve světě a pomáhají nám jim lépe porozumět. Například vládní činitelé se mnohdy bohužel snaží mít tyto informace pod kontrolou a v reportážích dochází k cenzuře. Propaganda je tedy odrazem vize vlády, která cíleně vybírá a schvaluje zprávy (Jackson, 2020).

„Cílem moderní propagandy není jen dezinformovat nebo vám vnutit cizí názory. Jde o to vyčerpat kritické myšlení a zcela vymazat pravdu.“ Garry Kasparov (Gregor a Vejvodová 2018, s.14).

Mluvíme-li o dezinformacích, nesmíme zapomenout na propagandu, jež využívá dezinformace jako nejefektivnější nástroj. Cílem propagandy je ovlivnit publikum a úmyslně ovlivnit jeho myšlenky, názory, chování a dosáhnout cíleného záměru propagandisty. Prostředky šíření propagandy se časem vyvíjely, od kamenných sloupů až po internet. Zdokonalily se, ale jejich podstata zůstala totožná – manipuluje a ovlivňuje společnost. V knize se uvádí tři směry propagandy:

a) **bílá propaganda** (public relations) – pracuje s pravdivými a objektivními informacemi, jejich cílem je ovlivnit mínění veřejnosti, mobilizovat obyvatele či propagaci určitého hnutí

b) **černá propaganda –** koresponduje s negativními představami o propagandě, využívá polopravdy, věrohodně se tvářící dezinformace, jejichž cílem je pošpinění a oslabení protivníka, působí skrytě a zdroje bývají většinou falešné či zavádějící

c) **šedá propaganda** – koreluje mezi dvěma předchozími směry propagandy, informace se mohou jevit jako neutrální až pozitivní, ve většině případů (ne vždy) využívá argumenty, které jsou založeny na pravdivé podstatě a jsou objektivně prezentovány, jejich znakem je složité ověření informací a jejich původní zdroj nemusí být zcela zřejmý, díky čemuž se stává nejtajemnějším typem propagandy (Gregor a Vejvodová, 2018).

1.2 Misinformace

Misinformace je neúmyslně a nesystematicky šířená zavádějící nebo nesprávná informace. Jejich cílem není ovlivnit rozhodování nebo názory příjemců. Přestože se jedná o neutrální jev, mohou misinformace vést ke stejnému výsledku jako šíření dezinformací, pokud jsou šířeny ve velkém rozsahu a bez patřičných oprav. Tyto jevy jsou obvyklou součástí veřejné

diskuse demokratické společnosti. Většina takových fenoménů není v zájmu demokratického státu a uskutečňuje se jakožto právo na svobodu projevu. Pro Ministerstvo vnitra jsou důležité pouze ty dezinformace a propaganda, které mohou negativně ovlivnit vnitřní bezpečnost České republiky (dále jen „ČR“). Z pohledu trestního práva se jedná o případy, které naplňují skutkovou podstatu trestných činů, ale i v případech, kdy dezinformační nebo propagandistické jednání neporušuje žádný první předpis (jedná se o většinu), může nadále značit nebezpečí pro vnitřní bezpečnost státu. Například se jedná o tzv. praní špinavých informací, kdy v návaznosti na sebe odkazují zdroje na původní „špinavý“ původ či neověřený původ informace, který se následně „očistí“ a mohou sloužit jako podklad pro seriózní média (Mvcr, 2022).

1.3 Hoax

Hoax definuje nepravdivou zprávu, která zvýhodňuje určitou stranu. Termín hoax pochází z anglického slova *„hocus“* a znamená obelhání, omámení někoho (Huďo, 2019), falešnou nebo poplašnou zprávu, mystifikaci, podvod, výmysl apod. (hoax.cz, 2022).

Díky hoaxům v mediálním prostoru můžeme dosáhnout překrucování faktů nebo vytváření situací, kdy se všechna tvrzení stanou podobně pravděpodobná. Cílem je vytvoření nedůvěry k autoritám, mediím a faktům. Hoaxy se často objevují na sociálních sítích, snadno ovlivňují veřejné mínění obyvatel a staly se zbraněmi v hybridní válce. Někdy se mluví i o spolupráci s vládami a úřady různých států. Média využívají hoaxy k získání důvěry veřejnosti. Odhalení hoaxů se může zjistit okamžitě, ale mohou mít také dlouhodobé trvání, dokonce i několik let (Huďo, 2019).

Za hoaxy označujeme poplašné a zbytečné řetězové zprávy, které se často objevují na internetu. Můžeme se s nimi setkat na sociálních sítí, v e-mailech a ve většině případů pobízejí k dalšímu rozeslání a sdílení. Hoaxy mohou mít jakýkoli obsah, mohou to být zábavné informace, prosby o pomoc, petice nebo varování před virovým ohrožením, někdy se také snaží zničit pověst jednotlivce či skupiny nebo zneužít osobní údaje (Gregor a Vejvodová, 2018).

2 DEEP FAKES

V dnešní době může už skoro každý vytvořit Deep fakes, i když ještě před pár lety byl tento termín na svém počátku. S rozvojem technologie se zdokonaluje umělá inteligence a používá se k vytvoření nebo k odhalení Deep fakes. Následující kapitola obsahuje informace z historie Deep fakes, vysvětluje samotný pojem, zabývá se umělou inteligencí a Generativní adversariální sítí, popisuje technologie odhalující samotné Deep fakes a zabývá se informační bezpečností z hlediska legislativy. Na závěr kapitoly jsou ukázány možnosti zneužití Deep fakes v ochraně obyvatelstva a také první zmínka varování před problematikou Deep fakes na mezinárodní úrovni, včetně orgánů zajišťující informační bezpečnost.

2.1 Historie Deep fakes

V roce 1997 byla poprvé zaznamenána první snaha o tvorbu Deep fakes pomocí programu „Video Rewrite“, který vytvořili: Christoph Bregler, Michele Covell a Malcolm Slaney. Upravili existující videozáznam mluvící osoby tak, že nahradili stávající slova za nová, která byla obsažena v jiné zvukové stopě. Učinili tak všichni pomocí techniky strojového učení, aby byl systém schopen navázat spojení mezi zvuky vytvářenými subjektem videa a tvarem jeho tváře. Program byl původně určen pro aplikace ve filmovém dabingu, což umožnilo upravit filmovou sekvenci tak, aby synchronizovala pohyby rtů herců s novým zvukem (historyofinformation, 2022).

Na počátku nového tisíciletí se nedělo mnoho nových věcí, protože se počítačové vidění posunulo hlouběji do světa rozpoznávání obličejů. Vývoj na tomto poli přinesl drastická zlepšení technologií, jako je sledování pohybu, které učinilo dnešní Deep fakes přesvědčivější.

Program Face2Face, vydaný v roce 2016, upravoval videozáznam obličeje člověka tak, aby zobrazoval kopírování výrazů obličeje jiné osoby v reálném čase. Bylo to provedeno pomocí kamery, která nezachycovala hloubku, což umožňovalo provádět techniku pomocí běžných spotřebitelských kamer (emmasanders, 2022).

Termín Deep fake vznikl v prosinci 2017. Anonymní uživatel na online platformě Reddit, který si říkal Deepfake, používal tuto technologii, aby přeměnil tváře některých celebrit pro účel vytváření pornografie. Přestože byl z Redditu vykázán, mnoho napodobitelů ho nahradilo na jiných platformách, což vedlo k vytvoření více než 10 000 Deep fakes. Četné

Deep fakes, které kolovaly po internetu, se omezily na neodborné hobbymarkety, kteří s potěšením překrývají tváře celebrit na tělech pornohvězd nebo nutí politiky říkat vtipné věci. Deep fakes mohou být zábavné, ale ne pokud jde o politiku a pornografii. Představuje to alarmující hrozbu pro demokracii a volební integritu nebo jako součást dezinformačních kampaní (Adams, 2019).

V lednu 2018 byla spuštěna desktopová aplikace s názvem FakeApp. Tato aplikace umožňuje svým uživatelům snadno vytvářet a sdílet videa se vzájemně prohozenými tvářemi.

V dubnu 2018 se na internetu objevilo video s Jordanem Peelem a prezidentem Obamou. Později ve videu je odhaleno, že Jordan Peele byl ve skutečnosti ten, kdo mluvil a „vkládal" slova do úst prezidenta Obamy. I když to všechno vypadalo velmi přirozeně, bylo to falešné[1].

V srpnu 2018 výzkumníci na Kalifornské univerzitě Berkeley publikovali práci zavádějící falešnou taneční aplikaci, která může vytvořit dojem profesionální taneční schopnosti pomocí UI-technologie. Tento projekt aplikoval Deep fake na celé tělo, spíše než jen na hlavu, na kterou se předchozí práce zaměřovaly[2].

Od roku 2020 existuje mnoho aplikací na tvorbu Deep fakes za využití umělé inteligence, které dokážou dokonce klonovat lidské hlasy po 5 sekundách poslechu. V březnu 2020 vznikají první aplikace i na mobilní telefony a v dnešní době má skoro každý schopnost vytvořit poněkud přesvědčivé Deep fakes, a to je opravdu skvělé, ale ne vždy je to využito dobře (emmasanders, 2022).

2.2 Deep fakes

Deep fakes je druh „syntetických médií", což znamená média (včetně obrázků, zvuku a videí), která jsou buď manipulována, nebo zcela generována umělou inteligencí. Technologie soustavně usnadňují a zpřístupňují manipulaci s médii. Nedávné pokroky v oblasti umělé inteligence ji však posouvají ještě dále, protože dají strojům sílu generovat zcela syntetická média, ze kterých může vyplynout mnoho pozitivních a negativních dopadů pro společnost. Z tohoto důvodu je Deep fakes definováno jako každé syntetické médium, které je používáno k dezinformačním a misinformačním účelům (Shick, 2020).

[1] viz. video https://www.youtube.com/watch?v=cQ54GDm1eL0
[2] viz. video https://www.youtube.com/watch?v=PCBTZh41Ris

Deep fakes je lidská zobrazovací technologie, která využívá umělou inteligenci ke střídání lidských obrazů. Používá algoritmus označovaný jako „generativní kontradiktorní síť“ k položení jiné fotografie nad zdrojovou fotografii, což je proces známý v digitálním grafickém světě jako „Superimpozice“. V ostatních případech se fotografie neodkládají, jsou jednoduše kombinované nebo smíšené. Mohou být použity buď pro statické snímky nebo pohyblivé obrazy využívající umělou inteligenci k vytvoření realisticky vypadajících padělků. Deep fakes nejsou zrovna úplné padělky, pokud zkoumáte slovo do hloubky. Jsou vlastně skutečným obsahem, který byl zfalšován a restrukturalizován tak, aby zobrazoval něco jiného. Dodatečným efektem je, že dochází k všeobecnému snížení důvěry ke všem videím, která jsou nyní prohlížena. Široka veřejnost nerozezná, zda jsou videa, na která se dívají skutečná, nebo se jedná o dokonalý podvrh. Je to relativně snadné, jakmile jsou vhodné nástroje na místě pro práci. S dobrým počítačovým systémem, softwarem a informacemi o tom, jak provádět vizuální a audiovizuální úpravy si „každý“ může vymyslet realisticky vypadající obsah. (Young, 2019).

2.3 Umělá inteligence

Umělá inteligence (dále jen „UI“) byla kdysi výlučnou doménou sci-fi, ovšem nyní je to praktická realita. Počítačoví vědci se snaží přijít na to, jak vtisknout počítačům umělou inteligenci, a to už od svého vynálezu v 50. letech minulého století. V 80. letech 20. století byla komunita UI rozdělena na dva tábory. Skupina k rozvoji umělé inteligence zvolila přístup založený na pravidlech, kdy se počítače naprogramovaly, jedno pravidlo po druhém. Druhý tábor předpokládal, že nejlepším způsobem, jak vyvinout umělou inteligenci by bylo strukturovat stroje, tak aby se učily samy napodobováním nervových sítí v lidském mozku, a aby zpracovávaly data pro rozhodování. Takto by se stroje učily díky „zkušenosti“ stejně jako lidé. Tato teorie byla řádně prověřena až v roce 2000, kdy poprvé bylo dostatek dat a procesních výkonů k jejímu vyzkoušení. Výzkumníci zjistili, že tato metoda funguje a byla pojmenována „hluboké učení“. V posledním desetiletí se rozvoj hlubokého učení posunul reálné UI kupředu, z něhož se rodí četné aplikace. Například technologie rozpoznávání obličejů, zde jsou systémy strojového učení cvičeny pomocí rozsáhlého datového souboru lidských tváří, dokud se je samostatně nenaučí s dokonalou přesností rozpoznávat. Výzkum umělé inteligence se vyznačuje svou povahou za open-source, což znamená, že špičkový výzkum, nástroje a software jsou často volně sdíleny na internetu (Schick, 2020).

Jednoduše řečeno jde o strojovou nebo automatizovanou verzi lidské inteligence a kognitivních schopností. Díky této inovaci došlo k obrovským skokům v oblasti informatiky, programování a komunikace. Umělá inteligence může být silná nebo slabá. Slabá umělá inteligence je vyvíjena a naprogramována pro konkrétní úkol. To znamená, že nemohou pracovat mimo obor, pro který je postaven. Dobrým příkladem je Alexa od Amazonu a Siri od Applu, jsou to chytré virtuální asistentky vycvičené poslouchat a provádět hlasové příkazy. Silné umělé inteligence jsou ty, které vykonávají obecné úkoly, které nejsou omezeny na určitý typ, když jsou postaveny před úkol a nepotřebují vstup člověka, než jej bude moci provést (Young, 2019).

Kategorie umělé inteligence:

a) analytická – k analýze a rozhodování do budoucna čerpá z informací získaných z posledních zkušeností (např. lidských bytostí)

b) člověkem inspirovaná – čerpá z vlastností jak lidského poznání, tak emocí. Rozhodnutí se nejen přezkoumávají, analyzují, ale posuzují se i emocionálně. Je to proto, že umělá inteligence se naučila chápat lidské emoce a začlenit je do nich.

c) humanizovaná umělá inteligence – obsahuje kognitivní i emocionální rysy lidské inteligence. Inovace, jako je například robotický osobní asistent, dokážou smysluplně interagovat s lidmi (Shick, 2020).

Využití umělé inteligence:

a) zdravotnictví – firmy a zdravotnická zařízení dnes metodu strojového učení využívají k lepším a přesným diagnózám, kterých lidé nemusí dosáhnout. Jednou z nejlepších zdravotnických technologií na světě je dnes IBM Watson. Tento stroj rozumí nejen přirozeným jazykům, ale také odpovídá na všechny otázky, které jsou kladeny (Young, 2019).

   Během šíření Covid-19 se UI používá při termovizích na letištích i jinde. Při vyšetření může pomoci rozpoznat infekci z počítačových tomografických snímků plic. V neposlední řadě byla také použita k poskytnutí údajů pro sledování šíření choroby (europarl.europa, 2021).

b) podnikání – úkoly, které dříve prováděli lidé, nyní provádějí stroje prostřednictvím robotické automatizace procesů. Do CRM platforem a analytiky jsou vkládány algoritmy strojového učení, které poskytují informace o zlepšování služeb

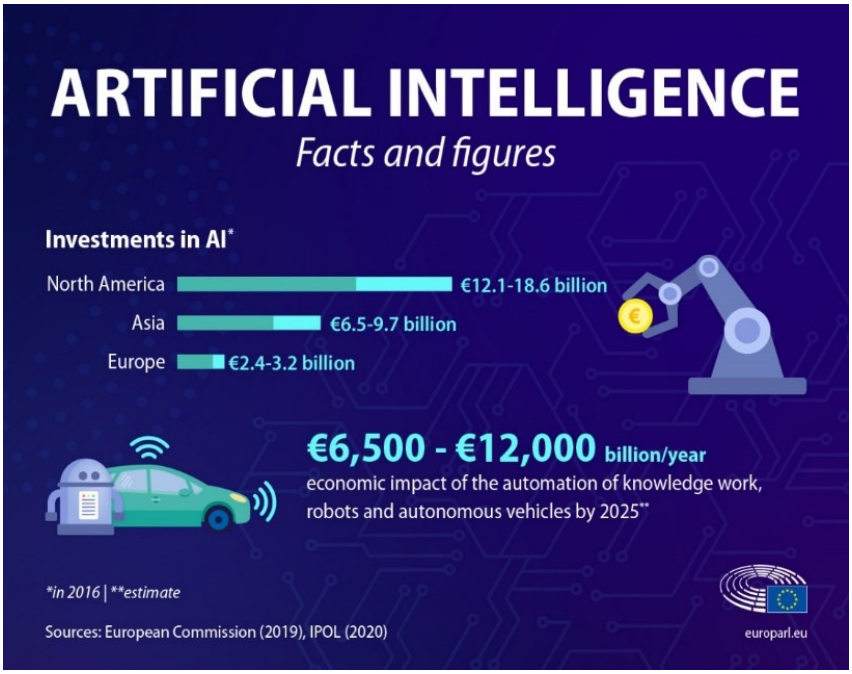
zákazníkům pro podniky. Webové stránky nyní využívají chatbota k poskytování okamžitých služeb svým zákazníkům bez lidských zásahů.

c) audiovizuální tvorba – využití umělé inteligence k vytváření videí a audiozáznamů, které jsou výsledkem hlubokého učení, vyvolalo otázky znepokojení. Použití pokročilých nástrojů umělé inteligence k vytvoření obsahu zobrazujícího událost nebo akci, která se nikdy neuskutečnila, je něco, co jistě přitáhne pozornost. Nicméně nástup Deep fake umožněný použitím algoritmů umělé inteligence není ani dobré, ani špatné. Její využití a účinek závisí výhradně na tom, kdo takovou technologii využívá a pro jaké účely. Tato technologie je často zneužívána a tím se stává spíše hrozbou (Young, 2019).

d) automobilový průmysl – samořiditelné auto (někdy nazývané autonomní automobil nebo auto bez řidiče) je vozidlo, které používá kombinaci senzorů, kamer, radaru a umělé inteligence pro cestování mezi destinacemi bez lidské obsluhy. Aby se vozidlo kvalifikovalo jako plně autonomní, musí být schopno navigovat bez lidského zásahu do předem určeného cíle po silnicích, které nebyly přizpůsobeny pro jeho použití (techtarget, 2019).

e) nakupování na internetu a cílená reklama – UI je široce využívána k poskytování individuálních doporučení lidem, a to například na základě jejich předchozího vyhledávání a nákupů nebo jiného chování na internetu.

f) kybernetická bezpečnost – systémy umělé inteligence mohou pomoci rozpoznat a bojovat proti kybernetickým útokům a jiným kybernetickým hrozbám na základě nepřetržitého vkládání dat, rozpoznávání vzorců a zpětného sledování útoků (europarl.europa[1], 2021).



Obrázek 1 Investice do umělé intelgence (europarl.europa[2].eu)

2.4 Generativní adversariální síť

Generativní adversariální síť (dále jen „GAN“) vyvinul Ian J. Goodfellow v roce 2014. GAN se skládají ze dvou neuronových síťových modelů (generátor a diskriminátor), které mezi sebou soutěží. Mohou analyzovat, zachycovat a kopírovat variace v rámci datové sady. Generátor ve své aplikaci na technologii Deep fakes vytvoří falešný videoklip a nechá diskriminátor, aby zjistil, zda je klip pravý nebo falešný. Pokaždé, když diskriminátor správně identifikuje videoklip jako falešný, dává generátoru vodítko, co nedělat při vytváření dalšího klipu. Jak se generátor zlepšuje ve vytváření falešných videoklipů, diskriminátor se zlepšuje v jejich rozpoznávání. Naopak, jak se diskriminátor zlepšuje v odhalování falešných videí, generátor se zlepšuje v jejich vytváření. Jinými slovy, diskriminátor pomáhá generátoru zjistit, zda s výsledným videem nejsou chyby. Výsledky jsou videa, která jsou tak přesvědčivá, a často nutí lidi myslet si, že jsou skutečná (Ahirwar, 2019).

Kromě škodlivých aplikací GAN v Deep fake, GAN mají poněkud užitečné praktické aplikace, které zahrnují:

a) Syntéza textu k obrázku

Generování obrázků z textových popisů je vzrušující aplikací GANů. To je užitečné ve filmovém průmyslu, protože GAN je schopen vytvořit film automaticky ze scénáře.

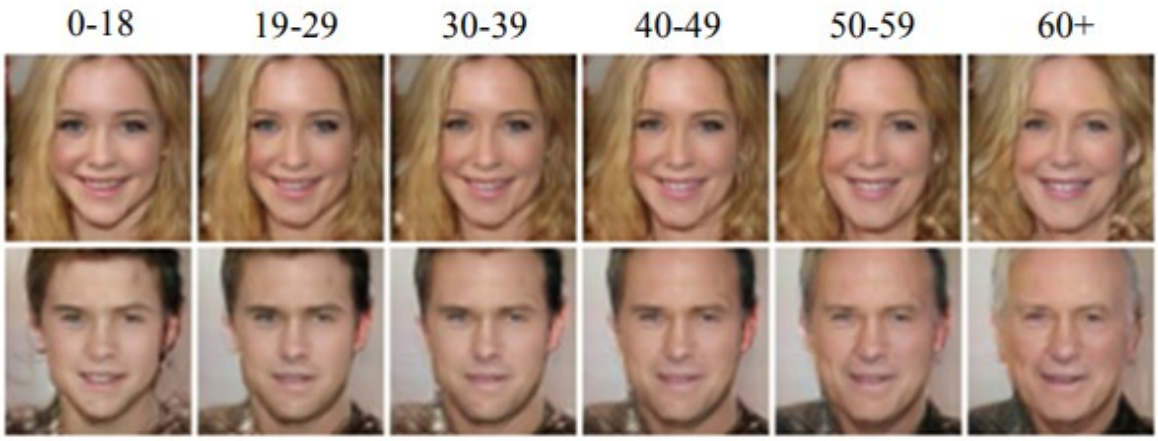
Generování videí pomocí GANů dynamiky scény lze také použít k vytváření videí jako rozšíření textu ke generování obrázků. Mohou vytvářet video obsah za kratší dobu.

b) Generování obrazu z vizuálních atributů

GAN může být použit ke generování realistických snímků poté, co je vyškolen na vizuální atributy náčrtového obrazu. Tato technologie se využívá například v kriminalistice, kdy policie může pomocí popisného náčrtu oběti automaticky vytvořit realistický obraz zloděje. Poté obrázek použije k vyhledávání ve své databázi, aby zloděje vyhledali pomocí náčrtu a markantů.

c) Stárnutí obličeje

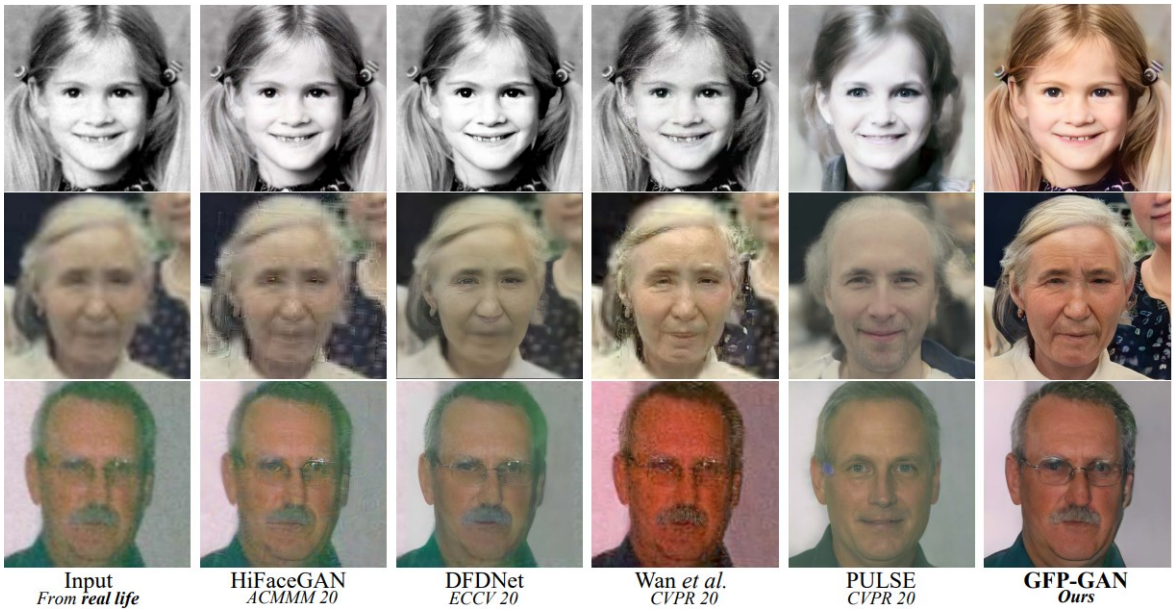
To je velmi užitečné jak pro zábavní průmysl, tak pro sledovací průmysl. Pro ověření tváří ve společnostech je to obzvláště užitečné, protože jak zaměstnanci nebo pracovníci stárnou, tak korporace nemusí měnit své bezpečnostní systémy. K vytváření snímků v různých věkových kategoriích lze použít Age Conditional Generative Adversarial Network (Age-cGAN), kterou lze následně využít k posilnění modelu pro ověřování obličeje.



Obrázek 2 Face aging (Antipov; Baccouche; Dugelay; 2017)

d) Generování obrazu ve vysokém rozlišení

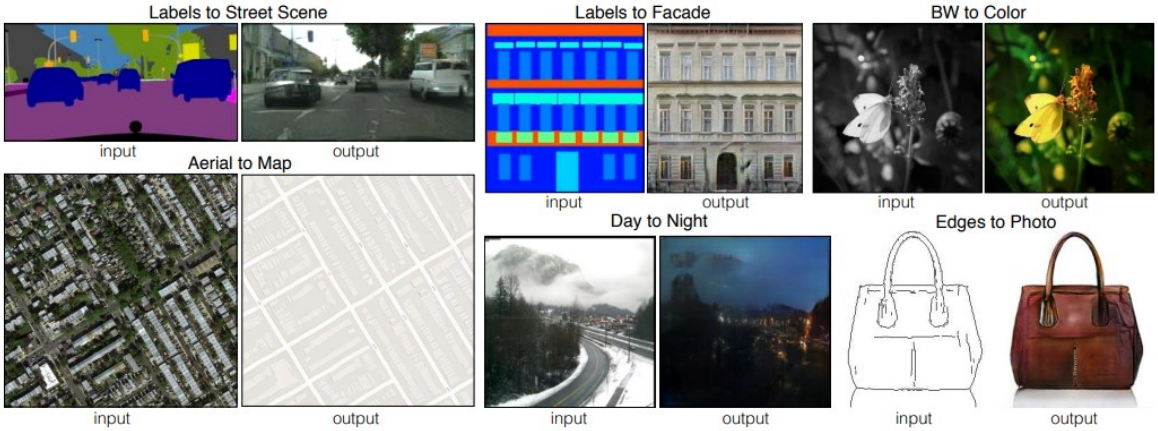
GANy mohou být použity ke generování snímků ve vysokém rozlišení, aniž by se ztratily podstatné detaily ze snímků pořízených fotoaparátem s nízkým rozlišením.



Obrázek 3 Restoration faces (Wang a kol., 2017)

e) Převod obrazu na obraz

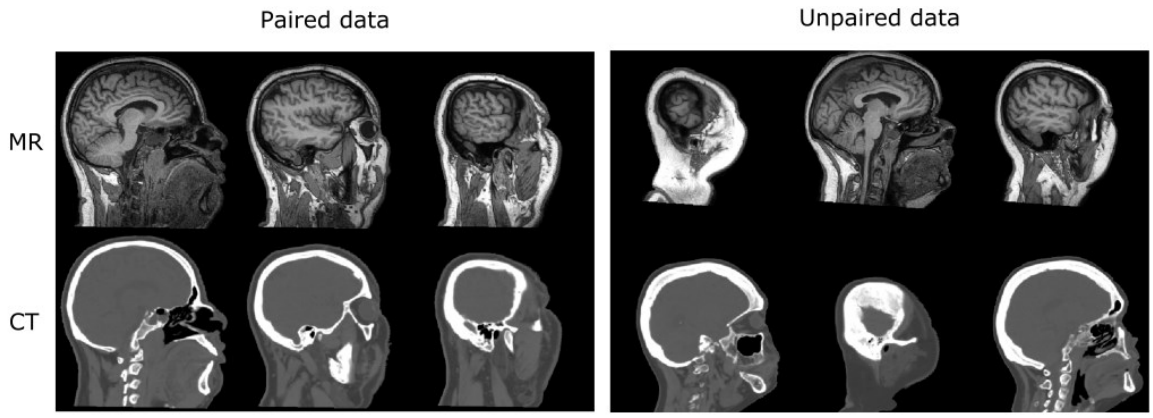
Převod obrazu na obraz lze automaticky použít k převodu snímků pořízených ve dne na snímky pořízené v noci, k převodu náčrtů na obrazy, k převodu černobílého obrazu na barevný obraz a k převodu leteckých snímků na satelitní nebo mapové snímky.



Obrázek 4 Image-to-image (Isola a kol., 2017)

f) Syntéza využívána v lékařství:

GAN lze použít v lékařské oblasti pro syntézu dat ze skenování počítačové tomografie z obrazů magnetické rezonance za účelem snížení dávky radiace (Adams, 2019).



Obrázek 5 Deep MR to CT synthesis using unpaired data (Wolterink a kol., 2017)

2.5 Technologie pro odhalení Deep fakes

Umělá inteligence může být také použita k odhalení Deep fakes, nejen k jejímu vytvoření. Studie provedené profesorem Siwei Lyu odhalila, že výměny a střídání obličeje vytváří nesrovnalosti v rozlišení obrazu, při kterých dochází při tvorbě Deep fakes. Neurální sítě zodpovědné za vynález technologie Deep fake, mohou být také použity k rozpoznání nedostatků napříč četnými snímky ve vývoji videa, který je důsledkem střídání tváří. Výzkumníků v boji pro odhalení Deep fakes v USA přibývá díky programu Media Forensics, který vede organizace Defense Advanced Research Projects Agency (DARP). Tento program podporuje výrobu technologií pro automatické testování pravosti mediálního obsahu, ať už se jedná o fotografii nebo video (Young, 2019).

Pravděpodobnost odhalování se postupem času zvyšuje a zároveň je to i díky vzájemné spolupráci na odhalování Deep fakes. Facebook, Partnership on AI, Microsoft a akademici z mnoha univerzit se spojili, aby vytvořili Deepfake Detection Challenge (DFDC)[3]. Primárním cílem výzvy je vytvořit unikátní technologii, kterou lze využít k detekci Deep fakes videí, obrázků a audio obsahu (Adams, 2019).

Tento boj vedený proti Deep fakes je obtížný, protože navzdory tomu, jak vyspělé mohou být technologie vynalezené k boji a potlačení Deep fakes, tak zároveň postupuje jejich tvorba. Připusťme, že stav ověřovacích technologií tohoto jevu nebude dokonalý. Je nešťastné, že nejsofistikovanější ověřovací metoda pro Deep fake nemusí být na stejné úrovni jako nejsofistikovanější metoda generování zmiňovaného jevu. Další nevýhodou je,

[3] odkaz ke stažení: https://dfdc.ai/login

že tato „řešení“ nemohou ovlivnit průběh čehokoliv, není-li využit v praxi. Jinými slovy, v boji proti Deep fakes nelze dosáhnout dopadu, nebudou-li tyto technologie využity, aby byly odhaleny. Propojenost internetu má propagativní povahu, která umožňuje, aby se jakýkoliv obsah, který je na něj nahrán, se dále šířil. To znamená, že Deep fake nahraný na internet nakonec dosáhne zamýšlené cílové skupiny, aniž by musel být včas detekován. S otázkou důvěry k jakémukoliv obsahu, který může být nahrán, ať už je autentický nebo falešný, bude situace stále horší, pokud existují protikladné soudy o tom, že obsah (obraz videa) je skutečný nebo vykonstruovaný. Lidé se také budou zmítat mezi přijetím Deep fake jako reálného kvůli jeho věrohodnosti nebo přijetím verdiktu softwaru, který takový obsah označuje jako falešný (Shick, 2020).

3 INFORMAČNÍ BEZPEČNOST

Informační technologie zpracovávají čím dál větší množství informací s různou kvalitou a hodnotou. Pro ochranu hodnotných informací se využívá těchto zásad:

- Přístupnost pouze pro oprávněné osoby.
- Zachování korektnosti informací.
- Zjistitelnost údajů o vytvoření, změně nebo odstranění informace.
- Dostupnost v případě potřeby využití informací.
- Zamezení nekontrolovatelnému vyzrazení či úniku (Čandík, 2010).

3.1 Triáda CIA

- Confidentiality (důvěrnost) – mlčenlivost souvisí s tím, že data organizace zůstávají soukromá. To často znamená, že přístup k datům nebo jejich modifikaci by měli mít pouze oprávnění uživatelé a procesy.
- Integrity (zásadovost) – integrita znamená, že datům lze důvěřovat. Měla by být udržována ve správném stavu, udržována tak, aby s nimi nemohlo být manipulováno a měla by být správná, autentická a spolehlivá.
- Availability (dostupnost) – stejně jako je důležité, aby neoprávnění uživatelé byli drženi mimo data organizace, data by měla být k dispozici oprávněným uživatelům, kdykoliv o to budou žádat. To znamená udržovat v chodu systémy, sítě a zařízení (Samonas a Coss, 2014).

Obrázek 6 CIA Triáda (kobalt.io)

3.2 Parkerian Hexad (rozšíření triády CIA)

V roce 2002 Donn B. Parker představil rozšířenou verzi triády CIA, která spočívala v přidání dalších tří prvků.

Obrázek 7 Parkerian Hexad (cs.lewisu.edu)

- Possession/Control (vlastnictví/kontrola) – hlavní myšlenkou je, že důvěrná data mohou být vlastněná a kontrolovaná neoprávněnou osobou nebo skupinou, aniž by se skutečně porušila důvěrnost (např. pokud zloděj vlastní zapečetěnou obálku s cizím obsahem, do doby otevření, tak se nejedná o porušení důvěrnosti (podkapitola 3.1).
- Authenticity (autenticita/pravost) – internet nám všem umožnil dělat prakticky cokoliv a vše z našich domovů. Díky těmto možnostem a mnoha dalším byly vyvinuty technologie poskytující zákazníkům důvěru a vědomí, že stránky, které navštěvujeme jsou legitimní a komunikace je bezpečná (např. předání kódu prostřednictvím SMS nebo e-mailu).
- Utility (užitečnost) – užitečnost je popisována jako zásadní součást tohoto modelu, která nemůže být podceňována. Jedná se data, které když nejsou v užitečném stavu nebo formě jsou v podstatě nepoužitelná (např. pokud dojde k zašifrování a neznáme klíč, data jsou dostupná, ale nejdou využít) (Pender-Bey, 2012).

4 DEEP FAKES A FAKE NEWS V KONTEXTU INFORMAČNÍ BEZPEČNOSTI Z HLEDISKA LEGISLATIVY

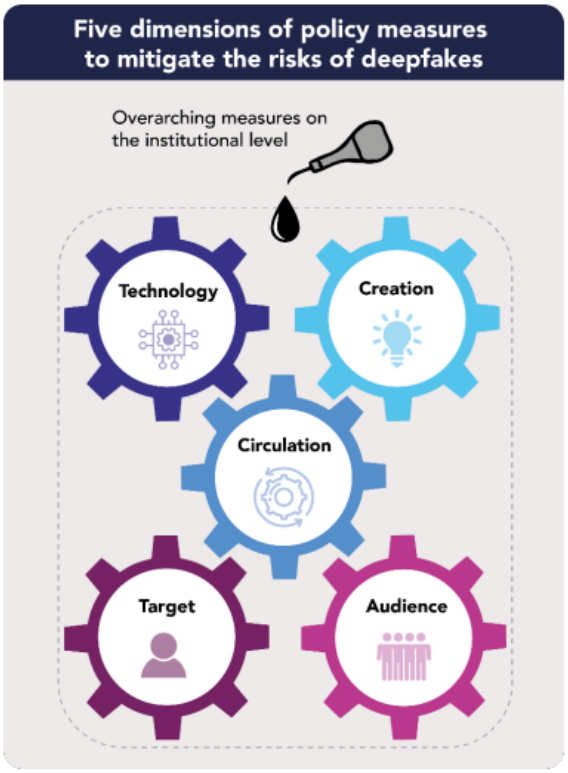
Problematika Deep fakes a Fake news v současné době není zatím legislativně upravena v České republice.

4.1 Problematika Deep fakes na úrovni Evropské politiky

Evropský parlament vydal tuto studii v červenci 2021, ve které je mimo jiné vysvětlen pojem Deep fakes, viz. Kapitola 2. V reakci na možná rizika a obavy tato zpráva hodnotí technické, společenské a regulační aspekty Deep fakes. Hodnotí využití základních technologií pro tvorbu Deep fakes a upozorňuje, že se rychle vyvíjejí a jsou den ode dne levnější a přístupnější. K rychlému rozvoji a šíření Deep fakes dochází i na základě měnícího se mediálního systému. Hodnocení rizik spojených s Deep fakes ukazuje, že mohou mít psychologickou, finanční a společenskou formu, včetně kaskádových jevů a jejich dopady mohou sahat od jednotlivce až po celou společnost. Dále uvádí konkrétní regulační nedostatky v jednotlivých směrnicích:

- Regulační rámec pro UI.
- Obecné nařízení o ochraně údajů.
- Autorské právo a právech s ním souvisejících.
- Směrnice o elektronickém obchodu.
- Zákon o digitálních službách.
- Směrnice o audiovizuálních médiích.
- Kodex praxe v oblasti dezinformací.
- Akční plán proti dezinformacím.
- Akční plán pro demokracii.

Ve studii je tato problematika konkrétně rozebrána a zároveň zkoumána i regulace v zemích mimo EU (USA, Čína, Indie, Taiwan). Závěr studie uvádí identifikaci pět dimenzí „životního cyklu“ Deep fake, které by tvůrci politik, mohli vzít v úvahu při prevenci a řešení nepříznivých dopadů Deep fakes. (europarl.europa[3], 2021).



Obrázek 8 "Životní cykly Deep fake“ (europarl.europa[3].eu)

4.2 Možnosti zneužití Deep fakes v ochraně obyvatelstva

Hrozby zneužití Deep fakes lze rozdělit do čtyř kategorií:

a) společenské (rozdmýchávání sociálních nepokojů a politické polarizace)

b) právní (falšování elektronických důkazů, krádež identity)

c) osobní (obtěžování a šikana, nekonsenzuální pornografie)

d) kybernetická bezpečnost (vydírání, podvody a manipulace s finančními trhy)

Padělané pasy s Deep fake fotografií bude obtížné odhalit. Ty by totiž mohly být využity k usnadnění mnoha dalších trestných činů, od krádeží identity, přes obchodování s lidmi, až po nedovolené přistěhovalectví a nelegální pohyb teroristů. Phishing by se mohl posunout na novou úroveň, pokud podvodná zpráva bude obsahovat video nebo hlas důvěryhodného přítele. Phishingové útoky BEC, které pronikají do organizací, by mohly být podpořeny obrazovým sdělením a hlasem totožným se skutečným hlasem výkonného ředitele organizace. Tím by úspěšnost zmiňovaného druhu útoku dosáhla samozřejmě vyšší úrovně (securityweek, 2022).

4.3 První zmínka varování na mezinárodní úrovni

Dne 19. 11. 2020 byla zveřejněna první vypracovaná zpráva od European Police Office (EUROPOL), institutu OSN pro výzkum meziregionálního zločinu a spravedlnosti (UNICRI) a agentury Trend Micro, která varovala před využitím umělé inteligence pro páchání kriminality. Dokument uvádí výhody využívání UI, ale také možná rizika. Pracovníkům donucovacích orgánů, tvůrcům politik a nevládním organizacím byly prostřednictvím tohoto dokumentu předány informace a navrhnuta doporučení, jak tato rizika zmírnit. Deep Fakes bylo zmíněno jako nejznámějším možná hrozba zneužití UI. Zpráva došla k závěru, že kyberzločinci budou využívat UI novým způsobem útoku, tudíž bude potřeba nových technologií pří prověřování účinku (např. využití v dezinformačních kampaní nebo za účelem vydírání) (europol.europa, 2020).

4.4 Orgány zajišťující informační bezpečnost

Bezpečnost je založena na důvěře. Deep fakes poskytují důvěru tam, kde by žádná důvěra existovat neměla.

4.4.1 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB) je ústřední správní orgán pro kybernetickou bezpečnost. Zahrnuje ochranu utajovaných informací v informačních a komunikačních systémech a také se zabývá problematikou veřejně regulované služby navigačního systému Galileo (nukib[1], 2022).

Mezi hlavní činnosti úřadu můžeme zahrnout:

- Práci vysoce odborných specialistů v oblasti kybernetické bezpečnosti a kryptografické ochrany.
- Práci vládního bezpečnostního týmu, tzv. Vládní CERT České republiky (GovCERT.cz).
- Spolupráci s ostatními CERT a CSIRT bezpečnostními týmy v ČR a ve světě.
- Přípravu národních bezpečnostních standardů v oblasti kybernetické bezpečnosti.
- Stanovení bezpečnostních standardů pro informační systémy v našem státu, tzv. kritická informační infrastruktura.

- Stanovení ochrany utajovaných informací v oblasti informačních a komunikačních systémů.
- Přípravu zákonů a podzákonných norem v oblasti kybernetické bezpečnosti
- Vlastní výzkum a vývoj atd. (nukib[2], 2022).

Česká republika se umístila v roce 2021 na 3. místě v největším cvičení kybernetické bezpečnosti na světě. Národní tým ČR tvořili zástupci státního a soukromého sektoru i akademické sféry. Účastnilo se 22 týmů z celého světa a cvičení se nazývalo Locked Shields 2021, pořádalo ho NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Česká republika byla koordinována Národním úřadem pro kybernetickou a informační bezpečnost (nukib[3], 2022). Cvičení probíhalo i letos v roce 2022, ovšem zástupci ČR již neobhájili 3. místo a toto místo získal estonsko-gruzínský tým, druhé místo obsadil tým polsko-litevský a cvičení vyhrál tým z Finska (ccdcoe, 2022).

4.4.2 Vládní zmocněnec pro oblast medií a dezinformací

Vláda České republiky přijala prohlášení, kterým se ostře vymezila proti hybridnímu působení proti zájmům ČR, související s agresí Ruské federace proti Ukrajině. Deklarovala v něm mimo jiné, že v aktuální krizové situaci nehodlá šíření dezinformací proti zájmům ČR a partnerů v NATO a EU tolerovat (vlada[1], 2022).

Vláda dne 2. března 2022 rozhodla usnesením č. 153 o zřízení funkce zmocněnce pro oblast medií a dezinformací, který bude působit při Úřadu vlády jako poradní orgán vlády a jeho úkolem bude komunikace s příslušnými ministry a vedoucími pracovníky orgánů státní správy a také součinnost se složkami státu, které se zabývají oblastmi médií a dezinformací. Vláda 23. března 2022 na tento post jmenovala Ing. Michala Klímu (vlada[2], 2022).

4.5 Předsednictví České republiky v Radě Evropské unie

Česká republika dne 1.7.2022 převzala předsednictví v Radě Evropské unie. České předsednictví bude zaměřeno na 5 vytyčených pilířů. Jeden z těchto pilířů je zaměřen na posílení evropských obranných kapacit a bezpečnost kybernetického prostoru, kde se i mimo jiné uvádí boj proti dezinformacím v rámci řešení na mezinárodní úrovni (czech-presidency.consilium.europa, 2022).

DÍLČÍ ZÁVĚR

Teoretická část práce se zabývá problematikou Deep fakes a s tím souvisejícím jevem Fake news. V první řadě byla vysvětlena základní terminologie jako propaganda, misinformace a hoax, které se také využívají pro zmatení osob. Dále jsme si ve stručnosti uvedli historii Deep fakes, zabývali se umělou inteligencí, určili její kategorizaci a následní využití. Vysvětlili jsme si GAN a ukázali jsme si užitečné praktické aplikace, např. na stárnutí obličeje nebo syntézu, která je využívána v lékařství, a také jsme se zabývali technologiemi odhalující Deep fakes. V neposlední řadě jsme si uvedli, jaká je informační bezpečnost na úrovni České republiky a Evropské politiky. V teoretické části jsme si Deep fakes vysvětlili, jmenovali několik příkladů, abychom na ni mohli navázat praktickou částí diplomové práce a navrhnout scénář hrozby Deep fakes v ochraně obyvatelstva a také zjistit, jaké je povědomí tohoto jevu mezi širokou veřejností napříč věkem a vzděláním.

II. PRAKTICKÁ ČÁST

5 SCÉNÁŘ HROZBY DEEP FAKES V OCHRANĚ OBYVATELSTVA

V kapitole „Scénář hrozby Deep fakes v ochraně obyvatelstva“ se budeme věnovat tvorbě několika scénářů, které můžou představovat hrozbu napříč různými odvětvími.

5.1 Tvorba vlastního scénáře

Na základě poznatků z rešeršní práce uvedené v teoretické části práce byl navržen následující scénář hrozby Deep fakes v ochraně obyvatelstva. Scénář hrozby Deep fakes má demonstrovat negativní a nebezpečný vliv působení na bezpečnost (nejen) České republiky. Studovaný scénář nevychází z reálné situace, ale skládá se z potenciálně možných případů využitých pro tento scénář.

Navrhuji katastrofický scénář, při kterém by došlo k systematickému šíření Deep fakes jako hrozby vyvolávající synergický účinek či dominový efekt. Vycházím z předpokladu, že tvorba Deep fake videa již není pro obyčejné uživatele výpočetní technologie nereálná. Myslím, že každý člověk, kdo má zájem se může stát tvůrcem Deep fakes, které se může snadno a nekontrolovatelně šířit po sociálních sítích, e-mailech a dalších kanálech. Následkem by bylo ovlivnění mysli, či chování obyvatel. Tímto navrženým scénářem by mohlo dojít k vyvolávání strachu, oslabení morálky a případné bezmocnosti u obyvatel státu, mohlo by dojít i na hmotné škody.

Scénář na úrovni České republiky

Během současného předsednictví České republiky v Radě Evropské unie, by případné šíření Deep fakes s předsedou vlády nebo jinými vládními činiteli mohlo způsobit značnou nedůvěru ve stát u obyvatel země a mezi zástupci ostatních států Evropské unie, což by mohlo značně ohrozit naši bezpečnost. Mohly by se například šířit smyšlené zprávy o korupci, které by dehonestovaly stát. Dále by mohly být využity aplikace s využitím klonování hlasu našeho předsedy vlády, jehož výroky by se staly nástrojem k vyvolání strachu nebo nenávisti u obyvatel státu a celé EU. Takové jednání by ohrozilo důvěru v předsedající stát, byl by také poškozen samotný předseda vlády, či další vládní činitelé a rovněž celá politická strana, ve které je předseda vlády členem.

Scénář na úrovni ekonomiky

V návaznosti na předchozí scénář by na mezinárodní úrovni mohlo nastat embargo mezi dotčenými státy i případné přerušení dodávek nerostných surovin, díky čemuž by se ohrozila i celá ekonomika České republiky. Následkem toho by vznikly nepokoje, rabování, krádeže,

vandalismus a mohla by být ovlivněna finanční situace občanů způsobená touto krizí. Záleželo by na závažnosti Deep fakes, které by bylo vypuštěno „do světa“.

Scénář na úrovni náboženství

Deep fakes se může objevit i v různých náboženstvích, kdy by mohlo dojít ke zneužití víry věřících. Vzpomeňme si na teroristický útok na redakci časopisu Charlie Hebdo, ke kterému došlo v roce 2015 na základě otisknutí zesměšňující karikatury Mohameda. Následkem toho bylo násilí na nevinných lidech, z čehož můžeme usuzovat, že problematika Deep fakes se jeví jako velmi závažný problém a může ohrožovat i prvky kritické infrastruktury, a tedy bezpečnost státu.

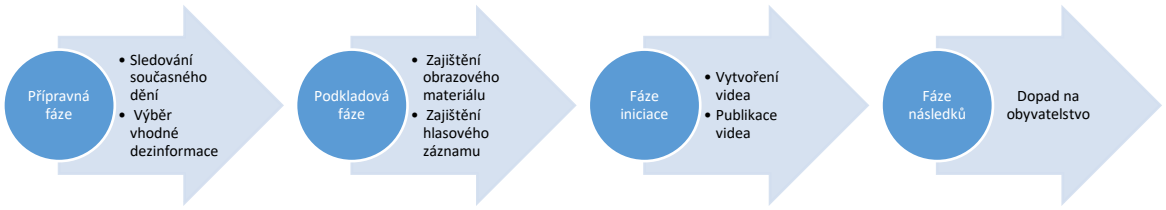
Scénář na úrovni vědy

Deep fakes lze zkrátka využít (nebo zneužít) v jakémkoli odvětví. Stoupá rovněž větší obliba a využívání umělé inteligence, např. v Japonsku nebo USA napříč různými odvětvími, např. ve zdravotnictví, automobilovém průmyslu, v cílené reklamě nebo dokonce i v kybernetické bezpečnosti (viz. podkapitola 2.3). Pomocí umělé inteligence lze v dnešní době již dokončit rozepsanou knihu, vytvořit obraz umělce či vytvořit obrázek na základě textu. Nelze tedy přisuzovat pouze negativní vliv umělé inteligence.

Scénář na úrovni ochrany duševního zdraví obyvatel

Nejděsivější „zbraní“ Deep fakes považuji vyvolání nedůvěry ve vlastní smysly, na které během života spoléháme. Tato skutečnost oslabuje naši schopnost uvažovat a zároveň vyvolává pocity strachu, beznaděje a vzbuzuje pochyby. Šíření Deep fakes záměrně tyto pocity vyvolává, cílí na naše slabiny, může vést dlouhý „mentální boj“ a oslabovat víru v samotnou pravdu. Následkem toho by mohly být stávky lidu, demonstrace, které by se zároveň mohly stát cílem nebezpečného teroristického útoku. Měli bychom se snažit být na pozoru a důkladně selektovat věrohodné zdroje, ze kterých přijímáme informace a pokusit se využívat kritické myšlení.

Tento scénář se v dnešní době nemusí zdát úplně nereálný. Dříve bychom něčemu takovému nemuseli věřit a jev jako je Deep fakes bychom mohli považovat za úplnou fikci, ale při neúprosně rostoucím technologickém pokroku už je možné opravdu ledacos.



Obrázek 9 Diagram scénáře zneužití Deep fakes (vlastní)

Na diagramu výše jsou zobrazeny fáze scénáře zneužití Deep fakes. V přípravné fázi sledujeme současné dění, vybíráme vhodné dezinformace, v další podkladové fázi zajišťujeme obrazový materiál a hlasový záznam. Ve fázi iniciace je tvořeno video a následně jej publikujeme. V poslední fázi následků sledujeme dopad na obyvatelstvo (viz. kapitola 4.2, kde jsou uvedeny příklady).

5.2 Tvorba vlastního Deep fake videa

Při práci s GAN se využívají tzv. „datasets“ (dále jen „souhrny dat“), která se využívají i při odhalování Deep fakes. Dají se nalézt mimo jiné[4], kde jich je nespočet. V případě Deep fakes se jedná převážně o souhrn fotek/videí, ale také i zvukových stop. Tyto souhrny dat jsou vytvořeny za účelem lepší a snazší spolupráce při vytváření kvalitnějších softwarů. Ke stažení jsou také například CT snímky rakovin plic[5], rozdělení věkových kategorií dle věku[6] a jiné (viz kapitola 2.4).

[4] https://datasetsearch.research.google.com/
[5] https://github.com/ymirsky/CT-GAN
[6] https://datasetsearch.research.google.com/search?src=2&query=facial%20age&docid=L2cvMTFqbno4ejF0Nw%3D%3D

Jednotlivé softwary jsou volně dostupné například na github.com. Pro jejich lepší a snazší využití je znalost programovacích jazyků výhodou. Další variantou využití může být colab.research.google.com, kde nalezneme snazší variantu užívání otevřeného softwaru. Za pomocí sešitu, ke kterému se připojíme, stačí pouze stisknout v předvyplněných buňkách „Spustit akci“ a můžeme využít daný software. Této metody jsem využil i já při tvorbě vlastního Deep fake videa, jelikož chci poukázat na poměrně snadnou metodu vytvoření Deep fake u které stačí pouze jedna fotografie dané osoby.

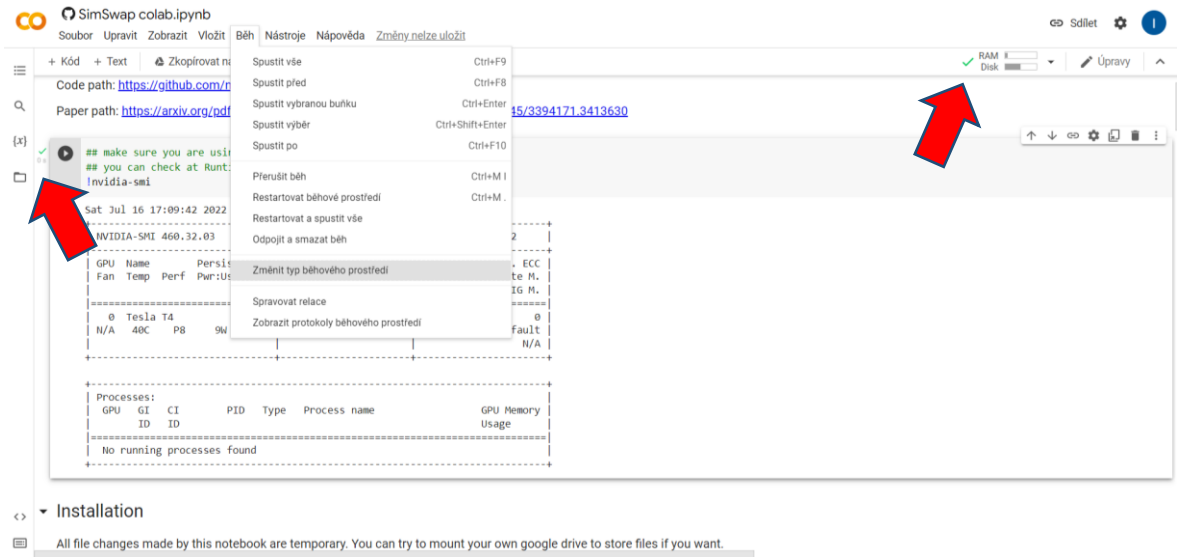
5.3 Postup tvorby Deep fake

Prostředků, pomocí kterých lze vytvořit Deep fake je mnoho. Já jsem si zvolil jednodušší variantu, abych poukázal na snadné zneužití této techniky. Při tvorbě vlastního videa jsem využil dostupného sešitu na rozhraní[7]. Použití je snadné, stačí dodržovat níže uvedený postup.

Obrázek 10 Připojení k danému sešitu (colab.research.google.com[1])

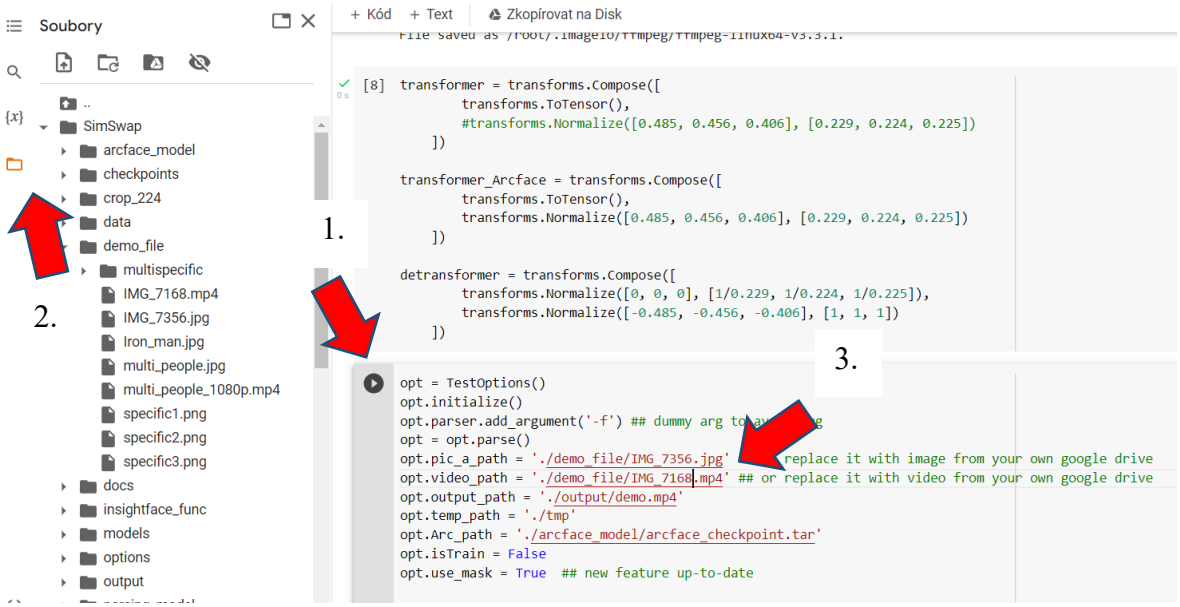
Nejprve se musíme připojit (viz 1. krok na obrázku 10) a následně stiskneme „Spustit buňku“ (viz 2. krok). Tento krok se spuštěním dané buňky budeme opakovat ještě 7krát.

7 https://colab.research.google.com/github/neuralchen/SimSwap/blob/main/SimSwap%20colab.ipynb#scrollTo=wwJOwR9LNKRz



Obrázek 11 Úspěšné připojení k sešitu (colab.research.google.com[1])

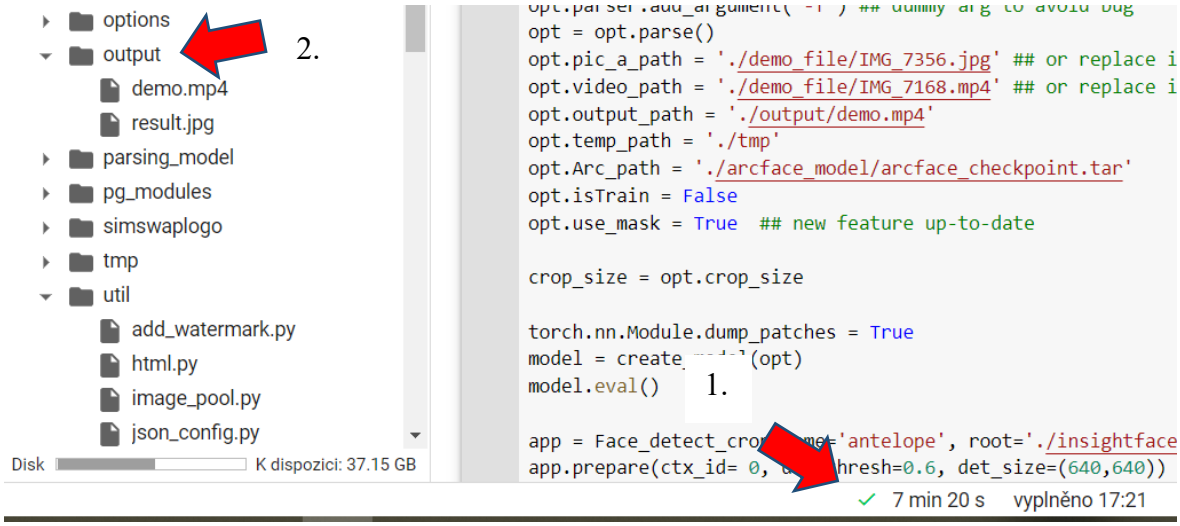
Po úspěšném připojení musíme zkontrolovat typ běhového prostředí, kde vyberete GPU. Následně spustíme všechny ostatní buňky (viz. 2. krok na obrázku 11). Pamatujme však, že každá spuštěná buňka se načítá rozdílnou dobou trvání a musíte vyčkat do úplného načtení (tedy 100 %).



Obrázek 12 Nahrání souborů (colab.research.google.com[1])

U tohoto kroku se pozastavíme, než spustíme danou buňku. Rozklikneme si složku se soubory (oranžová složka na obrázku 12) a otevřeme složku „demo_file“ ve složce „SimSwap“, kam přetáhneme požadované soubory, ze kterých chceme vytvořit Deep fake video. Následně přepíšeme (u kroku č. 3) názvy souborů na ty, které chceme využít. V mém

případě se jedná o fotografii IMG_7356.jpg a video IMG_7168.mp4. Následně můžeme stisknout „Spustit buňku“ a vyčkat na zhotovení výsledného videa.

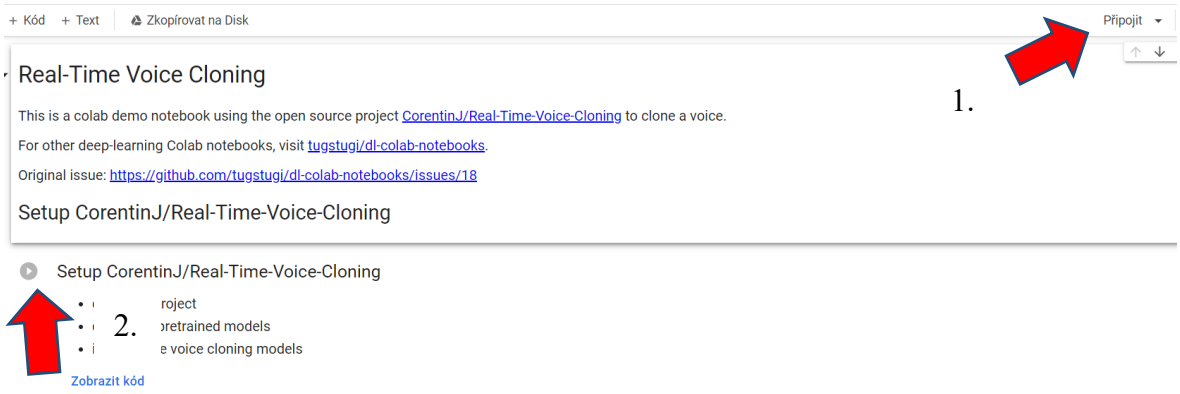


Obrázek 13 Zhotovené Deep fake (colab.research.google.com[1])

Po uplynutí potřebné doby na tvorbu Deep fake (7 minut a 20 sekund) v mém případě nalezneme námi vytvořené Deep fake video ve složce „output“ s názvem „demo.mp4 (viz. 2. krok na obrázku č. 13).

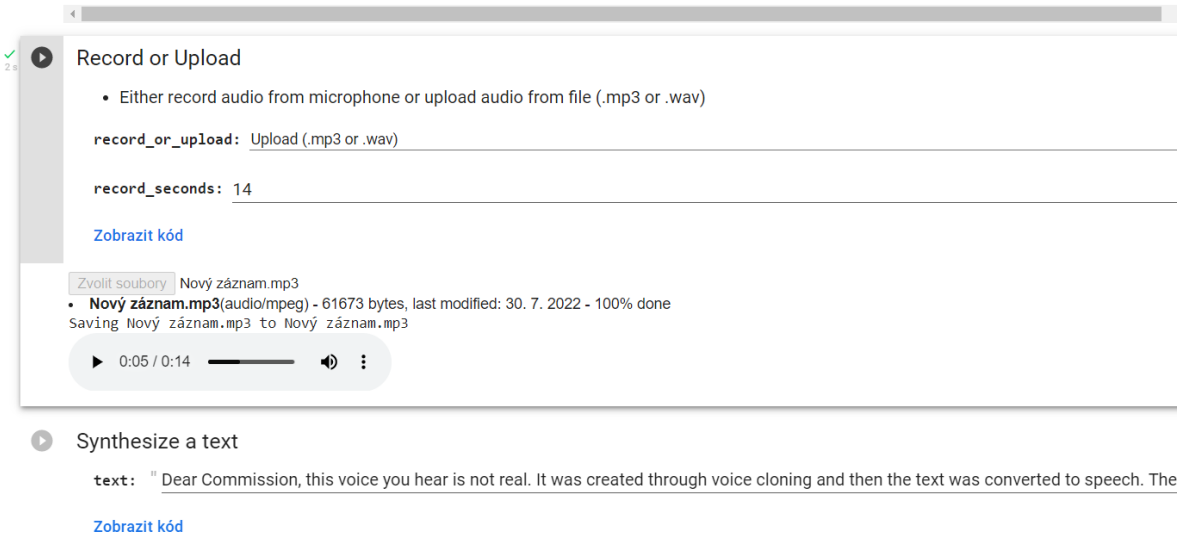
5.4 Postup klonování hlasu

Při vytvoření Deep fake podle návodu uvedeného v podkapitole 6.1 nastává otázka, zda chceme změnit i hlas. Máme na výběr z mnoha možností, buď originální audio ponecháme, dále můžeme využít přesvědčivého dabéra, anebo využijeme pokročilé klonování hlasu. Při tvorbě Deep fake videa jsem se snažil nalézt snazší a zároveň kvalitní variantu, rovněž tomu je i u klonování hlasu, kdy jsem využil možnost, díky které může využít klonování hlasu „každý“. Pomocí sešitu pro syntézu textu na řeč (TTS, text-to-speech), bylo nutné nejprve extrahovat hlas osoby, kterou chceme využít pro sdělení informací ve vlastním Deep fake videu.



Obrázek 14 Připojení k sešitu (colab.research.google.com[2])

Připojíme se s k hostovanému běhu (viz. krok 1 na obrázku 13) a následně stiskněme „Spustit buňku“ (viz. krok 2 na obrázku 14).



Obrázek 15 Nahrání hlasové nahrávky (colab.research.google.com[2])

Zvolíme, že chceme nahrát hlasový soubor a dále zvolíme délku souboru. Následně napíšeme text, který chceme naklonovat a stiskneme „Spustit buňku“. Tento krok se musí opakovat vícekrát pro lepší kvalitu výsledné zvukové nahrávky.

Pro vytvoření Deep fake byly využity prostředky, které nemusí být použity stejným způsobem pro uskutečnění mého scénáře uvedeného v kapitole 5. Existuje nespočet metod pro vytvoření Deep fake nebo pro klonování hlasu, které jsou propracovanější, ale spíše jsem chtěl poukázat na jejich snadné používání. V důsledku technologického rozvoje budou nejspíš tyto softwary kvalitnější a automatizované, tudíž „každý“ bez větších dovedností bude moct vytvořit těžko rozeznatelné Deep fake. V případě, kdy chcete vytvořit takřka

dokonalé Deep fake video i se zvukovou nahrávkou, tak jsou programátorské znalosti výhodou, ale existuje mnoho školících videí, jak správně postupovat.

Využil jsem pro vytvoření Deep fake sebe a kamaráda, který mi dal svolení k tvorbě videa. V případě zneužití Deep fakes se nedá svolení očekávat a může ho využít kdokoli. V případě spojení obrazu a hlasu osoby za účelem vytvoření Deep fakes lze vygenerovat zcela syntetická média, ze kterých může vyplynout mnoho negativních dopadů pro společnost.

6 DOTAZNÍKOVÉ ŠETŘENÍ

V této části diplomové práce se budeme zabývat kvantitativním výzkumem pomocí metody dotazníkového šetření. Dotazník obsahuje 18 otázek: 3 uzavřené (identifikační), 10 uzavřených, 3 polootevřené a 2 otevřené. Dotazník probíhal anonymně a byl sestaven za využití portálu Survio. Sběr dat probíhal prostřednictvím sociálních sítí, kde se potýkáme s nejčastější formou šíření Fake news a Deep fakes. Celkem dotazník navštívilo 469 osob, avšak potřebný čas k vyplnění si udělalo 207 respondentů.

Průzkum byl proveden formou dotazníkového šetření, kdy po sesbírání dat byly vytvořeny přehledné grafy pomocí Microsoft Excel a následně okomentovány zjištěné výsledky.

6.1 Hypotézy

Hypotézy byly definovány na základě

H1 Povědomí o Fake news bude u respondentů vyšší než znalost Deep fakes.

H2 Předpokládáme, že lidé s vyšším dosaženým vzděláním mají větší povědomí ohledně dané problematiky, jelikož se jedná převážně o problematiku probíranou na vysokých školách.

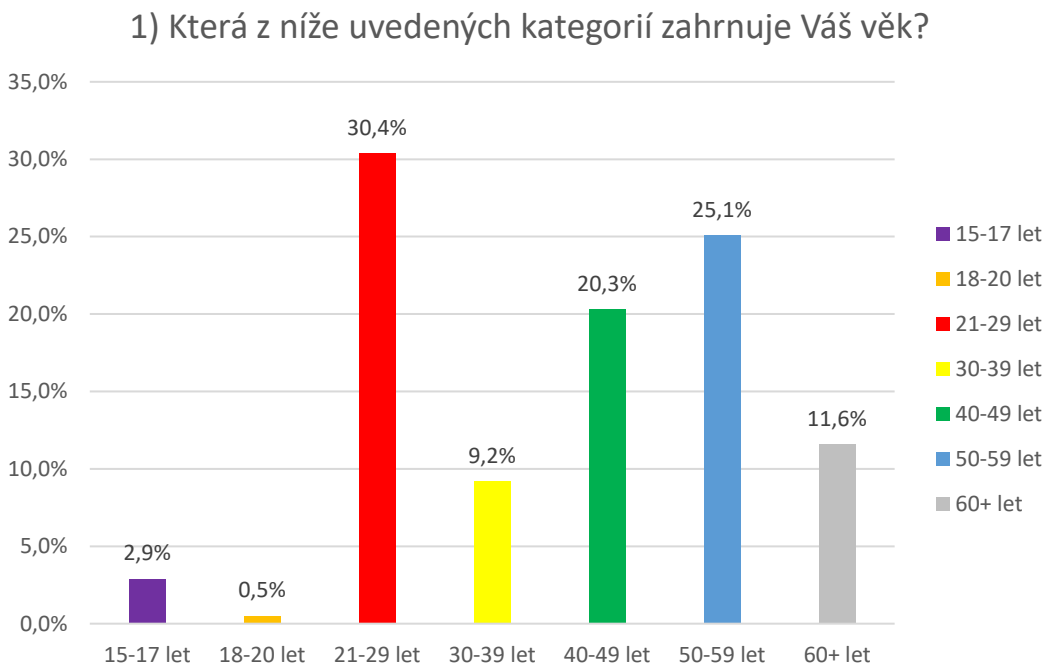
H3 Předpokládáme, že respondenti nebudou schopni rozeznat originály fotek od Deep fakes.

H4 Respondenti nepovažují problematiku Deep fakes a Fake news za hrozbu.

Cílem dotazníkového šetření bylo zjistit povědomí obyvatel o problematice Fake news a Deep fakes a také vyhodnotit, zda je obyvatelé považují za hrozbu.

6.2 Výsledky dotazníkového šetření

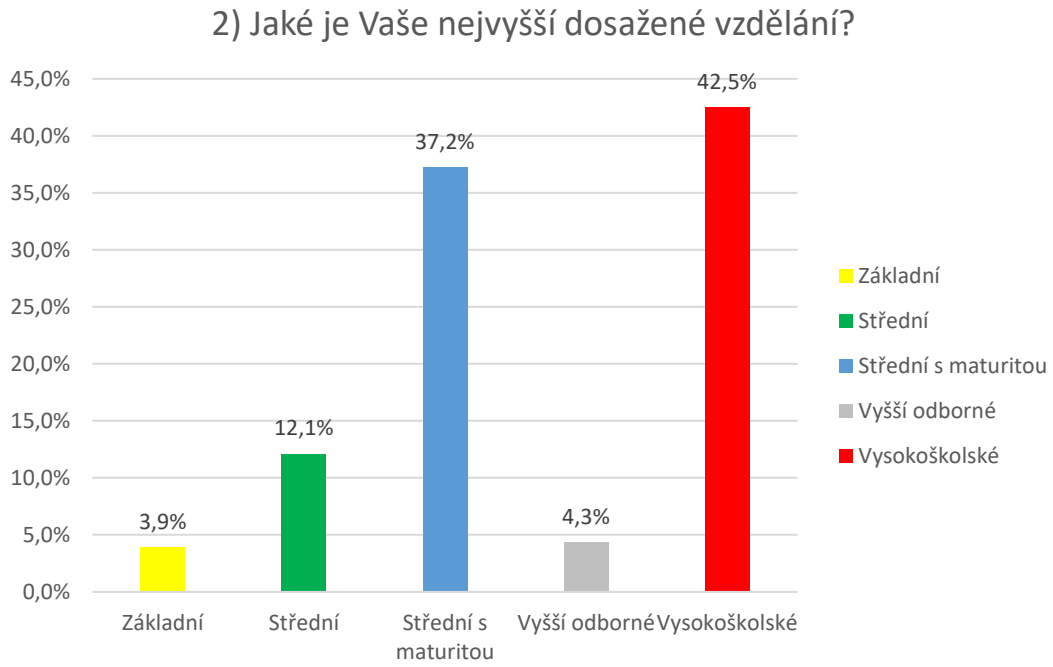
Výsledky odpovědí na 1. otázku, která se týkala věkových kategorií respondentů je znázorněna na obrázku 16.



Obrázek 16 Grafické zobrazení odpovědí na 1. otázku (vlastní)

Dotazník vyplnilo v kategorii 15-17 let 6 respondentů (2,9 %), v kategorií 18-20 let 1 respondent (0,5 %) a nejpočetnější skupinou byla kategorie 21-29 let s 63 respondenty (30,4 %). Další zvolenou kategorií 30-39 let tvořilo 19 respondentů (9,2 %), třetí nejpočetnější skupinou byla 40-49 let kategorie se 42 respondenty, druhou nejvíce zastoupenou kategorií byla 50-59 let s 52 respondenty (25,1 %). Poslední věkovou kategorií 60+ tvořila skupina 24 respondentů (11,6 %).

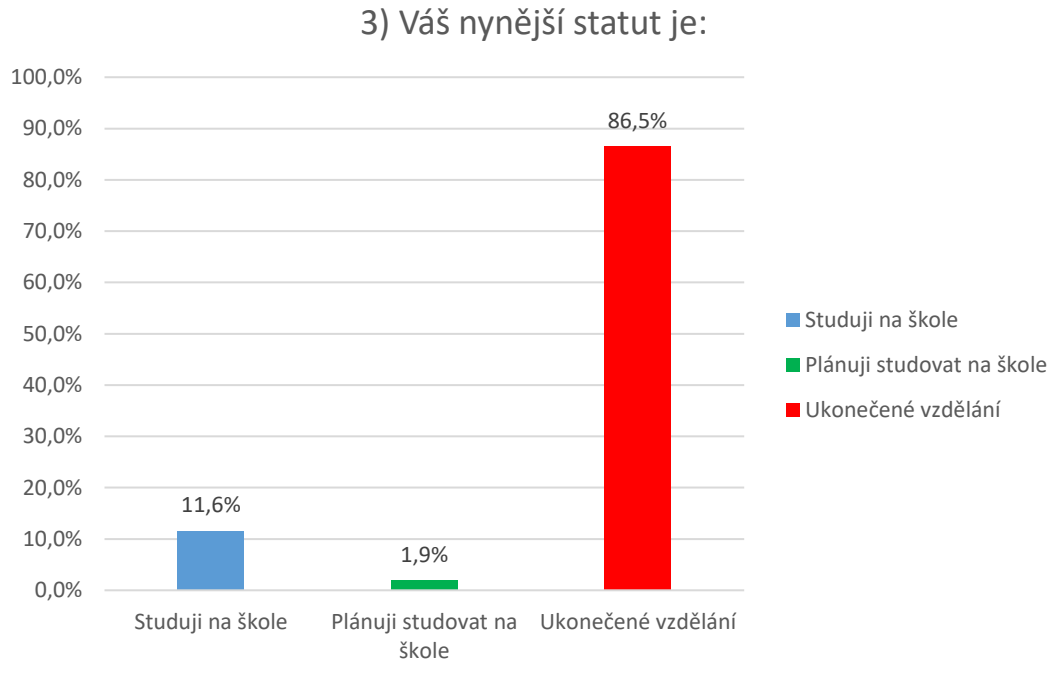
Vyhodnocení otázky č. 2: Druhá otázka byla identifikační se zaměřením na nejvyšší dosažené vzdělání u respondentů. Výsledky jsou zobrazeny na obrázku 17.



Obrázek 17 Grafické zobrazení odpovědí na 2. otázku (vlastní)

Vyhodnocení výše uvedené otázky sloužilo společně s vyhodnocením otázek č. 4 a č. 8 k potvrzení či vyvrácení hypotézy H2, která bude předmětem diskuze.

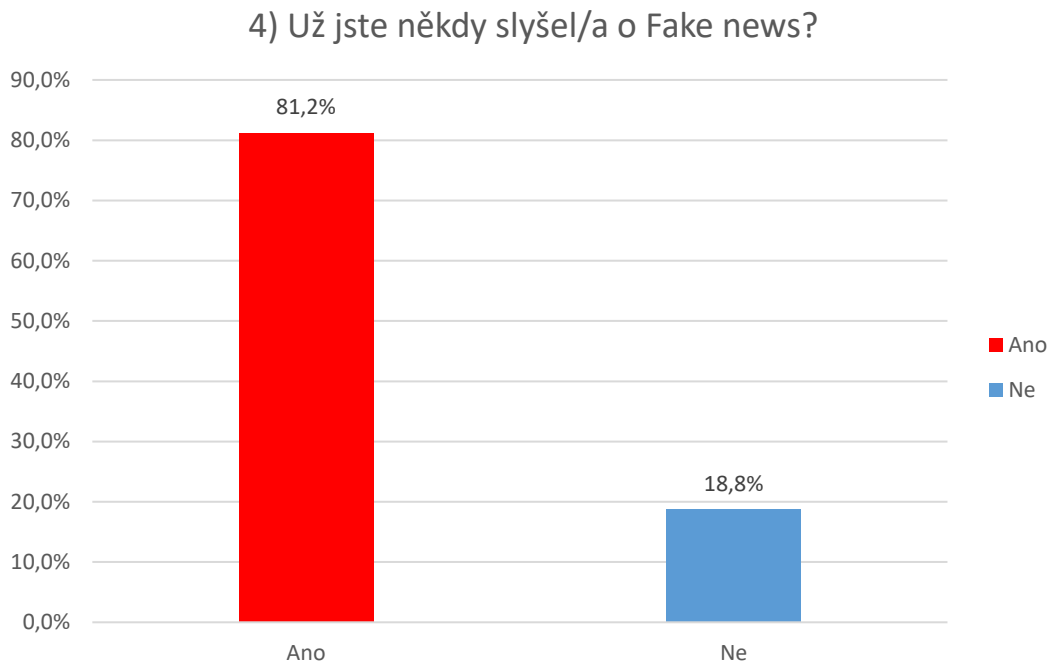
Vyhodnocení otázky č. 3: Třetí otázka byla identifikační. Výsledky jsou zobrazeny na obrázku 18.



Obrázek 18 Grafické zobrazení odpovědí na 3. otázku (vlastní)

Otázka sloužila sekundárně k vyhodnocení otázky č. 2

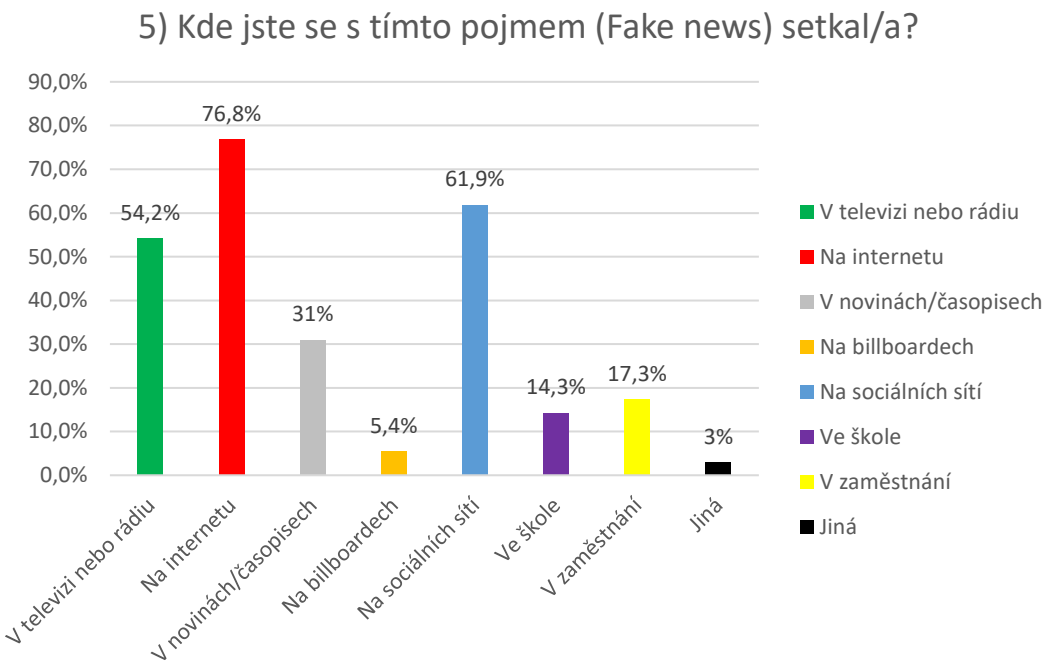
Vyhodnocení otázky č. 4: Při odpovědi na čtvrtou otázku bylo využito logické pravidlo. V případě zvolení odpovědi „Ano“ pokračovali respondenti na následující otázku, ovšem v případě odpovědi „Ne“ byl dotazovaný přesunut na otázku č.7, kde mu byl tento pojem vysvětlen. Výsledky jsou zobrazeny na obrázku 19.



Obrázek 19 Grafické zobrazení odpovědí na 4. otázku (vlastní)

Celkem 168 respondentů (81,2 %) slyšelo o Fake news a zbylých 39 (18,8 %) dotázaných se s pojmem nesetkalo.

Vyhodnocení otázky č. 5: Díky logickému pravidlu na tuto otázku odpovídalo 168 respondentů. Výsledky jsou zobrazeny na obrázku 20.



Obrázek 20 Grafické zobrazení odpovědí na 5. otázku (vlastní)

Otázka měla za úkol zjistit, kde se dotazovaní setkali s problematikou Fake news. Při výběru možnosti „Jiná“ (3 %) bylo uvedeno:

- v divadle,
- v běžné konverzaci,
- od syna.

Vyhodnocení otázky č. 6: Otázka byla otevřená a měla za úkol zjistit reálné povědomí o znalosti Fake news a zda respondenti umí správně i tento pojem vysvětlit. Na šestou otázku rovněž odpovídalo 168 respondentů, tedy ti, kteří se setkali s Fake news. Výsledky jsou zobrazeny formou tabulky 1.

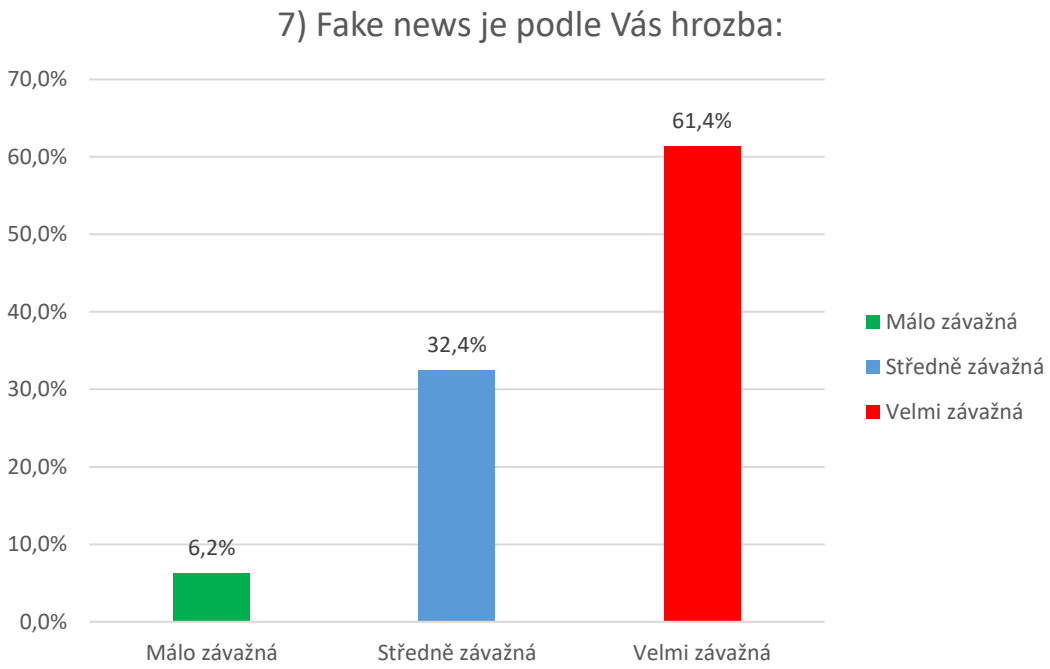
Tabulka 1 Vyhodnocení odpovědí na 6. otázku (vlastní)

Odpověď	Počet odpovědí
Dezinformace	20
Dezinformační zprávy	5
Falešné zprávy	52
Lživé zprávy	14

Nepravdivé zprávy	44
Smyšlené zprávy	4
Zavádějící zprávy	12
Klamné zprávy	5
Neověřené zprávy	7
Informace zavádějícího charakteru	2

Většina respondentů (165) mělo povědomí o pojmu Fake news, pouze 3 odpovědi byly vyhodnoceny jako nevhodné. Dále byl počet správných odpovědí přidán k poměru k odpovědím na otázku č. 11, čímž bude zjištěno potvrzení nebo vyvrácení hypotézy H1.

Vyhodnocení otázky č. 7: Sedmá otázka měla za úkol zjistit, za jak závažnou hrozbu shledávají respondenti problematiku Fake news. Výsledky jsou zobrazeny na obrázku 21.

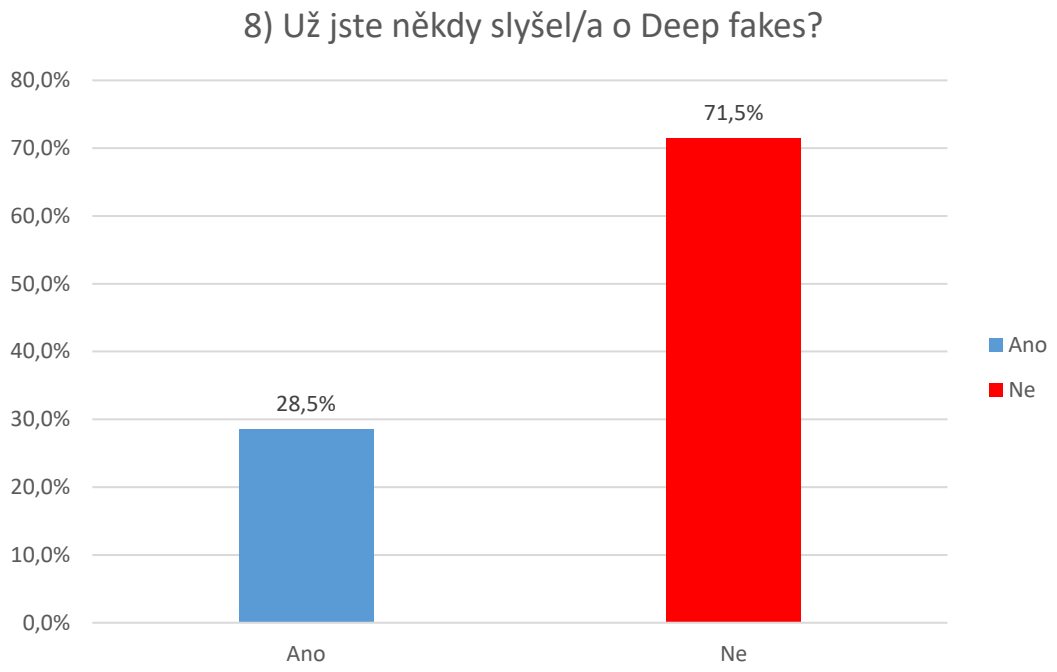


Obrázek 21 Grafické zobrazení odpovědí na 7. otázku (vlastní)

Na výše uvedenou otázku odpovídalo všech 207 respondentů, jelikož byli k této otázce přesměrování i ti, kteří odpověděli „Ne“ u otázky č. 4, „Už jste někdy slyšel/a o Fake news?“. Tato otázka byla uvedena vzdělávající formou, kde byl vysvětlen pojem Fake news a následně mohli všichni respondenti odpovědět na danou otázku.

Vyhodnocení výše uvedené otázky sloužilo společně s vyhodnocením otázek č. 12 k potvrzení čí vyvrácení hypotézy H4, která bude předmětem diskuze.

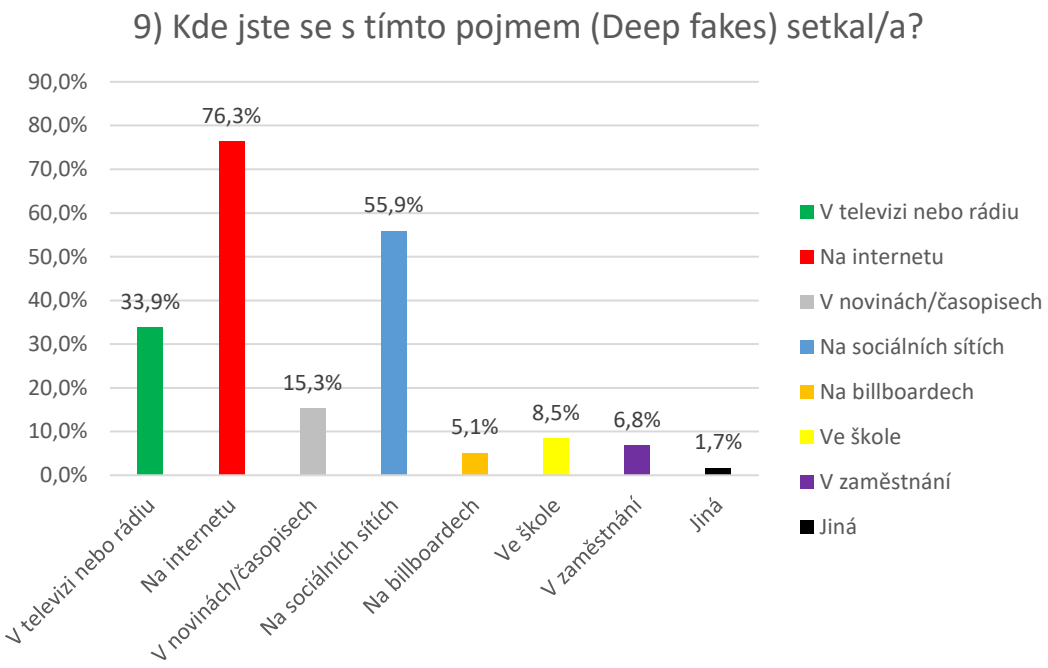
Vyhodnocení otázky č. 8: Osmá otázka měla za úkol zjistit, zda se respondenti setkali s pojmem Deep fakes. Při odpovědi na danou otázku bylo využito logické pravidlo. V případě volby odpovědi „Ano“ pokračovali respondenti na následující otázku, ovšem v případě odpovědi „Ne“ byl dotazovaný přesunut na otázku č.12, kde mu byl tento pojem vysvětlen. Výsledky jsou zobrazeny na obrázku 22.



Obrázek 22 Grafické zobrazení odpovědí na 8. otázku (vlastní)

Celkem 59 respondentů (28,5 %) slyšelo o Deep fakes a zbylých 148 respondentů (71,5 %) o pojmu neslyšelo.

Vyhodnocení otázky č. 9: Díky logickému pravidlu na tuto otázku odpovídalo 59 respondentů. Výsledky jsou zobrazeny na obrázku 23.

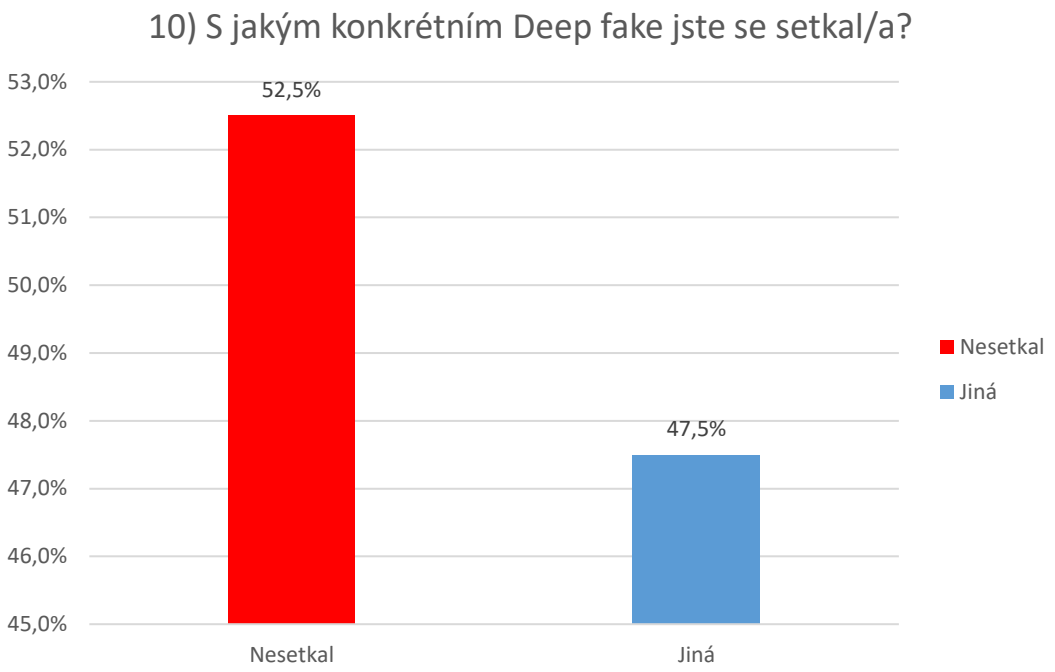


Obrázek 23 Grafické zobrazení odpovědí na 9. otázku (vlastní)

Otázka měla za úkol zjistit, kde se dotazovaní nejčastěji setkali s problematikou Deep fakes. Při výběru možnosti „Jiná“ (1,7 %) bylo uvedeno:

- zkoušel jsem vytvořit.

Vyhodnocení otázky č. 10: Úkolem dané otázky bylo zjistit o jaké konkrétní případy Deep fakes se jednalo. Díky logickému pravidlu na tuto otázku odpovídalo 59 respondentů. Výsledky jsou zobrazeny na obrázku 24.



Obrázek 24 Grafické zobrazení odpovědí na 10. otázku (vlastní)

S žádným konkrétním případem se nesetkalo 31 dotazovaných (52,5 %) a zbylých 28 dotazovaných (47,5 %) uvedli konkrétní případ Deep fake. Při výběru možnosti „Jiná“ bylo uvedeno:

- video s prezidentem Milošem Zemanem
- nahrazení obličeje ve videích u celebrit a státníků
- video s Donaldem Trumpem
- video s Barackem Obamou
- video s královnou Alžbětou II.
- pornografie
- video s prezidentem Ukrajiny Volodomyrem Zelenskym.

Všechny zmíněné možnosti se staly virálními na internetu, ovšem u Deep fake královny Alžběty II. se jednalo o mezinárodní upozornění na tuto hrozbu prostřednictvím televize při vánočních svátcích v roce 2020.

Vyhodnocení otázky č. 11: Otázka byla otevřená a měla za úkol zjistit reálné povědomí o znalosti Deep fakes a zda respondenti umí správně i tento pojem vysvětlit. Na jedenáctou

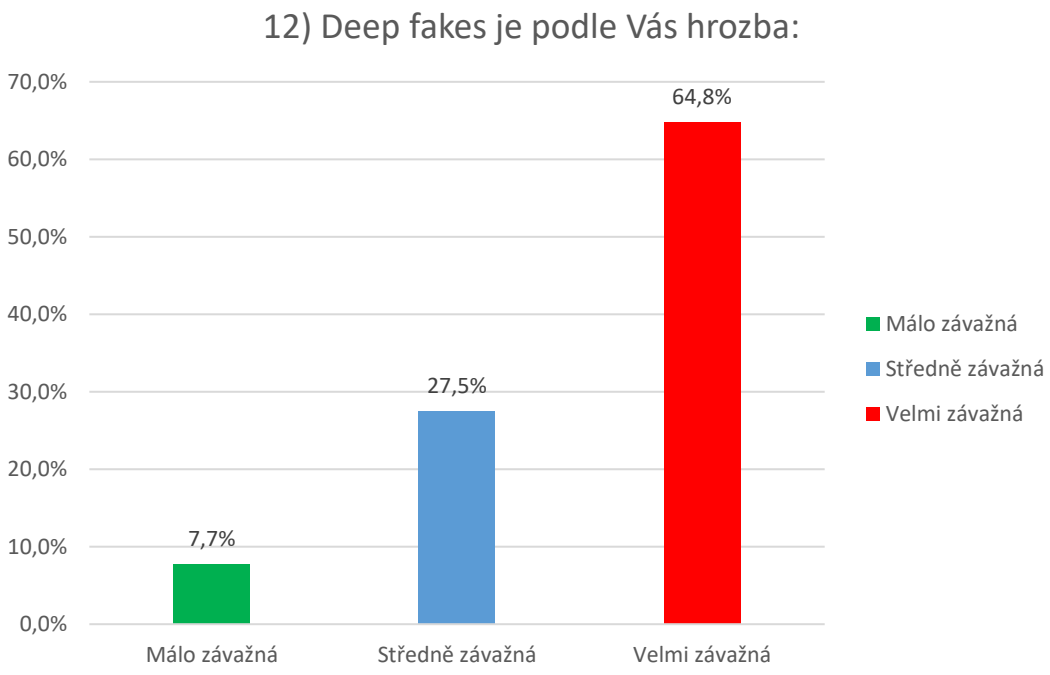
otázku rovněž odpovídalo 59 respondentů, tedy ti, kteří se setkali s Deep fakes. Výsledky jsou zobrazeny formou tabulky 2.

Tabulka 2 Vyhodnocení odpovědí na 11. otázku (vlastní)

Odpověď	Počet odpovědí
Manipulace s obličeji např. jejich pozměňování a vydávání za pravé.	10
Zneužití hlasu a podoby známé osoby ve zfalšovaném videu.	10
Podvržené obrazové a zvukové materiály s cílem ovlivnit.	6
Modifikace lidské tváře pomocí umělé inteligence, resp. její záměna, navázání nejčastěji na mluvené slovo, které reálně "nepronáší" zobrazovaná osoba.	1
Upravené fotografie, videa, zvuky, které vypadají jako opravdové.	5
UI vytvářející přesvědčivá videa, obrázky a jiné záznamy s cílem ovlivnit.	3
Digitálně upravené video s falešnou osobou vydávající se za skutečnou.	5

Z celkového počtu 59 respondentů mělo povědomí o pojmu Fake news 40 dotazovaných a 19 odpovědí byly vyhodnoceny jako nesprávné.

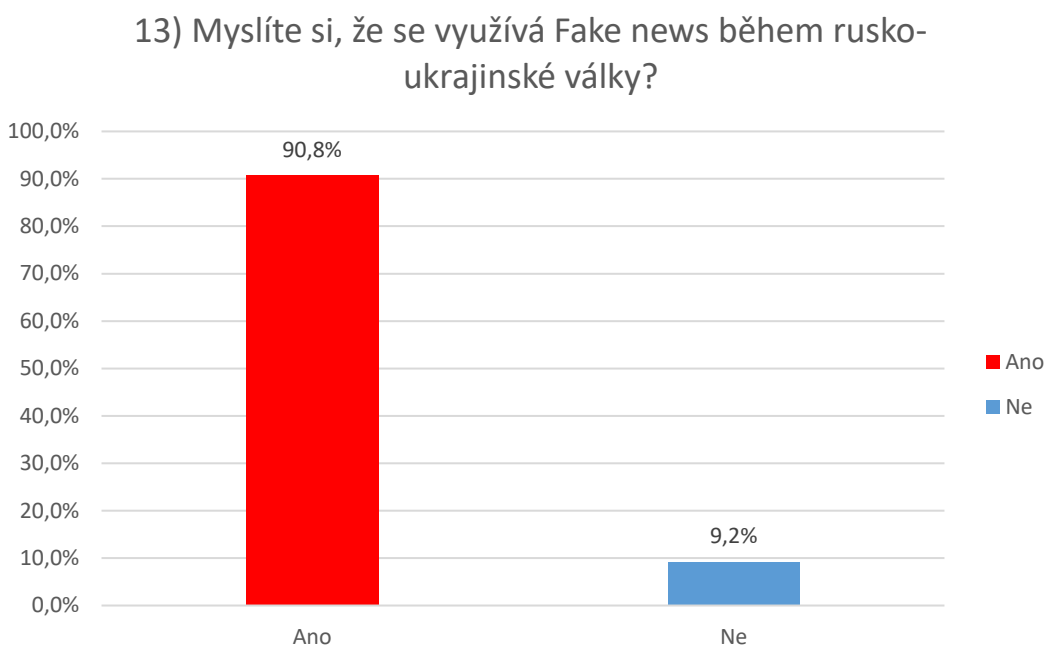
Vyhodnocení otázky č. 12: Dvanáctá otázka měla za úkol zjistit, za jak závažnou hrozbu shledávají respondenti Deep fakes. Výsledky jsou zobrazeny na obrázku 25.



Obrázek 25 Grafické zobrazení odpovědí na 12. otázku (vlastní)

Na výše uvedenou otázku odpovídalo všech 207 respondentů, jelikož byli k této otázce přesměrování i ti, kteří odpověděli „Ne“ u otázky č. 8, „Už jste někdy slyšel/a o Deep fakes?“. Tato otázka byla uvedena vzdělávající formou, kde byl vysvětlen pojem Deep fakes a následně mohli všichni respondenti odpovědět na danou otázku.

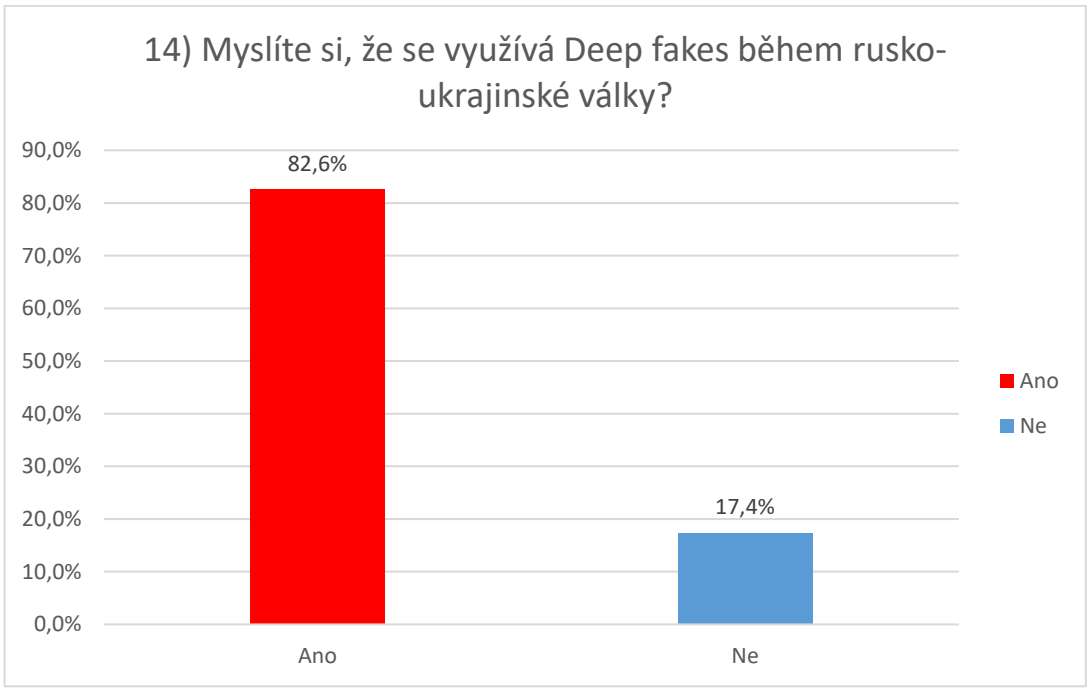
Vyhodnocení otázky č. 13: Třináctá otázka měla za úkol zjistit, zda si respondenti myslí, že se Fake news může využívat během rusko-ukrajinské války, která ovlivňuje politickou situaci. Výsledky jsou zobrazeny na obrázku 26.



Obrázek 26 Grafické zobrazení odpovědí na 13. otázku (vlastní)

Celkem 188 respondentů (90,8 %) si myslí, že se Fake news využívá během rusko-ukrajinské války a 19 dotazovaných (9,2 %) sdílelo opačný názor.

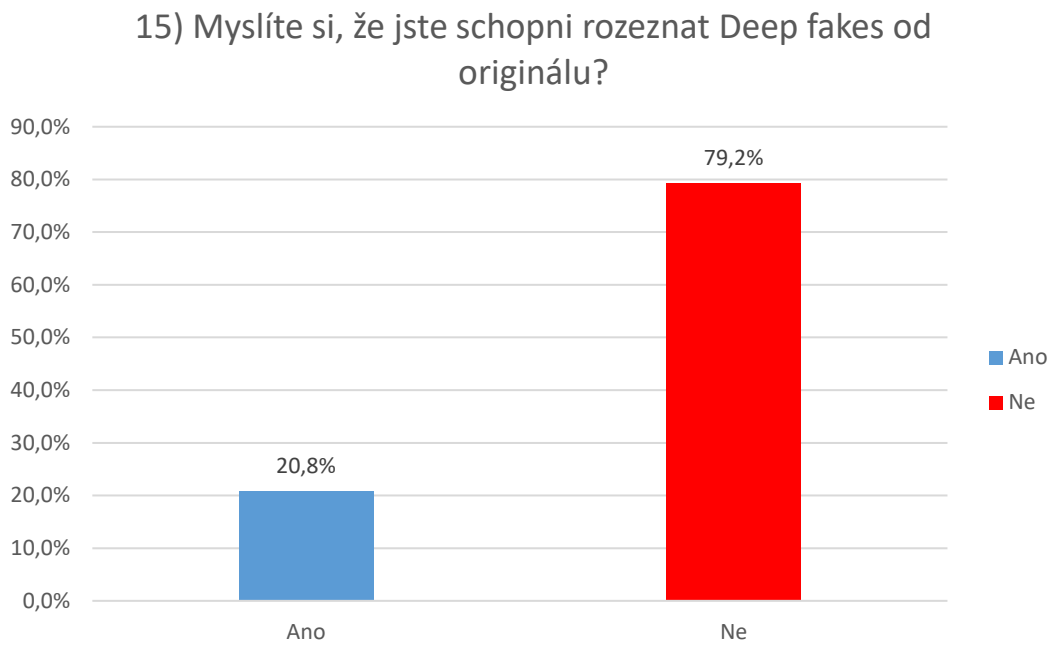
Vyhodnocení otázky č. 14: Čtrnáctá otázka měla za úkol zjistit, zda si respondenti myslí, že se využívá i Deep fakes během rusko-ukrajinské války, která ovlivňuje politickou situaci. Výsledky jsou zobrazeny na obrázku 27.



Obrázek 27 Grafické zobrazení odpovědí na 14. otázku (vlastní)

Celkem 171 respondentů (82,6 %) si myslí, že se využívá Deep fakes během rusko-ukrajinské války a 36 dotazovaných (17,4 %) bylo opačného názoru. Otázka č. 12 měla značný vliv tuto otázku, kde bylo Deep fakes vysvětleno, takže i přes neznalost pojmu Deep fakes odpovídalo všech 207 respondentů. Výsledky jsou zobrazeny na obrázku 28.

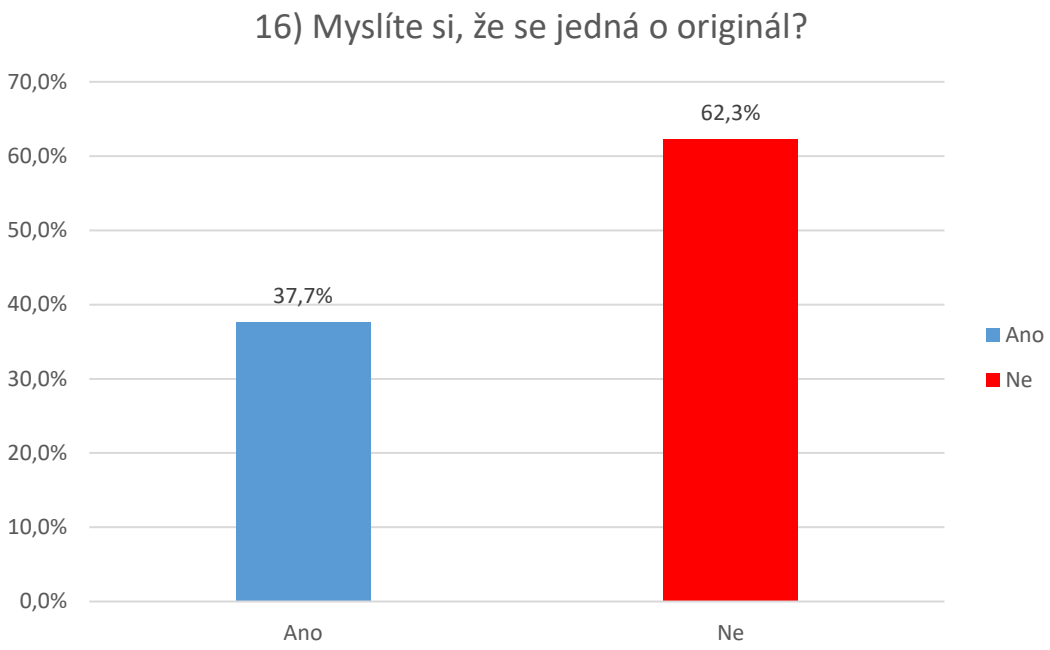
Vyhodnocení otázky č. 15: Patnáctá otázka měla za úkol zjistit, zda si respondenti myslí, že budou schopni rozeznat Deep fakes od originálu.



Obrázek 28 Grafické zobrazení odpovědí na 15. otázku (vlastní)

Celkem 43 respondentů (20,8 %) si myslí, že by dokázalo rozeznat Deep fakes od originálu a 164 dotazovaných (79,2 %) je opačného názoru. Z výsledku lze vyvodit, že respondenti přistupují k dané problematice s rozvahou.

Vyhodnocení otázky č. 16: Respondenti měli za úkol rozhodnout o fotografii, zda se jedná o originál. Výsledky jsou zobrazeny na obrázku 29.



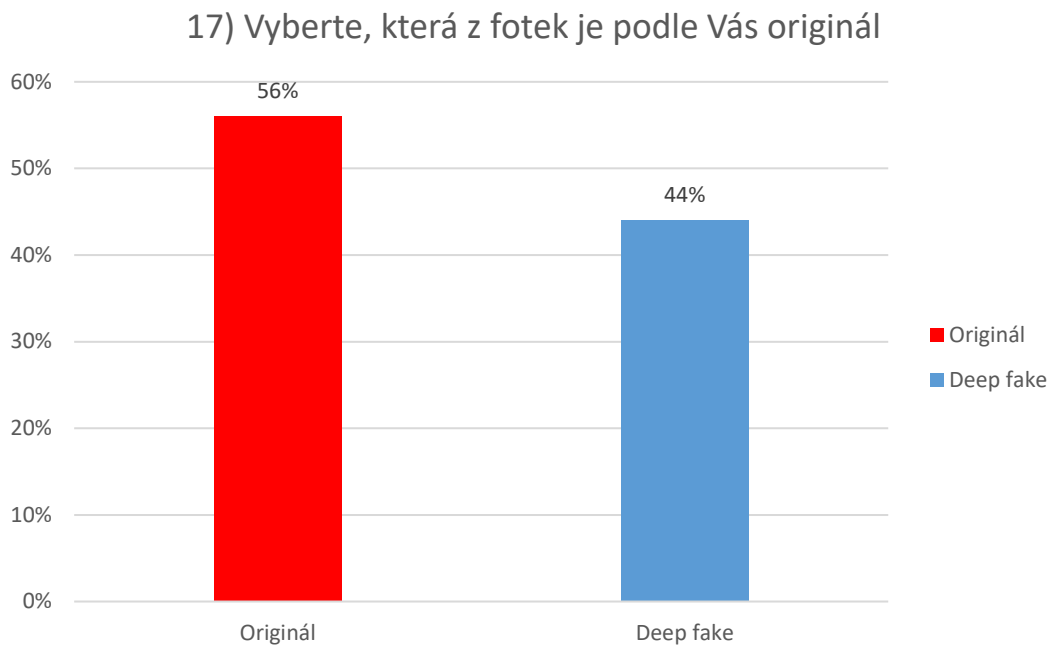
Obrázek 29 Grafické zobrazení odpovědí na 16. otázku (vlastní)

Celkem 78 respondentů (37,7 %) usoudilo, že se jedná o originál a 129 dotazovaných (62,3 %) považovalo fotografii za Deep fake. Správná odpověď byla možnost „Ne“, jednalo se o Deep fake. Otázka sloužila k potvrzení, čí vyvrácení hypotézy H3, která bude předmětem diskuze.

U šestnácté otázky byla využita Deep fake fotografie z projevu ukrajinského prezidenta Volodomyra Zelenského[8], kde vyzýval ke složení zbraní svých vojáků. Zmiňované Deep fake bylo vytvořeno s cílem oslabit morálku ukrajinské armády a snažilo se podnítit kapitulaci vojáků Ukrajiny. Projev se však nikdy neuskutečnil.

Vyhodnocení otázky č. 17: Respondenti měli za úkol vybrat fotografii, která je originál. Výsledky jsou zobrazeny na obrázku 30.

[8] viz. zde: https://www.news.com.au/world/europe//news-story/60a94b058b34564911aeb47ae6dc5e81



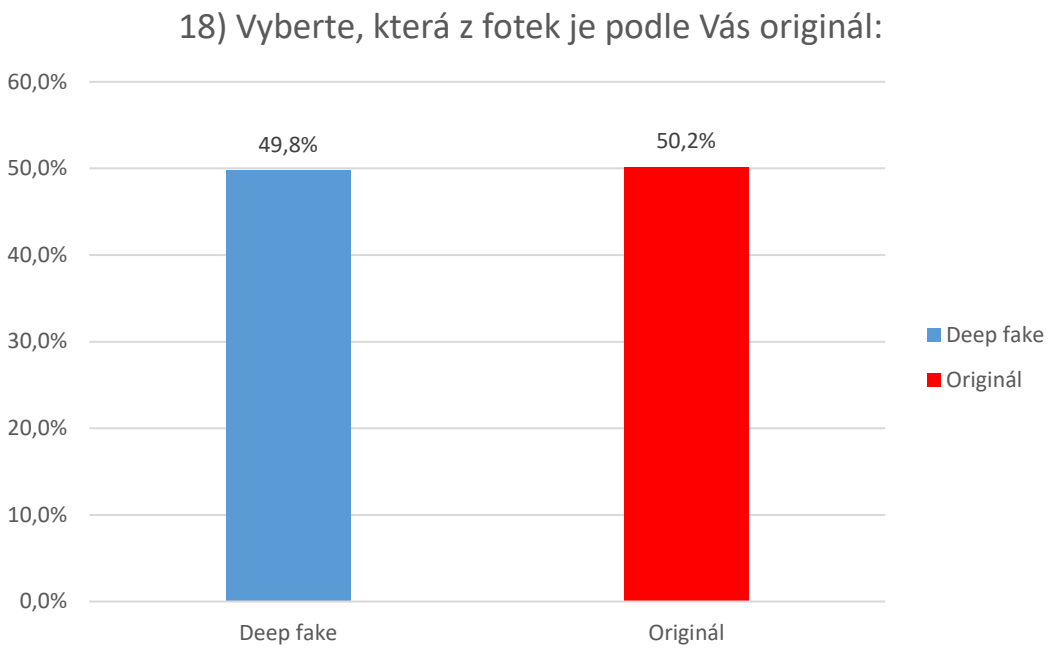
Obrázek 30 Grafické zobrazení odpovědí na 17. otázku (vlastní)

Celkem 116 respondentů (56 %) usoudilo správně, že se jedná o originál a 91 dotazovaných (44 %) zvolilo fotografii za Deep fake[9].

Otázka sloužila k potvrzení, čí vyvrácení hypotézy H3, která bude předmětem diskuze.

Vyhodnocení otázky č. 18: Respondenti měli za úkol vybrat originální fotografii. Výsledky jsou zobrazeny na obrázku 31.

[9] viz zde: https://spectrum.ieee.org/facebook-ai-launches-its-deepfake-detection-challenge#toggle-gdpr



Obrázek 31 Grafické zobrazení odpovědí na 18. otázku (vlastní)

U poslední otázky zvolilo 103 respondentů (49,8 %) možnost originál a rozhodla pouze jedna odpověď, protože 104 respondentů si myslelo, že se jedná o Deep fake. Určujícími faktory byla zřejmě skutečnost, že se jednalo o velmi zdařilé Deep fake a také známá tvář herce Toma Cruise[10], díky čemuž respondenti nepředpokládali, že se může jednat o Deep fake.

Otázka sloužila k potvrzení, čí vyvrácení hypotézy H3, která bude předmětem diskuze.

V závěrečné části dotazníkového šetření byla doporučena respondentům Deep fake videa ke zhlédnutí, která jim více přiblížila problematiku Deep fakes.

[10] viz. https://www.theverge.com/2021/3/5/22314980

7 SNÍŽENÍ MÍRY RIZIKA DEEP FAKES

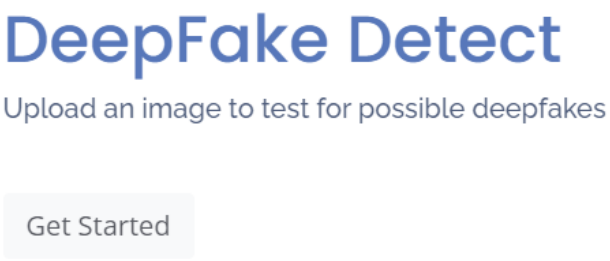
V závěrečné kapitole budou uvedeny možnosti, jak snížit míru rizika výše zmiňované hrozby. Cílem této části práce bude snížit nebo eliminovat účinky Deep fakes i Fake news na obyvatelstvo.

7.1 Odhalení pomocí DeepFake-Detect

Odhalit Deep fakes je velmi náročné, jelikož se neustále vyvíjí jejich tvorba a jsou více a více propracovanější, jak jsem uvedl v teoretické části. Způsobů k jejich odhalení je několik, avšak užívání nebývá snadné, já jsem si vybral jednoduchou metodu, kterou by mohl zvládnout každý.

Využil jsem on-line metodu, která je dostupná na internetové stránce[11].

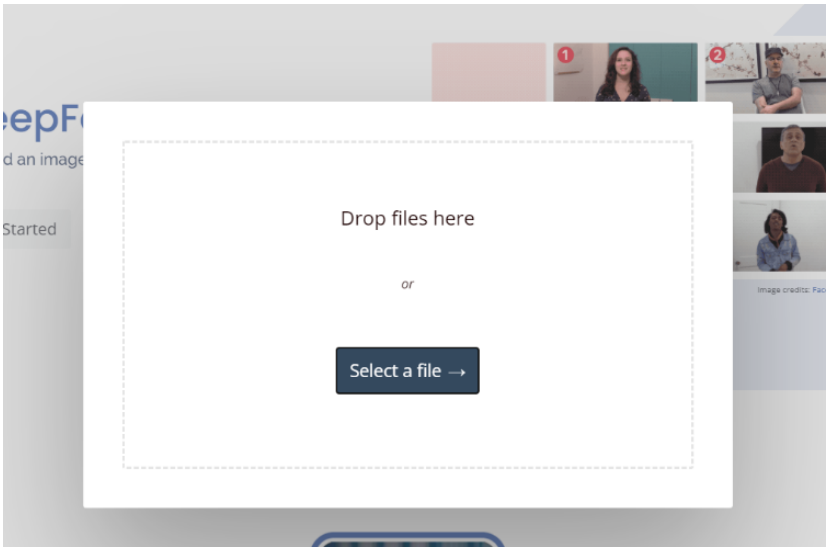
Klikneme na „Get Started“.



Obrázek 32 Aplikace na detekci Deep fakes (deepfake-detect.com)

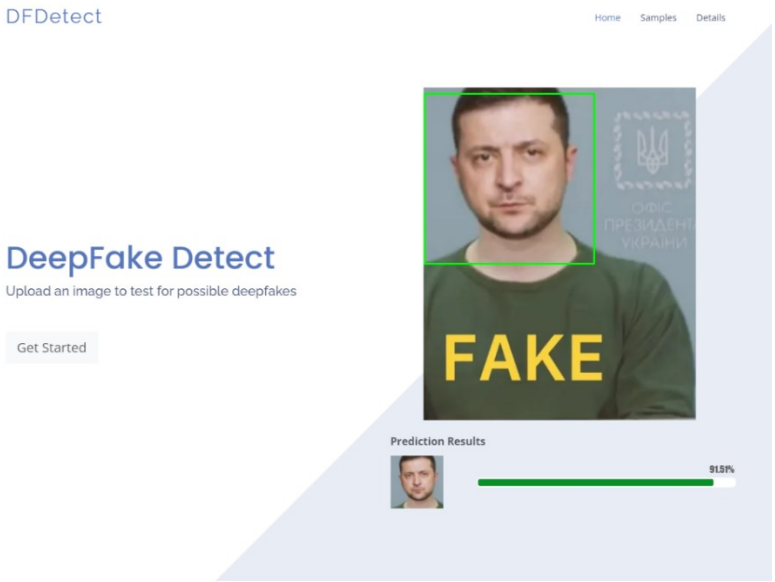
Dále zvolíme „Select a file“ a nahrajeme soubor z počítače.

[11] Dostupná zde: https://deepfake-detect.com/



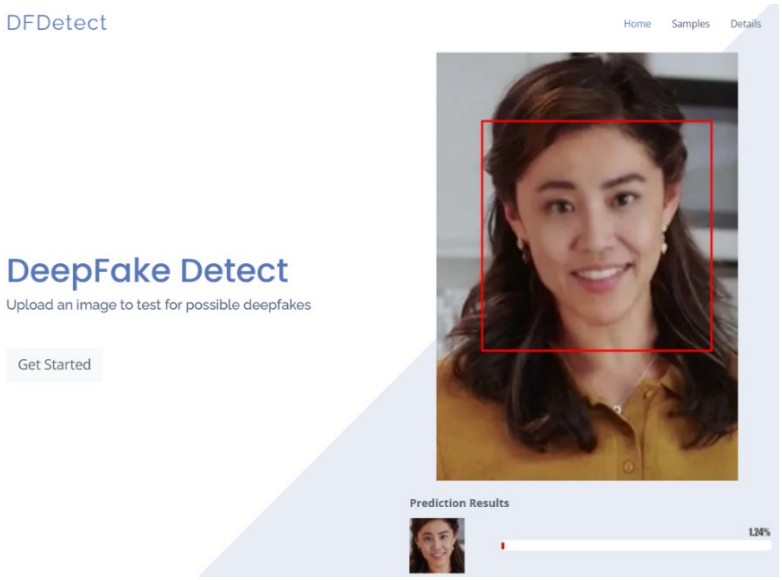
Obrázek 33 Nahrání souboru (deepfake-detect.com)

Využil jsem fotografie z otázek obsažených v dotazníku, jedná se o otázky č.16, č. 17 a č. 18.

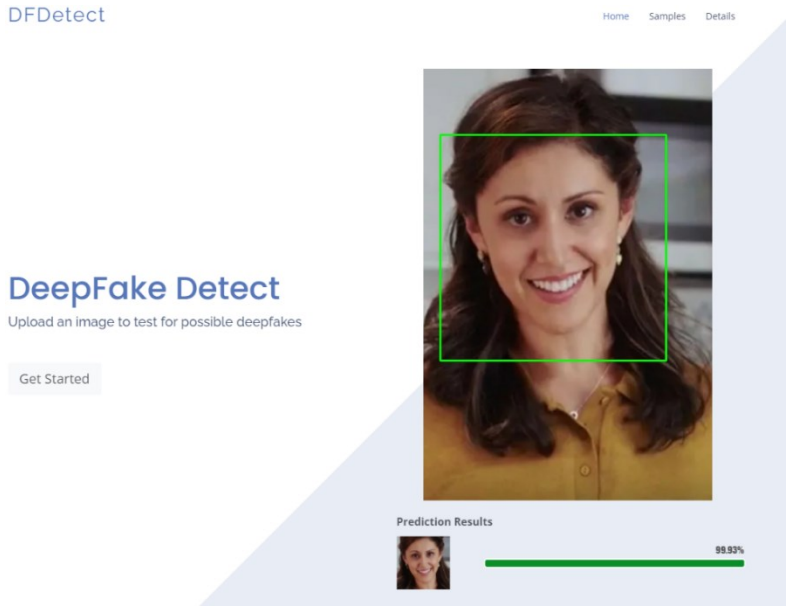


Obrázek 34 Vyhodnocení fotografie z otázky č. 16 (deepfake-detect.com)

Naneštěstí i v tomhle případě software nedokázal rozeznat Deep fake. Dále byly nahrány fotografie využité v otázce č. 17.

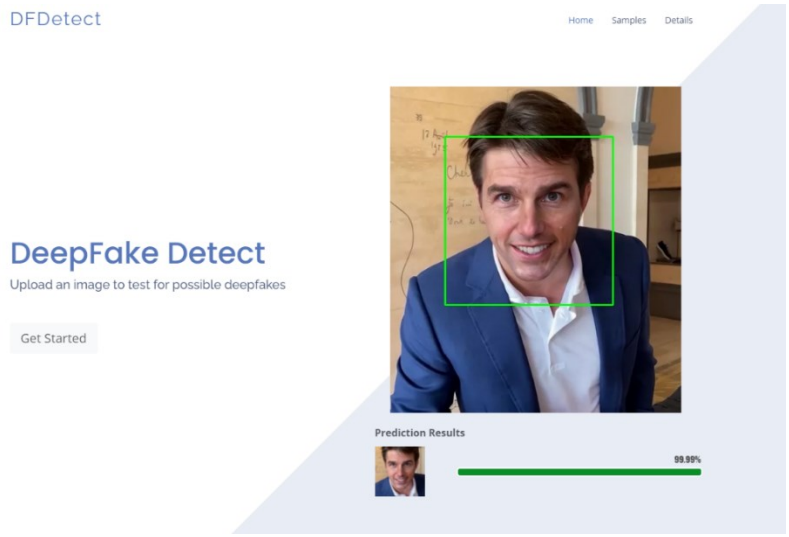


Obrázek 35 Vyhodnocení fotografie z otázky č. 17 (deepfake-detect.com)

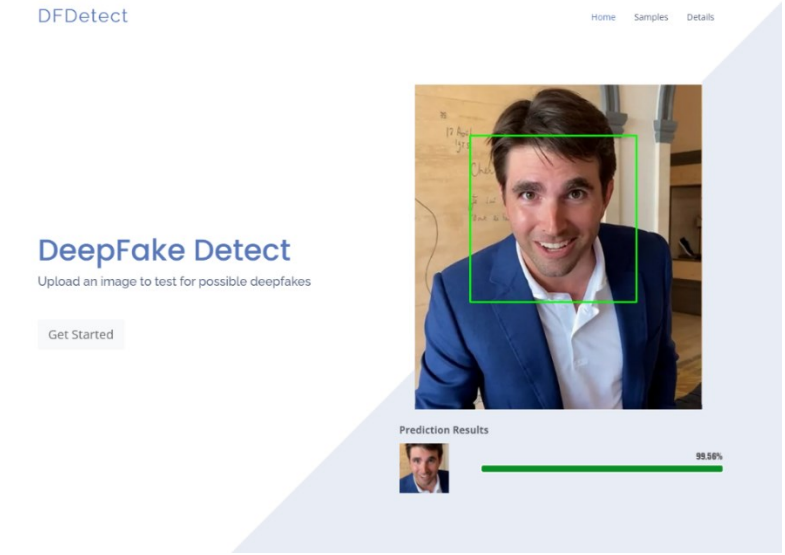


Obrázek 36 Vyhodnocení fotografie z otázky č. 17 (deepfake-detect.com)

Software byl schopen rozeznat Deep fake na základě nahraného souboru. Následně byly nahrány fotografie využité u otázky č. 18.



Obrázek 37 Vyhodnocení fotografie z otázky č. 18 (deepfake-detect.com)



Obrázek 38 Vyhodnocení fotografie z otázky č. 18 (deepfake-detect.com)

V tomhle případě bohužel už software nebyl schopen rozeznat Deep fake, jelikož se jedná o velmi zdařilou tvorbu a nelze tedy spoléhat na obdobné platformy rozeznávání Deep fakes od originálů.

7.2 Diskuze

Cílem dotazníkového šetření bylo zjistit povědomí obyvatel o problematice Fake news a Deep fakes a také vyhodnotit, zda je obyvatelé považují za hrozbu. Stěžejním cílem dotazníku bylo také informovat o dané problematice prostřednictvím otázek u kterých respondenti obdrželi vysvětlení, co daný pojem znamená.

- H1 Povědomí o Fake news bude u respondentů vyšší než znalost Deep fakes.

Hypotéza H1byla potvrzena.

Povědomí o Fake news byla u respondentů vyšší než znalost Deep fakes a to značně. Pojem Fake news dokázalo vysvětlit 165 z 207 respondentů, kdežto v případě Deep fakes „pouze“ 40 respondentů.

- H2 Předpokládáme, že lidé s vyšším a vysokoškolským dosaženým vzděláním mají větší povědomí ohledně dané problematiky, jelikož se jedná převážně o problematiku probíranou na vysokých školách.

Hypotéza H2 byla potvrzena.

Fake news z 97 respondentů s vyšším a vysokoškolským dosaženým vzděláním neznalo celkem 9. V porovnání s ostatními 110 respondenty pojem Fake news nedokázalo vysvětlit 33 osob. Deep fakes neznalo 73 osob z 97 respondentů. V porovnání s ostatními 110 respondenty tuto problematiku neznalo 98 osob. Nabízí se tedy možnost varování před těmito druhy hrozeb např. prostřednictvím hromadných sdělovacích prostředků.

- H3 Předpokládáme, že respondenti nebudou schopni rozeznat originály fotek od Deep fakes.

Hypotéza H3 byla vyvrácena.

Respondenti byli schopni rozeznat originály fotek od Deep fakes ve všech případech (celkem třech), ovšem výsledky nebyly úplně přesvědčivé při rozdílech 24,6 %, 12 % a 0,4 % ve prospěch originálů. Při rozdílu 0,4 % rozhodoval pouze 1 hlas ve prospěch originálu. V otázce bylo využito velmi známého herce Toma Cruise a respondenti zřejmě předpokládali fakt, že se nemůže jednat o Deep fakes.

- H4 Respondenti nepovažují problematiku Deep fakes a Fake news za hrozbu.

Hypotéza H4 byla vyvrácena.

Pouze 13 respondentů hodnotilo Fake news za malou hrozbu a v případě Deep fakes se jednalo o 16 respondentů. Deep fakes byla zvolena 134 respondenty jako velmi vážná hrozba a Fake news zvolilo 127 dotazovaných.

7.3 Navrhovaná opatření pro snížení vlivu Deep fakes a Fake news

Pro snížení nebo úplnou eliminaci účinků Deep fakes a Fake news na obyvatelstvo by mělo být zásadní:

- Ověřovat zdroje.
- Využívat relevantní zdroje (např. odborné publikace s uvedeným autorem textu).
- Prozkoumávat videa dopodrobna (nesrovnalosti v obraze, nekonzistentní stíny, nepravidelnost nebo absence mrkání, nepřirozené pohyby apod.).
- Nečerpat informace pouze z jednoho zdroje.
- Nerozesílat dále neověřené informace a videa.
- Snaha o kritické myšlení.
- Využívat aplikace pro odhalení Deep fakes (ani ty nejsou bohužel neomylné).

Myslím si, že je především důležité klást důraz na vzdělávání v oblasti dané problematiky, šířit osvětu mezi veřejností a informovat o možných nebezpečných vlivech Deep fakes a Fake news na veřejnou volbu.

V každodenním životě bychom měli omezit šíření Deep fake a falešných zpráv např. prostřednictvím sociálních sítí, když neznáme původ informací a zdroj.

Cílem vlády by mělo být sankciování osob na základě tvorby nového zákona za opakované šíření, Fake news, hoaxů a dalších zavádějících informací přes sociální sítě a internet. Uskutečnění daného cíle je velmi obtížné, jelikož se šíření zpráv uskutečňuje prostřednictvím kyberprostoru a následná identifikace strůjců falešných zpráv je náročná. Dalším omezujícím faktorem, který znesnadňuje tvorbu daného zákona můžeme shledat, mimo jiné, ústavní právo svobody projevu. Výjimky upravené podle trestního zákoníku, ovšem mohou omezit dané právo ve speciálních případech např. šíření poplašné zprávy, pomluvy apod. Obdobným způsobem by tomu mohlo být i u šíření a vytváření falešných zpráv, ale zde nastává otázka, kdo a jakým způsobem by zvolil druh a obsah daných zpráv a vytyčit hranice, abychom se neodvrátili od způsobů demokracie.

V případě Deep fakes bych navrhoval obdobný zákon (fungující i v jiných zemí ve světě), pomocí kterého by byly sankciované osoby, které vytvoří Deep fakes za účelem dezinformace osob nebo jejich dehonestaci. V porovnání s návrhem zákona týkajícího se šíření falešných zpráv tento se zdá uskutečnitelnější, ovšem s postupně rostoucím vývoje

technologie a umělé inteligence bude těžší rozeznat originál od Deep fake. I v tomto případě se jedná o šíření Deep fakes prostřednictvím kyberprostoru, kde identifikace osob a jejich sankciování je náročná. Osoba, která vytvořila Deep fake ani nemusí pocházet z České republiky a následné sankciování dané osoby je hůře uskutečnitelné.

Časové prodleva mezi nalezením a reakcí na Deep fakes, Fake news, hoaxů a dalších zavádějících zpráv hraje významnou roli, jelikož už může být jejich primární cíl dávno naplněn, tedy ovlivnit masy osob. V případě dehonestujících Deep fakes, které mají za cíl osobám uškodit na pověsti, cti, soukromí nebo dobrému jménu může značně narušit psychiku.

ZÁVĚR

Diplomová práce se zabývala scénářem hrozby Deep fakes v ochraně obyvatelstva. V teoretické části práce jsme si vysvětlili základní pojmy Deep fakes a Fake news, které spolu úzce souvisejí. Jmenovali jsme si jednotlivé typy Fake news, představili si historii Deep fakes, charakterizovali si umělou inteligenci, Generativní adversariální síť a v neposlední řadě také technologie pro odhalení Deep fakes. V další kapitole jsme se zabývali problematikou informační bezpečnosti.

V praktické části práce jsem navrhl scénář hrozby Deep fakes v ochraně obyvatelstva, který se skládá z potenciálně možných případů, které by mohly nastat. Součástí práce byl také dotazník pro obyvatele České republiky, který měl za úkol zjistit povědomí veřejnosti o Fake news a Deep fakes. Z dotazníkového šetření vyplynulo, že 79,7 % respondentů zná pojem Fake news a „pouze“ 19,3 % dokázalo vysvětlit problematiku Deep fakes. U následujících otázkách byly zmiňované pojmy respondentům vysvětleny, aby mohli odpovídat i na následující otázky a zároveň dotazníkové šetření sloužilo jako vzdělávací prostředek v dané problematice. Dále z dotazníkového šetření vyplynulo, že respondenti považují Fake news a Deep fakes za velmi závažné hrozby a také si myslí, že se využívají při rusko-ukrajinské válce. Respondenti si myslí, že nedokážou rozeznat Deep fakes od originálu, ovšem po vyhodnocení otázek zaměřených na rozlišování Deep fakes od originálu tomu tak nebylo.

V další kapitole byly vyhodnoceny stanovené hypotézy. První hypotéza H1 předpokládala, že povědomí o Fake news bude u respondentů vyšší než znalost Deep fakes a byla potvrzena. Druhá hypotéza H2 předpokládala, že lidé s vyšším a vysokoškolským dosaženým vzděláním mají větší povědomí ohledně dané problematiky, jelikož se jedná převážně o problematiku probíranou na vysokých školách a byla potvrzena. Třetí hypotéza H3 předpokládala, že respondenti nebudou schopni rozeznat originály fotek od Deep fakes a byla vyvrácena. Čtvrtá hypotéza H4 předpokládala, že respondenti nepovažuji problematiku Deep fakes a Fake news za hrozbu a byla vyvrácena.

Dále jsme se zabývali odhalením Deep fakes pomocí DeepFake-Detect, kdy jsem využil on-line metodu běžně dostupnou na internetu.

Závěrem diplomové práce byla tvorba vlastního Deep fake videa včetně klonování hlasu. Zvolil jsem sebe a svého kamaráda, který s tvorbou souhlasil. Byla použita metoda, která vytvoří Deep fakes na základě jedné fotografie. Dále byly doporučeny návrhy a opatření pro snížení vlivu Deep fakes a Fake news.

Fake news se v každodenním životě vyskytuje bohužel často. Na základě vytvořeného scénáře a při stoupajícím vývoji technologie se dá očekávat, že hrozba Deep fakes bude mít vzrůstající tendenci v budoucnu. Na základě vytvořených scénářů lze předpokládat, že se s tímto jevem můžeme setkat napříč různými odvětvími.

SEZNAM POUŽITÉ LITERATURY

ADAMS, Maurice. *Deepfake technology & 2020 u.s. electrions: a threat to democracy and how to spot deepfakes*. Independently published. Dallas, 2019. ISBN 978-1705466322.

AHIRWAR, Kailash, 2019. *Generative Adversarial Networks Projects: Build next-generation generative models using TensorFlow and Keras.* Packt Publishing. ISBN 978-1789136678.

BOESE, Alex a Eva KADLECOVÁ, 2019. *Hroši žerou trpaslíky!*. Brno: CPress. ISBN 978-80-264-2716-2.

GREGOR, Miloš a Petra VEJVODOVÁ, 2018. *Nejlepší kniha o fake news, dezinformacích a manipulacích!!!*. Brno: CPress. ISBN 978-80-264-1805-4.

HUĎO, Ľubomír a Petr ŽANTOVSKÝ, 2019. *Mediální krysy, aneb, Jak novináři manipulují*. Praha: Česká citadela. ISBN 978-80-907399-4-9.

JACKSON, Tom, Cristina GUITAN a Pavel PELÍŠEK, 2020. *Fake news*. Brno. ISBN 978-80-7565-659-9.

SHICK, Nina. *Deep Fakes and the Infocalypse: What You Urgently Need To Know.* Monoray, 2020. ISBN 978-1913183523.

YOUNG, Norbert. *Deepfake technology: Complete Guide to Deepfakes, Politics and Social Media.* Independently published, 2019. ISBN 978-1078494694.

Elektronické zdroje

ANTIPOV, G.; BACCOUCHE, M.; Dugelay, J. *Face aging* [online]. 2017 [cit. 2022-03-15]. Dostupné z doi: 10.1109/ICIP.2017.8296650.

CCDCOE. News [online]. 2022 [cit. 2022-07-07]. Dostupné z: https://ccdcoe.org/news/2022/finland-wins-cyber-defence-exercise-locked-shields-2022/

COLAB.RESEARCH.GOOGLE.COM[1]. *Obrázek 10, 11, 12, 13* [online]. 2021 [cit. 2022-05-20]. Dostupné z: https://colab.research.google.com/github/neuralchen/SimSwap/blob/main/SimSwap%20colab.ipynb#scrollTo=wwJOwR9LNKRz

COLAB.RESEARCH.GOOGLE.COM[2]. *Obrázek 14 a 15* [online]. 2022 [cit. 2022-05-20]. Dostupné z: https://colab.research.google.com/github/tugstugi/dl-colab-notebooks/blob/master/notebooks/RealTimeVoiceCloning.ipynb#scrollTo=WZjKkvGF1Y-i

CZECH-PRESIDENCY.CONSILIUM.EUROPA. *Priority* [online]. 2022 [cit. 2022-07-01]. Dostupné z: https://czech-presidency.consilium.europa.eu/cs/program/priority/

ČANDÍK, Marek. *Informační bezpečnost* [online]. 2022 [cit. 2022-06-17]. Dostupné z: https://www.cybersecurity.cz/data/candik2.pdf

DEEPFAKE-DETECT.COM. *Obrázek 31–37* [online]. 2022 [cit. 2022-07-20]. Dostupné z: https://deepfake-detect.com/

EMMASANDERS. *History* [online]. 2022 [cit. 2022-03-04]. Dostupné z: http://www.emmasanders.nl/history.html

EUROPARL.EUROPA[1]. *Society* [online]. 2021 [cit. 2022-03-15]. Dostupné z: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

EUROPARL.EUROPA[2]. *Investice do umělé inteligence 2020* [online]. 2020 [cit. 2022-03-15]. Dostupné z: https://www.europarl.europa.eu/news/en/headlines/priorities/artificial-intelligence-in-the-eu/20201015STO89417/ai-rules-what-the-european-parliament-wants

EUROPARL.EUROPA[3]. *Řešení problematiky Deep fakes na úrovni Evropské politiky* [online]. 2021 [cit. 2022-07-15]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

EUROPOL.EUROPA. *Malicious Uses and Abuses of Artificial Intelligence* [online]. 2020 [cit. 2022-06-17]. Dostupné z: https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

HISTORYOFINFORMATION. *Origins of Deepfakes* [online]. 2022 [cit. 2022-03-04]. Dostupné z: https://www.historyofinformation.com/detail.php?id=4792

HOAX. *Co je to hoax* [online]. 2022 [cit. 2022-07-07]. Dostupné z: https://www.hoax.cz/hoax/co-je-to-hoax

ISOLA, P. a kol. *Image-to-Image*. [online]. 2017 [cit. 2022-03-19]. Dostupné z doi: 10.1109/CVPR.2017.632.

KOBALT.IO. *CIA Triáda* [online]. 2020 [cit. 2022-06-17]. Dostupné z: https://kobalt.io/confidentiality-integrity-and-availability-in-cyber-security/

MVCR. *Definice dezinformací a propagandy* [online]. 2022 [cit. 2022-06-16]. Dostupné z: https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx

NEWS. *Europe* [online]. 2022 [cit. 2022-07-09]. Dostupné z: https://www.news.com.au/world/europe//news-story/60a94b058b34564911aeb47ae6dc5e81

NÚKIB[1]. *O NÚKIB* [online]. 2022 [cit. 2022-07-07]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

NÚKIB2. *O Úřadu* [online]. 2022 [cit. 2022-07-07]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

NÚKIB[3]. *Aktuality* [online]. 2022 [cit. 2022-07-07]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1702-cesko-se-umistilo-na-3-miste-v-nejvetsim-cviceni-kyberneticke-bezpecnosti-na-svete/

PENDER-BEY, Georgie. *Parkerian Hexad* [online]. 2012 [cit. 2022-06-17]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

SAMONAS, Spyridon a David COSS. JISSec. *The CIA strikes back: redefining confidentiality, integrity and availability in security* [online]. March 2014, vol. 10, iss. 3, [cit. 2022-06-17]. ISSN: 1551-0123. Dostupné z: http://www.proso.com/dl/Samonas.pdf

SECURITYWEEK. *Fraud and Identity Theft* [online]. 2022 [cit. 2022-06-17]. Dostupné z: https://www.securityweek.com/deepfakes-are-growing-threat-cybersecurity-and-society-europol

SPECTRUM.IEEE. Artificial intelligence [online]. 2019 [cit. 2022-07-09]. Dostupné z: https://spectrum.ieee.org/facebook-ai-launches-its-deepfake-detection-challenge#toggle-gdpr

TAEB, M. a H. CHI. *Comparison of deepfake detection techniques through deep learning* [online]. 2022 [cit. 2022-03-15]. Dostupné z doi: 10.3390/jcp2010007.

TECHTARGET. *Robotics* [online]. 2019 [cit. 2022-03-15]. Dostupné z: https://www.techtarget.com/searchenterpriseai/definition/driverless-car

THEVERGE. Artificial intelligence [online]. 2021 [cit. 2022-07-09]. Dostupné z: https://www.theverge.com/2021/3/5/22314980

VLÁDA[1]. *Zmocněnci vlády* [online]. 2022 [cit. 2022-05-18]. Dostupné z: https://www.vlada.cz/cz/ppov/zmocnenci_vlady/vladni-zmocnenec-pro-oblast-medii-a-dezinformaci-194841/

VLÁDA[2]. *Aktuálně* [online]. 2022 [cit. 2022-05-18]. Dostupné z: https://www.vlada.cz/cz/media-centrum/aktualne/novym-vladnim-zmocnencem-pro-oblast-medii-a-dezinformaci-se-stal-michal-klima-195260/

WANG X. a kol. *Restoration faces*. [online]. 2017 [cit. 2022-03-15]. Dostupné z doi: 10.1109/CVPR46437.2021.00905.

WOLTERINK, J. a kol. *Deep MR to CT synthesis using unpaired data* [online]. 2017 [cit. 2022-03-20]. Dostupné z doi: 10.1007/978-3-319-68127-6_2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CRM	Customer relationship management
DARP	Defense Advanced Research Projects Agency
DFDL	The Deepfake Detection Challenge
EUROPOL	European Police Office
GAN	Generativní adversariální síť
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
UI	Umělá inteligence
UNICRI	United Nations Interregional Crime and Justice Research Institute

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK „PRŮZKUM O POVĚDOMÍ FAKE NEWS A DEEP FAKES“

Průzkum o povědomí Fake news a Deep fakes

Dobrý den,

věnujte, prosím, několik minut Vašeho času k vyplnění následujícího dotazníku. Dotazníkové šetření je určené pro osoby starší 15 let a bude sloužit jako materiál pro průzkum v diplomové práci. Tento dotazník je anonymní, tak prosím o věrohodné informace, děkuji za vyplnění.

1 Která z níže uvedených kategorií zahrnuje Váš věk?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ 15–17 ◯ 18–20 ◯ 21–29 ◯ 30–39 ◯ 40–49 ◯ 50–59 ◯ 60+

2 Jaké je Vaše nejvyšší dosažené vzdělání?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Základní ◯ Střední ◯ Střední s maturitou ◯ Vyšší odborné ◯ Vysokoškolské

3 Váš nynější statut je:

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Studuji na škole ◯ Plánuji studovat na škole ◯ Ukončené vzdělání

4 Už jste někdy slyšel/a o Fake news?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

5 Kde jste se s tímto pojmem (Fake news) setkal/a?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ V televizi nebo rádiu ☐ Na internetu ☐ V novinách/časopisech ☐ Na billboardech ☐ Na sociálních sítích ☐ Ve škole

☐ V zaměstnání

☐ Jiná...

6 Co podle Vás znamená Fake news?

Fake news jsou falešné zprávy vydávané za skutečné s cílem ovlivnit chování lidí a všeobecné povědomí.

Zdroj: www.infoz.cz/fake-news

7 Fake news je podle Vás hrozba:

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Málo závažná ◯ Středně závažná ◯ Velmi závažná

8 Už jste někdy slyšel/a o Deep fakes?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

9 Kde jste se s tímto pojmem (Deep fakes) setkal/a?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ V televizi nebo rádiu ☐ Na internetu ☐ V novinách/časopisech ☐ Na sociálních sítích ☐ Na billboardech ☐ Ve škole

☐ V zaměstnání

☐ Jiná...

10 S jakým konkrétním Deep fake jste se setkal/a?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Nesetkal

◯ Jiná...

11 Co podle Vás znamená Deep fakes?

Deep fakes jsou uměle vytvořená videa snažící se nahradit obličeje ve videu obličejem někoho jiného, využívající pokročilých metod umělé inteligence a strojového učení.

Zdroj: www.infoz.cz/deepfake

12 Deep fakes je podle Vás hrozba:

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Málo závažná ◯ Středně závažná ◯ Velmi závažná

13 Myslíte si, že se využívá Fake news během rusko-ukrajinské války?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

14 Myslíte si, že se využívá Deep fakes během rusko-ukrajinské války?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

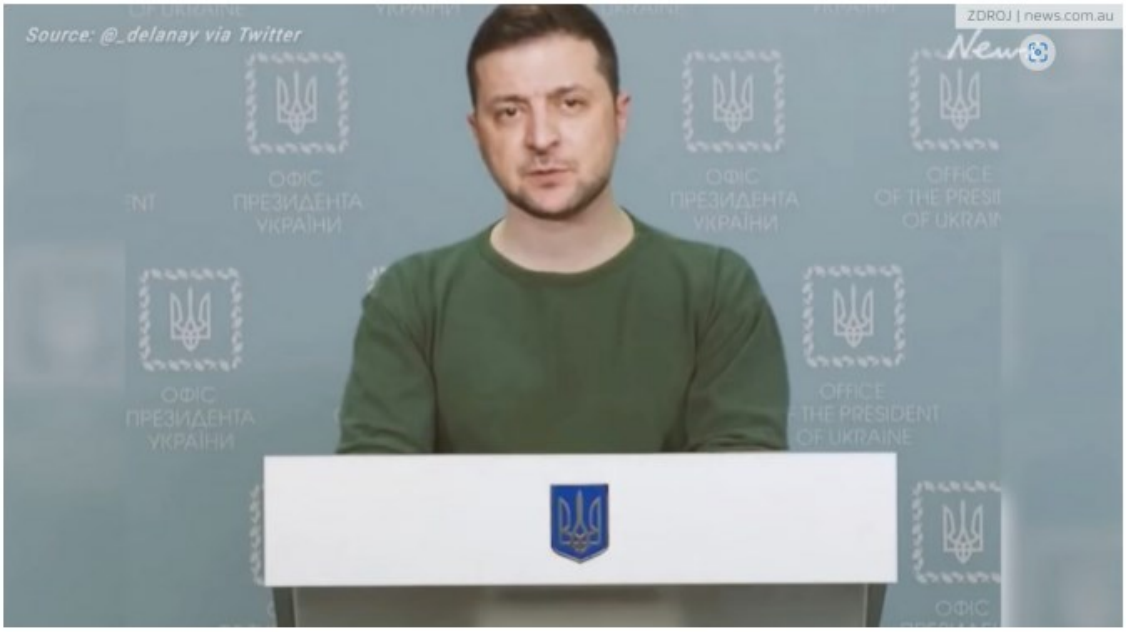
15 Myslíte si, že jste schopni rozeznat Deep fakes od originálu?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

16 Myslíte si, že se jedná o originál?

Nápověda k otázce: *Zdroj: https://www.news.com.au/world/europe//news-story/60a94b058b34564911aeb47ae6dc5e81*



◯ Ano ◯ Ne

Jednalo se o Deep fake, více viz https://www.news.com.au/world/europe//news-story/60a94b058b34564911aeb47ae6dc5e81

17 Vyberte, která z fotek je podle Vás originál:

Nápověda k otázce: *Zdroj: https://spectrum.ieee.org/facebook-ai-launches-its-deepfake-detection-challenge#toggle-gdpr*


◯ ◯

Originál vlevo, Deep fake vpravo, více viz https://spectrum.ieee.org/facebook-ai-launches-its-deepfake-detection-challenge#toggle-gdpr

18 Vyberte, která z fotek je podle Vás originál:

Nápověda k otázce: *Zdroj: https://www.theverge.com/2021/3/5/22314980*

Deep fake vlevo, originál vpravo, více viz https://www.theverge.com/2021/3/5/22314980

Mnohokrát Vám děkuji za Váš čas věnovaný vyplnění mého dotazníku.

V případě zájmu o řešenou problematiku doporučuji zhlédnout následující videa:

Deep fake - Miloš Zeman, prezident ČR (CZ): www.youtube.com/watch?v=FzMnDwpKJrI

Deep fake - Tom Cruise, herec (EN): www.youtube.com/watch?v=wq-kmFCrF5Q