

UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

INSTITUT KOMUNIKAČNÍCH STUDIÍ A ŽURNALISTIKY

KATEDRA ŽURNALISTIKY



**SVOBODA PROJEVU NA INTERNETU A CENZURA JAKO
PROSTŘEDEK K OCHRANĚ SOUKROMÍ UŽIVATELŮ**

BAKALÁŘSKÁ PRÁCE

JANA BRIŠOVÁ

2020

PROHLÁŠENÍ

1. Prohlašuji, že jsem předkládanou práci zpracoval samostatně a použil jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne 21. 5. 2020

Jana Brišová

BIBLIOGRAFICKÝ ZÁZNAM

Brišová, Jana. *Svoboda projevu na internetu a cenzura jako prostředek k ochraně soukromí uživatelů*. Praha, 2020. 87 s. Bakalářská práce (Bc.). Univerzita Karlova, Fakulta sociálních věd, Institut komunikačních studií a žurnalistiky. Katedra žurnalistiky. Vedoucí diplomové práce doc. PhDr. Václav Moravec, Ph.D., Ph.D.

ROZSAH PRÁCE: 143 729 znaků

AUTOR PRÁCE: Jana Brišová

STUDIJNÍ PROGRAM: Žurnalistika

VEDOUČÍ PRÁCE: PhDr. Václav Moravec, Ph.D., Ph.D.

ROK OBHAJOBY: 2020

ABSTRAKT

Cílem této práce je poskytnout komplexní analýzu svobody projevu na internetu, jejího porušování a možností uchování soukromí v kyberprostoru založenou na teoretickém průzkumu práva na svobodu projevu, práva na soukromí a zejména jejich ochrany. V návaznosti na tuto teoretickou analýzu pak práce přistupuje k zevrubné analýze digitálního prostředí jako prostoru k realizaci svobody projevu i k narušování osobnostních práv. Zkoumá také vstřícnost digitální sféry k požadavkům uživatelů na uchování soukromí, porušování práva na svobodu projevu a cenzuru internetu, což demonstruje na kazuistikách zemí, jež k těmto krokům přistupují. Na to navazuje hledáním způsobů, které umožňují internetovou cenzuru obejít včetně možnosti anonymního pohybu na internetu. Anonymita rozebírá také jako nástroj k zajištění ochrany soukromí, jakož i zdroje nástrah a nebezpečí.

ABSTRACT

The aim of this thesis is to provide a complex analysis of free speech on the internet, violation of this right and was how to protect own privacy in cyberspace based on a theoretical exploration of protection of free speech, right to privacy and collision of these rights. Based on this theoretical analysis this thesis seeks to provide a comprehensive analysis of the cyberspace as a space to realize free speech as well as violating of right to privacy. This thesis also explores the responsiveness of the Internet to the users' demands on privacy, violations of the right to freedom of expression, and censorship of the Internet, as demonstrated by the case studies of countries taking these steps. This is followed by a research for ways to circumvent Internet censorship, including the possibility of anonymity on the Internet. Anonymity is also discussed as a tool to protect privacy as well as sources of dangers.

KLÍČOVÁ SLOVA

svobodný projev, svoboda projevu na internetu, cenzura, ochrana soukromí, anonymita, digitální stopa

KEYWORDS

free speech, free speech on the Internet, censorship, privacy protection, anonymity, digital footprint

TITLE

Free speech on the Internet and censorship as a way to protect users' privacy

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala panu PhDr. Václavu Moravcovi, Ph.D., Ph.D. za veškeré konstruktivní rady, kterými mě vedl na správnou cestu, i za přizpůsobení svých konzultací bezprecedentní situaci, z níž náš svět ale dozajista vyjde silnější a zodpovědnější. Stejně tak bych chtěla poděkovat mým přátelům, zejména Tomáši Šedivému, který mi svou oporou vždy usnadní a zpříjemní jakýkoli úkol, včetně psaní této práce.

OBSAH

Úvod	1
1. Projev na cestě ke svobodě.....	5
1. 1. <i>Teoretické vymezení pojmu projev a jeho relativní výklad</i>	5
1. 1. 1. Kritéria ústavou chráněného projevu	7
2. Právní úprava svobody projevu v ČR	13
3. Zásahy do svobody projevu	15
3. 1. <i>Charakter zásahů do svobody projevu a kdy je lze připustit</i>	15
3. 2. <i>Formy zásahů do svobody projevu</i>	17
3. 2. 1. Předběžné zásahy.....	17
3. 2. 2. Následné zásahy	19
3. 3. <i>Typy regulace svobody projevu</i>	20
3. 3. 1. Obsahově neutrální regulace	20
3. 3. 2. Obsahově zaměřená regulace	20
4. Právní úprava ochrany osobnosti v ČR.....	23
4. 1. <i>Ochrana osobnosti v soukromém právu</i>	24
4. 2. <i>Ochrana osobnosti ve veřejném právu</i>	25
5. Svoboda projevu v kolizi s osobnostními právy	28
5. 1. <i>Střet dvou ústavních práv</i>	28
5. 2. <i>Kritéria posuzování pro rozhodnutí o precedenci práva</i>	29
5. 2. 1. Objekt difamujícího sdělení	29
5. 2. 2. Obsah a forma projevu.....	30
5. 2. 3. Status autora	32
5. 2. 4. Úmysl, cíl, motiv	32
6. Digitální prostředí jako prostor k realizaci svobody projevu	33
6. 1. <i>Komparace éry tradičních a digitálních médií v kontextu svobody projevu</i>	33
6. 2. <i>Šíření informací na internetu a digitální stopa uživatelů</i>	37
6. 2. 1. Právo být zapomenut	39
6. 2. 2. Privacy paradox.....	40
6. 3. <i>Zásahy do práva na svobodu projevu specifické pro on-line prostředí</i>	41
6. 3. 1. Dimenze internetové cenzury	44

6. 3. 2.	Metody omezování přístupu k obsahu	46
6. 3. 3.	Kazuistiky implementované internetové cenzury	49
6. 3. 4.	Boj proti internetové cenzuře a její obcházení.....	54
6. 3. 5.	Hrozby v kyberprostoru a cenzura jako nástroj k ochraně uživatelů.....	57
6. 4.	<i>Anonymita jako zdroj bezpečnosti i nebezpečí na internetu</i>	<i>59</i>
6. 4. 1.	Důvody využívání anonymity	61
6. 4. 2.	Jak anonymity dosáhnout.....	63
6. 4. 3.	Pozitivní implikace anonymity.....	64
6. 4. 4.	Negativní implikace anonymity.....	67
6. 4. 5.	Možná pravidla využívání anonymity a jak s ní nakládat	68
Závěr	70	
Zdroje.....	73	
Seznam grafů.....	85	
Seznam obrázků.....	86	
Seznam příloh	87	
Přílohy.....	88	

ÚVOD

V dnešním moderním a globalizovaném světě je téměř jakýkoli pohyb na internetu určitou, více či méně veřejnou, formou projevu. On-line chatování, networking, čtení zpráv na zpravodajských serverech, stahování souborů a mnohé další. To vše v digitálním světě představuje způsoby získávání nebo sdílení informací.¹ Historicky nebývalý technologický vývoj v posledních dvou stoletích umožnil a následně závratně urychlil jejich okamžité šíření všude po světě, a také k nim poskytl volný přístup.

Už po nejméně dvě desetiletí převládající a stále aktuální světový trend představují sociální sítě, které způsobily obrovský rozmach sdílení osobních a citlivých dat na internetu. Obsah vytvářený uživateli, a to jak ten veřejně přístupný, tak i ten sdílený mezi jednotlivci nebo jejich skupinami, je v on-line prostředí uchováván. Tvorba i uchovávání ovšem představují transakci informací, a ta může být monitorována třetími stranami. Téměř každý krok jakékoli osoby v prostředí internetu proto může být sledován například poskytovateli internetového připojení, a v tom případě se stává přístupným také státu.²

Esenciálním předpokladem pro svobodné vyjadřování názorů, politických výroků nebo například náboženských přesvědčení je soukromý prostor každého člověka zbavený všech zásahů od státu, soukromého sektoru i ostatních spoluobčanů. Zásahy do soukromí, a to jak fyzického, tak virtuálního, znamenají omezení svobody projevu. Svoboda projevu je nicméně základním lidským právem, který má pevné vazby a kořeny v demokraticky fungující společnosti, protože umožňuje lidem volně se podílet na veřejné diskusi stejně jako šířit vlastní myšlenky a vytvářet si vlastní význam, který tvoří jejich osobnost.³

¹ NYST, Carly. *El derecho a la privacidad y a la libertad de expresión: dos caras de la misma moneda: (Two sides of the same coin – the right to privacy and freedom of expression)*

² Tamtéž.

³ BALKIN, Jack M. *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*

Přestože se díky novým technologiím svět stává propojenějším a tyto technologie také představují skvělý nástroj k šíření ideologie svobodného projevu napříč celým světem⁴, svoboda projevu na internetu vyvolává také důležité a závažné otázky. Některé země například tvrdí, že by mohla zapříčinit politickou nestabilitu. Komunikace na sociálních sítích, předně Twitteru a Facebooku, pomohla totiž například rozdmýchat revoluce Arabského jara, které v roce 2011 zmítaly Středním východem a severní částí Afriky.⁵

Dále svoboda projevu na internetu umožňuje sdílet a šířit potenciálně kontroverzní projevy týkající se osobních charakteristik jednotlivců, jejich zájmů, sexuální orientace, etnicity, národností a podobných témat. Těsným kontaktem kultur zvyšuje svoboda projevu riziko útoků a vzniku hate speech⁶ vůči jednotlivcům v on-line prostředí, které mají často za následek interkulturní konflikty. Ty pak mohou vyústit v nepokoje, násilí a konflikty i mimo virtuální svět.

Svoboda projevu má sice pevné a neotřesitelné postavení v demokratické společnosti, jeho ochranu v on-line prostředí je ale nutné uvážene a zodpovědně vybalancovat s právem na soukromí. Stále zde totiž existují hrozby v rámci ideologie svobodného projevu, které by neměly být podceněny. Je to právě svoboda projevu, na kterou je, více než v případě ostatních základních práv a svobod, potřeba nahlížet nejen jako na prostředek k co nejbohatšímu trhu lidských myšlenek, postojů a názorů. Proto je zapotřebí ji podrobovat i kritickému pohledu, zda její limity s ohledem na potřeby a vývoj společnosti jsou ještě schopny tuto společnost chránit, či je potřeba tyto limity upravit.⁷ Právě tyto limity musí zaručovat, že svobodu projevu nebude možné zneužít, a to jak proti jednotlivci, tak skupinám obyvatel. I přes to, že se zákony vždy snaží držet krok se všemi výdobytky novodobé společnosti, zejména pak s nezastavitelným technologickým pokrokem,

⁴ STEVENSON, Christopher. *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*, s. 531-533

⁵ SCHMITT, Michael N. a Louise ARIMATSU. *Yearbook of International Humanitarian Law: Volume 14, 2011*

⁶ Hate speech je enávistný projev, který šíří nebo podněcuje diskriminaci, nenávist nebo násilí proti jednotlivci či skupině například na základě jejich rasy, národnosti, etnicity, vzhledu, náboženského vyznání apod.

⁷ SMÍLEK, Ondřej. *Svoboda projevu a její meze*

v mnoha směrech je možné narazit na nedostatky⁸ a snaha o jejich řešení je předmětem rozsáhlých a neutichajících diskusí. Tato práce se mimo jiné zabývá jednou z těchto problematických a diskutabilních otázek, a to právě kolizí práva na svobodu projevu s právem na soukromí.

Cílem této práce je poskytnout komplexní analýzu svobody projevu na internetu, jejího porušování a možností uchování soukromí v kyberprostoru založenou na teoretickém průzkumu práva na svobodu projevu, práva na soukromí a zejména jejich ochrany.

Práce nejdříve prozkoumává relativní pojem „projev“. Dále zjišťuje, jaké projevy je možné ústavně chránit a které již do ústavního vymezení tohoto pojmu zařadit nelze, a tudíž na ně není možné ani aplikovat právo na svobodný projev. Práce soustředí také na podmínky, za jakých je možné svobodu projevu omezit a jakým způsobem tak lze učinit. Díky rozboru právní úpravy ochrany osobnosti v České republice pak práce proti tomuto základnímu lidskému právu staví rovnocenné právo na svobodný projev a předkládá možnosti řešení tohoto střetu v závislosti na sadě kritérií, podle kterých se pro precedenci toho či onoho práva soudně rozhodne.

V návaznosti na teoretickou analýzu práva na ochranu svobody projevu, soukromí a jejich kolize pak práce přistupuje k zevrubné analýze digitálního prostředí jako prostoru k realizaci svobody projevu i k narušování osobnostních práv. Zprvu poskytuje komparaci možnosti realizace svobodného projevu v tradičních a digitálních médiích. Následně zkoumá vstřícnost digitální sféry k požadavkům uživatelů na uchování soukromí. V neposlední řadě se práce zabývá porušováním práva na svobodu projevu a cenzurou internetu, které demonstruje na kazuistikách zemí, jež k těmto krokům přistupují. Popsán je i jistý druh internetové cenzury, ke kterému dochází v České republice. Práce poté hledá možnosti a způsoby, které umožňují internetovou cenzuru obejít. Na tuto problematiku poté navazuje rozbor anonymního pohybu na internetu jako nástroje k zajištění ochrany soukromí i zdroje nástrah a nebezpečí.

⁸ MARSOOF, A. *Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression*

Touto analýzou svobody projevu a práva na soukromí v kontextu digitálních médií hledá práce odpověď na následující výzkumné otázky:

***VO1:** Je možné si v digitálním prostředí uchovat soukromí a jak toho docílit i přes distinktivní rysy internetu, tedy trvalého uchovávání veškerých informací, které do něj kdy byly vloženy, a nemožnost vrátit tento krok zpět?*

***VO2:** Přináší technologický vývoj také negativní implikace či hrozby pro uživatele, jejich lidská práva a svobody?*

***VO3:** Je možné aplikovanou internetovou cenzuru nějakým způsobem obcházet a práva na svobodu projevu se domáhat?*

***VO4:** Je absolutní svoboda na internetu nutně ideálním stavem a je internetová cenzura za každých podmínek nežádoucí?*

Protože není zpracováno dostatečné množství lokálních empirických studií analyzujících tuto problematiku či některá její dílčí subtémata, je práce prvním pokusem o komplexní analýzu ochrany svobody projevu a ochrany soukromí v digitálním prostředí založenou na teoretickém poznání těchto ústavních práv. Práce souborně poskytuje informace o možné cenzuře i cenzuře potlačující základní lidská práva a svobody a předkládá možnosti obcházení této cenzury včetně detailního rozboru způsobů k tomu určených. Zároveň nevynechává ani anonymitu jako jednu z výhod i nástrah digitálního prostředí, jíž analýzu uzavírá.

1. PROJEV NA CESTĚ KE SVOBODĚ

Podoba projevu a jeho svobodného vyjadřování, jak je chápeme dnes, jsou výsledkem dlouhého historického vývoje a cesty k liberalizaci společnosti. Zřejmě nejsignifikantnější podíl na dnešní podobě svobodného projevu měl vývoj po druhé světové válce. Ten navazoval na výdobytky osvícenství a prvních kroků k demokracii, na jejichž počátku stojí přelomové liberální myšlenky Johna Stuarta Milla a vývoj po revolucích ve Francii a Anglii. Nejvýznamnějším dokumentem dodnes zůstává Všeobecná deklarace lidských práv schválená v roce 1948 Valným shromážděním OSN. Ta ve svém článku 19 stanovuje, že každý má právo na svobodu přesvědčení a projevu.⁹ Na deklaraci pak navázal Mezinárodní pakt o občanských a politických právech z roku 1966, ke kterému doposud přistoupilo 173 států světa a 6 dalších pakt podepsalo, ovšem zatím neratifikovalo (např. Čína).¹⁰ Z Všeobecné deklarace vychází taktéž Evropská úmluva o ochraně lidských práv, nejdůležitější lidskoprávní dokument sjednaný v rámci Rady Evropy a podepsaný v roce 1950. Na Všeobecnou deklaraci pak navazují úmluvy a listiny jednotlivých států, jimiž se zavazují k ochraně lidských práv, včetně Listiny základních práv a svobod, jež je součástí ústavního pořádku České republiky.

1. 1. TEORETICKÉ VYMEZENÍ POJMU PROJEV A JEHO RELATIVNÍ VÝKLAD

Teoretické ukotvení samotného pojmu *projev* je značně problematické a veskrze relativní. Obecně si ho lze vykládat dvěma způsoby. První z nich ho chápe jako všestranný výraz pro veškeré lidské jednání či projev vůle. Z tohoto pohledu můžeme za projev považovat jakékoli jednání, jež je znatelné navenek. V tomto případě sem spadají všechny způsoby, jakými lze veřejně vyjádřit svůj názor, myšlenky, umělecké smýšlení, argumentaci apod.¹¹ Podle způsobu předávání informací se komunikace, jejíž prostřednictvím je projev sdělován, dělí na verbální, nonverbální a elektronickou.¹² Verbální komunikaci lidé

⁹ OSN. *Všeobecná deklarace lidských práv*

¹⁰ UNITED NATIONS. *International Covenant on Civil and Political Rights*

¹¹ JÄGER, Petr a Pavel MOLEK. *Svoboda projevu: Demokracie, rovnost a svoboda slova*, s. 27

¹² ŘEHOŘ, Petr. *Manažerská komunikace*

realizují prostřednictvím jazyka a řeči za pomoci slov (mluvou i písmem). Komunikace nonverbální naproti tomu zahrnuje všechna mimoslovní sdělení, které člověk vědomě i nevědomě předává svému okolí. Elektronickou komunikaci pak můžeme chápat jako proces sdělování a vyměňování informací za pomoci elektronických prostředků. V tomto případě nelze do projevu zahrnout myšlenkové procesy, které navenek identifikovatelné nejsou. Tento fakt je důležitý zmínit zejména proto, že svoboda myšlení, svoboda svědomí a také svoboda náboženského vyznání spadají pod ochranu Listiny základních práv a svobod, konkrétně se jimi zabývá v článku 15.

Druhý způsob chápání pojmu „projev“ představuje jeho ústavněprávní vymezení. Tato definice slouží k identifikaci formy chování, kterou je nebo už není možné do rámce svobody projevu zařadit, aby bylo následně možné zvažovat, zda je lze tento „projev“ ústavně chránit nebo ho je naopak třeba v souladu s ústavními podmínkami omezit.

Ve většině ústav a úmluv je často jen vágně specifikováno, na jaké jednání má svoboda projevu dopadat. Evropská úmluva o ochraně lidských práv ve svém čl. 10 právo konkretizuje na názory, informace, myšlenky, dále také hovoří o obousměrné garanci (zastávat, rozšiřovat a přijímat). V rámci Listiny základních práv a svobod v ČR je konkretizována pouze svoboda projevu, a to v čl. 17 (rozbor české legislativní úpravy svobody projevu poskytuje kapitola 4.). V Listině však není blíže specifikován projev per se. Z formulace lze ale vyčíst, že rozhodně není vztažen na veškeré lidské jednání projevené navenek. Svoboda projevu negarantuje jakékoli „projevení se“ navenek, tedy jakékoli jednání či chování. Zde je možné hovořit spíše o svobodě jednotlivce jako takové. Naopak pro vymezení rozsahu svobody projevu je důležité rozlišovat mezi „projevem“ v ústavním slova smyslu a jiným projevením se (tak, jak může projevení se chápat český jazyk, například jak bylo nastíněno výše).¹³ Proto, abychom byli schopni individuálně posuzovat, zda daný projev spadá pod svobodu projevu, či již představuje jednání, je nutné si vytyčit kritéria, kterým bude rozhodování podléhat.

¹³ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 39-41

1. 1. 1. KRITÉRIA ÚSTAVOU CHRÁNĚNÉHO PROJEVU

Jak už bylo zmíněno, v ústavněprávní rovině je zabezpečena svoboda pouze některých projevů. Je proto potřeba projevy odlišit od jednání, díky čemuž bude možné stanovit, na co se ústavněprávní úpravy o svobodě projevu vztahují a na co se již ústavní regulace svobody projevu aplikovat nedá. Hranice, která odděluje projev od ostatního jednání není v mnoha případech dostatečně dobře zřetelná a definovatelná, a to zejména kvůli nejednoznačnému právnímu vymezení, které je způsobené komplexitou této problematiky. Pro toto odlišení stanovuje Michal Bartoň ve své knize *Svoboda projevu: principy, garance, meze* několik kritérií, která při posuzování individuálních případů mohou být nápomocná.

1.1.1.1. Změna normativního prostředí

Jedno z kritérií nabízí K. Greenwalt. Toto kritérium rozlišuje, zda projev „mění normativní prostředí“, jinými slovy, zda vytváří nové závazky a nároky.¹⁴ Tuto „situation-altering“, jak jednání nazývá, považuje více za jednání („action“) než za projev („speech“).¹⁵ Takové jednání mohou představovat například nejrůznější dohody, nabídky, hrozby, vyhrožování, příkazy, pokyny a další. Loupež, navádění k trestnému činu, legální i nelegální dohody a domluvy jsou touto optikou činy, které určitým způsobem mění situaci mezi aktéry a nemůžeme je tedy považovat za sdělení myšlenek. I v tomto kritériu ale můžeme nalézt určité slabiny. Jsou jimi tzv. slabé imperativy („weak imperatives“), které se, pokud jsou správně použity, pohybují na pomezí mezi činem a projevem. Slabé imperativy si je možné představit jako určité prosby nebo žádost, které svou intenzitou nedosahují pokynu ani hrozby (tedy nemění normativní prostředí), ale mohou obsahovat kupříkladu vyjádření pocitů nebo hodnot.¹⁶ Greenwalt tento rozdíl demonstruje na dvou výroku „řeknu vše o tvém pobytu ve vězení, pokud nezaměstnáš mou sestru“ (zde je patrná hrozba nebo vydírání, a je proto podle Greenwalta jednáním) a „prosím, zaměstnej mou sestru“ (zde je na rozdíl od předchozího možné vyčíst prosbu, a proto je na tento výrok podle něj možné aplikovat režim svobody projevu).¹⁷

¹⁴ GREENAWALT, Kent. *Fighting Words: Individuals, Communities, and Liberties of Speech*, s. 6

¹⁵ Tamtéž.

¹⁶ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 43

¹⁷ GREENAWALT, Kent. *Fighting Words: Individuals, Communities, and Liberties of Speech*, s. 7.

U řady pokynů, výzev, hrozeb a příkazů je také pro exaktní stanovení možnosti aplikace práva na svobodu projevu potřeba vzít v potaz míru vážnosti dané hrozby nebo míru její adresnosti. V případě, že v novinách vyjde článek s výzvou „Demisi!“, považuje se takový výrok více za vyjádření politického názoru než za konkrétní pokyn. Naopak pokud například premiér vyzve ministra slovy „podej demisi!“, stává se takový výrok pokynem, protože se pro daného ministra mění normativní prostředí a očekává se jeho reakce.¹⁸

Kritérium změny normativního prostředí tedy nehledá dělící linii mezi projevem a jiným jednáním v obsahu projevu, ale v jeho povaze.¹⁹ Síla a efekt mohou z výroku učinit jednání, zatímco pouhý obsah a význam vždy zachová projev v mezích možnosti aplikace svobody projevu. J. L. Austin tyto tři sféry označuje jako lokuční akt (obsah, pouhé pronesení slov), ilokuční akt (síla, tato sféra výroku má charakter uskutečnění určitého jednání pomocí slov) a perlokuční akt (tento akt charakterizuje účinky nebo reakci, kterou projev může vyvolat).²⁰ V případě vyhrožování násilím je potlačen význam a prim hraje síla (ilokuce), naopak u šíření poplašného hlášení je pozornost kladena na efekt (perlokuce). Čím více bude přítomen aspekt významu, tím spíše je třeba zvažovat aplikaci režimu svobody projevu.²¹

1.1.1.2. *Expresivní jednání*

V případě snahy o rozlišení projevu od jednání předsouvá toto kritérium do popředí cíl a účel jednání. Má-li být primárním cílem ochrany svobody projevu zajištění možnosti vyjadřovat vlastní myšlenky, názory či postoje, je samotná forma vyjádření až na druhém místě. V rámci dogmatiky svobody projevu bývají činy, které mají za cíl primárně vyjádřit názor či postoj, často nazývány jako tzv. expresivní či symbolické jednání. Tento čin lze ilustrovat na jednoduchém příkladu – poničení portrétu. Jak Bartoň uvádí, to může být jak součástí například úklidu, tak formou určitého projevu názoru, protestu. Existuje samozřejmě také řada omezení a regulací ošetřující takovéto projevy, které se realizace svobody projevu sice dotýkají, ovšem pouze okrajově. Jsou zaváděna zejména za účelem ochrany jiných hodnot či práv (ochrana majetku, životního prostředí apod.) a jsou

¹⁸ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 43

¹⁹ Tamtéž.

²⁰ AUSTIN, John Langshaw. *Jak udělat něco slovy*, s. 101-112

²¹ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 44-47

obsahově neutrální. Zákaz vstupu na trávník tedy není zaveden za účelem znemožnění na něm realizovat svobodu projevu, ale reguluje takové jednání za účelem pouhé ochrany trávníku. Přesto je při zavádění takových omezení a regulací nutno brát v potaz, zda daným jednáním, o jehož potenciálním omezení se diskutuje, může být taktéž vyjadřován postoj či názor. Pokud ano, je nutné zvážit míru incidentního dopadu této regulace na svobodu projevu.²²

Jistou formou expresivního jednání je i volba oblékání a doplňků, nápisů či symbolů, které jsou na oděvu umístěné. Protože se představa jednotlivců o tom, co vše lze považovat za vyjádření projevu, může značně lišit, je důležité, aby symbolický projev nesl určité poselství, ale zároveň aby i ostatní pochopili, že se o poselství jedná. Nezáleží tedy pouze na subjektivní představě o tom, v jaké míře určitým jednáním postoj vyjadřuje, ale také na objektivním zhodnocení schopností a možností takový projev vnímat.²³

1.1.1.3. Fyzický útok (vůči osobě či věci)

Toto kritérium by bylo taktéž možné zařadit pod expresivní jednání, svým výlučným charakterem a závažností je ale dobré ho uvést samostatně. Fyzický akt vůči osobě či věci je často také formou projevu agresora, například jeho nenávisti. I vandalismus ve formě graffiti spadá do této kategorie, protože jsou ve většině případů realizovány na cizích pozemcích či předmětech a proti vůli vlastníka. Při posuzování bude klíčovým kritériem to, zda je případný postih motivován omezením projevu, nebo ochranou jiných hodnot. I když symbolické projevy jistým způsobem rozšiřují svobodu projevu z klasických kanálů (mluvené slovo, obraz, text) na komunikaci za pomoci symboliky, není možné si je vykládat jako garanci svobody všeobecné.²⁴ To by vyústilo v takovou situaci, že by jakýkoli přestupek i trestný čin musel být přezkoumáván podle zásad svobody projevu.

1.1.1.4. Vážnost, bezprostřednost, adresnost, nebezpečí

Dalším důležitým kritériem pro rozhodnutí ve prospěch restrikce určitých typů projevu je jeho nebezpečnost a v jejím rámci pak také vážnost a bezprostřednost. Na vyhrožování, které je obsahem například skandování demonstrantů, bude nahlíženo jako na vyjádření

²² BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 44-47

²³ Tamtéž.

²⁴ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 50-53

politického postoje (politika bývá ze své povahy často vyhrocenou tematikou) spadajícího pod svobodu projevu, naopak pokud budou stejné výroky součástí bezprostřední komunikace dvou osob, nebude s nimi nakládáno stejně.²⁵

Prim v rámci tohoto kritéria hraje také míra adresnosti jednání, která také souvisí s mírou jeho vážnosti. Adresné vyhrožování násilím bude vždy vážnějšího charakteru než vyhrožování skupině osob vymezené pouze obecně²⁶ (například právě ve vyjádření politického postoje). Pokud zde tedy hrozba nabývá ve svém adresování konkrétnosti, nemůžeme ji hodnotit dle režimu svobody projevu.

1.1.1.5. Mlčení a vynucené projevy

Jistou formou projevu představuje také mlčení nebo nečinnost v takovém případě, kdy je jedinec k aktivnímu vyjádření názoru či postoje nucen. V americkém státě Západní Virginie soud v jednom z případů, kterým se zabýval, například uznal povinnost vzdávat poctu státní vlajce jako porušení svobody projevu.²⁷ Právo mlčet patří také do rámce svobody projevu a často je úzce spjato se svobodou vyznání.²⁸

Existují ovšem taktéž uzákoněné vynucené projevy. V mediální sféře je to například specifické požadavky na obsah v rozhlasových a televizních vysíláních, jako jsou zákazy vysílání určitého obsahu, nebo opačně povinnosti vysílat některé typy pořadů, dbát na vyváženost obsahu apod.²⁹

1.1.1.6. Společenská hodnota

Oproti kritériu změny normativního prostředí, které zkoumá spíše než obsah sdělení jeho charakter, je společenská hodnota jeho protipólem. Posuzováním společenské hodnoty projevu posuzujeme jeho obsahového zaměření. Protože samotné posouzení společenské hodnoty projevu značně podléhá subjektivnímu hodnocení a samotné kritérium je vcelku vágní a nejednoznačné, bylo by možné ve jménu tohoto kritéria z režimu svobody projevu

²⁵ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 50-53

²⁶ Tamtéž.

²⁷ OYEZ. *West Virginia State Board of Education v. Barnette*

²⁸ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 55-59

²⁹ Tamtéž.

vyloučit celou řadu nepopulárních a společensky neužitečných či škodlivých verbálních jednání, která normálně do svobody projevu patří (různé formy hanobení, projevy rasismu, obscenita, urážky apod.). I když se jedná o omezení takto společensky „nehodnotných“ projevů, je nutné tak činit v souladu s ústavními podmínkami pro omezování svobody projevu. Kupříkladu v USA, kde je ochrana svobody projevu, kterou garantuje interpretace Prvního dodatku Ústavy USA, velmi silná, neexistují žádné výslovné podmínky pro omezení svobody projevu. Určité projevy jsou pak proto vyřazovány z ústavní ochrany stanovením, že o projev v ústavním slova smyslu nejde, a proto není chráněn (v USA označován jako „unprotected speech“).³⁰ Toto rozdělení na chráněný a nechráněný projev bývá označováno jako dvouúrovňová či víceúrovňová teorie svobody projevu.³¹ Zejména tedy v USA a v další řadě států, kde neexistují ústavní podmínky k omezení svobody projevu, je klíčové rozlišení toho, co projevem je a co už je považováno za jednání, a tedy pod ochranu svobody slova nespadá.

Společenská hodnota může pro projevy představovat kritérium k částečnému omezení svobody projevu, nikoliv však k úplnému. Mezi nechráněné projevy jsou kvůli své nízké společenské hodnotě a minimálnímu přínosu veřejné debatě často řazeny útočné a agresivní projevy, výhrůžky, podněcování, obscenita, dětská pornografie, nepravdivá tvrzení a částečně také komerční projevy.³²

Pokud bychom všechna výše uvedená kritéria měli shrnout, můžeme z projevu ve smyslu čl. 17 Listiny základních práv a svobod v ČR vyčlenit taková jednání, která:

- a) mění normativní prostředí mezi původcem projevu a jeho adresátem,
- b) jsou výhrůžkou, hrozbou či obdobným jednáním s adekvátní mírou vážnosti a adresností,
- c) jsou fyzickým útokem (bez ohledu na to, jak intenzivní útok je, a na skutečnost, že byl útokem vyjádřen názor).

³⁰ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 55-59

³¹ FARBER, Daniel. *The First Amendment*

³² VOLOKH, Eugene. *The First Amendment and Related Statutes: Problems, Cases and Policy*, s. 13-210.

Na druhou stranu můžeme do projevu ve stejném smyslu zařadit jednání, která zdánlivě kritériím projevu nepodléhají. Jsou jimi:

- a) jednání, jež se díky své expresivnosti stávají projevem,
- b) nekonání či mlčení v případě, že jde o vynucený projev a subjekt dává nekonáním najevo svůj názor.³³

Protože se jedná o vymezení veskrze teoretické, v diferenciaci mezi projevem, který spadá pod ochranu svobody projevu, a jiným jednáním, které do tohoto práva zahrnuto není, je potřeba vždy každý případ posuzovat individuálně s přihlédnutím k veškerým okolnostem a počítat s výskytem jistých hraničních případů. Toto rozdělení tedy vždy bude do značné míry relativní.

³³ SMÍLEK, Ondřej. *Svoboda projevu a její meze*, s. 17

2. PRÁVNÍ ÚPRAVA SVOBODY PROJEVU V ČR

Svoboda projevu je spolu s ostatními lidskými právy zakotvena v právně nejsilnějším právním předpisu, a to v Usnesení předsednictva České národní rady č. 2/1993 Sb. ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.³⁴ Tato ustanovení lze samozřejmě aplikovat i na projevy v on-line prostředí, které taktéž poskytuje uživatelům prostor k realizování tohoto práva. Svoboda projevu je zakotvena konkrétně v článku 17, který uvádí:

- (1) Svoboda projevu a právo na informace jsou zaručeny.*
- (2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.*
- (3) Cenzura je nepřípustná.*
- (4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.*
- (5) Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon.³⁵*

Tento úvodní článek Oddílu druhého Listiny základních práv a svobod ustanovuje svobodu projevu jako jedno z politických práv, jimiž jednotlivcům zaručuje možnost účasti na politickém chodu státu. Mimo to můžeme také konstatovat, že právo na svobodu projevu se týká vztahu státu a jednotlivce, tudíž je subjektivním veřejným právem.³⁶

Pokud přistoupíme k analýze jednotlivých odstavců článku 17 upravující právo na svobodu projevu, přiznává Listina základních lidských práv a svobod České republiky každému jejímu občanovi dvě samostatná práva, a to svobodu projevu a právo na informace. I když jsou tato dvě základní práva samostatná, jejich vztah je velmi úzký a v mnohém se doplňují, či dokonce překrývají. V širším smyslu je právo na informace obecnou

³⁴ ČESKO. Ústavní zákon č. 2/1993 Sb.: Listina základních práv a svobod

³⁵ Tamtéž.

³⁶ SMÍLEK, Ondřej. *Svoboda projevu a její meze*, s. 18

součástí garance svobody projevu, v tom užším ale s právem na informace koresponduje aktivní povinnost státu konat, respektive informace poskytovat.³⁷ V právu na informace můžeme více než v právu na svobodu projevu spatřovat jeho politický charakter základního práva. Tomu také nasvědčuje zákon č. 106/1999 Sb. o svobodném přístupu k informacím, ve kterém jsou blíže specifikovány záruky a limity práva na informace.³⁸

Odstavce 2 až 4 článku 17 Listiny dále konkretizují a doplňují formulaci svobody projevu formulovaném v odstavci prvním. Zatímco první část druhého odstavce poskytující výčet způsobů vyjádření názorů a do jisté míry ztotožňující „projev“ s „vyjádřením vlastního názoru“ nemůže být nijak omezena, u druhé části je zapotřebí počítat s možností zákonného omezení vyhledávání, přijímání a rozšiřování idejí a informací.³⁹ Podle čtvrtého odstavce článku 17 Listiny totiž může vláda k takovému omezení přistoupit za předpokladu, že omezení slouží k ochraně:

- a) práva a svobody druhých,
- b) bezpečnosti státu,
- c) veřejné bezpečnosti,
- d) veřejného zdraví a mravnosti.

Tato práce se následně zaměří zejména na bod první, do kterého spadají osobnostní práva včetně práva na soukromí a ochranu osobnosti, na jejichž kolizi s právem na svobodu projevu v prostředí internetu se práce zaměřuje.

³⁷ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 79

³⁸ ČESKO. *Zákon č. 106/1999 Sb., o svobodném přístupu k informacím*

³⁹ SMÍLEK, Ondřej. *Svoboda projevu a její meze*, s. 20

3. ZÁSAHY DO SVOBODY PROJEVU

3. 1. CHARAKTER ZÁSAHŮ DO SVOBODY PROJEVU A KDY JE LZE PŘI- PUSTIT

V případě, že dle výše zmíněných kritérií dojde k rozhodnutí učinit do svobody projevu zásah (a opět se bavíme i o on-line prostředí), je podle M. Bartoně obecně možné rozdělit charakter těchto zásahů na:

1. omezení ve vztahu k informacím
 - a. omezení vyhledávání informací, respektive přístupu k nim,
 - b. omezení šíření informací,
 - i. omezení šíření pravdivých informací,
 - ii. omezení šíření nepravdivých informací,
2. omezení ve vztahu k názorům,
 - a. omezení v přístupu k názorům,
 - b. omezení šíření názorů,
3. omezení nesouvisející s obsahem projevu.

U omezení k přístupu k informacím (bod [1 a](#)) není zapotřebí rozlišovat mezi přístupem k pravdivým či nepravdivým informacím, protože i kdybychom dohledávali nepravdivou informaci, stále se jedná o vyhledávání pravdivého faktu, tedy jímž je pouhá existence onoho nepravdivého tvrzení. Omezení přístupu k informacím je pak dáno důvody bezpečnostními (utajované informace), ochranou práv třetích osob (citlivé údaje, ochrana soukromí, autorská práva, obchodní tajemství) nebo ochranou zájmů na fungování justice (informace ze soudních spisů).⁴⁰

V případě omezení šíření informací (bod [1 b](#)) je už mezi pravdivými a nepravdivými informacemi rozlišovat nejen nutné, ale i logické a podstatné. Co se týče omezení šíření pravdivých informací, důvody k takovým krokům se v zásadě shodují s těmi, pro které

⁴⁰ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 125-126

není možné mít k těmto informacím ani přístup, tedy z důvodů možného ohrožení bezpečnosti, zásahů do osobnostních práv či práv duševního vlastnictví třetích osob či zásahů do činnosti justice, respektive práva na spravedlivý proces. Důvodem pro omezení šíření nepravdivých informací bývá především skutečnost, že tvrzená nepravda může být v určitém ohledu nebezpečná či škodlivá (například šíření poplašné zprávy). Specifickou otázkou pak bývají pak tzv. revizionistické projevy, tedy popírání či zpochybňování určitých historických událostí spojených se závažnými zločiny (například genocida, zločiny proti lidskosti, holocaust).⁴¹

Omezením přístupu k názorům (bod [2 a](#)) je zamýšleno, spíše než obecný přístup k informacím, právo názory slyšet. V tomto případě se tedy nejedná o subjektivní právo, ale spíše podpůrný argument zdůrazňující dopad restrikce svobody projevu na utlumení veřejné debaty a omezení plurality názorů.⁴²

Základem zásahů do svobody projevu ve vztahu k omezení názorů je omezení jejich šíření či sdělování (bod [2 b](#)). Není zde relevantní, zda jsou pravdivé či nikoli, hlavními kritérii při rozhodování o restrikcích bude míra expresivnosti, vulgárnosti, útočnosti či obsahové nebezpečnosti názoru. Takové názory mohou být nebezpečné, zraňující či škodlivé. Cílem zásahů do projevů takové povahy je pak typicky ochrana osobnostních práv, popřípadě důstojné činnosti státních orgánů či úředních osob, mravnosti, veřejného pořádku či bezpečnosti.⁴³

I přes tato vymezení stále platí, že zásahy veřejné moci do subjektivních názorů by měly být spíše výjimečné a posuzovány případ od případu.

Omezením nesouvisejících s obsahem projevu ([bod 3](#)) se práce krátce věnuje v podkapitole [3. 3. 1.](#). Obecně platí, že restrikcemi sledovaný cíl nijak nesouvisí se sdělovaným obsahem omezovaného projevu.

⁴¹ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, str. 127-128

⁴² Tamtéž.

⁴³ Tamtéž.

3. 2. FORMY ZÁSAHŮ DO SVOBODY PROJEVU

Zásahy do svobody projevu, a to jak v off-line, tak v on-line světě, mohou nabývat dvou forem. První z nich je předběžná, tedy zásahy preventivní, u kterých je možné posuzovat jejich závažnost podle povahy a intenzity. Druhou skupinu představují zásahy následné, tedy forma určitého postihu za uskutečnění projevu. Obecně platí, že předběžné zásahy do výkonu určitých ústavně zaručených práv jsou již ze své podstaty závažnější než zásahy následné. Svoboda projevu jako politické právo je součástí i práv jako shromažďovací či sdružovací. Některá z takových práv se pak dotýkají přístupu do veřejné diskuse, zásahy do svobody projevu pak mohou tento přístup znemožnit. Proto je mocenské znemožnění či pozdržení vstupu do veřejné diskuse vždy závažnější než některé aktéry z diskuse vyloučit ex post za porušení pravidel.⁴⁴

3. 2. 1. PŘEDBĚŽNÉ ZÁSAHY

3.2.1.1. *Cenzura*

Do předběžných zásahů spadá například cenzura. Ta je obecně považována za jednu z nejzávažnějších forem omezování svobody projevu a v demokratických státech je nepřijatelná. Český právní kontext cenzuru nedefinuje ani v rovině ústavní, ani zákonné. Cenzura je tedy běžně vykládána jako státní kontrola informací, obsahů a materiálů určených k uveřejnění zejména v hromadných sdělovacích prostředcích.⁴⁵ Jejím jádrem je předběžné znemožnění zveřejnění určitého projevu. Zákaz cenzury tak ústavně brání nežádoucí preventivní filtraci informací a názorů vstupujících do veřejné diskuse. Listina základních práv a svobod v čl. 17 odst. 3 cenzuru výslovně zakazuje a svým zněním tak dále konkretizuje obecnou garanci svobody projevu a její přípustné výjimky. Listina tedy stanovuje, že svobodu projevu je možno za vymezených podmínek omezit, nikoliv však formou cenzury.⁴⁶ Odstavec 3 stručně zakazující cenzuru však není základním právem jednotlivce, adresátem tohoto zákazu je moc veřejná. Pokud se bavíme například o sporech mezi novináři a jejich nadřízenými či vydavateli uvnitř sdělovacího prostředku či mezi příspěvateli do diskuse na internetových fórech a správci těchto diskusí, nejedná

⁴⁴ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, str. 127-128

⁴⁵ ADAMOVIČ, Karolína. *Politologický slovník*, s. 21

⁴⁶ Tamtéž.

se o cenzuru v právním slova smyslu, která by dle listiny byla nepřipustná, nýbrž o tzv. seberegulaci nebo také samoregulaci či autocenzuru daného média či příslušného fóra, která je nejen přípustná, ale pro rozumné fungování veřejného mediálního prostoru a jeho subjektů často nezbytná,⁴⁷ ovšem pozbývá reálný právní základ.

I u cenzury je se možné setkat s rozlišením na předběžnou a následnou. Pokud platí, že cenzurou je pouze preventivní omezení, je následná cenzura protimluvem. Při zachování smyslu ústavního zákazu cenzury je za předběžnou cenzuru možné považovat institucionální znemožnění určitý text vůbec vyhotovit či pronést určitý projev⁴⁸. Následnou cenzurou se potom rozumí úřední kontrola publikace sice po jejím vyhotovení, ale předtím, než začne být šířena, přičemž nepřipustné pasáže se například dodatečně začerní. I tak bude tedy zachován prvek předběžnosti, tedy že se zabrání dalšímu šíření a pro určitou část publika se přístup k obsahu znemožní.⁴⁹ V případě této následné cenzury může dojít také k ukládání trestů, pokud publikované obsahy nejsou v souladu s nařízeními.

Cenzurou zakotvenou v Listině je podle Wagnerové a kol. třeba rozumět cenzuru předběžnou.⁵⁰ Tomuto názoru oponuje V. Knapp, který ve smyslu článku 17 odst. 3 Listiny cenzurou rozumí cenzuru jak předběžnou (preventivní), tak následnou.⁵¹

Následnou cenzurou může být taktéž zabavování či jiné znemožnění šíření materiálů, jejichž obsah zákon vyjímá z množiny projevů chráněných Listinou.⁵² Následná cenzura je v přímé souvislosti s možností zákonného omezení svobody projevu podle čl. 17. odst. 4 Listiny – následná cenzura tedy může být povolena, musí však být vykládána ve smyslu tohoto odstavce, který stanovuje meze svobody projevu.⁵³ Český právní řád ovšem

⁴⁷ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, str. 131

⁴⁸ Předběžnou cenzuru prováděla například komunistická strana v Československu v 50. a 60. letech 20. století prostřednictvím Hlavní správy tiskového dohledu – publikován směl být jen takový obsah, který její pracovníci předem schválili a opatřili cenzurním číslem, a publikování jakéhokoli jiného obsahu bylo trestné.

⁴⁹ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, str. 133

⁵⁰ WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod: komentář*, s. 432–433.

⁵¹ PAVLÍČEK, Václav. *Ústava a ústavní řád České republiky: komentář*, s. 160.

⁵² SMÍLEK, Ondřej. *Svoboda projevu a její meze*, s. 21

⁵³ Tamtéž.

nerozlišuje cenzuru na předběžnou a následnou. Cenzura je tedy běžně vykládána jako státní kontrola informací, obsahů a materiálů určených k uveřejnění zejména v hromadných sdělovacích prostředcích.⁵⁴ Jejím jádrem je předběžné znemožnění zveřejnění určitého projevu. Zákaz cenzury taky ústavně brání nežádoucí preventivní filtraci informací a názorů vstupujících do veřejné diskuse.

3.2.1.2. Předběžná opatření

Jiné formy předběžných omezení můžeme od cenzury odlišit, pokud omezení nespočívá v povinnosti předkládat obsah projevu předem ke schválení, ale je reakcí na konkrétní tvrzenou protiprávnost, která může být šířením daného obsahu způsobena. Jedná se tak o ochranu individuálního práva na návrh jeho nositele.⁵⁵ Taková omezení představují předběžná opatření, která by mohla být považována za přípustná (s ohledem na obecný zákaz cenzury) zejména z důvodu nevratnosti možné újmy. Realizace takových zásahů by ale měla přijít výhradně ze strany soudů, nikoli orgánů výkonné moci. Předběžná opatření vydávaná soudy mohou mimo jiné obsahovat též povinnost zdržet se určitého jednání, což v praxi může znamenat také zákaz zveřejnit text, zákaz odvíšlat určitou reportáž či zákaz distribuce konkrétní knihy apod.⁵⁶ Mezi předběžné zásahy můžeme zařadit zabavení materiálů ke zveřejnění či nutnost licencování nebo získání určitého druhu povolení potřebného k realizaci svobody projevu.

3. 2. 2. NÁSLEDNÉ ZÁSAHY

Jak již bylo zmíněno, omezení *ex post* jsou svým charakterem mnohem závažnější než omezení předběžná. Následným omezením je od autorů sporných sdělení či osob, které za obsah sdělení nesou právní odpovědnost (například vydavatelů tisku nebo provozovatelů vysílání), právní odpovědnost vyvozována.

Jednak tedy musí být posouzena legitimita zásahu do svobody projevu (zda omezení podléhá podmínkám pro možnost omezení podle Listiny a Evropské úmluvy), důležitým rozměrem je ale také, jakými prostředky bude postih realizován (povaha trestu), jakou bude

⁵⁴ ADAMOVIČ, Karolina. *Politologický slovník*, s. 21.

⁵⁵ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, str. 133-134

⁵⁶ Tamtéž.

mít trest intenzitu (výše trestu) a jaké následky vyvolá. Rozsudky jako trestní stíhání, povinnost se omluvit, finanční náhrada či další sankce nemají pouze funkci reparační či satisfakční, ale zároveň preventivní. Zvolená sankce je tak důležitá jak pro subjekt, tak zejména pro budoucí veřejnou debatu, pro kterou může být neadekvátně zvolený druh trestu a jeho výše odstrašující, a trest tak může vyvolat silnější utlumení veřejné debaty, než je žádoucí.⁵⁷

3. 3. TYPY REGULACE SVOBODY PROJEVU

Jedním z nejdůležitějších a nejobecnějších kritérií, podle kterého můžeme diferenciovat typy možných omezení svobody projevu, je přítomnost prvku obsahové regulace. Podle toho můžeme regulaci dělit na obsahově neutrální a obsahově zaměřenou.

3. 3. 1. OBSAHOVĚ NEUTRÁLNÍ REGULACE

Za obsahově neutrální považujeme regulaci takovou, jež není zaměřena na poselství, které chce autor projevem předat, ale na jiné aspekty onoho projevu, jakými může být například způsob jeho realizace (např. vylepování plakátu, instalování billboardů apod.), doba (např. šíření sdělení ve večerních hodinách za předpokladu, že narušuje noční klid) nebo místo (např. prostor s různými ekologickými omezeními atp.). Omezení tedy může být realizováno za účelem ochrany jiných práv či hodnot, které nesouvisejí se sdělovaným obsahem.⁵⁸ Taková omezení sledují jiný cíl, než je zamezit šíření určitého sdělení.

3. 3. 2. OBSAHOVĚ ZAMĚŘENÁ REGULACE

Obsahově zaměřená regulace oproti té neutrální má za cíl omezit poselství, které je projevem sdělováno. Tento typ regulace představuje omezení závažnějšího charakteru, neboť stát se zde z role moderátora, který reguluje diskusi celoplošně, pasuje do role jednoho z účastníků diskuse tím, že rozhoduje, jaké členy do diskuse vpustí nebo z již probíhající diskuse vyloučí kvůli tomu, co chtějí sdělit.

⁵⁷ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 147

⁵⁸ STONE, Geoffrey R. Content-Neutral Restrictions

3.3.2.1. Regulace názoru

Omezení názoru je jedním z nejzjevnějších případů obsahově zaměřené regulace. Jejím předmětem je konkrétní názor, postoj, idea a v praxi se nevyskytuje často.⁵⁹

3.3.2.2. Regulace tématu

Omezení tohoto typu se oproti omezení názoru nevztahuje pouze na jeden z postojů v rámci diskuse o určitém tématu, ale na samotné téma jako takové. Takové omezení ovšem může stejně jako určitou názorovou skupinu ochraňovat, tak necíleně názor této skupiny potlačovat. Pokud by byla s cílem zabránit verbálním útokům na homosexuální menšinu zakázána diskuse na téma sexuální orientace, vedlejším a nežádoucím efektem by bylo znemožnění této minoritě prosazovat svá práva.⁶⁰

3.3.2.3. Regulace obsahu a symbolických projevů

Specifickou kategorií představují taková jednání, u kterých je sporné, zda je můžeme jejich charakteristikou zařadit mezi projevy, či nikoli. V případě, že bude určité jednání vyhodnoceno jako projev, bude také na jeho případnou regulaci nahlíženo jako na omezování svobody projevu a bude zapotřebí posoudit, zda omezení podléhá ústavním podmínkám, za kterých je možné projev omezit. Dále je zapotřebí stanovit, zda je jednání regulováno kvůli svému obsahu, nebo zda je regulace obsahově neutrální. V případě takzvaných symbolických projevů bude posuzování konkrétních případů ještě komplikovanější. Jako příklad zde může sloužit nakládání se státní vlajkou, nebo dokonce její demonstrativní spálení. Několik soudních rozhodnutí, které takové jednání vyhodnotila jako expresivní projev a postih za její spálení označila jako obsahovou restrikcí⁶¹ (omezení bylo tedy shledáno jako protiústavní zásah do svobody projevu), může soužit jako precedens k případům, které budou následovat. Spornými případy bývá často právě expresivní jednání, nicméně pod ochranu spadá jak obsah projevu, tak i emoce, které spoluvytváří jeho vyznění. Vulgární projevy tedy nemůžeme automaticky považovat za protiprávní jen kvůli jejich expresivitě.

⁵⁹ WEINSTEIN, James. *Hate Speech, Pornography, And Radical Attacks On Free Speech Doctrine*, s. 36.

⁶⁰ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, 170

⁶¹ ELY, John Hart. *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*

Tato dichotomie na obsahově neutrální a obsahově zaměřenou regulaci je klíčová zejména v USA, kde představuje hlavní faktor určující přísnost uloženého trestu. V Evropě, zejména z důvodu možnosti omezení svobody projevu, která je ukotvena v evropských ústavách i Evropské úmluvě o ochraně lidských práv, je případ od případu vyvažována na jedné straně hodnota svobody projevu a na druhé hodnota práva, se kterým koliduje.

4. PRÁVNÍ ÚPRAVA OCHRANY OSOBNOSTI V ČR

Ochrana osobnosti je jedním ze základních lidských práv, je zaručeno každému člověku a chrání ho před zásahy veřejných i soukromých subjektů do jeho fyzické i psychické integrity.⁶² Právo na ochranu osobnosti je aplikováno a možno vymáhat samozřejmě i v on-line prostředí.

Toto základní lidské právo je chráněno jak na úrovni ústavní, tak zákonné. Nejvyšší ústavní ochranu zajišťuje Listina základních práva svobod v člancích 7, 8, 10, 12 a 13, které garantují ochranu nedotknutelnosti osoby, osobní svobody, cti a lidské důstojnosti, dobré pověsti a jména. Garantují také ochranu před neoprávněným zásahem do soukromého a rodinného života, ochranu osobních údajů, obydlí a listovního tajemství.⁶³ Soukromí, rodinný život, obydlí a korespondenci chrání také ve svém článku 8 Evropská úmluva o ochraně lidských práv.⁶⁴

Chráněné zájmy jednotlivce tedy můžeme rozdělit do několika kategorií – osobní život jednotlivce, rodinný život, soukromí v prostorovém rozměru a důvěrnost komunikace.⁶⁵ Tato práce se s ohledem na své téma bude dále soustředit především na soukromí a osobní život jednotlivce.

Na zákonné úrovni je právo na ochranu osobnosti upraveno především v zákoně č. 89/2012 Sb., tedy občanském zákoníku, a speciální úprava některých dílčích otázek je obsažena v dalších zákonech, jako je například zákon č. 40/2009 Sb., tedy trestním zákoníku ve znění pozdějších předpisů.⁶⁶

⁶² POUPEROVÁ, Olga. *Regulace médií*, s. 217-218

⁶³ ČESKO. *Ústavní zákon č. 2/1993 Sb.: Listina základních práva a svobod*

⁶⁴ EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA. *Evropská úmluva o ochraně lidských práva*

⁶⁵ MORAVEC, Ondřej. *Mediální právo v informační společnosti*, s. 142.

⁶⁶ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 27

4. 1. OCHRANA OSOBNOSTI V SOUKROMÉM PRÁVU

Hlavním předpisem, jenž zajišťuje ochranu osobnosti, je Občanský zákoník (zákon č. 89/2012 Sb.). Věnuje se mu především v §3 odst. 1 a 2 písm. a):

„(1) Soukromé právo chrání důstojnost a svobodu člověka i jeho přirozené právo brát se o vlastní štěstí a štěstí jeho rodiny nebo lidí jemu blízkých takovým způsobem, jenž nepůsobí bezdůvodně újmu druhým.

(2) Soukromé právo spočívá zejména na zásadách, že

a) každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí.“⁶⁷

Podrobněji se ochraně osobnosti dále věnuje v oddíle pátém, který chrání jméno a bydliště člověka, ale zejména v oddíle šestém (Osobnost člověka) v § 81 až § 117, pro účely této práce zejména § 81 až § 90. Zásadním je ustanovení § 81, které v odst. 1 poskytuje nejen ochranu osobnosti člověka, ale také povinnost ctít svobodné rozhodnutí žít podle svého. Odst. 2 poté obsahuje generální klauzuli s výčtem hodnot, kterým Občanský zákoník poskytuje ochranu.⁶⁸ Mezi ty patří ochrana života, důstojnosti, zdraví, vážnost, čest, soukromí, projevy osobní povahy a právo žít v příznivém prostředí.

Tyto zákonné úpravy se shodují s vymezením práva na ochranu osobnosti v Listině základních práv a svobod i Evropské úmluvě o ochraně lidských práv a dále je konkretizují. Ustanovení § 82 Občanského zákoníku však navíc zakládá nároky člověka při neoprávněném zásahu do těchto práv, kdy má člověk právo domoci se upuštění od zásahu, případně odstranění následku, a dokonce po smrti člověka toto právo přechází na osoby blízké.⁶⁹

⁶⁷ ČESKO. § 81 zákona č. 89/2012 Sb., občanský zákoník

⁶⁸ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 28.

⁶⁹ Tamtéž.

Zákon §84 ustanovuje, že „zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.“⁷⁰ Takové svolení je potřebné taktéž pro rozšiřování této podoby.

V § 86 až § 90 zákon zakazuje zasáhnout do soukromí člověka bez zákonného důvodu. Nesmí být narušeny především soukromé prostory, nelze sledovat soukromý život či písemnosti a nesmí o tom být ani pořizovány a šířeny záznamy.

Pokud tato ustanovení vztáhneme na prostředí internetu, v případě, že dojde ke zveřejnění fotografie konkrétní osoby bez jejího souhlasu, má právo se bránit. Může se jednat například o případy, kdy se osoba na internetu vydává za někoho jiného, kdy dojde ke zveřejnění fotografie ze soukromého života nebo zveřejnění fotografie, o jejímž pořízení neměla předmětná osoba tušení.

Dotčená osoba má při zásahu do svých osobnostních práv podle § 2894 až § 2971 právo na náhradu nemajetkové újmy, a to primárně způsobem morální satisfakce. Pokud není toto odčinění dostatečné, má osoba právo na náhradu finanční. Ke každému případu je ale nutné přistupovat individuálně. Pokud by například v prostředí internetu byly pouze mazány komentáře a příspěvky, mohlo by takové jednání být považováno za zasahování do svobody projevu.

4. 2. OCHRANA OSOBNOSTI VE VEŘEJNÉM PRÁVU

Osobnost člověka je chráněna také ve veřejném právu, a to v odvětvích trestního a správního.

V trestním právu chrání osobnost člověka § 181 (trestný čin poškození cizích práv) a § 184 (trestný čin pomluvy) vymezením trestných činů proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství. Chráněným objektem jsou hodnoty vymezené čl. 10 Listiny základních lidských práv a svobod (ochrana osobní cti, dobré pověsti a jména).⁷¹ Ke spáchání takového trestného činu je třeba se dopustit podvodného jednání,

⁷⁰ ČESKO. § 81 zákona č. 89/2012 Sb., občanský zákoník

⁷¹ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 30

keré způsobí vážnou újmu na právech jiné osoby.⁷² Objektem takového trestného činu je i pomluva spáchaná prostřednictvím sdělovacích prostředků, tedy i internetu. Nepravdivý údaj se může týkat jednání, chování či vlastností oběti trestného činu a může následně způsobit újmu v zaměstnání, poškodit vztahy v rodině nebo způsobit jinou závažnou újmu.⁷³ Pokud pachatel spáchá pomluvu prostřednictvím internetu, můžeme ji považovat za velmi efektivní, protože se zde může informace dostat k velmi širokému, předem neurčenému, okruhu osob a je vysoce pravděpodobné, že se informace dostane k většině osob, jež oběť trestného činu zná. Pro oběť to tedy znamená mnohem horší dopad, proto dikce trestního zákoníku stanovuje, že pachatel takto spáchaného činu může být potrestán vyšším trestem.⁷⁴

Správní právo taktéž upravuje některá protiprávní jednání zasahujících do ochrany osobnosti, avšak tato jednání jsou typicky méně společensky závažná (přestupky či delikty), proto se nejčastěji řeší sankcemi.⁷⁵

Zákon č. 200/1990 Sb., zákon o přestupcích v § 49 odst. 1 písm. a) vymezuje přestupek proti občanskému soužití jako takový, který je spáchán ublížením na cti, urážkou nebo vydáním v posměch. Ublížení na cti je nutné posuzovat podle konkrétních okolností, ovšem nezáleží na tom, zda byl výrok pronesen veřejně nebo soukromě, před dotčenou osobou nebo někým jiným. Za takové jednání lze ve správním řízení uložit pokutu.⁷⁶ Pokud je ale projev učiněn v mezích ustanovení čl. 17 Listiny základních lidských práv a svobod, projev nenaplnuje požadavek protiprávnosti, a tudíž se nejedná o přestupek ani trestný čin, za který může být uložena sankce či trest.

Ublížení na cti, urážku i zesměšnění je samozřejmě možné páchat i v prostředí internetu. Zda se jedná o přestupek proti občanskému soužití, či o trestný čin pomluvy je nutné

⁷² JELÍNEK, Jiří a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*, s. 241.

⁷³ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 31

⁷⁴ Tamtéž.

⁷⁵ JELÍNEK, Jiří a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*, s. 43.

⁷⁶ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 32

posuzovat individuálně podle intenzity zásahu do osobnostního práva, způsobu provedení či úmyslu osoby, která se takového jednání dopustila.⁷⁷

⁷⁷ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 32

5. SVOBODA PROJEVU V KOLIZI S OSOBNOSTNÍMI PRÁVY

5. 1. STŘET DVOU ÚSTAVNÍCH PRÁV

Právo na ochranu osobnosti a svobodu projevu jsou dvě ze základních lidských práv představující zásadní hodnoty v demokratické společnosti. Proto je také třeba je náležitě ochraňovat, a to jak ve světě reálném, tak v tom virtuálním. Tato dvě práva se ale už ze své obecné povahy poměrně často dostávají do konfliktu. Je potřeba je proto vyvažovat, aby se nedošlo k narušení rovnováhy ústavou zaručených práv.⁷⁸ V případě, že se do kolize se svobodou projevu dostanou osobnostní práva, nejedná se o střet veřejných hodnot, jako jsou veřejná bezpečnost nebo bezpečnost státu, ale o konflikt dvou ústavně zaručených práv, přičemž osobnostní představují individuální základní práva třetích osob. Těmi jsou zejména ochrana cti, důstojnosti, soukromí, dobré pověsti či dobrého jména. V souvislosti s dotčením těchto práv se nejčastěji jedná o nactiutrhání, difamacii, urážku či pomluvu. I když je svoboda projevu i osobnostní práva stejnou měrou chráněna ústavou, ochrana práv třetích osob je výslovně v lidskoprávních katalogích zmiňována jako jeden z legitimních cílů pro omezení svobody projevu.⁷⁹

Dle právní teorie můžeme rozlišit dva typy konfliktů. Prvním z nich je takzvaný *nepravý konflikt*. Ten je běžně charakterizován jako kolize základního práva a veřejného zájmu. Při nepravém konfliktu platí, že výjimky z jednoho ústavně zaručeného práva (svobody projevu) z důvodu ochrany ústavně předvídaného legitimního cíle je třeba aplikovat restriktivně, tedy v pochybnostech vždy rozhodovat ve prospěch svobody projevu.⁸⁰

Druhým je takzvaný *pravý konflikt*, který lze obecně charakterizovat jako střet dvou základních, stejně postavených práv. V této situaci záleží na uvážení a rozhodnutí soudů, které z práv vyhodnotí v konkrétních případech jako hodné přednostní ochrany. K co možná nejspravedlivějšímu rozhodnutí slouží soudům test proporcionality, tedy

⁷⁸ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 39

⁷⁹ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 238-239

⁸⁰ Tamtéž.

právní princip, který má za úkol zaručit, aby při konfliktu dvou sobě si konkurujících subjektivních práv bylo hodnotnější z nich chráněno, avšak s minimálním dopadem na to právo, ke kterému se rozhodnutí nepřiklonilo.⁸¹ Zde ovšem výjimky ze svobody projevu nelze aplikovat restriktivně, neboť výjimkou zároveň chráníme jiné kolidující základní právo, tudíž není možné určit, které z práv je základem a které výjimkou z něj.⁸²

Nabízejícím se řešením takových konfliktů by se mohla zdát prioritizace jednoho ze základních práv, nicméně obě jednotlivá práva jsou natolik rovnocenná a natolik důležitá pro zachování demokratických principů ve společnosti, že je nutné na každý případ střetu nahlížet individuálně. Hierarchizací, která by byla možná aplikovat paušálně na všechny případy by nevyhnutelně vedla k zásahům do ústavně zaručených práv, které by ne vždy byly spravedlivé.

5. 2. KRITÉRIA POSUZOVÁNÍ PRO ROZHODNUTÍ O PRECEDENCI PRÁVA

Při vyvažování svobody projevu a ochrany osobnosti a upřednostnění jednoho ústavně chráněného práva před druhým je zapotřebí brát v úvahu jistá kritéria, která dopomohou k co možná nejobjektivnějšímu a nejspravedlivějšímu rozhodnutí.

5. 2. 1. OBJEKT DIFAMUJÍCÍHO SDĚLENÍ

Prvním kritériem, jež je nutné vzít při vyvažování svobody projevu a ochrany osobnostních práv v potaz, je status osoby, které mohlo do osobnostních práv být zasaženo, respektive vůči které byl projev namířen. Tyto osoby jsou rozlišovány na soukromé a veřejné, které dále členíme na veřejně činné a veřejně známé.

Co se osob veřejně činných týče, za ty považujeme osoby, které se participují na chodu veřejné moci (například politici, soudci). Vzhledem k tomu, že tyto osoby ustávají ve veřejných funkcích, je možné jejich kritiku, potažmo satiru považovat za jistý způsob kontroly. Nesmí však takový projev svým obsahem překročit únosnou mez zásahu

⁸¹ HERCZEG, Jiří. *Meze svobody projevu*, s. 46

⁸² BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 239

do osobnostních práv.⁸³ Čím více se samotný obsah projevu bude týkat veřejné činnosti oné osoby, tím spíše bude ochrana projevu posílena (tím více bude platit presumpce práva na svobodný projev). Tato mez favorizující svobodu projevu v rámci veřejného zájmu je oproti ochraně osobnostních práv soukromé osoby tím vyšší, čím vyšší pozici osoba zastává.⁸⁴ Když už je zapotřebí zásah státní moci do svobody projevu učiněného vůči osobě veřejně činné, je tak potřeba učinit pouze v míře nezbytné, aby zásah neovlivnil svobodné utváření názorů.

V případě osob veřejně známých, za které považujeme sportovce, umělce a další osoby vynikající ve svých činnostech, bude ochrana osobnostních práv silnější, na rozdíl od osob veřejně známých díky svým aktivitám v záležitostech veřejného zájmu (lobbisté, advokáti apod.), jejichž míra ochrany práv bude shodná jako v případě osob veřejně činných. Osoby veřejně známe musí z podstaty svého povolání snášet vyšší míru zásahů do svých osobnostních práv než osoby soukromé. Protože však nezastávají pozici pověřenou výkonem veřejné moci, bude ochrana jejich soukromého života vyšší než u osob veřejně činných. Takové zacházení by mohlo být lehce považováno za rozporuplné s demokratickým principem rovnosti, avšak míra nestejného zacházení musí být úměrná míře odlišnosti, kterou objekt difamace vykazuje. Osoby veřejně činné i známe by s ohledem na svou profesi měly prokázat vyšší míru tolerance zasahování do svých osobnostních práv.⁸⁵

5. 2. 2. OBSAH A FORMA PROJEVU

Klíčovým kritériem při rozhodování o možném zásahu do ústavně zaručených práv je samozřejmě obsah projevu. Existují dva charakteristické druhy neoprávněných zásahů do osobnostních práv – tzv. *difamující (nebo také skutková) tvrzení* a tzv. *hanobící kritika (někdy také hodnotící soudy)*.⁸⁶

⁸³ MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu*, s. 40

⁸⁴ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 244

⁸⁵ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 249-252

⁸⁶ HERCZEG, Jiří. *Meze svobody projevu*, s. 67.

5.2.2.1. *Skutková tvrzení*

Za skutková tvrzení je považováno sdělování faktů, u kterých následně posuzujeme, zda jsou pravdivá, či nikoliv. Jedná se o prosté sdělování skutečnosti bez subjektivního nároku autora. Vztah mezi projevem a realitou je objektivní a pravdivost, úplnost i přesnost informací sdělovaných projevem lze prokázat dokazováním.⁸⁷ I zde se můžeme setkat s mezními případy projevů, které svým obsahem vykazují aspekty jak skutkového tvrzení, tak hodnotících soudů. Děje se tak zejména ve chvíli, kdy projevem autor tvrdí určitou skutečnost za pomoci subjektivně zabarvených slov či naopak hodnotící soudy evokují určitá fakta. Proto je třeba na výroky nahlížet v širším kontextu a posuzovat vyznění celého textu, nikoliv výroky z kontextu vyjímát.⁸⁸ Skutkové tvrzení tedy překračuje meze svobody projevu tehdy, je-li nepravdivé nebo pravdu zkresluje, přesahuje-li přípustnou intenzitu nebo zasahuje-li do osobnostních práv třetích osob.⁸⁹

5.2.2.2. *Hodnotící soudy (hanobící kritika)*

Zasáhnout do osobnostních práv člověka je možné také zejména prostřednictvím hodnotících soudů. Takový projev se vyznačuje svým subjektivním zabarvením vetknutým mu jeho autorem. I zde můžeme rozlišit dva druhy hodnotících soudů, a to vyjádření preferencí a hodnocení okolního světa.⁹⁰ Rozdíl se ukrývá v tom, že v hodnocení okolního světa lze nalézt prvek skutkového tvrzení (pokud má informace reálný základ – např. „tvůj bratr je nezodpovědný“), které by tak projev řadilo pod ochranu svobody projevu.⁹¹ U hodnotících soudů je tedy zapotřebí prozkoumat, zda a nakolik je jejich základ objektivní, tedy zda se sdělovaná kritika zakládá na pravdě. Rozdíl mezi kritikou přípustnou a kritikou, která může zasahovat do osobnostních práv objektu, lze charakterizovat tak, že oprávněná kritika se drží v mezích kritiky věcné a je přiměřená obsahem i formou.⁹²

⁸⁷ DOLEŽÍLEK, Jiří. *Právo na odpověď a na dodatečné sdělení podle nového tiskového zákona*, s. 433.

⁸⁸ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 260

⁸⁹ SMÍLEK, Ondřej. *Svoboda projevu a její meze*, s. 31

⁹⁰ POST, Robert C. *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine v. Falwell*, s. 652-653

⁹¹ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 262

⁹² HERCZEG, Jiří. *Meze svobody projevu*, s. 69.

5. 2. 3. STATUS AUTORA

Další kritérium představuje status autora projevu. Například co se týká politiků a politických stran, v jejich případě je s ohledem na ochranu demokracie, plurality názorů a možnosti veřejné diskuse důležité zachování co možná nejširší svobody projevu. V potaz lze také brát, jak moc je osoba veřejně známá a jak velké publikum běžně oslovuje a podle toho jí přisuzovat vyšší míru odpovědnosti za své nároky.⁹³ Tisk a média zaobírají v tomto ohledu zvláštní postavení, neboť jim je v rámci svobodného projevu přisuzována vyšší míra ochrany.⁹⁴

5. 2. 4. ÚMYSL, CÍL, MOTIV

Jedním z kritérií je také úmysl, cíl nebo motiv autora daného projevu. Při zvažování, které z uvedených práv upřednostnit, je nutné zohlednit dobrou víru, úmysl či nedbalost ve vztahu k pravdivosti informace, cíl poškodit difamovanou osobu či naopak míru snahy informace ověřit. Čím více se autor bude snažit najít svým výrokem pravdu či verifikovat údaje, tím spíše bude jeho projev chráněn.

⁹³ BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*, s. 266

⁹⁴ SMÍLEK, Ondřej. *Svoboda projevu a její meze*, s. 33

6. DIGITÁLNÍ PROSTŘEDÍ JAKO PROSTOR K REALIZACI SVOBODY PROJEVU

Dynamické a neustále se rozšiřující digitální prostředí, zejména pak to on-line, významně ovlivňuje každý aspekt našeho života. Stejný vliv má i na možnosti svobodného vyjadřování. Počet digitálních platforem nezadržitelně roste a jakýkoliv obsah je v tuto chvíli jednoduše dostupný v horizontu několika vteřin. S dostupností informací a globalizací také souvisí dnes už téměř úplné smazání územních informačních hranic, která před érou digitálních médií víceméně ustanovovala možný dosah informací. Nyní si může téměř každý uživatel zobrazit obsah publikovaný z jakékoli části světa. Jedinou překážkou tak může být snad jen bariéra jazyková, kterou už ale díky sofistikovaným překládacím nástrojům lze taktéž velmi snadno zbořit. Jurisdikce jednotlivých států pak v tomto ohledu hrají stále menší roli, a to právě proto, že digitální data jsou dostupná odkudkoli.

I když by se mohlo zdát, že digitální sféra a internet jsou prostředím extra legem a že tedy představují jakýsi štít před právní regulací, opak je pravdou. Kyberprostor je stejně jako každé jiné prostředí prostorem sociálním a platí v něm stejná pravidla jako všude jinde. Mezi zmiňovaná pravidla spadá samozřejmě i ta právní, včetně ústavně chráněné svobody projevu i jí rovnocenných osobnostních práv. Ta se, jak je podrobně popsáno v podkapitole [5.1](#), dostávají v rámci digitální síťové komunikace do častých střetů a jejich rozřešení mají nezřídka kdy za úkol soudy. Projevy ve virtuálním světě se nijak neliší od projevů, na které jsme zvyklí z jiných médií a sociálních prostorů, a proto neexistuje důvod, proč by měl být kyberprostor imunizován od klasické regulace. A to i přes to, že rozdíly v jeho charakteristice i v možnostech využívání práva na svobodný projev v jeho rámci jsou ve srovnání s ostatními sociálními prostory markantní a nepopíratelné. Nejasné hranice svobody projevu a ochrany soukromí patří mezi hlavní rozdíly, v nichž se digitální média od těch tradičních liší.

6.1. KOMPARACE ÉRY TRADIČNÍCH A DIGITÁLNÍCH MÉDIÍ V KONTEXTU SVOBODY PROJEVU

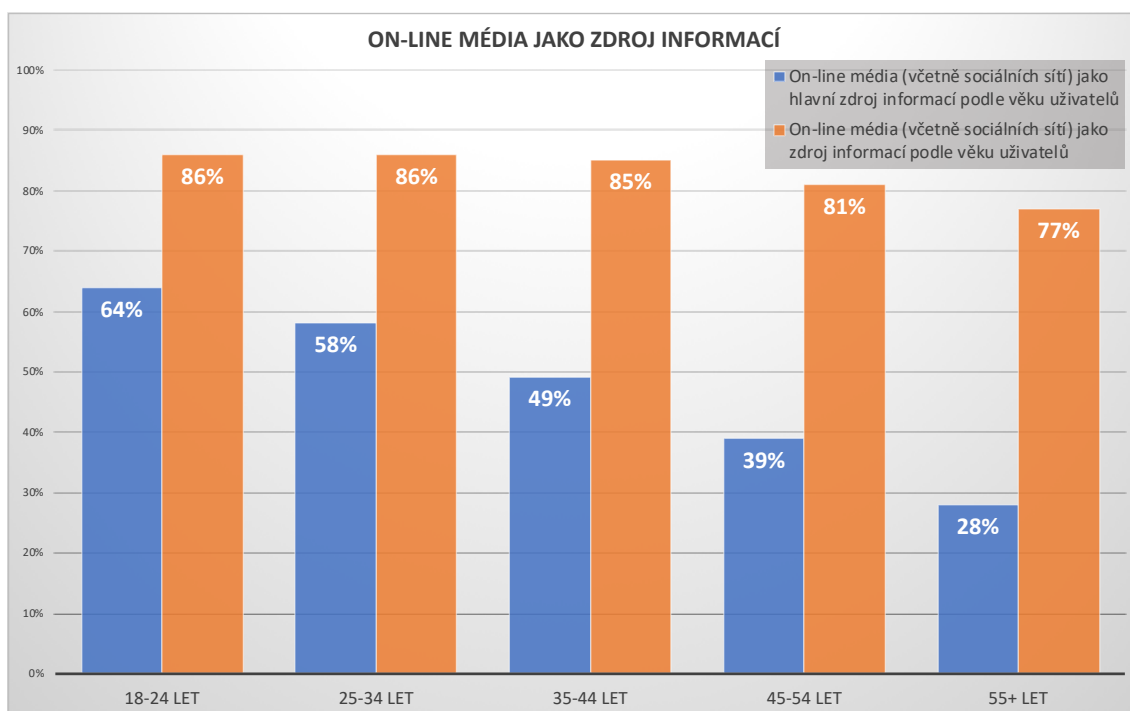
S nástupem digitálních a on-line médií se tradiční mediální svět razantně proměnil a s tím i realizování svobody projevu v něm. Jak už bylo zmíněno výše, digitální média

kompletně zbourala územní hranice (jak hranice státu pro celostátní média, tak třeba hranice krajské pro média lokální), které dříve dosah informací značně limitovaly. Uživatel z jakéhokoliv koutu světa, až na výjimky, má nyní přístup k nepřebornému množství informací. Nepoměrné je i ono množství informací, které může dohledat. Zatímco v éře tradičních médií by vyhledávání určitého článku či relace znamenalo několik hodin strávených v archivech, internetové prostředí představuje v podstatě nekonečnou databázi všech informací, které do něj kdy byly vloženy. S tím je spojená také problematika zveřejňování informací na internetu a prakticky nemožné vzetí tohoto kroku zpět. Toto téma je blíže rozebráno v kapitole [6.2](#).

Éra tradičních médií byla také vždy charakteristická svým gatekeepingem, tedy procesem výběru informací ke zveřejnění v médiích. Celospolečenská témata byla de facto konstruktem novinářů a jejich výběru, které zprávy splňují základní zpravodajské hodnoty a které je relevantní zpracovat a do tisku umístit. Novináři tak fungují jako jakýsi filtr informací, z nichž vybírají ty zpravodajsky nejhodnotnější, které se dostanou až ke koncovému čtenáři. To může mít za následek deformaci pohledu čtenářů na realitu. Absolutní objektivitu je totiž téměř nemožné dosáhnout už kvůli tomu, že každý novinář vybírá a vyhodnocuje relevanci informací ze svého pohledu, tedy s jistou mírou subjektivitu, a zároveň i s ohledem na mediální i organizační rutinu daného média.

Šíření informací v digitálních médiích nemůže být od způsobu těch klasických odlišnější. Možnosti internetu přinesly zcela novou dimenzi chápání svobody slova a možnosti projevu. Šíření informací v kyberprostoru je neuvěřitelně snadné a taková změna kvantity informací přinesla svými důsledky i nevyhnutelnou změnu jejich kvality. Do prostředí internetu proudí každou vteřinu miliony dat, které nejsou žádným způsobem revidovány. S touto novou dobou se objevil i nový termín *informační obezita*, který je, více než kterýkoliv jiný, pro dobu digitálních médií velmi distinktivní. Odkazuje k takové informační přesycenosti nynějšího světa, že je pro uživatele nadměrně obtížné se v takovém množství orientovat nebo si z nich vybrat ty, jež jsou kvalitní a jimiž je vhodné se zabývat. V případě tradičních médií usnadní orientaci i práci s výběrem kvalitních informací zejména veřejnoprávní média, která jsou povinna vydávat ověřené a objektivní informace a mají za své obsahy zodpovědnost. Internetové prostředí naproti tomu představuje ideální prostor pro šíření fake news, hoaxů a dezinformačních obsahů, které mohou čtenáře uvést v omyl a významně zasahovat do osobnostních práv třetích osob. Pro velkou část

populace je internet (hlavním) zdrojem informací (*viz graf č. 1*), volné šíření dezinformací a hoaxů v tomto prostoru proto může mít obrovský vliv na utváření názorů ve společnosti, a tím i nedozírný dopad na fungování demokratického systému. Kdokoli tedy může bez fyzické nebo duševní námahy oslovit i s nepravdivou informací velký počet dalších uživatelů a zároveň přijímat jejich okamžité reakce. Na rozdíl od klasických médií, kde je autor článku, reportáže či jiného výstupu přímo jmenován, je ale internet silně anonymním prostředím (anonymita je podrobně prozkoumána v kapitole [6.4.](#)). Proto je často téměř nemožné autory takových projevů dohledat.



Graf č. 1: On-line média jako zdroj informací

Zdroj: REUTERS INSTITUTE. *Digital News Report 2017, 2019*

Éru tradičních a digitálních médií značně odlišuje i rychlost zveřejňování informací a doba od zpracování tématu novinářem po čas, kdy se daná informace dostane k recipientovi. Fungování tradičních médií, oproti digitálnímu prostoru, totiž podléhá klasické mediální logice. Pravidla pro vydávání obsahu jsou mnohem striktnější, než je tomu v on-line prostoru. Novináři se musí řídit redakčními uzávěrkami a recipienti se k obsahu dostanou buď týž den, ale až v předem stanovený čas (v případě televize), nebo až následující ráno s vydáním denního tisku. Oproti tomu v on-line prostoru se informace dostávají do světa okamžitě a stejně rychle k nim mají přístup všichni uživatelé.

Jak již bylo zmíněno, v klasických médiích mohla své právo na svobodu projevu využívat jen hrstka lidí, a to díky charakteru svého povolání. Digitální sféra tuto možnost pro všechny narovнала. Volný a všeobecný přístup k internetu umožnil nejen příjem, ale i šíření a prosazování názorů maximálnímu počtu uživatelů, kteří se tak mohou aktivně zapojovat do občanské společnosti, a to v mnohem vyšší míře než kdykoli dříve. Digitální sféra do mediálního prostředí vnesla výraznou demokratizaci vedoucí k rovné možnosti využívání občanských svobod. Na druhou stranu ale také přinesla do internetových diskusí (zejména na zpravodajských a publicistických serverech) obrovskou vlnu nenávistných projevů namířených proti publikovanému materiálu či autorovi samotnému. O velké části těchto projevů je možné říci, že zasahují do osobnostních práv autorů či těch, o kterých projevy pojednávají. Projevy zasahují do osobnostních práv často svou vulgárností, nezřídka kdy jsou neetické, rasistické, xenofobní či jinak netolerantní. Zde vyvstává otázka, do jaké míry by měl organizátor či zprostředkovatel diskuse takové projevy filtrovat, mazat nebo ještě jinak postihovat. Zásahem by ale zároveň zasahoval do svobody projevu, což zákon umožňuje pouze v určitých případech (viz kapitola [3.](#)).

Dalším aspektem, ve kterém se modely liší, je typ komunikace. Zatímco v tradičním modelu převládá jednosměrná a formát one-to-many, ve kterém byla ochrana svobody projevu důležitá zejména pro novináře, v tom digitálním jasně vítězí obousměrná a formát se transformoval na many-to-many. Nejen, že recipienti mohou v reálném čase reagovat na předkládané informace, ale také se z nich stávají samotní tvůrci obsahu. Dříve byla pro tvůrce bariérou distribuce obsahu, ta ovšem v éře digitálních médií zaniká. Ani špičková kvalita sdíleného audiovizuálního obsahu už není výsadou bohatých mediálních domů. Dnes má téměř každý smartphone s kvalitním fotoaparát a svůj osobní počítač, které poskytují, co se zpracování obsahu týče, velmi široké možnosti.

Nová, digitální éra kompletně proměnila mediální prostředí a s ním i využívání práva na svobodu projevu. V jistých ohledech digitální prostředí otevírá uživatelům nespočet možností k vyjadřování vlastních názorů, politických postojů, nabízí jim snazší kontrolu politických činitelů a jsou schopni se více podílet na aktivní občanské společnosti. Na druhou stranu ale tato éra nesmírně zjednodušila a zefektivnila celou řadu kriminálních činností, které jsou v demokratické společnosti samozřejmě nežádoucí.

6. 2. ŠÍŘENÍ INFORMACÍ NA INTERNETU A DIGITÁLNÍ STOPA UŽIVATELŮ

Co se jednou dostane na internet, už tam zůstane navždy. Tak zní jeden z obecných popisů digitálního prostředí. I když uživatel na sociálních sítích upraví okruh spřátelených uživatelů, kterým chce svůj obsah zobrazovat, kdokoli z nich může pořídit kopii jeho výroku a šířit dál mezi další uživatele. Tím má informace potenciální šanci dostat se mezi neodhadnutelné množství uživatelů, tedy dokonce i ty, o kterých autor projevu nikdy neslyšel a které nezná. Nad šířením informací a komu budou zpřístupněny tedy uživatel nemá dohled, a proto si ani nemůže být jist, že jím sdílené informace nebudou zneužity případně využity proti němu. Tato možnost kontroly nad tím, jaké informace, komu, kdy a na jak dlouho budou zveřejněny a jak s nimi může být nakládáno dále se souhrnně označuje jako *právo na informační sebeurčení*, které je tak v podstatě součástí práva na ochranu soukromí.⁹⁵ Nad čím ale oproti šíření informací můžeme mít dohled, je do jisté míry počet a druhy informací, které o sobě internetu sdělíme a všem jeho uživatelům zpřístupníme. Soubor všech vyhledatelných informací se souhrnně nazývá *digitální stopa uživatele*. Tyto informace můžeme rozdělit do třech kategorií. První jsou ty snadno dohledatelné, ke kterým má přístup každý a je možné je dohledat prostřednictvím internetového vyhledávače. Mezi ty patří každý příspěvek na sociálních sítích, v internetových diskusích, registrace na internetových stránkách apod. Druhou kategorií jsou informace poloveřejné, které uživatel sdílí pouze s jím předem určeným okruhem lidí. Poslední skupinu představují informace náročněji zjistitelné, jakými jsou například technické záznamy na navštívených webových stránkách, cookies⁹⁶ apod. Způsobů a míst, kde uživatel může o sobě zanechat informace, je tedy celá řada. K úplnému zamezení sdílení těchto informací

⁹⁵ TOKOŠOVÁ, Kamila. *Právo na zapomnění*

⁹⁶ Cookie je možné popsat jako malý textový soubor vytvořený webovou stránkou a ukládaný do počítače uživatele, díky kterému ho daná webová stránka při opětovné návštěvě rozpozná a zobrazí dříve navolené preference. Díky tomu je možné uživateli zobrazovat personalizovanou reklamu na základě toho, co si prohlížel, co vyhledával apod. Cookies ale schraňují pouze informace, které uživatel stránce vědomě poskytne, nemá přístup do souborů v počítači. Cookies jsou tedy pro subjekty na internetu synonymem pro on-line trackování, které může představovat pro uživatele hrozbu. Proto v dnešní době Evropská komise od roku 2002 požaduje po každé webové stránce, aby návštěvníci s takovým „sledováním“ vyjádřili informovaný souhlas. Souhlas musí být udělen ještě před tím, než stránka začne ukládat data na počítač uživatele a opětovně k nim přistupovat.

by došlo pouze v případě, že bychom přestali využívat internet, a i to by nemuselo být dostatečně účinné. Stále zde mohou příbuzní či přátelé zanechávat část naší stopy například sdílením společných fotografií. Dalším způsobem minimalizování digitální stopy je co možná nejvyšší stupeň anonymity. Té je věnována podkapitola [6.4.](#) zaměřující se na její pozitivní i negativní implikace nebo způsoby, jak jí dosáhnout. Obecná rada k zanechání co možná nejmenší digitální stopy vedoucí k snazšímu zachování a ochraně vlastního soukromí je vždy uvážit, co sdílíme a k jakým informacím o nás samých dovolujeme ostatním přístup. Správné nastavení soukromí na jednotlivých platformách, ale i v samotném prohlížeči, by mělo být základem.

Časté mazání cookies a střežení, kde je povolujeme, je dalším krokem k vyššímu zabezpečení osobních informací. Každá cookie má šest základních parametrů, z nich nejdůležitější je její doba platnosti, která určuje, jak dlouho bude ve vyhledávací uživatele aktivní. Rozdělit je můžeme na dočasné a trvalé. Dočasné cookies jsou v počítači uchovávány pouze po dobu relace prohlížeče a po jeho zavření jsou vymazány. Oproti tomu permanentní soubory cookie se do počítače ukládají na dobu své platnosti, která je předem určena nastavením prohlížeče nebo samotné cookie. Ta tedy po uzavření prohlížeče z počítače vymazána není, obvykle je uchovávána na měsíc, rok apod. Permanentní cookies vedle informací vyloženě poskytnutých uživatelem také vysledovávají jeho všeobecné chování na internetu, zejména co se vyhledávání týče, a jeho uživatelské preference pro konkrétní weby.⁹⁷

Cookies sice neznamenaají žádné nebezpečí pro počítačový systém, hardware ani software, nešíří počítačové viry ani nemají přístup na pevný disk (tam pouze prohlížeč jejich informace uchovává), přece jen jsou to stále jen velmi malé textové soubory. Pro zachování soukromí a anonymity uživatele jsou ale klíčové. Jsou v nich totiž zapsané všechny informace, které webovým stránkám poskytnete, při platbách na internetu tedy i údaje o kreditní kartě. Zakázání cookies pro uživatele sice bude znamenat, že při každé návštěvě webových stránek bude muset znovu zadávat všechny své přihlašovací údaje i opětovně vyplňovat formuláře a podobně, z hlediska zachování soukromí v prostředí internetu a zabezpečení digitální i reálné identity je ale pravidelné mazání cookies velmi důležité.

⁹⁷ WEBOPEDIA. *What is persistent cookie?*

6. 2. 1. PRÁVO BÝT ZAPOMENUT

Mezi možnosti, jak určitým způsobem ex post ovlivnit výskyt informací, které jsou o daném uživateli v kyberprostoru k nalezení, je právo být zapomenut. Dá se považovat za jednu z esencí práva na ochranu soukromí jednotlivce, která spočívá zejména v tom, že uživatel má právo na vymazání seznamu výsledků vyhledávání webového prohlížeče provedeného na základě jména osoby nebo informace této osoby se týkající.⁹⁸ Základ tohoto práva je zakotven ve směrnici č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů přijaté v roce 1995 Evropským parlamentem a Radou. O podobu, jakou má dnes, se ale zasloužil hlavně rozsudek velkého senátu Soudního dvora EU ze dne 13. 5. 2015 ve věci Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos a Mario Costeja González, který začal pracovat s právem být zapomenut, které ve směrnici předtím chybělo. V návaznosti na tento rozsudek přijala společnost Google jako nejrozšířenější webový vyhledávač postup, na základě kterého je možné požádat o výmaz konkrétních URL odkazů z vyhledávání.⁹⁹ K tomu byl vytvořen formulář ([viz příloha č. 1](#))¹⁰⁰, kde musí uživatel přesně specifikovat, jaké informace žádá vymazat a na jakých důvodech se jeho žádost zakládá. Podmínky jsou ale přísné a společnost Google drtivě většině žadatelů nevyhoví, protože podle ní na digitální zapomnění nemají nárok. V případě, že se žadatel pustí do soudních sporů, se dostává do paradoxní situace, protože v případě mediálního zájmu o kauzu bude znám přesně pro ty informace, kvůli jejichž vymazání se soudními spory vůbec začal. Tento efekt je běžně znám také jako efekt Streisand effect. Pokud bude jeho žádost naopak schválena, je zapotřebí počítat s tím, že dojde k vymazání uvedených URL odkazů z webového prohlížeče pouze v rámci národní, respektive evropské verze webového prohlížeče. A ani v tomto prostředí informace nevymaže beze stopy, ale upozorní, že vyhledávaný výsledek byl vymazán.¹⁰¹ Časté je také nepochopení principu tohoto práva na vymazání. Uživatelé často presumují, že touto cestou se jim podaří vymazat informace z prostředí internetu. Touto cestou, v případě schválení požadavku dojde k vymazání informace jen a pouze z výsledků vyhledávání, a tedy se nejedná o stažení

⁹⁸ ŠVEC, Michal. *Tzv. „právo být zapomenut“ a jeho uplatnění v praxi*

⁹⁹ Tamtéž.

¹⁰⁰ Formulář je také dostupný na support.google.com/legal/contact/lr_eudpa?product=websearch&hl=cs

¹⁰¹ ŠVEC, Michal. *Tzv. „právo být zapomenut“ a jeho uplatnění v praxi*

předmětných informací z webových stránek. O to je zase nutné požádat provozovatele oné webové stránky.

6. 2. 2. PRIVACY PARADOX

Se sdílením osobních informací uživatelů na internetu souvisí také zajímavý fenomén obecně známý jako *privacy paradox*. Mnoho studií soustředících se na soukromí uživatelů v prostředí internetu ukázalo, že uživatelé se obávají o své soukromí na internetu a jeho udržení, ale zřídka tyto obavy promítnou do svého on-line zacházení se soukromými informacemi a chování na internetu vůbec.¹⁰² Uživatelé často tvrdí, že při pohybu v digitální sféře je zachování jejich soukromí jednou z priorit, ale už nepodnikají odpovídající kroky, kterými by ho chránili, a sdílejí ho takřka bezmyšlenkovitě. Faktorů, které toto protiřečící si chování ovlivňují, může být hned několik. Některé studie považují tento paradox za vysoce kontextuální, tedy že chování se v odlišných kontextech různí.¹⁰³ Další studie stanovují, že s vyšší personalizací užívaného on-line nástroje či webové stránky se zvyšují obavy uživatele o vlastní soukromí. I přesto ale uživatelé s vidinou možnosti využívání určitých funkcí, které jim usnadní práci (například s vyplňováním formuláře apod.), mají tendenci od svých obav upouštět.¹⁰⁴

Dichotomii mezi postoji a chováním lze dle studií vysvětlit také na základě tří rozhodovacích strategií, které předcházejí umístění osobních informací do kyberprostoru. První z nich je racionální vyhodnocení nákladů a přínosů, tedy porovnání důležitosti a důvěrnosti informací s benefity, které uživateli jejich odhalení přinese, přičemž ve většině případů převáží benefity. Uživatel tedy informaci sdílí výměnou za uspokojení určitých potřeb či zvýhodnění. Přestože jsou si uživatelé vědomi rizik se sdílením informace

¹⁰² BARTH, Susanne a Menno D. T. DE JONG. *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*

¹⁰³ KOKOLAKIS, Spyros. *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*

¹⁰⁴ BERGSTRÖM, Annika. *Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses*

spojených, přesvědčivost nabídky či výhody je většinou tak silná, že uživatel hrozby pro své soukromí upozadí a zanedbá.¹⁰⁵

Druhou strategií je iracionální vyhodnocení nákladů a přínosů charakteristické zkresleným vyhodnocením rizik. Ono zkreslení je způsobeno předsudky, jako je heuristické myšlení¹⁰⁶, (okamžité) uspokojení nebo časová nekonzistence zkresluje vyhodnocení rizik, kvůli kterému uživatel pak dochází k nesprávným závěrům, které ve většině případů opět favorizuje benefity sdílení informace nad jeho riziky.¹⁰⁷

Třetí kategorií představuje taková rozhodovací strategie, v rámci které nedochází k vyhodnocování nákladů a rizik vůbec, nebo jen velmi zanedbatelně. K této situaci může dojít například při chybné evaluaci hodnoty dat, ke kterým uživatel umožňuje přístup, či nedostatek informací o možnostech jejich ochrany pak vede k tomu, že vnímání rizik spojených s jejich uveřejňováním bude uživatelem potlačeno či úplně zanedbáno.¹⁰⁸

Všechny tři výše popsané rozhodovací strategie týkající se otázky ochrany osobních údajů mohou vysvětlovat onen rozpor mezi uživateli stanovovanými postoji k ochraně svého soukromí a jejich reálným chováním, známý jako *privacy paradox*.

6. 3. ZÁSAHY DO PRÁVA NA SVOBODU PROJEVU SPECIFICKÉ PRO ONLINE PROSTŘEDÍ

V dnešní době používá internet už přes polovinu populace jako nástroj ke komunikaci, zábavě, práci apod. Přístup k němu je ale napříč světem velice nerovnoměrný.

¹⁰⁵ BARTH, Susanne a Menno D. T. DE JONG. *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*

¹⁰⁶ Heuristické myšlení zkracuje myšlenkové procesy tak, že se naše mysl soustředí pouze na jeden aspekt komplexního problému, zatímco ignoruje ty ostatní. Tyto mentální procesy nám sice pomáhají se rychle rozhodovat a formovat naše úsudky, výsledky jsou ale zatíženy, právě kvůli rychlosti, chybovosti.

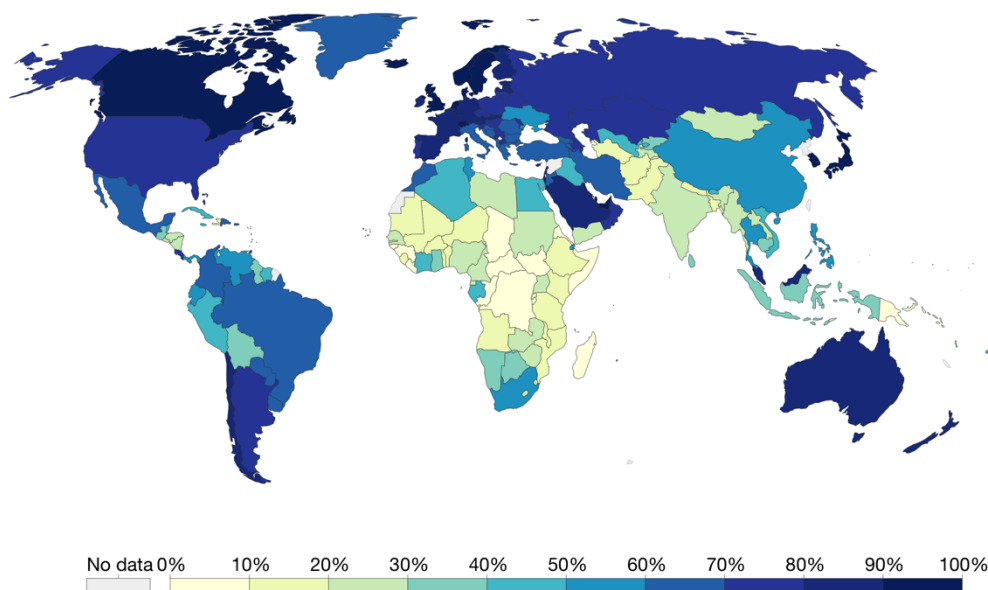
¹⁰⁷ BARTH, Susanne a Menno D. T. DE JONG. *Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources*

¹⁰⁸ BARTH, Susanne a Menno D. T. DE JONG. *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*

I přes emancipační potenciál internetu a jeho údajný ryze demokratický charakter k němu ale vlády některých zemí přistupují s obezřetností a pokoušejí se občanům přístup k jeho obsahům omezit či znemožnit úplně. Úroveň internetové penetrace (viz [obrázek č. 1](#)) pak spoluvytváří geografický vzhled on-line cenzury (viz [obrázek č. 2](#)).

Share of the population using the Internet, 2017

All individuals who have used the Internet in the last 3 months are counted as Internet users. The Internet can be used via a computer, mobile phone, personal digital assistant, games machine, digital TV etc.



Source: World Bank

OurWorldInData.org/technology-adoption/ • CC BY

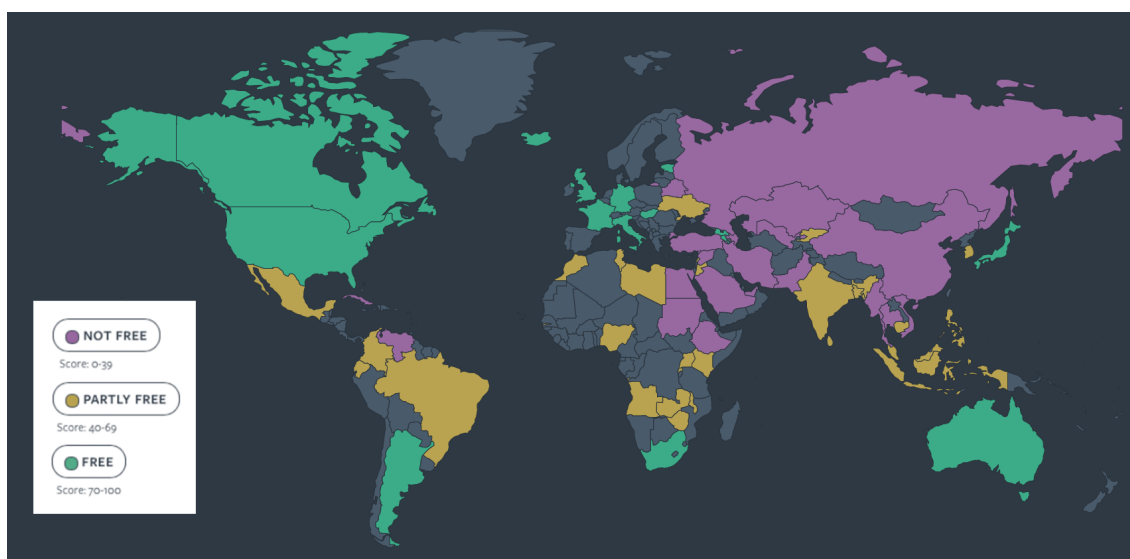
Obrázek č. 1: Mapa internetové penetrace ve světě

Zdroj: OURL WORLD IN DATA. Internet access: What share of people are online?

Právě internetová penetrace má na státní snahy o internetovou cenzuru totiž velký vliv. V autoritářských státech s relativně slabými občanskými společnostmi a v chudých státech, kde je internetová penetrace velmi nízká a občané využívají zejména internetové kavárny pro přístup k informacím on-line, je cenzura relativně snadná a odpor často slabý a neúčinný. Naproti tomu v demokratičtějších státech může být opozice organizovaná a efektivní. Se snižujícími se cenami technologií a techniky, rozšiřujícímu se osobnímu vlastnictví počítačů a se zvyšující se technologickou zdatností uživatelů je pro vládu také čím dál náročnější své občany sledovat a udržovat jejich disciplínu. Proto v takových státech bývají zaváděna striktnější opatření. S rostoucími příjmy obyvatel a vzdělaností se společnosti liberalizují, lidé jsou informovanější a vzrůstá i míra politické participace. To také způsobuje rozšiřování řad elit a jejich možností, jak aktivně a organizovaně

cenzuře odolávat. Interaktivní struktura decentralizovaného internetu a jeho neustálý vývoj vládě také komplikuje možnosti kybernetické manipulace.¹⁰⁹

Geografickou mapu internetové cenzury zobrazuje [obrázek č. 2](#). Zkoumané státy barevně dělí do tří kategorií. Zelenou barvou jsou označeny státy, které na základě výzkumu Freedom on the Net americké organizace Freedom House získaly skóre od 100 do 70, kde 100 je absolutní svoboda a 0 nejtvrďší cenzura a omezení. Žlutou jsou označeny státy se ziskem od 69 do 40, což jejich svobodu na internetu značí jako částečně omezenou a fialová barva pak zvýrazňuje státy, které proti svobodě projevu ve svém kyberprostoru bojují nejtvrďšími možnými prostředky.¹¹⁰ Na následujícím obrázku je na světové mapě vidět proměna skóre mezi roky 2018 a 2019 (viz [obrázek č. 3](#)). Nejtmaší červená znamená pokles skóre o 3 a více bodů a zvýrazňuje tedy státy, ve kterých se situace internetové cenzury meziročně zhoršila. Nejsytější zelená signalizuje pravý opak. Graf s přesným skóre jednotlivých zemí je přílohou této práce (viz [příloha č. 2](#)) stejně jako tabulka znázorňující, jaké druhy opatření a omezení svobody projevu v nich se v nich mezi roky 2018 a 2019 vyskytly (viz [příloha č. 3](#)).

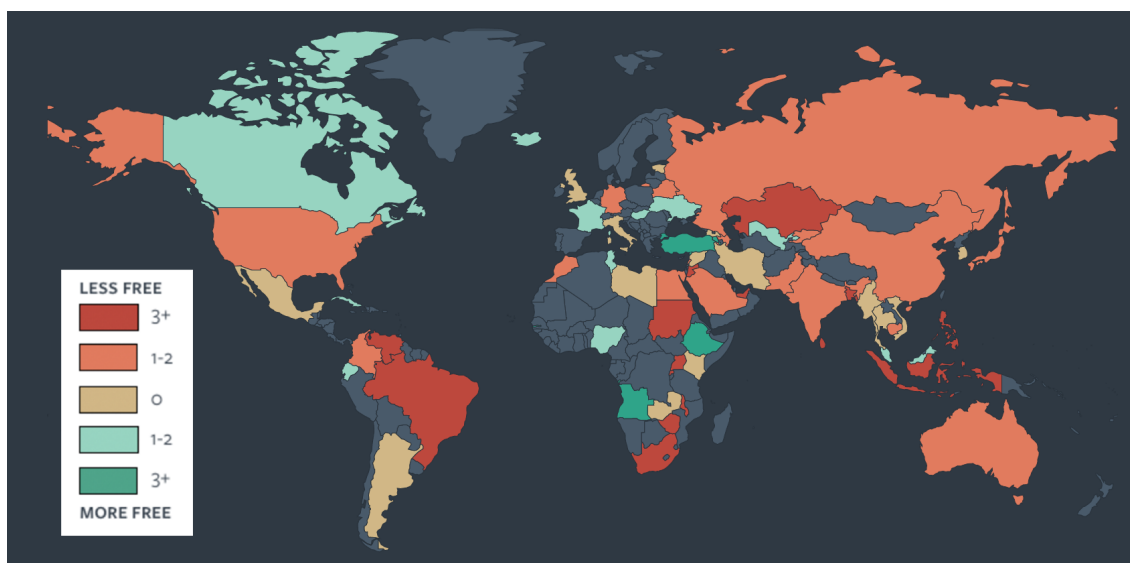


Obrázek č. 2: Geografické znázornění on-line cenzury ve vybraných zemích

¹⁰⁹ WARF, Barney. *Geographies of global Internet censorship*

¹¹⁰ Freedom House každoročně vydává dokumenty týkající se lidských práv a svobod včetně analýzy svobody na internetu. Aktuálně provádí tento výzkum v 65 státech světa, což ho činí nejkompexnějším ve své tematice. Metodologie výzkumu je dostupná na <https://freedomhouse.org/reports/freedom-net/freedom-net-research-methodology>

Zdroj: FREEDOM HOUSE. Internet Freedom Status



Obrázek č. 3: Proměna skóre svobody projevu ve vybraných zemích mezi roky 2018 a 2019

Zdroj: FREEDOM HOUSE. Internet Freedom Status

Celá řada vlád i v dnešní době agresivně omezuje a zamezuje svým občanům přístup k internetu. V drtivé většině se jedná o obsahově zaměřenou cenzuru (viz kapitola [3.3.2.](#)). Opozici a „odboj“ brojící proti tvrdé cenzuře tvoří většinou pouze diaspora nebo malé skupiny vzdělaných jedinců v daných státech, kteří mají ale jen minimální vliv a šanci domoci se změny.¹¹¹

6. 3. 1. DIMENZE INTERNETOVÉ CENZURY

Možnost přístupu na internet ve většině případů kopíruje ochotu vlád tento přístup umožnit. Většinou se ale nejvyšší vládní představitelé obávají právě onoho emancipačního potenciálu internetu a jeho demokratického charakteru, který dává hlas těm, kteří dříve nemohli být slyšet, včetně politické opozice, což může autokratické vlády podkopávat.¹¹² Proto vlády používají širokou škálu nástrojů represe, kterými upevňují svou moc, vytváří prostředí plné strachu a snaží se eliminovat disent.

¹¹¹ KALATHIL, Shanthi a Taylor C. BOAS. *Open Networks Closed Regimes: The Impact of the Internet on Authoritarian Rule*

¹¹² WARF, Barney. *Geographies of global Internet censorship*

Po celém světě můžeme vysledovat několik různých vládních motivů k internetové cen-
zure, a tedy i několik druhů. Patří mezi ně politická represe disentu včetně aktivistů
za lidská práva (například Čína, Írán, Myanmar), náboženská kontrola potlačující šíření
myšlenek považovaných za kacířské (celá řada arabských států), ochrana duševního vlast-
nictví včetně omezení nelegálního stahování filmů a hudby nebo kulturní restrikce, která
je součástí systematického utlačování sexuálních i etnických menšin (například zamezo-
vání přístupu k webovým stránkám v určitém jazyce). Vlády zavádějí cenzuru taktéž
s odkazem na ochranu národního bezpečí, sociální stability i veřejné morálky před obsa-
hem narušujícím etiku jako pornografie, hazardní hry a v poslední době i terorismus.¹¹³
V jistých případech (jako je například dětská pornografie, záběry vražd apod.) považují
cenzuru za opodstatněnou. Někteří autoři také zastávají názor, že k boji proti kyberanar-
chii či předcházení trestným činům je určitý stupeň internetové cenzury přípustný, do-
konce i žádoucí.¹¹⁴

Implementovaná internetová cenzura zasahuje do přístupu k internetu, funkčnosti i ob-
sahu.¹¹⁵ Obecně ji charakterizuje několik kritérií:

- *dostupné náklady* (protože náklady na technologie i lidskou sílu umožňující inter-
netovou cenzuru jsou velmi vysoké, představují klíčové kritérium, které přímo
rozhoduje o tom, jak silnou cenzuru je možné uvést do provozu),
- *rozsah cenzury* (rozsah cenzurovaných komunikačních metod)
- *míra cenzury* (počet lidí a zařízení, na které se bude cenzura vztahovat),
- *rychlost* (reakční doba cenzorů)
- *technická úroveň* (na jaké úrovni bude cenzura implementována – zda budou cen-
zurované například celé servery, webové stránky, nebo jen koncoví uživatelé),
- *nízká míra přesnosti* (také falešná negativa, využitý způsob internetové cenzury
není schopen zablokovat všechnen obsah, ke kterému měl být uživatelům odepřen
přístup),

¹¹³ WARF, Barney. *Geographies of global Internet censorship*

¹¹⁴ KATYAL, Neal Kumar. *Criminal Law in Cyberspace*, s. 1100

¹¹⁵ ERIKSSON, Johan a Giampiero GIACOMELLO. *Who Controls the Internet? Beyond the Obstnacy
or Obsolescence of the State*, s. 206–210.

- *přílišná důkladnost* (také falešná pozitiva, využitý způsob zablokuje o mnoho více obsahu, než bylo nutno cenzurovat),
- *náročnost obcházení* (jak snadno se lze dostat k cenzurovanému obsahu).¹¹⁶

Implementovaná internetová cenzura se pak podle těchto kritérií různí od zcela neomezeného přístupu (například v Dánsku) až po kompletní zákaz přístupu na internet (například v Severní Koreji). Vlády, které ve svých zemích usilují o svrchovanost nad kybernetickým prostorem, si při zavádění svých neliberálních omezení často ani neuvědomí jejich vedlejší efekty jako zpomalení inovací, negativní publicitu, která může vést až k mezinárodnímu vyčlenění z diplomatických jednání, omezený cestovní ruch nebo třeba stažení nadnárodních korporací ze země, tudíž i snížení profitů.¹¹⁷ Jako příklad lze uvést rozhodnutí společnosti Google o svém stažení z čínského trhu v roce 2010. Pro společnost Google, která se pyšní tím, že je zdrojem informací, totiž nebylo akceptovatelné přistoupit na opatření, která posilují a prosazují cenzuru.¹¹⁸

6. 3. 2. METODY OMEZOVÁNÍ PŘÍSTUPU K OBSAHU

Existuje celá řada různých technik, kterých vlády využívají k zamezení přístupu k internetu, z nichž většina je technického rázu. Na tyto způsoby se tato podkapitola bude dále zaměřovat, avšak považují za vhodné zmínit se i o dalších způsobech netechnického charakteru. Mezi ty můžeme započítat například schvalování zákonů zakazujících publikování a šíření určitého druhu obsahu, neformální žádosti o smazání obsahu (většinou pod určitou výhrůžkou), diskriminující ceny za internetové připojení, manipulace s hardwarem nebo softwarem, diskriminující licence a smlouvy s poskytovateli internetového připojení, finanční sankce, zatýkání či věznění za sdílení zakázaných témat, zabavování počítačů a jiné techniky, šíření počítačových virů, tajné odposlouchávání a monitorování konverzací, výhrůžky, fyzické útoky, vraždy, vyhrožování rodině a příbuzným, komplikování postavení v práci či například propouštění ze zaměstnání. Tyto kroky vedou

¹¹⁶ LEBERKNIGHT, Christopher S. a kol. *A Taxonomy of Internet Censorship and Anti-Censorship*

¹¹⁷ VILLENEUVE, Nart. *The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace*

¹¹⁸ HELFT, Miguel a David BARBOZA. *Google Shuts China Site in Dispute Over Censorship*

samotné uživatele k seberegulaci a upouštění od sdílení informací z důvodu strachu o vlastní bezpečnost.

Z technických metod, skrz které probíhá blokování či filtrování nežádoucího obsahu, je důležité zmínit zejména blacklistování, cenzurování konkrétních styčných bodů, mazání odkazů z vyhledávání, dynamická analýza obsahu a kompletní odstranění obsahu z internetu.

Blacklistování můžeme definovat jako zařazení konkrétního klíčového slova, názvu domény či IP adresy na seznam nežádoucích obsahů určených k zablokování. K tomu jsou využívány metody jako blokování IP adres, podvržení DNS¹¹⁹ nebo blokování konkrétních URL adres skrze proxy. Tyto techniky slouží k zablokování přístupu ke konkrétním webovým stránkám, doménám nebo IP adresám. Blokování klíčových slov, které odstraňuje konkrétní slova z vyhledávání nebo zamezuje přístup k webovým stránkám, jejichž URL obsahuje konkrétní slovo, je jednou z pokročilejších metod cenzurování, jíž využívá stále více států.¹²⁰

Cenzurování a filtrování může být implementováno na jakékoli úrovni internetové hierarchie, tedy na odlišných styčných bodech. Nejpřísnější cenzuru představuje úroveň páteře internetu, čímž bude ovlivněn přístup v celé zemi. Nejčastěji je však dle nařízení vlády cenzura implementována poskytovateli internetových služeb za použití jakékoli z výše uvedených i dalších technik nebo jejich kombinace. Dále může být filtrování implementováno na institucionární úrovni, čehož využívají společnosti, vládní organizace nebo školy. Mimo vlády toto filtrování využívají také společnosti jako prevenci používání počítačů na pracovišti k rekreačním účelům.¹²¹ Poslední úrovní je pak filtrování jednotlivých uživatelů podle jejich IP adres.

¹¹⁹ Systém doménových jmen (Domain Main System), který převádí název domény (např. www.dvtv.cz) na IP adresu, takže prohlížeč může zobrazit internetový obsah. Podvržení DNS pak funguje tak, že zadanou doménu (www.dvtv.cz) DNS přeloží na podvrženou IP adresu (ale ve doménovém řádku se bude zobrazovat stále táž vyhledávaná doména v přesném znění, takže uživatel nepostřehne, že prohlížeč ve skutečnosti zobrazí podvrženou stránku).

¹²⁰ OPENNET INITIATIVE. *About Filtering*

¹²¹ Tamtéž.

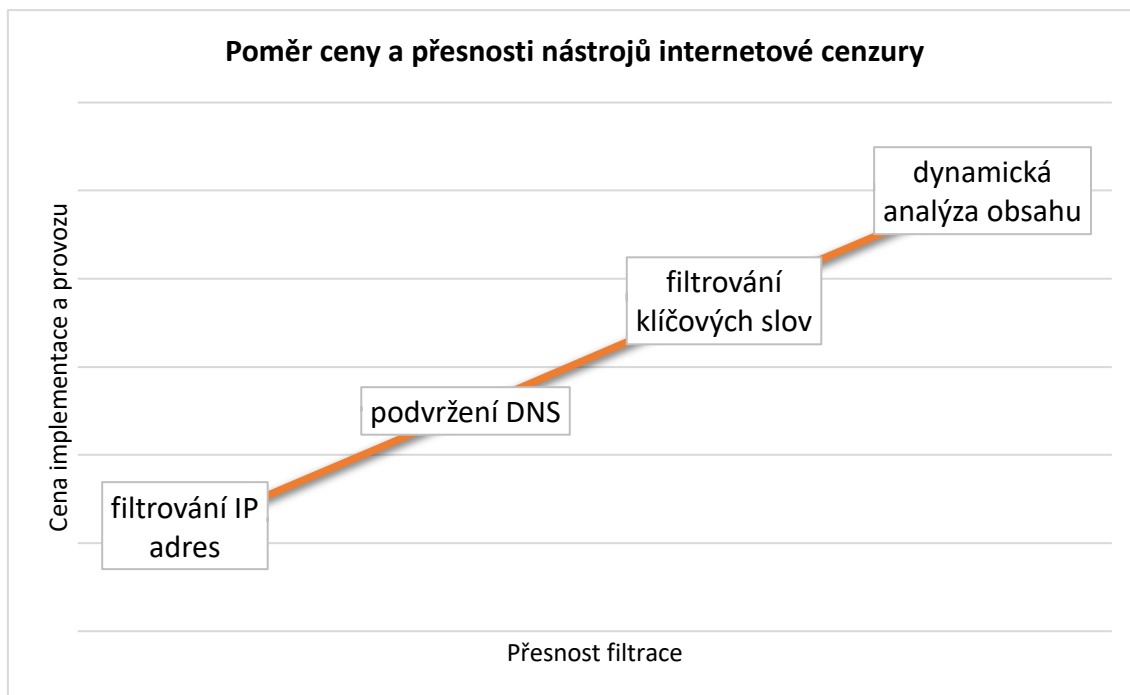
Mazání odkazů z vyhledávání představuje, spíše než blokování přístupu na určité weby, ztížení jejich vyhledávání. Tento způsob cenzury využívá i řada demokratických států za účelem ochrany osobnostních práv či z etických důvodů.

Při dynamické analýze obsahů dochází k podrobnému zkoumání a čtení obsahů na požadovaných webových stránkách. Tento velmi náročný způsob cenzury je vysoce efektivní, ovšem velmi nákladný.

Kompletní odstranění znamená odstranění webových stránek s nevhodným nebo nezákonným obsahem. V některých zemích postačí zaslat majiteli oznámení o zastavení činnosti s hrozbou následných právních kroků k přesvědčení o zrušení webových stránek. Pokud má stát kontrolu nad servery s doménami, může jim jednoduše zrušit registraci.¹²²

Exaktního filtrování dosáhnout téměř nelze, vždy je zde možnost nedostatečné přesnosti či přílišné důkladnosti (viz podkapitola [6.3.1.](#)). Dalším důvodem je také velmi rychle se vyvíjející technologie či specifický jazyk využívaný na internetu (i k předávání tajných zpráv), se kterými mají vlády často problémy držet krok. Míra cenzury tak většinou reflektuje míru demokracie v daném státě, pružnost reagování na kritiku zvenčí (například od jiných států) či podle dostupných finančních prostředků. S rostoucími nároky na přesnost blokování a filtrování také vzrůstá cena. Kupříkladu filtrování IP adres je jedním z nejlevnějších možných nástrojů on-line cenzury, je však značně nepřesný a často dochází k [falešným negativům](#) (nízká míra přesnosti) nebo [falešným pozitivům](#) (přílišná přesnost). Poměr ceny a přesnosti demonstruje [graf č. 2](#). Výběr filtrovací metody nicméně nezáleží jen na poměru cena-výkon, ale také na dalších proměnných kritériích popsanych výše.

¹²² OPENNET INITIATIVE. *About Filtering*



Graf č. 2: Poměr ceny a přesnosti nástrojů internetové cenzury

Zdroj: Vlastní zpracování

Za předpokladu, že je některá z výše uvedených technických metod využita, uživatel si také ani nemusí být vědom, že je podroben cenzuře, protože filtrování obsahu je velmi náročné technicky zaznamenat.¹²³

6. 3. 3. KAZUISTIKY IMPLEMENTOVANÉ INTERNETOVÉ CENZURY

6.3.3.1. Čína

Internetová cenzura v nejlidnatější zemi světa je jednou z nejtvrdějších vůbec.¹²⁴ V průzkumu Freedom on the Net získala za rok 2019 pouhých 10 bodů ze 100. Komunistická strana Číny už dlouhou dobu uplatňuje striktní a centralizovanou cenzuru. Stát povoluje používání internetu, ale pouze podle svých pravidel. Se zprovozněním internetu nebyly restriktce tolik přísné, jak se ale počet čínských uživatelů rozrůstal a s ním i počet projevů vymezujících se vůči vládě a jejím nařízením, začala okolo roku 2000 komunistická

¹²³ WARF, Barney. *Geographies of global Internet censorship*

¹²⁴ FREEDOM HOUSE. *Freedom on the net: China*

strana cenzuru zpřísnovat.¹²⁵ Postupně se tak kyberprostor stal nástrojem moci režimu. V dnešní době provozuje Čína nejrozsáhlejší a technologicky nejsložitější systém internetové cenzury na světě. Čínský prezident Si Ťin-Pching odůvodňuje svou represivní politiku tím, že i internet je zapotřebí podrobit právu státu v zájmu zachování suverenity a bezpečnosti ve státě.¹²⁶

Všechna čínská cenzurní opatření bývají nazývána jako „Velký čínský firewall“ (Great Firewall of China) a byl spuštěn v roce 2006 čínskou iniciativou „Zlatý štít“ (Golden Shield), která ho vyvinula ve spolupráci s americkými společnostmi Nortel a Cisco Systems.¹²⁷ Tento systém umožňuje rozeznávat obličejové tváře a hlasy všech obyvatel Číny a slouží jako vzor pro další autokratické režimy po celém světě. Zlatý štít byl dokonce exportován na Kubu, do Íránu nebo Běloruska.¹²⁸ Velký čínský firewall zahrnuje cenzurní opatření jako monitorování obsahu, který by mohl být v rozporu s politickým pořádkem, sledování e-mailových komunikací, soukromých zpráv, blokování IP adres, podvrhování DNS, filtrování klíčových slov apod. I přístup k běžným webovým službám jako Yahoo! nebo Google jsou velmi striktně omezena. Pro monitorování obsahu je velmi známa tzv. *50 cent party* (nebo také *5 mao party*), skupina levné pracovní síly, které najímá a využívá vláda k manipulování veřejného mínění ve prospěch režimu. Tyto komentátoři monitorují obsah na internetu a zaplavují sociální síť stranickými komentáři a propagandou prostřednictvím falešných profilů (tento jev je možné vysledovat i v českém prostředí sociálních sítí, a to hlavně u příspěvků hnutí ANO nebo populistického hnutí SPD)¹²⁹.

Velkou část cenzury ovšem zajišťují samotné internetové společnosti¹³⁰, které v Číně operují za předem učených cenzurních podmínek a monitorují chatovací místnosti, síťové služby, vyhledávače, video weby apod. Policie kontroluje i internetové kavárny, kde musí lidé vždy před použitím počítačů s připojením na internet poskytnout své osobní údaje, což zajistí jejich případnou dohledatelnost. Webové stránky pomáhající obcházet cenzuru

¹²⁵ BI, Jianhai. *The Internet Revolution in China: The Significance for Traditional Forms of Communist Control*

¹²⁶ REPORTERS SANS FRONTIÈRES. *RSF Report: "China's Pursuit of a New World Media Order"*

¹²⁷ LAKE, Eli. *Hacking the Regime*

¹²⁸ WARF, Barney. *Geographies of global Internet censorship*

¹²⁹ DOČEKAL, Daniel. *Noemi Maixner a ti druzí. Odkud se berou falešné účty, které milují politiky?*

¹³⁰ MACKINNON, Rebecca. *China's Censorship 2.0: How companies censor bloggers*

jako anonymizer.com nebo proxify.com jsou samozřejmě blacklistovány. Na každém zařízení byl už ve výchozím nastavení (i v nově zakoupených zařízeních) instalován software QQ pro okamžité zasílání zpráv, který monitoroval soukromé konverzace. Tento program byl předchůdcem WeChatu, který aktuálně používá přes 1 miliardu uživatelů. Data, která společnost WeChat shromažďuje, nejsou šifrována a jsou spravována Čínskými servery. Distinktivním je pro šíření čínské propagandy a monitorování uživatelů i vyhledávač Baidu, který je po Googlu nejužívanějším vyhledávačem na světě. Nabízí dokonce velmi podobné služby včetně přesné kopie on-line encyklopedie Wikipedia. Tyto softwary představují pro čínský režim významný zdroj cenzury, vlivu a dohledu.¹³¹

Čínská vládní cenzura také občas způsobuje problémy se zahraničními investory. Jak už bylo popsáno výše na konci kapitoly [6.3.1.](#), v roce 2010 se z čínského trhu stáhla například společnost Google. I společnost Facebook byla v roce 2009 v Číně vládou zakázána. Od té doby jeho zakladatel a CEO Mark Zuckerberg podniká všechny možné kroky k opětovnému proniknutí na čínský trh, včetně fotografování se s prezidentem Si Ťin-Pchingem nebo při kondičním běhu s přáteli na Náměstí Nebeského Klidu v Pekingu, kde v červnu roku 1989 došlo k masakru tisíců pokojných demonstrantů za demokracii.

Tato opatření efektivně zamezují přístup k informacím pro-demokratickým aktivistům, obhájčům lidských práv, tibetským separatistům i náboženským skupinám jako Fa-lung-kung, které režim označuje jako teroristy. Toto hnutí ve spolupráci s americkými programátory vyvinulo mimo jiné software k obcházení cenzury Freegate, který nabídlo například i disentu v Íránu a dalších zemích.¹³² Čínská cenzura i její odpor své taktiky a strategie v reakci na chování druhé strany neustále mění. Výhledově ale dle mého názoru, a vzhledem k polymorfní povaze internetu, budou omezení dříve nebo později postupně selhávat.

6.3.3.2. *Země arabského světa a internetová cenzura za arabského jara*

Většina arabských zemí uplatňuje principy přísné cenzury, Žurnalisté, editoři, blogeři a další autoři obsahu, který umisťují na internet, čelí trestům za oslabování arabské víry,

¹³¹ REPORTERS SANS FRONTIÈRES. *RSF Report: "China's Pursuit of a New World Media Order"*

¹³² LAKE, Eli. *Hacking the Regime*

zatravování vládních činitelů nebo obhajování nemorálního chování. Svou cenzuru pak vlády ospravedlňují ochranou islámských hodnot a morálky.¹³³ Cenzura také může generovat zisky pro vládu, a to prostřednictvím monopolizace státem vlastněných společností (například omezeným přístupem ke konkurenčním telekomunikačním společnostem). Za zřejmě nejpřísnější vůči přístupu k internetu a možnostem svobodného projevení z nich můžeme považovat Sýrii (skóre 17), Saudskou Arábii (25). Mnoho arabských států následuje model právě Saudské Arábie. Tam byl internet zprovozněn, až když si vláda byla jista, že ho má pevně v rukou. Celá páteř internetu je ve vlastnictví státu, vytvořil rozsáhlou firewallovou síť, která řídí tok informací. Podle průzkumu OpenNet iniciativy v roce 2004 bylo saudsko-arabským režimem zakázáno na 400 000 webových stránek, z nichž převážnou část tvořil obsah pro dospělé, on-line hry, rekreační weby, on-line nakupování, Yahoo! a dokonce například webové stránky, které obsahovaly slova jako „prsa“, třebaže v lékařském kontextu.¹³⁴ Jakýkoli pokus o přístup na takové stránky stát samozřejmě detekuje, což podporuje rozsáhlou autocenzuru.

Bahrajn (26) a Jordánsko (47) blokuje přístup ke Google Earth a Skypu s odvoláním na ochranu národní bezpečnosti¹³⁵, zatímco Sýrie blokuje například přístup ke všem serverům zahraničního zpravodajství v kurdštině a všechny domény s koncovkou „.il“ (Izrael).¹³⁶

Internetová vládní cenzura představuje silné téma i pro události arabského jara probíhajícího od konce roku 2010 a v některých státech až do současnosti. Díky protestům došlo ke svržení autoritářských vládců v Tunisku (64), Libyi (49), Egyptě (26) a Jemenu. Právě díky internetovým nástrojům a digitální gramotnosti některých Arabů, kteří dokázali obejít blokovací a filtrovací softwary, se do světa dostala videa a zprávy do zahraničních zpravodajství a lidé prostřednictvím sociálních sítí (zejména Facebooku a Twitteru) například i organizovali demonstrace.¹³⁷ Například v Egyptě se během revoluce v roce 2011 zvýšil počet tamních občanů využívajících Facebook o 30 % a počet tweetů vyjadřujících

¹³³ WARF, Barney. *Geographies of global Internet censorship*

¹³⁴ Tamtéž.

¹³⁵ BBC News. *Bahrain blocks opposition websites*

¹³⁶ SHISHKINA, Alisa a Leonid ISSAEV. *Internet Censorship in Arab Countries: Religious and Moral Aspects*

¹³⁷ HUANG, Carol. *Facebook and Twitter key to Arab Spring uprisings: report*

se o politice vzrostl z průměrných 2 500 na 230 000 denně.¹³⁸ Odpovídající byla ale také odpověď arabských vlád. V Egyptě a Libyi vláda podnikla bezprecedentní krok a na určitou dobu kompletně znemožnila přístup k internetu¹³⁹, syrská elektronická armáda (SEA) zamezila přístup k množství webových stránek, které podněcovaly vzpuru proti vládě, a rozšířila i software, jímž odepřela přístup ke zpravodajským webům jako Al Jazeera, BBC News nebo syrské televizní společnosti Orient TV.¹⁴⁰

6.3.3.3. *Filtrování a blacklistování v ČR*

I v České republice je možné vysledovat určitý druh filtrování. Ten ale neimplementuje vláda, nýbrž poskytovatelé internetového připojení. Společnost Telefónica O2 Czech Republic potvrdila blokování přístupu na stránky podle blacklistu britské společnosti Internet Watch Foundation obsahující zejména weby s dětskou pornografií a jiným nevhodným a nelegálním obsahem.¹⁴¹ Společnost Vodafone blokuje pouze obsah s dětskou pornografií, nikoli už „jiný nelegální obsah“.¹⁴² Se zmíněnou společností spolupracuje i třetí z velké trojky mobilních operátorů, společnost T-Mobile, která filtruje jednotlivé URL (nikoli domény) obsahující dětskou pornografii, dětskou prostituci, obchod s dětmi, pedofilní zájem a další nelegální sexuální praktiky se vztahem ke zneužívání dětí.¹⁴³

Otázkou je, nakolik je blokování podle společnosti řídící se britskou jurisdikcí a jejích standardů aplikovatelné na českou internetovou krajinu. Další kritika této praxe se zaměřuje na fakt, že o zařazení webů na blacklist této organizace nerozhoduje soud.

Jistá míra blokování se týká i stránek nabízejících obsah jako filmy nebo hudba k nelegálnímu stažení. Zprostředkovatel (například hostingová firma) podle české právní úpravy za obsah, který poskytuje, odpovědnost nenese, avšak pokud je majitelem práv

¹³⁸ CAMBIÉ, Silvia. *Lessons from the front line: The Arab Spring demonstrated the power of people—and social media*

¹³⁹ REPORTERS SANS FRONTIÈRES. *Journalists confined to their hotels, Internet disconnected*

¹⁴⁰ OPENNET INITIATIVE. *Syrian Electronic Army: Disruptive Attacks and Hyped Targets*

¹⁴¹ MACICH, Jiří. *Telefónica O2 potvrdila filtrování stránek*

¹⁴² PETERKA, Jiří. *Stalo se: Vodafone přehodnotil své blokování Internetu*

¹⁴³ T-MOBILE CZECH REPUBLIC. *T-Mobile pomáhá v boji proti zneužívání dětí blokováním nelegálního obsahu*

na nelegální praktiky upozorněn, je povinen obsah stáhnout.¹⁴⁴ K předcházení sdílení porušující autorská práva poskytovatelé internetového připojení také čas od času blokují peer2peer sítě¹⁴⁵. K takovému blokování dochází také i v rámci privátních sítí institucí (škol, soukromých společností). Tento způsob pirátství je ovšem už poněkud zastaralý. Zatímco v roce 2010 byl peer2peer provoz zodpovědný až za polovinu internetového provozu¹⁴⁶, v roce 2017 už to bylo pouhých 5 %.¹⁴⁷ Velký vliv na to má zejména masivní rozšíření legálních streamovacích služeb jako Netflix, HBO GO apod. Když už se ale filmy nelegálně sdílí, využívají k tomu uživatelé například Google Drive a někteří kreativní dokonce i aplikaci Mapy Google.¹⁴⁸

6. 3. 4. BOJ PROTI INTERNETOVÉ CENZUŘE A JEJÍ OBCHÁZENÍ

Přestože existuje a bylo vyzkoušeno mnoho technologických metod k obcházení internetové cenzury, jen velmi málo z nich mělo do této chvíle v zemích s internetovou cenzurou reálný dopad na transformování či ovlivnění veřejné politiky. Aby byly anti-cenzurní technologie a metody opravdu účinné, musí být navrženy nejen tak, aby poskytovaly neomezený přístup k internetu, ale musí být vyvinuty s cílem transformovat veřejnou politiku a vynutit zrušení cenzurních opatření. Protože digitální cenzura sestává jak z dimenze technologické, tak z politické a sociální, některé autokratické režimy pochopily, že pro účinnou regulaci je zapotřebí nejen pokročilé technologie, ale sofistikovaně je kombinovat s politickými opatřeními a autocenzurou samotných občanů vynucovanou například tvrdými tresty. K poražení internetové cenzury proto musí opozice napadnout všechny tyto tři dimenze.¹⁴⁹

Z technologického hlediska existují dvě metody, které by potenciálně vedly k destabilizaci řízení informací. První vyžaduje převahu zahraničních příznivců anti-cenzury

¹⁴⁴ HOUSKA, Ondřej. *Poskytovatelé internetu nemusí blokovat stránky s nelegálním obsahem automaticky, jen na příkaz soudu*

¹⁴⁵ Peer2peer sítě využívány zejména k výměně a distribuci dat, kupříkladu videí, filmů nebo hudby.

¹⁴⁶ VAN DER SAR, Ernesto. *BitTorrent Still Dominates Global Internet*

¹⁴⁷ BOŘÁNEK, Roman. *Piráteň pomocí torrentů už tolik nefrčí, ve velkém se sdílí i přes Google Drive*

¹⁴⁸ SINGH, Manish. *With Torrent Sites Facing the Heat, Pirates Get Creative With Google Drive and Other Services*

¹⁴⁹ LEBERKNIGHT, Christopher S. a kol. *A Taxonomy of Internet Censorship and Anti-Censorship*

v technologickém vývoji a možnostech. Z iniciativ bojujících proti internetové cenzuře a za svobodu projevu ve světě můžeme zmínit zejména pařížskou nevládní organizaci Reportéři bez hranic¹⁵⁰ (RSF), OpenNet Iniciativu¹⁵¹ nebo americkou nevládní neziskovou organizaci Freedom House¹⁵². Ty se aktivně zasazují o rušení internetových cenzur po celém světě i o odstraňování jednotlivých webových stránek z vládních blacklistů. Toto řešení má ale spíše krátkodobý charakter a záleží na finančních možnostech regulátorů, zda dokážou se svou opozicí držet krok.

Druhým přístupem je navrhování takových technologií, které maximalizují náklady na provozování cenzurních technologických sítí nebo zvýší mezinárodní povědomí o důsledcích internetové cenzury.¹⁵³ K takovému úspěšnému případu došlo v roce 2009 při iránských volbách, respektive při protestech proti volebním podvodům. Vláda se následně pokoušela crackovat internetovou komunikaci protestujících, ti však dokázali digitální blokády obejít a poslat do světa video a twitterové příspěvky o násilném potlačování demonstrujících. V návaznosti na to se USA rozhodla ve své zahraniční politice maximálně prioritizovat podporu neomezeného přístupu k internetu všude ve světě.¹⁵⁴

Jak už bylo zmíněno, pro opravdu efektivní boj proti cenzuře je zapotřebí syntetizovat dimenzi technologickou, politickou a sociální a zaútočit na jejich zranitelná a slabá místa. Účinným východiskem může být takové řešení, které bude z technologického hlediska navrženo dostatečně dobře natolik, aby bylo schopné destabilizovat politické a sociální struktury.¹⁵⁵

Způsoby obcházení se různí podle kritérií:

- *dostupnost* (pokud se k anti-cenzurní technologii cíloví uživatelé nemají, jak dostat, je jejich existence a vývoj zbytečný),

¹⁵⁰ REPORTERS SANS FRONTIÈRES . *Our activities*

¹⁵¹ OPENNET INITIATIVE. *About ONI*

¹⁵² FREEDOM HOUSE. *Our Issues*

¹⁵³ LEBERKNIGHT, Christopher S. a kol. *A Taxonomy of Internet Censorship and Anti-Censorship*

¹⁵⁴ GORMAN, Siobhan. *Web Access Is New Clinton Doctrine*

¹⁵⁵ LEBERKNIGHT, Christopher S. a kol. *A Taxonomy of Censors and Anti-Censors*

- *uživatelská přívětivost* (snadnost využívání technologie představuje klíčový parametr k možnosti jejího rozšíření mezi co největší počet uživatelů, a nejen pro ty technologicky zdatné),
- *ověřitelnost a důvěra* (možnost uživatele ověřit, že technologie nebo systém není ve skutečnosti monitorovacím nástrojem vlády nebo na ni není nějakým způsobem napojen),
- *rozsah* (kolik způsobů komunikace lze anti-cenzurní technologií pokrýt),
- *bezpečnost* (nejzásadnější kritérium zajišťující, aby uživatel nebyl při obcházení cenzury odhalen),
- *možnost zapírání* (když bude uživatel vysledován nebo chycen, jak může obcházení cenzury zapřít),
- *výkonnost* (v jaké míře anti-cenzurní technologie limituje tu cenzurní).¹⁵⁶

Mezi anti-cenzurní řešení je možné zahrnout snahy o přístup k internetovému připojení v zahraničí, které není zatíženo filtrováním nebo blokováním, například využitím proxy serverů, VPN připojení nebo anonymizačních softwarů jako TOR.

Proxy server je zkráceně prostředník, ve formě počítače nebo softwaru, mezi klientem a serverem, který klienta chrání před proniknutím do klientské sítě a je jedním z možností, jak vytvořit firewall. Lze využít také jako nástroj k obcházení cenzury. Namísto přímého připojení k cílovému serveru odešle uživatel požadavek proxy serveru, který ho pak realizuje, získá data z cílového serveru a odešle je uživateli. Je možné také využívat celou síť proxy serverů, přičemž čím více jich uživatel využije, tím vyššího stupně anonymity dosáhne.

VPN, zkratka z anglického „virtual private network“ (tedy virtuální privátní síť) představuje nástroj k soukromému propojení a šifrované komunikaci mezi několika počítači v rámci veřejné sítě. VPN server se kupříkladu z určitého místa připojí k internetu, a k serveru se připojí počítač uživatele. Jako zdroj připojení k internetu se pak jeví onen VPN router, nikoli zařízení uživatele. VPN také šifruje veškerá data, která uživatel odešlá či přijímá, čímž uživateli zajišťuje vysokou míru anonymity.

¹⁵⁶ LEBERKNIGHT, Christopher S. a kol. *A Taxonomy of Censors and Anti-Censors*

TOR je příkladem anonymizačního softwaru. Projekt, který funguje na takzvaném Onion Routing, zajišťuje maximální anonymitu přenosu dat skrz internet, chrání osobní údaje, svobodu projevu i soukromí uživatelů před sledováním aktivit na internetu. TOR přesměrovává připojení uživatele mezi spoustou dobrovolně připojených hostitelů, takže jej nikdo nedokáže vystopovat. Nicméně tato síť je hojně využívána zejména díky své anonymní charakteristice k přístupu na tzv. darknet, který slouží jako prostředí ke kriminálním aktivitám jako nelegální obchod, šíření dětské pornografie, organizace teroristických skupin apod.

6. 3. 5. HROZBY V KYBERPROSTORU A CENZURA JAKO NÁSTROJ K OCHRANĚ UŽIVATELŮ

Mimo snahy o vládní represe obyvatel lze cenzuru internetu prostřednictvím blokování či filtrování určitých webových stránek využít také pro ochranu veřejnosti a jejich zájmů.

Vzhledem k tomu, že internet dal hlas opravdu všem, stal se ideálním prostředím i pro kyberšikanu. Urážky, zesměšňování, stalkování, ostrakizace a další její formy jsou časté zejména u dětí a mladistvých. Stát se obětí některého z těchto způsobů poškozování může mít pro oběť trvalé následky v podobě psychických problémů, v krajních případech vede až k sebevraždám. Šikanování on-line se pak může promítnout i do chování mimo on-line svět a vyústit tak i ve fyzické útoky.

Další z možných hrozeb, ke kterým může a dochází prostřednictvím internetu a které mohou narušovat veřejné zájmy, je podněcování nenávisti proti národnostním, sexuálními a dalším minoritám, distribuce pirátských kopií filmů, knih nebo hudby či využívání internetu teroristickými a jinými násilnými skupinami jako nástroje pro vnitřní organizaci. Poslední zmíněný příklad lze ilustrovat na využívání sociálních sítí teroristickou organizací ISIS k rekrutování džihádistů. Její členové také využívali Facebook a Twitter k šíření propagandy a násilí.¹⁵⁷

Právě kvůli tomuto problematickému obsahu stále více provozovatelů platforem pro on-line komunikaci vytváří pravidla jejich užívání, se kterými musí před jejich využitím

¹⁵⁷ AWAN, Imran. *Cyber-Extremism: Isis and the Power of Social Media*

uživatel vyjádřit souhlas. Tato pravidla zakazují povětšinou všechny výše zmíněné aktivity. V pravidlech si také vyhražují právo mazat obsah, jenž bude pravidla porušovat. Problémem je, že tato ustanovení nemají žádný právní základ. Pokud tedy provozovatel uživateli odstraní obsah, může se proti tomuto kroku obrátit na soud s tím, že došlo k porušení ochrany svobody projevu.

6. 4. ANONYMITA JAKO ZDROJ BEZPEČNOSTI I NEBEZPEČÍ NA INTERNETU

S obrovským rozmachem a rozvojem internetu od jeho uvedení do provozu je sociální chování lidí na této unikátní platformě předmětem mnoha vědeckých studií. Internet totiž umožňuje všem osobám realizování svobodného projevu a poskytuje jim mediální prostor, ke kterému měl dříve přístup pouze limitovaný počet lidí s odvoláním na jejich žurnalistickou či uměleckou profesi. Jedním ze zajímavých fenoménů internetové komunikace hodných vědecké pozornosti už z důvodu možné kolize práva na svobodu projevu s osobnostními právy je využívání anonymity. Internet se díky své deindividualizované povaze stal mekkou pro nejrůznější druhy jejího využívání. On-line prostředí zprostředkovává politickou diskusi, umožňuje všechny druhy komunikace interpersonální nevyjímaje, je ale i prostředím velmi vhodným k páčání trestných činů. Zda by uživatelé ve světle všech nezákonných praktik, které jim anonymita umožňuje, měli mít možnost v internetovém prostředí vystupovat anonymně, nebo by anonymita měla být zcela zakázána, je už dlouho předmětem debat vědců, politiků i provozovatelů a zprostředkovatelů internetové komunikace. Zákazem možnosti vystupovat v prostředí internetu anonymně by bylo významně zasaženo do ústavně zaručeného práva na soukromí, jak ale dohnat k zodpovědnosti ty, kteří této možnosti zneužívají? Jako všechny fenomény má i tento své pozitivní i negativní aspekty, které budou v rámci této práce dále rozebrány.

Anonymitu využívanou v prostředí internetu lze definovat jako neidentifikovatelnost uživatele, nemožnost ostatních uživatelů identifikovat určitou osobu či možnost před ostatními uživateli vlastní identitu skrýt, a to jak v širokém sociálním kontextu, tak při internetové komunikaci dvou jednotlivců.¹⁵⁸ Být na internetu anonymní znamená, že osobu není možné identifikovat na základě ani jedné ze sedmi dimenzí určující identitu.

Těmito dimenzemi jsou:

- jméno osoby,

¹⁵⁸ CHRISTOPHERSON, Kimberly M. *The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog"*

- její aktuální lokace,
- využitý pseudonym, který se může týkat pravého jména osoby či její lokace,
- využitý pseudonym, který sice nelze spojit se specifickými informacemi o totožnosti osoby, ale poskytuje k identitě určitá vodítka,
- behaviorální dimenze zahrnující vzorce chování osoby,
- členství v sociálních skupinách,
- dovednosti a další rysy, které by indikovaly personální charakteristiky a vlastnosti osoby.¹⁵⁹

Samotnou anonymitu v on-line prostředí internetu pak můžeme rozčlenit do tří kategorií. První z nich je již definovaná úplná anonymita, které lze ovšem dosáhnout jen velmi těžko a za použití složitých technických nástrojů a procesů. Následuje pseudonymita, kdy svou identitu uživatel nahrazuje pseudonymem, který může nabývat nejrůznějších podob (například jméno filmového hrdiny, oblíbeného zpěváka apod.). Pseudonymizaci či šifrování se provádí i například k zabezpečení osobních údajů podle GDPR.¹⁶⁰ Určitou formou anonymity je také krádež identity, kdy uživatel záměrně využívá osobní údaje třetí osoby a jako daná osoba vystupuje, nejčastěji za účelem podvodného či nezákonného jednání nebo k předstírání vyšší autority.

Uživatelé internetu přistupují k ukrytí své identity zejména ve snaze uchránit své soukromí. Dle mnohých studií patří mezi uživatele, kteří si svou identitu za tímto účelem vědomě střeží, často zejména takzvaní whistleblowři¹⁶¹, dále členové stigmatizované skupiny, lidé vyhledávající citlivý obsah, hackeři nebo slídivové.¹⁶²

Velká část uživatelů, zejména vyšší věková skupina, leckdy ale ani netuší, k čemu by jim taková anonymita v on-line prostředí mohla sloužit, před čím by je mohla ochránit, nebo si této možnosti ani dokonce nejsou vědomi. Většina uživatelů pak není obeznámena

¹⁵⁹ MARX, Gary T. *What's in a Name? Some Reflections on the Sociology of Anonymity*

¹⁶⁰ EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. *GDPR (obecné nařízení): 8. Zabezpečení osobních údajů*

¹⁶¹ Informátoři, kteří upozorní orgány oprávněné k prověření či zakročení proti nelegitimním, neetickým či nezákonným probíhajícím praktikám nebo upozorní na podezřelé či trestné jednání policii či novináře. Často jimi bývají bývalí či stávající zaměstnanci oné instituce.

¹⁶² KANG, Ruogu a kol. *Why do people seek anonymity on the internet?*

s tím, kdo všechno má k datům, jež v rámci jedné webové stránky souhlasili poskytovat, přístup a ani jak se k nim třetí strany mohou dostat. Na většině webových stránek stačí zaškrtnout jedno políčko, čímž s poskytováním dat uživatel vyjádří souhlas, ale už si nepřčte, co za data a za jakých podmínek vlastně poskytuje. Vzhledem k jejich typické délce je to pochopitelné a číst dokumenty o zpracování osobních údajů na všech stránkách, které uživatel navštěvuje, ani není reálné. Podmínky ale mohou obsahovat klauzule o možnosti zpracování, využívání i přístupu k osobním datům, které mohou uživatele v nejzazším případě i značně poškodit.

6. 4. 1. DŮVODY VYUŽÍVÁNÍ ANONYMITY

Dle studie Ruongu Kanga a kol. pod záštitou pittsburské Carnegie Mellon University, která zkoumá důvody, proč lidé vystupují v on-line prostředí anonymně, využívají uživatelé nejčastěji anonymitu instrumentálně nebo sociálně.

Mezi instrumentální anonymitu můžeme zařadit aktivity s cílem získat informace, tedy například stahování souborů či prosté vyhledávání informací. Jedním z často zmiňovaných důvodů využití anonymity k tomuto typu on-line aktivity představuje zabránění vyhledávači sesbírat informace o hledaném obsahu, na jejichž základě by pak zobrazoval personalizované reklamy. Jako další důvod pak studie identifikovala fakt, že uživatelé nepovažují za podstatné s navštěvovanou stránkou sdílet osobní data, která by sloužila jen k marketingovým účelům společnosti.

Pod anonymitu sociální pak podle zmiňované studie spadají typy on-line aktivit jako komunikace v zájmových skupinách, komunikace na sociálních sítích, sdílení uměleckých děl, výtvorů, fotografií či videí s očekávaným hodnocením, vyhledávání pomoci, prodej a koupě zboží, účast v diskusi o politice či hodnocení a doporučování zboží a služeb.

Více než polovina dotazovaných využívala anonymitu v rámci výše zmíněných aktivit pro jejich nezákonnost či neetičnost, nebo se zapojovali do společností zavrhaných aktivit jako je procházení webů zobrazujících násilí nebo pornografii. Dále pak anonymitu

využívali k nelegálnímu stahování souborů, šíření hate speech nebo vyhledávání osobních informací o třetích osobách.¹⁶³

Obecně lze z výsledků vyvodit, že uživatelé využívají možnosti anonymity pro realizování těch aktivit, které pro ně představují riziko zhoršení či ztráty sociálního statusu, které mohou zapříčinit neakceptování či zavržení jejich názorů potažmo jich samých v jejich sociální bublině či jejich blízkými nebo těch aktivit, které pro ně mohou představovat osobní či bezpečnostní rizika jako například ztrátu majetku či zaměstnání, vydání k trestnímu stíhání, uložení finančních či jiných sankcí nebo dokonce odnětí svobody. Díky anonymitě se v on-line prostředí mohou vyhnout on-line útokům, obtěžování či trollingu.

Výše zmíněna osobní rizika mohou pro uživatele představovat on-line predátoři, organizace, uživatelé, které osoba zná, a taktéž ti, kteří jsou pro ni neznámí. On-line predátoři pak mohou být kriminálníci, hackeři, scammeři¹⁶⁴, stalkeři a další osoby, kterým uživatelé připisují nekalé záměry jako krádež identity, zneužití osobních dat (jako tomu bylo například v kauze Cambridge Analytica¹⁶⁵) či kreditní karty, spamování a další. Za organizace, které představují určitý druh hrozby, lze považovat zejména vládu, jež má v moci nelegální on-line aktivity potrestat, a obchodní společnosti, které mohou osobní data uchovávat a za úplatu je poskytnout třetím stranám k šíření marketingových sdělení či spamu.¹⁶⁶ I osoby, které uživatel zná, mohou představovat riziko. V případě, že se s někým v reálném životě uživatel nepohodne, může o něm daná osoba začít v prostředí internetu šířit nepravdivé informace, pomluvy apod.

¹⁶³ KANG, Ruoga a kol. *Why do people seek anonymity on the internet?*

¹⁶⁴ Internetový podvodník

¹⁶⁵ Skandál celosvětově známý jako Cambridge Analytica, jež své jméno bere od společnosti, která je jeho tvůrce, je perfektním příkladem toho, jak mohou být uživatelská data zneužita. V tomto případě byla data využita k dost možná nejméně etickému cíli, a to k personalizování politické reklamy, která měla za úkol ovlivnit chování voličů u amerických prezidentských voleb v roce 2016. Dále se spekuluje, že byla touto společností shromážděná uživatelská data využita také pro personalizaci politické reklamy při referendu o Brexitu ve Velké Británii. Spekuluje se také o možném napojení na Rusko, a to skrze blízký kontakt nejvyšších představitelů společnosti Cambridge Analytica a společnosti Lukoil. O této spojitosti se však jen spekuluje. V případě jejího potvrzení by byla jen dalším důkazem o nelegálních krocích a vměšování se Ruska do politického boje ve světových velmocích.

¹⁶⁶ KANG, Ruoga a kol. *Why do people seek anonymity on the internet?*

Mimo důvody, které mohou představovat hrozbu, uživatelé také často skrývají svou identitu, protože se tak cítí například v debatách či při přispívání do diskusních fór více uvolněni, serióznější a anonymita jim může také dodávat odvalu o určitých tématech vůbec diskutovat. Dalším motivem také může být snaha o oddělení život v on-line a off-line světě, tak aby aktivity ani v jednom ze světů neměly na ten druhý vliv.

6. 4. 2. JAK ANONYMITY DOSÁHNOUT

Existují dvě strategie, které uživatelé mohou využít k zajištění anonymity a k zajištění ochrany své i svých osobních údajů, a to technická a behaviorální. Technická strategie odkazuje k odstranění či neposkytnutí jakýchkoliv osobních identifikačních informací a existuje celá řada způsobů, jak toho docílit. Uživatelé si mění IP adresy¹⁶⁷, využívají proxy servery, VPN, anonymizující systémy jako TOR či jiné způsoby šifrování dat (tyto způsoby anonymizace jsou blíže popsány v kapitole [6. 3. 4.](#)). Pro většinu uživatelů jsou ale tyto způsoby velmi komplikované a využívají je tak pouze uživatelé s vyšší technologickou zdatností. Snazší a laikům dostupnější variantou je úprava nastavení internetových vyhledávačů, zejména co se ukládání cookies či procházení internetu v anonymních variantách prohlížečů týče. To ale uživateli zajistí anonymitu pouze pro ostatní uživatele či webové stránky, před poskytovatelem internetového připojení tento krok ovšem technická osobní data neskryje.

Druhou strategií je strategie behaviorální, tedy že uživatel ke skrytí své identity využívá behaviorální metody. V praxi to znamená, že uživatel nesdílí na internetu svoje soukromé informace nebo sdílí falešné informace (fiktivní jméno, falešná profilová fotka, smyšlené základní údaje apod.). Tento způsob dosahování anonymity ale poskytuje anonymitu pouze pro ostatní uživatele nebo aplikace, ovšem ostatní citlivá data, která je možná skrýt technickými metodami, jsou dostupná například poskytovateli internetového připojení¹⁶⁸, od kterého si tato data může v případě provozování nelegálních aktivit vyžádat policie.

¹⁶⁷ Unikátní adresa každého zařízení, které je připojeno k síti a podle které lze zjistit například údaje o geografické poloze.

¹⁶⁸ KANG, Ruogu a kol. *Why do people seek anonymity on the internet?*

6. 4. 3. POZITIVNÍ IMPLIKACE ANONYMITY

I anonymita jako fenomén on-line komunikace může mít na sociální interakce i uživatele samotné nejenom negativní, ale také pozitivní dopady.

Díky anonymitě mohou například lidé ve státech s autoritářskými režimy využívat možnost anonymity k vyjadřování svých politických postojů, které jsou často v dané zemi ventilovat zakázány. Mohou díky anonymitě také sdílet informace o dění v zemi, které se vláda snaží před světem utajit (kupříkladu šíření informací o poměrech a dodržování lidských práv v Severní Koreji). Anonymitu lze také využít k zasílání tipů novinářům či policii o určitém podezřelém jednání, které díky tomu může vyplout na povrch a pomoci znevýhodňovaným osobám dostat se z nepříznivé životní situace.

Pozitivní dopady má anonymita i ve více individuální rovině. Lidé mají tendenci pod rouškou anonymity otevřeně více diskutovat o velmi osobních tématech, které by kvůli studu nikdy osobně s nikým neprobírali. Mohou to být témata jako psychické problémy, sexuální problémy, zdravotní stav, lidé jsou často otevření i v tematice sexuálního zneužívání, zkušenostech z pozice obětí trestných činů apod. Tato otevřenost je pak prospěšná nejen pro samotné uživatele, kteří se s takovými problémy svěřují. Už jen samotný fakt, že se s problémem svěří a někdo je vyslechne, je pro ně velmi přínosný. Tyto informace mohou navíc mít příznivý vliv i na ostatní uživatele s podobnými problémy. Daná osoba se pak ve své těžké životní situaci necítí osamělá a nepochopená.

Jednu z pozitivních implikací anonymity představuje také možnost vžít se za pomoci pseudonymity do pozice určité osoby a pochopit tak jeho sociální status, problémy, se kterými se například jako člen určité minoritní skupiny potýká apod. Když například za výzkumnými účely vědec vystupuje po určitou zkoumanou dobu v on-line prostoru jako žena nebo například člen národnostní menšiny, má možnost pochopit charakter jejich znevýhodňování a daný výzkum může třeba vést až ke změně legislativy ve prospěch stigmatizované skupiny.

Anonymita může mít také psychologické dopady na chování jednotlivců v rámci skupiny i skupiny samotné. Jednou z nejznámějších teorií, ke které sociální psychologové často odkazují při zkoumání sociálních skupin, je teorie deindividuace psychologa Philipa Zimbarda. Ten je také autorem proslulého a velmi kontroverzního stanfordského vězeňského

experimentu, kterým chtěl ověřit myšlenku, že sociální chování člověka je determinováno prostředím a rolí, kterou v něm zaujme.¹⁶⁹ Jeho teorie deindividuace popisuje efekt anonymity na sociální chování a vysvětluje anti-normativní kolektivní chování. Tato teorie říká, že lidé v davu se neřídí vlastním úsudkem (ztrácejí svou individualitu), snižuje se racionalita jejich uvažování (tedy tíhnou k afektovanému a impulzivnímu jednání) a mají tendenci jednat anti-normativně a anti-sociálně, čili více agresivně či krutě, než by jednali jako jednotlivci sami za sebe.¹⁷⁰ Tento deindividualizovaný stav vede k oslabení takových regulátorů chování, jakými jsou pocit viny, stud, strach, odpovědnost, a člověku tak snižuje hranici, při které ztrácí zábrany k anti-normativnímu či anti-sociálnímu chování.¹⁷¹ Aktuálnější teorie jsou toho názoru, že Zimbardova teorie nestačí k popsání vlivu anonymity na sociální chování ve skupině a je při takových výzkumech nutno brát v potaz celou řadu situačních, environmentálních i individuálních vlivů, jako jsou psychologické charakteristiky a pochody jednotlivce.¹⁷² Od 90. let se pak vědecké práce zaměřovaly na výzkum aplikace Zimbardovy deindividuační teorie na počítačovou a on-line komunikaci, a to za implementování takových sociálních proměnných, které při „face to face“ komunikaci nejsou dostupné (absence vizuálních a audio podnětů, asynchronní komunikace, izolace obou stran komunikace apod.).¹⁷³ V rámci výzkumu vlivu anonymity na sociální chování v počítačové a on-line komunikaci převládají dvě teorie. První z nich je tzv. *ekvalizační hypotéza*¹⁷⁴ (Equalization hypothesis) a SIDE teorie¹⁷⁵ (nebo také teorie sociální identifikace, akronym anglického „Social Identity model of Deindividuation Effects“).

¹⁶⁹ HONZÁK, Radkin. *Stanfordský experiment: Když člověk získá moc nad druhými, může se změnit k nepoznání*

¹⁷⁰ ZIMBARDO, Philip G. *The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos*

¹⁷¹ LEBERKNIGHT, Christopher S. a kol. *A Taxonomy of Censors and Anti-Censors*

¹⁷² CHRISTOPHERSON, Kimberly M. *The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog"*

¹⁷³ Tamtéž.

¹⁷⁴ DUBROVSKY, Vitaly a kol. *The Equalization Phenomenon: Status Effects in Computer-Mediated and Face-to-Face Decision-Making Groups*

¹⁷⁵ SPEARS, Russell a kol. *Computer-Mediated Communication as a Channel for Social Resistance*

Ekvalizační hypotéza pracuje s obecně známým a přijímaným faktem, že lidské chování je modifikováno faktory jako vzhled, pohlaví¹⁷⁶, rasa, věk, etnická příslušnost, atraktivita¹⁷⁷ či fyzické postižení¹⁷⁸ komunikačního protějšku a tyto charakteristiky také udávají jeho sociální vliv. Počítačem zprostředkovaná komunikace je schopna tyto proměnné vyfiltrovat a zredukovat, takže si uživatelé do svých komunikačních protějšků nejsou schopni projektovat stereotypy a vytvářet si předsudky. Ekvalizační hypotéza pak předpokládá, že díky absenci těchto podnětů v počítačem zprostředkované komunikaci nabudou osoby, které mají ve společnosti tradičně dokazatelně nižší sociální vliv (ženy, členové národnostních menšin, lidé s postižením apod.), výrazně vyššího vlivu. Autoři teorie také zastávají názor, že k tomu, aby tato jejich teorie platila, není zapotřebí anonymity úplně.¹⁷⁹ Tato teorie však má své limity, například fakt, že výzkum byl prováděn v laboratoři a mezi zcela neznámými lidmi, proto nemůže být teorie generalizována na komunikaci v jakémkoliv prostředí. Studie také prováděla výzkum s využitím genderově separovaných skupin, i když sociální rozdíly mezi muži a ženami jsou dobře známé a dokázané, proto zanedbání tohoto faktoru výsledky studie taktéž značně limituje.¹⁸⁰

S ohledem na limity Zimbardovy deindividuační teorie i ekvalizační hypotézu je obecně přijímanou teorií vlivu anonymity na chování uživatelů v on-line komunikaci SIDE teorie. Ta je v podstatě reinterpetací deindividuační teorie, ale klade mnohem větší důraz na specifické situační proměnné, které udávají, zda anonymita vyústí v anti-normativní chování. Pro její kognitivní komponent je důležitá sociální a vizuální identita. Z výzkumu totiž vyplývá, že anonymita může působit pozitivně ve skupinách orientovaných na splnění určitého cíle. Za předpokladu kolektivní anonymity budou se budou její členové orientovat na splnění cíle celé skupiny spíše než na svůj vlastní prospěch.¹⁸¹ V případě,

¹⁷⁶ LOCKHEED, Marlaine E. a Katherine Patterson HALL. *Conceptualizing Sex as a Status Characteristic: Applications to Leadership Training Strategies*

¹⁷⁷ HATFIELD, Elaine a Susan SPRECHER. *Mirror, Mirror: The Importance of Looks in Everyday Life*

¹⁷⁸ ALLPORT, Gordon W. *The Nature Of Prejudice*

¹⁷⁹ DUBROVSKY, Vitaly a kol. *The Equalization Phenomenon: Status Effects in Computer-Mediated and Face-to-Face Decision-Making Groups*

¹⁸⁰ CHRISTOPHERSON, Kimberly M. *The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog"*

¹⁸¹ JOINSON, Adam N. *Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity*

že se v on-line prostředí utvoří anonymní skupina homosexuálů s cílem změnit legislativu za účelem zamezení jejich znevýhodňování, je implikace anonymity pozitivní. Pokud ale anonymitu využijí například sdružení neonacisté k šíření svých ideologií, budou implikace veskrze negativní.

Zda bude anonymita mít pro-sociální nebo anti-sociální dopad určuje strategický komponent SIDE teorie. Ten předpokládá, že jakmile uživatel pochopí, jakým způsobem anonymita ovlivňuje interpersonální komunikaci na internetu, začne této znalosti a anonymity strategicky využívat ke svému vlastnímu prospěchu. Podle toho, jak s anonymitou pak uživatel naloží, určuje, zda bude mít pozitivní či negativní implikace.¹⁸²

V rámci on-line komunikace by se tedy obecně dalo předpokládat, že díky anonymitě by si lidé mohli být v on-line prostředí více rovni, protože zde nepůsobí okolní faktory jako sociální status, pohlaví, rasa, vzdělání či zaměstnání. Hodnocení obsahu projevů anonymních uživatelů by tak nebylo těmito faktory polarizováno a měly by tedy být více objektivní. SIDE teorie, ke které se v tomto tématu vědecké kapacity přiklání, ale ukazuje, že je třeba brát v potaz spoustu situačních i psychologických faktorů a proměnných, které mohou chování v on-line komunikaci také značně ovlivnit.

6. 4. 4. NEGATIVNÍ IMPLIKACE ANONYMITY

Negativní dopady anonymity na osobnostní či jiná práva už zde byly čteně krát zmíněny. Tyto negativní implikace anonymity jsou taktéž ekvivalentem všech možných rizik, jímž mohou být uživatelé v on-line prostředí vystaveni (pachatelé kriminálních činností se samozřejmě snaží o absolutní anonymitu). Anonymita může být zneužita k ochraně a provozování kriminálních činností, jako je očerňování, pomluva, hate speech, stalkování, navádění k trestným činům, distribuce dětské pornografie, vyhrožování, rasová agitace, osobní útoky, podvody všeho druhu, zpronevěřování kreditních karet, krádež identity, krádež či obchodování s daty uživatelů, distribuce počítačových virů apod. Anonymita je také využívána k nenávistným či ofenzivním projevům. U těch je ale velmi náročné určit, zda překračují hranici zákona zásahem do osobnostních práv objektu oněch projevů,

¹⁸² CHRISTOPHERSON, Kimberly M. *The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog"*

nebo jsou jen nelibými projevy chráněnými ústavním právem na svobodu projevu. V těchto sporných případech se s dožadováním nápravy musí uživatelé, jež se stali terčem takových projevů, obrátit na soudy.

6. 4. 5. MOŽNÁ PRAVIDLA VYUŽÍVÁNÍ ANONYMITY A JAK S NÍ NAKLÁDAT

Zneužívání anonymity v on-line prostředí je natolik rozšířené, že mnozí volají po jejím celoplošném zákazu. Ten by ale představoval enormní zásah do osobnostních práv uživatelů. Vedlejším důsledkem absence ochrany anonymity by totiž mohla být omezení celospolečenské debaty, kdy by se lidé ze strachu do ní raději vůbec nezapojovali. Navíc by takový krok ani nebyl dostatečně dobře technicky možný. Je otázkou, zda by měli uživatelé mít možnost větší kontroly nad mírou své on-line anonymity a zda její pozitivní implikace převáží ty negativní. I když je tuto problematiku velmi obtížné právně uchopit, a to také z důvodu nespočtu senzitivních případů, určitá míra regulace anonymity je dle mého názoru na místě. Možnost anonymity a všech jejích druhů by měla být zachována, zákon by ale měl vyžadovat, aby bylo možné reálnou identitu pachatelů trestných činů, za dodržení všech zásad ochrany osobních údajů daného serveru, platformy či webové stránky, dohledat. S tím by také souvisela povinnost všech těchto jednotlivých platform a webových stránek zprostředkovávající komunikaci do svých zásad ochrany osobních údajů implementovat klauzule ošetřující, za jakých podmínek si vyhražují rozklíčovat anonymitu uživatele (například s policejním příkazem, příkazem soudu apod.). Provozovatel platformy by samozřejmě takové zásady musel dodržovat a v jiných než vyhrazených případech se anonymity nedotýkat. Uživatelům by ale podle mého názoru mělo být ponecháno právo vystupovat v on-line prostředí anonymně, a to s jakoukoli mírou i způsobem šifrování si sami zvolí. Pokud se uživatel rozhodne komunikovat skrz sérii anonymních serverů, měl by tu možnost mít, avšak každý z těchto serverů by musel mít ošetřené zásady ochrany osobních údajů tak, jak je nastíněno výše, aby bylo skutečnou identitu v nejzazších případech možné odhalit. Druhou možností, která by nevyžadovala povšechné modifikování zásad ochrany osobních údajů, představuje

uzákonění možnosti crackování¹⁸³ ze strany vládou pověřených osob, ale pouze v případě udělení soudního příkazu.¹⁸⁴

Co se odpovědnosti v případě zneužití anonymní komunikace k ilegálním činům týče, veškerou odpovědnost by měl nést pachatel. Žádný druh odpovědnosti by z mého pohledu neměl přecházet na provozovatele platformy, například za šíření nenávistných projevů. Jeho vlastnictví totiž v podstatě bylo také zneužito a využito jako nástroj k trestnému činu. Navíc v případě potřeby může policii poskytnout, podle zásad ochrany osobních údajů, jistá data, která mohou dopomoci k dopadení pachatele.

S ohledem na to, že zákony výslovně kriminální činy nijak specificky nezmiňují, zajisté by bylo vhodné ty nejčastější nelegální aktivity, jako je krádež dat, elektronický vandalismus nebo praní peněz v on-line prostředí, náležitě ošetřit.

Výše uvedené podněty směřují zejména na vládu a provozovatele platform v prostředí internetu. Základním kamenem jsou dle mého názoru dobře informovaní uživatelé s určitým stupněm internetové gramotnosti. Pokud se tedy uživatelé budou sebevzdělávat a aktivně se o tuto tematiku zajímat, bude mnohem méně pravděpodobné, že se stanou obětí některého z kyberzločinů nebo že jim bude zasaženo do jejich osobnostních práv. Na zvyšování internetové gramotnosti a edukaci veřejnosti o hrozbách, které jim v kyberprostoru hrozí, a způsoby, jak se před nimi chránit, se ale velmi efektivně může podílet opět i vláda a provozovatelé on-line komunikačních platform. Neustále se zlepšující stav obecné internetové gramotnosti by pak měl šanci razantně snížit počet případů nezákonných zásahů do osobnostních práv uživatelů.

¹⁸³ odstranění ochranných prvků

¹⁸⁴ JOHNSON, Dan. *Anonymity and the Internet: Anonymous communication is a cyberspace dilemma*

ZÁVĚR

Rozvoj internetu a digitální revoluce přinesly novou dimenzi možností svobodného projevu v kontrastu s érou tradičních médií a spoustu nových výzev pro sociální i politickou sféru světové společnosti. Tato platforma pro realizování svobodného projevu ale vedle rozvoje občanské společnosti i politické angažovanosti zároveň dala autoritářským režimům do ruky mocnou zbraň k šíření svých propagand, potlačování práv svých občanů a možnost jejich efektivní a plošné kontroly. Cenzura kyberprostředí se různí od filtrování dětské pornografie implementovaného ve většině států až po úplné odpojení internetového připojení v Severní Koreji.

Cílem této práce bylo poskytnout komplexní analýzu svobody projevu na internetu, jejího porušování a možností uchování soukromí v kyberprostoru.

I přesto, že na internetu jsou trvale uchovány všechny informace, které do něj kdy byly vloženy, je možné si uchovat, alespoň částečně, kýžené soukromí. Prvním a stěžejním krokem k uchování soukromí je vůbec informace kyberprostoru nesvěřovat, a to jak základní informace v podobě osobních a kontaktních údajů, fotografií apod., ale i informací techničtějšího rázu. K tomu, aby uživatel tento typ dat nezpřístupnil, lze využít celou řadu více či méně komplikovaných anonymizačních nástrojů, které zamezí, aby si internet ona data spojil s daným uživatelem. Na základě ochrany soukromí podle „práva být zapomenut“ z EU lze požádat i o odstranění obsahu, efektivita tohoto způsobu je ovšem diskutabilní a spíše nespolehlivá.

Dynamický a nezastavitelný vývoj technologií s sebou přináší pozitivní i negativní důsledky. Z pozitivních lze zmínit zjednodušení každodenních i těch nejsložitějších úkonů a nepřímo i liberalizaci společnosti, páčání trestných činů jednodušší než kdy dřív a možnost efektivnějšího zasahování do lidských práv a svobod patří mezi ty negativní. V zemích s autoritářskými režimy lze vysledovat tendence a kroky k omezování práv občanů cenzurou internetu, zamezování přístupu k informacím i uvalování trestů za projevování vlastních názorů, jež by mělo být všeobecně chráněným právem. Nejen vlády ale představují pro uživatele riziko. Stejně jako v reálném světě, lze i v tom digitálním páchat trestné činy v podobě krádeží dat, identit, vyhrožování, zpronevřování, krádeží, utlačování minorit, koordinace trestných činů mimo digitální prostředí, kyberšikany

apod. Tyto projevy a aktivity na internetu pak mohou mít reálné důsledky na život uživatelů i mimo digitální prostředí. Existují samozřejmě způsoby, jak se před nimi do jisté míry chránit, uživatelé ale musí oplývat alespoň základní digitální gramotností a uvědomit si hodnotu svého soukromí a bezpečnosti, které často s ochotou vymění za své větší pohodlí, usnadnění a personalizaci.

Vládně uvalenou cenzuru lze ovšem hned několika způsoby obcházet a bojovat za její zrušení, avšak s rizikem odhalení, které by pro uživatele znamenalo tvrdý trest. Způsobem s největší šancí na úspěch je kombinace technologické dimenze v podobě anonymizačních technik či šifrování dat, které minimalizují možnost dohledání uživatele, ale i tlaku na cenu a snahy o maximalizaci nákladů na provozování cenzury na mezinárodní úrovni, s dimenzí politickou (apel na zrušení zákonů legalizující cenzuru) a sociální (odolávání vyvolané atmosféry strachu vedoucí k autocenzuře samotných uživatelů). Jedině tato kombinace pak může mít reálný úspěch na transformování veřejné politiky v dané zemi.

Ani absolutní svoboda na internetu bez jakýchkoli zásahů vlády či provozovatelů ale nemusí představovat ideální řešení. Jak už bylo výše zmíněno, internet je ideálním a efektivním prostorem pro kriminální činnost všeho druhu s relativně nízkou pravděpodobností dohledání pachatele. V případě vážného porušení veřejného pořádku, bezpečnostních hrozeb či z jiných závažných důvodů je na místě možnost projevu v prostředí internetu určitým způsobem omezit, už dle Listiny základních práv a svobod, která omezení v určitých instancích povoluje. Toto omezení lze řešit implementováním jistého druhu cenzury jako je filtrování webových stránek obsahující dětskou pornografii, zneužívání dětí, stránek umožňující nelegální stahování obsahu bez autorského oprávnění apod., ke kterým se v demokratických státech ale spíše než vláda uchylují poskytovatelé internetového připojení. Určitý druh cenzury mohou zavádět i provozovatelé internetových komunikačních platforem, a to skrze pravidla jejich užívání a vyhrazení si práva na odstranění obsahu, který by tato pravidla překračoval. Takovému mazání obsahu však chybí právní základ, a tak je značně diskutabilní, i když odstraňovaný obsah se z pravidla týká nenávislných projevů, podněcování k rasové či jiné diskriminaci, kyberšikany apod.

S přesunem čím dál tím větší části sfér veřejného i soukromého života do on-line prostoru, budou se dle mého názoru i zavedené vládní procesy přesouvat do digitálního prostředí. To nevyhnutelně povede k větší transparentnosti a odpovědnosti vlád za svá konání.

Jak tato práce dokázala, technologizace společnosti a zvyšující se internetová penetrace vede k vyšší informovanosti občanů, vyšší politické angažovanosti i aktivnější občanské společnosti. To je ovšem v přímém rozporu se striktními cenzurními opatřeními autoritářských režimů i jejich ideologií. Jak se takové režimy vypořádávají s technologickým vývojem i zesilujícími pokusy o transformaci veřejné politiky k liberalizaci a zároveň si udrží kontrolu a moc představuje zajímavé téma pro další zkoumání.

ZDROJE

ADAMOVIČ, Karolina. *Politologický slovník*. Praha: C. H. Beck, 2001, 284 s.. ISBN 80-717-9469-4.

ALLPORT, Gordon W. *The Nature Of Prejudice*. USA: Basic Books, 1979, 576 s. ISBN 978-0-201-00179-2.

AUSTIN, John Langshaw. *Jak udělat něco slovy*. Praha: Filosofia, 2000, 172 s. ISBN 80-700-7133-8.

AWAN, Imran. *Cyber-Extremism: Isis and the Power of Social Media*. Society [online]. 2017, 54(2), 138-149 [cit. 2020-05-18]. DOI: 10.1007/s12115-017-0114-0. ISSN 0147-2011. Dostupné z: <http://link.springer.com/10.1007/s12115-017-0114-0>

BALKIN, Jack M. *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*. SSRN Electronic Journal [online]. Routledge, 2004, 2003, 79(1), 437-494 [cit. 2020-05-18]. DOI: 10.2139/ssrn.470842. ISBN 9781315089645. ISSN 1556-5068. Dostupné z: <http://www.ssrn.com/abstract=470842>

BARTH, Susanne a Menno D. T DE JONG. *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*. Telematics and Informatics [online]. 2017, 34(7), 1038-1058 [cit. 2020-05-18]. DOI: 10.1016/j.tele.2017.04.013. ISSN 07365853. Dostupné z: <https://linkinghub.elsevier.com/retrieve/pii/S0736585317302022>

BARTH, Susanne a Menno D. T. DE JONG. *Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources*. Telematics and Informatics [online]. 2019, (41), 55-69 [cit. 2020-05-18]. DOI: 10.1016/j.tele.2019.03.003. ISSN 07365853. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0736585317307724>

BARTOŇ, Michal. *Svoboda projevu: principy, garance, meze*. Praha: Leges, 2010, 384 s. ISBN 978-80-87212-42-4.

BBC News. *Bahrain blocks opposition websites*. BBC News [online]. 2002 [cit. 2020-05-18]. Dostupné z: http://news.bbc.co.uk/2/hi/middle_east/1895005.stm

BERGSTRÖM, Annika. *Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses*. Computers in Human Behavior [online]. 2015, 53(7), 419-426 [cit. 2020-05-18]. DOI: 10.1016/j.chb.2015.07.025. ISSN 07475632. Dostupné z: <https://linkinghub.elsevier.com/retrieve/pii/S0747563215300364>

BI, Jianhai. *The Internet Revolution in China: The Significance for Traditional Forms of Communist Control*. International Journal [online]. 2001, 56(3), 421-441 [cit. 2020-05-18]. DOI: 10.2307/40203576. ISSN 00207020. Dostupné z: <http://www.jstor.org/stable/10.2307/40203576?origin=crossref>

BOŘÁNEK, Roman. *Piráteční pomocí torrentů už tolik nefrčí, ve velkém se sdílí i přes Google Drive*. Root.cz [online]. 2017 [cit. 2020-05-18]. Dostupné z: <https://www.root.cz/clanky/pirateni-pomoci-torrentu-uz-tolik-nefrci-ve-velkem-se-sdili-i-pres-google-drive/>

CAMBIÉ, Silvia. *Lessons from the front line: The Arab Spring demonstrated the power of people—and social media*. Communication World [online]. 2012, 28-32 [cit. 2020-05-18]. ISSN 0744-7612. Dostupné z: http://www.silviacambie.com/wp-content/uploads/2011/03/CW_JF12_Lessons-from-Front-Line.pdf

ČESKO. § 1, §2 zákona č. 89/2012 Sb., občanský zákoník. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2020 [cit. 18. 5. 2020]. Dostupné z: <https://www.zakonypro-lidi.cz/cs/2012-89#1>

ČESKO. § 81 zákona č. 89/2012 Sb., občanský zákoník. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2020 [cit. 18. 5. 2020]. Dostupné z: <https://www.zakonypro-lidi.cz/cs/2012-89#p81>

ČESKO. *Ústavní zákon č. 2/1993 Sb.: Listina základních práv a svobod* [online]. 1992 [cit. 2020-05-18]. Dostupné z: <https://www.psp.cz/docs/laws/listina.html>

ČESKO. *Zákon č. 106/1999 Sb., o svobodném přístupu k informacím*. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2020 [cit. 18. 5. 2020]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106#f1945936>

CHRISTOPHERSON, Kimberly M. *The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog"*. *Computers in Human Behavior* [online]. 2007, 23(6), 3038-3056 [cit. 2020-05-18]. DOI: 10.1016/j.chb.2006.09.001. ISSN 07475632. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0747563206001221>

DEVITO, Joseph A. *Základy mezilidské komunikace*. Praha: Grada, 2008, 512 s. Expert (Grada). ISBN 978-80-247-2018-0.

DOČEKAL, Daniel. Noemi Maixner a ti druzí. *Odkud se berou falešné účty, které milují politiky?*. Lupa.cz: Server o českém internetu [online]. 2017 [cit. 2020-05-18]. Dostupné z: <https://www.lupa.cz/clanky/noemi-maixner-a-ti-druzi-odkud-se-berou-falesne-ucty-ktere-miluji-politiky/>

DOLEŽÍLEK, Jiří. *Právo na odpověď a na dodatečné sdělení podle nového tiskového zákona*. *Právní rozhledy: časopis pro všechna právní odvětví*. Praha: C. H. Beck, 2000, (10), s. 430. ISSN 1210-6410 1210-6410. Dostupné z: <https://www.beck-online.cz/bo/document-view.seam?documentId=nrptembqgbpxa4s7geyf6427gqzta&groupIndex=6&rowIndex=0>

DUBROVSKY, Vitaly a kol. *The Equalization Phenomenon: Status Effects in Computer-Mediated and Face-to-Face Decision-Making Groups*. *Human-Computer Interaction* [online]. 1991, 6(2), 119-146 [cit. 2020-05-18]. DOI: 10.1207/s15327051hci0602_2. ISSN 0737-0024. Dostupné z: https://www.researchgate.net/publication/242544877_The_Equalization_Phenomenon_Status_Effects_in_Computer-Mediated_and_Face-to-Face_Decision-Making_Groups

ELY, John Hart. *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*. Harvard Law Review [online]. 1975, 88(7), 1482-1508 [cit. 2020-05-18]. DOI: 10.2307/1340121. ISSN 0017811X. Dostupné z:

<https://www.jstor.org/stable/1340121?origin=crossref>

ERIKSSON, Johan a Giampiero GIACOMELLO. *Who Controls the Internet? Beyond the Obstinance or Obsolescence of the State*. International Studies Review [online]. 2009, 11(1), 205-230 [cit. 2020-05-18]. DOI: 10.1111/j.1468-2486.2008.01841.x. ISSN 15219488. Dostupné z: <https://www.jstor.org/stable/25482060?seq=1>

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. *GDPR (obecné nařízení): 8. Zabezpečení osobních údajů*. Úřad pro ochranu osobních údajů [online]. 2019 [cit. 2020-05-18]. Dostupné z: <https://www.uouu.cz/8-zabezpeceni-osobnich-udaju/d-27282/p1=3938>

EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA. *Evropská úmluva o ochraně lidských práv* [online]. 2010 [cit. 2020-05-18]. Dostupné z: https://www.echr.coe.int/Documents/Convention_CES.pdf

FARBER, Daniel. *The First Amendment*. New York: Foundation Press, 2014, 301 s. ISBN 978-1599417516.

FREEDOM HOUSE. *Explore the Map*. Freedom House [online]. [cit. 2020-05-21]. Dostupné z: <https://freedomhouse.org/explore-the-map?type=fw&year=2020>

FREEDOM HOUSE. *Freedom on the Net: An annual study of internet freedom around the world*. Freedom House [online]. [cit. 2020-05-21]. Dostupné z: <https://freedomhouse.org/report/freedom-net>

FREEDOM HOUSE. *Freedom on the net: China*. Freedom House [online]. 2019 [cit. 2020-05-18]. Dostupné z: https://freedomhouse.org/country/china/freedom-net/2019#footnote7_jcez5mj

FREEDOM HOUSE. *Our Issues*. Freedom House [online]. [cit. 2020-05-18]. Dostupné z: <https://freedomhouse.org/issues>

GOOGLE. *Odstranění obsahu na základě ochrany soukromí uživatelů z EU: Formulář žádosti o odstranění osobních údajů*. Google [online]. [cit. 2020-05-21]. Dostupné z: https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637256126945117129-1865430493&hl=cs&rd=1

GORMAN, Siobhan. *Web Access Is New Clinton Doctrine*. The Wall Street Journal [online]. 2010 [cit. 2020-05-18]. Dostupné z: http://online.wsj.com/article/SB10001424052748703405704575015461404882830.html?mod=rss_Politics_And_Policy

GREENAWALT, Kent. *Fighting Words: Individuals, Communities, and Liberties of Speech*. Princeton, New Jersey: Princeton University Press, 1996, 206 s. ISBN 9781400821679.

HATFIELD, Elaine a Susan SPRECHER. *Mirror, Mirror: The Importance of Looks in Everyday Life*. New York: State University of New York Press, 1986. ISBN 9781438406077.

HELFT, Miguel a David BARBOZA. *Google Shuts China Site in Dispute Over Censorship*. The New York Times [online]. San Francisco, 2010, 2010 [cit. 2020-05-18]. Dostupné z: <https://www.nytimes.com/2010/03/23/technology/23google.html>

HERCZEG, Jiří. *Meze svobody projevu*. Praha: Orac, 2004, 143. ISBN 80-861-9994-0.

HONZÁK, Radkin. *Stanfordský experiment: Když člověk získá moc nad druhými, může se změnit k nepoznání*. [online]. [cit. 2020-05-18]. Dostupné z: <https://psychologie.cz/stanfordsky-experiment/>

HOUSKA, Ondřej. *Poskytovatelé internetu nemusí blokovat stránky s nelegálním obsahem automaticky, jen na příkaz soudu*. iRozhlas [online]. 2013 [cit. 2020-05-18]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/poskytovatele-internetu-nemusi-blokovat-stranky-s-nelegalnim-obsahem-automatically-jen-na-prikaz-soudu_201311261234_mkopp

HUANG, Carol. *Facebook and Twitter key to Arab Spring uprisings: report*. The National: UAE [online]. 2011 [cit. 2020-05-18]. Dostupné z: <https://www.thenational.ae/uae/facebook-and-twitter-key-to-arab-spring-uprisings-report-1.428773>

JÄGER, Petr a Pavel MOLEK. *Svoboda projevu: Demokracie, rovnost a svoboda slova*. Praha: Auditorium, 2007, 195 s. ISBN 978-80-903786-5-0.

JELÍNEK, Jiří a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*. Praha: Leges, 2009, 1312 s. ISBN 978-80-7502-230-1.

JOHNSON, Dan. *Anonymity and the Internet: Anonymous communication is a cyberspace dilemma*. The Futurist [online]. 2000, s. 12 [cit. 2020-05-18]. ISSN 00163317. Dostupné z: <https://search.proquest.com/open-view/967e643810ece5c39d141e746dc5bb7c/1?pq-origsite=gscholar&cbl=47758>

JOHNSON, Adam N. *Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity*. European Journal of Social Psychology [online]. 2001, 31(2), 177-192 [cit. 2020-05-18]. DOI: 10.1002/ejsp.36. ISSN 0046-2772. Dostupné z: <http://doi.wiley.com/10.1002/ejsp.36>

KALATHIL, Shanthi a Taylor C. BOAS. *Open Networks Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington: Carnegie Endowment for International Peace, 2003, 217 s. ISBN 0-87003-194-5. Dostupné také z: <http://www.asu.edu/courses/pos445/Open%20Networks%20Closed%20Regimes.pdf>

KANG, Ruogu a kol. *Why do people seek anonymity on the internet?*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13 [online]. 2013, 2657-2666 [cit. 2020-05-18]. DOI: 10.1145/2470654.2481368. ISBN 9781450318990. Dostupné z: <http://dl.acm.org/citation.cfm?doid=2470654.2481368>

KATYAL, Neal Kumar. *Criminal Law in Cyberspace*. University of Pennsylvania Law Review [online]. 2001, 149(4), 1003-1114 [cit. 2020-05-18]. DOI: 10.2307/3312990. ISSN 00419907. Dostupné z: <https://www.jstor.org/stable/3312990?origin=crossref>

KOKOLAKIS, Spyros. *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon* [online]. 2017, (64), 122-134 [cit. 2020-05-18]. DOI: 10.1016/j.cose.2015.07.002. ISSN 01674048. Dostupné z: <https://linkinghub.elsevier.com/retrieve/pii/S0167404815001017>

LAKE, Eli. *Hacking the Regime*. The New Republic [online]. 2009 [cit. 2020-05-18]. Dostupné z: <https://newrepublic.com/article/68899/hacking-the-regime>

LEBERKNIGHT, Christopher S. a kol. *A Taxonomy of Internet Censorship and Anti-Censorship* [online]. 2010, 28 s. [cit. 2020-05-18]. Dostupné z: https://www.researchgate.net/publication/228451403_A_Taxonomy_of_Internet_Censorship_and_Anti-Censorship

LOCKHEED, Marlaine E. a Katherine Patterson HALL. *Conceptualizing Sex as a Status Characteristic: Applications to Leadership Training Strategies*. Journal of Social Issues [online]. 1976, 32(3), 111-124 [cit. 2020-05-18]. DOI: 10.1111/j.1540-4560.1976.tb02600.x. ISSN 00224537. Dostupné z: https://www.researchgate.net/publication/227791919_Conceptualizing_Sex_as_a_Status_Characteristic_Applications_to_Leadership_Training_Strategies

MACICH, Jiří. *Telefónica O2 potvrdila filtrování stránek*. Lupa.cz: Server o českém internetu [online]. 2009 [cit. 2020-05-18]. Dostupné z: <https://www.lupa.cz/clanky/telefonica-o2-potvrdila-filtrovani-stranek/>

MACKINNON, Rebecca. *China's Censorship 2.0: How companies censor bloggers*. First Monday [online]. 2009, 14(2) [cit. 2020-05-18]. DOI: 10.5210/fm.v14i2.2378. ISSN 13960466. Dostupné z: https://www.researchgate.net/publication/220168223_China%27s_Censorship_20_How_Companies_Censor_Bloggers

MARSOOF, A. *Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression*. International Journal of Law and Information Technology [online]. 2011, 2011, 19(2), 110-132 [cit. 2020-05-18]. DOI: 10.1093/ijlit/eaq018. ISSN 0967-0769. Dostupné z: <https://academic.oup.com/ijlit/article-lookup/doi/10.1093/ijlit/eaq018>

MARX, Gary T. *What's in a Name? Some Reflections on the Sociology of Anonymity*. The Information Society [online]. 1999, 15(2), 99-112 [cit. 2020-05-18]. DOI: 10.1080/019722499128565. ISSN 0197-2243. Dostupné z: <http://www.tandfonline.com/doi/abs/10.1080/019722499128565>

MATUŠŮ, Hana. *Ochrana osobnosti versus svoboda projevu na internetu* [online]. Olomouc, 2016, 56 s. [cit. 2020-05-18]. Dostupné z: <https://theses.cz/id/meenqj>. Diplomová práce. Univerzita Palackého v Olomouci. Vedoucí práce Michal Bartoň.

MORAVEC, Ondřej. *Mediální právo v informační společnosti*. Praha: Leges, 2013, 288 s. ISBN 978-80-87576-52-6.

NYST, Carly. *El derecho a la privacidad y a la libertad de expresión: dos caras de la misma moneda: (Two sides of the same coin – the right to privacy and freedom of expression)*. Cuestión de Derechos: Revisita electrónica [online]. Buenos Aires, Argentina: ADC - Asociación pod los Derechos Civiles, 2013, 2013, (4.), 24-32 [cit. 2020-05-18]. ISSN 1853-6565. Dostupné z: <https://www.apc.org/sites/default/files/ADC%20-%20Cuestion%20de%20derechos%20-%20Revista-numero4%20-%202013.pdf>

OPENNET INITIATIVE. *About Filtering*. Open Net Initiative (ONI) [online]. [cit. 2020-05-18]. Dostupné z: <https://opennet.net/about-filtering>

OPENNET INITIATIVE. *About ONI*. Open Net Initiative (ONI) [online]. [cit. 2020-05-18]. Dostupné z: <https://opennet.net/about-oni>

OPENNET INITIATIVE. *Syrian Electronic Army: Disruptive Attacks and Hyped Targets*. Open Net Initiative (ONI) [online]. [cit. 2020-05-18]. Dostupné z: <https://opennet.net/syrian-electronic-army-disruptive-attacks-and-hyped-targets>

OSN. *Všeobecná deklarace lidských práv*. [online]. New York, 1948 [cit. 2020-5-18]. Dostupné z: https://www.osn.cz/wp-content/uploads/2015/12/UDHR_2015_11x11_CZ2.pdf

OUR WORLD IN DATA. *Internet: Internet access: Our World in Data* [online]. [cit. 2020-05-21]. Dostupné z: <https://ourworldindata.org/internet#internet-access>

OYEZ. *West Virginia State Board of Education v. Barnette*. OYEZ [online]. 1943 [cit. 2020-05-18]. Dostupné z: <https://www.oyez.org/cases/1940-1955/319us624>

PAVLÍČEK, Václav. *Ústava a ústavní řád České republiky: komentář*. Praha: Linde, 2002, 1164 s. ISBN 80-720-1391-2.

PETERKA, Jiří. *Stalo se: Vodafone přehodnotil své blokování Internetu. Lupa.cz: Server o českém internetu* [online]. 2008 [cit. 2020-05-18]. Dostupné z:

<https://www.lupa.cz/clanky/stalo-se-vodafone-prehodnotil-sve-blokovani/>

POST, Robert C. *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine v. Falwell*. Harvard Law Review [online]. 1990, 103(3), 601-686 [cit. 2020-05-18]. DOI: 10.2307/1341344. ISSN 0017811X. Dostupné z: <https://www.jstor.org/stable/1341344?seq=1>

POSTMES, Tom a Russell SPEARS. *Deindividuation and antinormative behavior: A meta-analysis*. Psychological Bulletin [online]. 1998, 123(3), 238–259 [cit. 2020-05-18]. DOI: 10.1037/0033-2909.123.3.238. ISSN 1939-1455. Dostupné z:

<http://doi.apa.org/getdoi.cfm?doi=10.1037/0033-2909.123.3.238>

POUPEROVÁ, Olga. *Regulace médií*. Praha: Leges, 2010, 272 s. ISBN 978-80-87212-48-6.

REPORTERS SANS FRONTIÈRES. *Journalists confined to their hotels, Internet disconnected*. Reporters sans frontières (RSF) [online]. 2016 [cit. 2020-05-18]. Dostupné z: <https://rsf.org/en/news/journalists-confined-their-hotels-internet-disconnected>

REPORTERS SANS FRONTIÈRES. *Our activities*. Reporters sans frontières (RSF) [online]. [cit. 2020-05-18]. Dostupné z: <https://rsf.org/en/our-activities>

REPORTERS SANS FRONTIÈRES. *RSF Report: "China's Pursuit of a New World Media Order"*. Reporters sans frontières (RSF) [online]. 2019 [cit. 2020-05-18]. Dostupné z: <https://rsf.org/en/reports/rsf-report-chinas-pursuit-new-world-media-order>

REUTERS INSTITUTE. *Digital News Report 2017* [online]. Reuters Institute for the Study of Journalism, 2017 [cit. 2020-05-21]. Dostupné z: <http://www.digitalnewsreport.org/survey/2017/>

REUTERS INSTITUTE. *Digital News Report 2019* [online]. Reuters Institute for the Study of Journalism, 2019 [cit. 2020-05-21]. Dostupné z: <http://www.digitalnewsreport.org>

ŘEHOŘ, Petr. *Manažerská komunikace*. České Budějovice: Jihočeská univerzita v Českých Budějovicích, Ekonomická fakulta, 2012, 205 s. ISBN 978-80-7394-394-3.

SCHMITT, Michael N. a Louise ARIMATSU. *Yearbook of International Humanitarian Law: Volume 14, 2011*. Nizozemsko: Springer Science & Business Media, 2012, 506 s. ISBN 978-90-6704-855-2.

SHISHKINA, Alisa a Leonid ISSAEV. *Internet Censorship in Arab Countries: Religious and Moral Aspects. Religions* [online]. 2018, 9(11) [cit. 2020-05-18]. DOI: 10.3390/rel9110358. ISSN 2077-1444. Dostupné z: <http://www.mdpi.com/2077-1444/9/11/358>

SINGH, Manish. *With Torrent Sites Facing the Heat, Pirates Get Creative With Google Drive and Other Services*. Gadgets 360 [online]. 2017 [cit. 2020-05-18]. Dostupné z: <https://gadgets.ndtv.com/internet/features/creative-ways-pirates-use-google-drive-google-maps-to-torrent-movies-1745774>

SMÍLEK, Ondřej. *Svoboda projevu a její meze* [online]. 2014, 68 s. [cit. 2020-05-18]. Dostupné z: <https://is.cuni.cz/webapps/zzp/detail/103740/>. Diplomová práce. Univerzita Karlova. Vedoucí práce Radovan Suchánek.

SPEARS, Russell a kol. *Computer-Mediated Communication as a Channel for Social Resistance*. Small Group Research [online]. 2002, 33(5), 555-574 [cit. 2020-05-18]. DOI: 10.1177/104649602237170. ISSN 1046-4964. Dostupné z: <https://pdfs.semanticscholar.org/9cc4/aafc7b1494a3d8bf45f2b4a626fced38c1a9.pdf>

STEVENSON, Christopher. *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*. Boston College International and Comparative Law Review [online]. 2007, 30(2), 531-558 [cit. 2020-05-18]. Dostupné z: <https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1074&context=iclr>

STONE, Geoffrey R. *Content-Neutral Restrictions*. The University of Chicago Law Review [online]. 1987, 54(1), 46-118 [cit. 2020-05-18]. ISSN 0041-9494. Dostupné z: <https://chicagounbound.uchicago.edu/uclrev/vol54/iss1/2/>

ŠVEC, Michal. *Tzv. „právo být zapomenut“ a jeho uplatnění v praxi*. epravo.cz [online]. 2015 [cit. 2020-05-18]. Dostupné z: <https://www.epravo.cz/top/clanky/tzv-pravo-byt-zapomenut-a-jeho-uplatneni-v-praxi-98087.html>

T-MOBILE CZECH REPUBLIC. *T-Mobile pomáhá v boji proti zneužívání dětí blokováním nelegálního obsahu*. T-Mobile: Tiskové centrum [online]. 2010 [cit. 2020-05-18]. Dostupné z: <http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-pomaha-v-boji-proti-zneuzivani-deti-blokovanim-nelegalniho-obsahu.html>

TOKOŠOVÁ, Kamila. *Právo na zapomnění* [online]. Brno, 2016, 89 s. [cit. 2020-05-18]. Dostupné z: https://is.muni.cz/th/mgcnj/Tokosova_DP.pdf. Diplomová práce. Masarykova univerzita. Vedoucí práce Radim Polčák.

UNITED NATIONS. *International Covenant on Civil and Political Rights. United Nations Treaty Collection* [online]. 1966 [cit. 2020-05-18]. Dostupné z: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en

VAN DER SAR, Ernesto. *BitTorrent Still Dominates Global Internet*. TorrentFreak [online]. 2010 [cit. 2020-05-18]. Dostupné z: <https://torrentfreak.com/bittorrent-still-dominates-global-internet-traffic-101026/>

VILLENEUVE, Nart. *The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace*. First Monday [online]. 2006, 11(1) [cit. 2020-05-18]. DOI: 10.5210/fm.v11i1.1307. ISSN 13960466. Dostupné z:

https://www.researchgate.net/publication/220167505_The_filtering_matrix_Integrated_mechanisms_of_information_control_and_the_demarcation_of_borders_in_cyber-space

VOLOKH, Eugene. *The First Amendment and Related Statutes: Problems, Cases and Policy*. New York: Foundation Press, 2016, 1141 s. ISBN 978-1634605106.

WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer Česká republika, 2012. ISBN 978-80-7357-750-6.

WARF, Barney. *Geographies of global Internet censorship*. GeoJournal [online]. 2011, 76(1), 1-23 [cit. 2020-05-18]. DOI: 10.1007/s10708-010-9393-3. ISSN 0343-2521. Dostupné z: <http://link.springer.com/10.1007/s10708-010-9393-3>

WEBOPEDIA. *What is persistent cookie?*. Webopedia [online]. [cit. 2020-05-18]. Dostupné z: https://www.webopedia.com/TERM/P/persistent_cookie.html

WEINSTEIN, James. *Hate Speech, Pornography, And Radical Attacks On Free Speech Doctrine*. Colorado: Westview Press, 1999, 300 s. ISBN 978-0813327099.

ZIMBARDO, Philip G. *The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos*. In: Nebraska symposium on motivation. University of Nebraska press, 1969.

SEZNAM GRAFŮ

Graf č. 1: On-line média jako zdroj informací	35
Graf č. 2: Poměr ceny a přesnosti nástrojů internetové cenzury	49

SEZNAM OBRÁZKŮ

Obrázek č. 1: Mapa internetové penetrace ve světě.....	42
Obrázek č. 2: Geografické znázornění on-line cenzury ve vybraných zemích	43
Obrázek č. 3: Proměna skóre svobody projevu ve vybraných zemích mezi roky 2018 a 2019	44


SEZNAM PŘÍLOH

Příloha č. 1: Formulář žádosti společnosti Google o odstranění osobních údajů podle „práva být zapomenut“	88
Příloha č. 2: Skóre jednotlivých zemí ve výzkumu svobody projevu na internetu.....	91
Příloha č. 3: Druhy opatření a omezení svobody projevu ve vybraných zemích mezi roky 2018 a 2019	93

PŘÍLOHY

Příloha č. 1: Formulář žádosti společnosti Google o odstranění osobních údajů podle „práva být zapomenut“

Zdroj: GOOGLE. Odstranění obsahu na základě ochrany soukromí uživatelů z EU

☰Přihlásit se

Odstranění obsahu na základě ochrany soukromí uživatelů z EU

Nápověda ▾

Formulář žádosti o odstranění osobních údajů

Z důvodu ochrany soukromí můžete mít právo požádat o odstranění některých osobních údajů, které s vámi souvisejí.

Tento formulář je určen k odeslání žádosti o odstranění konkrétních výsledků Vyhledávání Google pro dotazy, které zahrnují vaše jméno. Chcete-li požádat o odstranění osobních údajů z jiné služby Google, odešlete žádost prostřednictvím formuláře dané služby, který naleznete na naší stránce [Odebrání obsahu z Googlu](#).

Chcete-li například požádat o odstranění osobních údajů z Bloggeru, odešlete žádost pomocí odpovídajícího formuláře služby Blogger.

Po odeslání žádosti se pokusíme vyvážit práva na soukromí jednotlivce se zájmem veřejnosti na přístup k informacím a s právy ostatních na distribuci informací. Můžeme například odmítnout odstranit některé informace o finančních podvodech, profesním pochybení, odsouzení za trestný čin nebo veřejném působení úředních osob.

K vyplnění tohoto formuláře budete potřebovat digitální kopii dokladu totožnosti. Pokud tuto žádost odesíláte jménem někoho jiného, budete muset dodat jejich doklad totožnosti.

* Povinné pole

VAŠE ÚDAJE

Země původu *

Zvolte zemi/oblast ▾

Jméno a příjmení *

Vaše vlastní jméno (i v případě, že žádost podáváte za někoho jiného, koho jste oprávněni zastupovat). Pokud někoho zastupujete, musíte mít oprávnění jednat jeho nebo jejím jménem.

Jméno:

Příjmení:

Kontaktní e-mailová adresa *

Jednám za... *

Pokud tuto žádost odesíláte za někoho jiného, uveďte svůj vztah k dané osobě (například „rodič“ nebo „zástupce“). Můžeme požádat o dokumentaci, která potvrdí, že jste oprávněni tuto osobu zastupovat.

- sebe
- klienta
- člena rodiny
- kamaráda
- Jiné

Váš právní vztah k osobě, jejímž jménem žádost odesíláte *

Podali jste nějakou žádost již dříve?

Pokud jste vy (nebo příslušná osoba) již požádali o odstranění adres URL s podobným obsahem, pomůžeme vám rychleji, když namísto odeslání nového oznámení odpovíte na e-mail, který jsme vám (nebo příslušné osobě) zaslali.

Chcete-li nám raději poslat nové oznámení, zadejte 14místné referenční číslo z předchozí žádosti. Bude mít přibližně takovýto formát: 1-111100001111. Naleznete jej v předmětu e-mailu, který jsme odeslali v reakci na předchozí žádost.

UVĚDTE, KTERÉ OSOBNÍ ÚDAJE CHCETE ODSTRANIT A KDE SE NACHÁZEJÍ

Pokud se toto oznámení týká několika důvodů porušení práv, níže odešlete pouze první z nich. Poté pod textovými poli klikněte na odkaz Přidat novou skupinu a přidejte další důvod.

Adresy URL obsahu s osobními údaji, který chcete odstranit *

Pomoc s vyhledáním adresy URL získáte kliknutím [sem](#).

Zadejte prosím jednu adresu URL na řádek. (Maximální počet řádků: 1000)

Důvod odstranění *

Pro každou adresu URL, kterou jste zadali, vysvětlíte:

- (1) jak se osobní údaje uvedené výše týkají osoby, jejímž jménem žádost podáváte, a
- (2) proč se domníváte, že by osobní údaje měly být odstraněny.

Příklad: „(1) Tato stránka se mě týká, protože A, B a C. (2) Tato stránka by měla být odstraněna, protože X, Y a Z.“

[Přidat novou skupinu](#) (Maximální počet skupin: 10)

Jméno použité ve vyhledávání *

Mělo by se jednat o jméno, jehož vyhledáním se zobrazí výsledky, které chcete odstranit. Chcete-li odeslat několik jmen (pokud se například vaše příjmení za svobodna liší od vašeho současného příjmení), vložte mezi jednotlivá jména lomítko („/“). Příklad: „Jana Černá / Jana Nováková“.

ČESTNÁ PROHLÁŠENÍ

Přečtěte si následující prohlášení a zaškrtnutím políček potvrďte, že s nimi souhlasíte.

- Souhlasím se zpracováním odeslaných osobních údajů v souladu s popisem níže: *

Osobní údaje, které uvedete v tomto formuláři (včetně e-mailové adresy a všech identifikačních údajů), a osobní údaje, které odešlete v další korespondenci, použije společnost Google LLC ke zpracování žádosti a splnění svých zákonných povinností. Podrobnosti o žádosti můžeme sdílet s úřady pro ochranu osobních údajů, avšak pouze v případě, že je potřebují k prošetření nebo kontrole našeho rozhodnutí. Většinou se jedná o případy, kdy se kvůli našemu rozhodnutí obrátíte na místní úřad pro ochranu osobních údajů. Pokud adresy URL z výsledků Vyhledávání v reakci na vaši žádost odstraníme, můžeme o nich sdílet podrobnosti příslušným webmasterům.

Upozorňujeme, že pokud jste přihlášení k účtu Google, můžeme váš příspěvek přidružit k danému účtu.

Prohlašuji, že informace v této žádosti jsou přesné a že jsem oprávněn(a) tuto žádost odeslat. *

Beru na vědomí, že pokud formulář nebude vyplněn správně nebo žádost bude neúplná, společnost Google ji nebude moci zpracovat. *

PODPIS

Stvrzeno podpisem dne: *

MM/DD/YYYY (např. "12/19/2010")

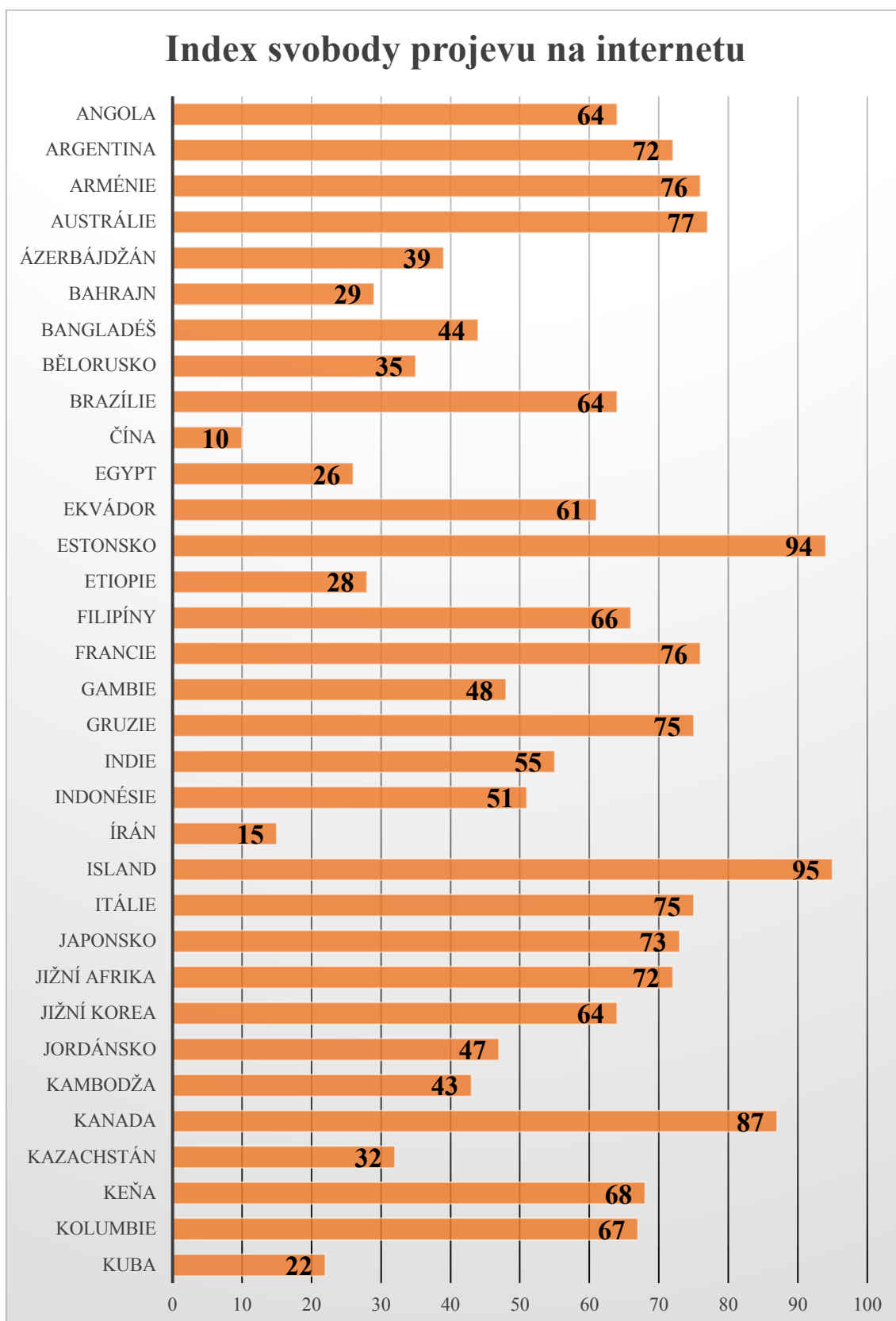
Podpis: *

Příklad: Jan Novák

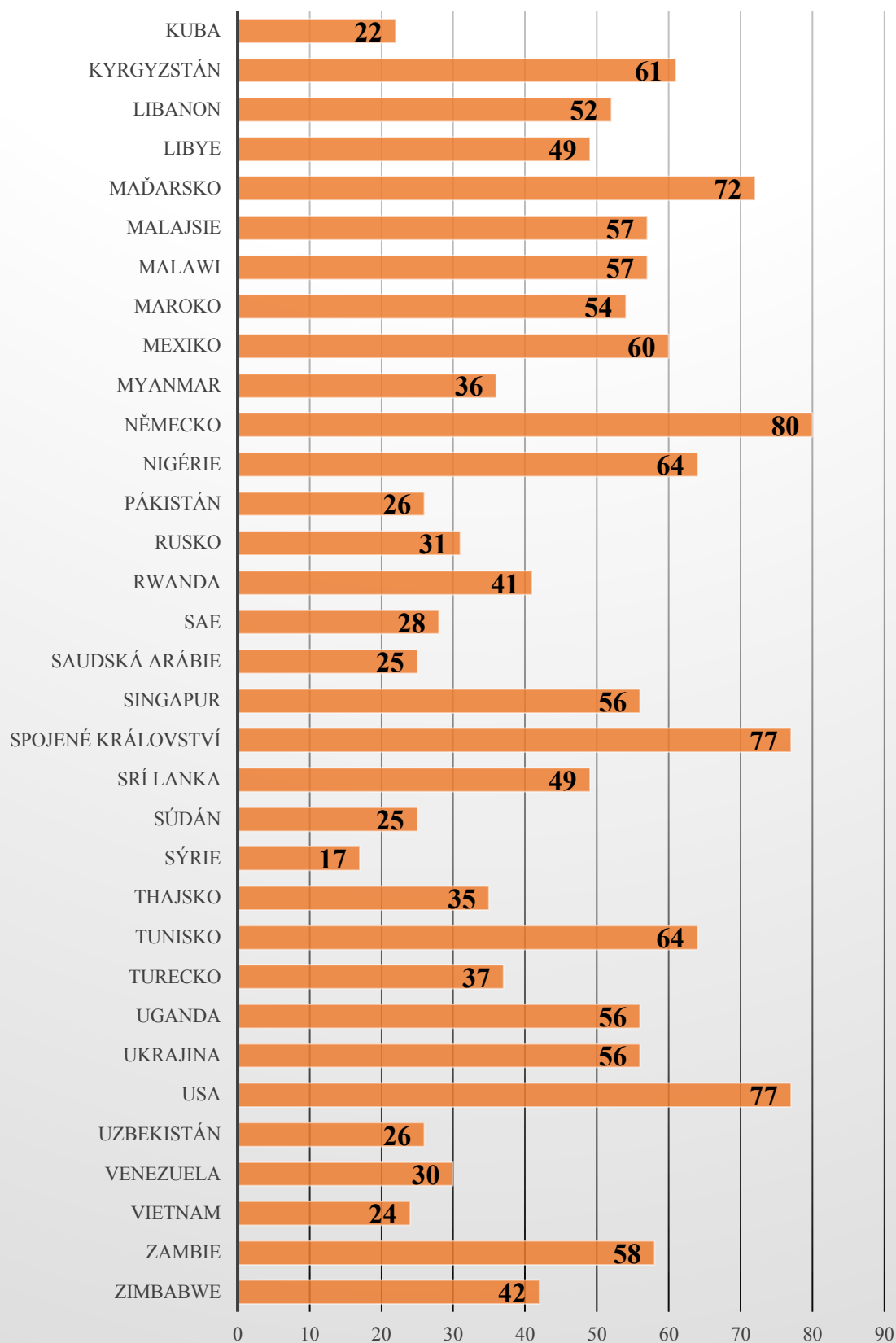
Zadáním celého jména výše nám poskytujete svůj digitální podpis, který vás právně zavazuje stejně jako podpis fyzický. Aby nahlášení proběhlo úspěšně, musí váš podpis přesně odpovídat křestnímu jménu a příjmení zadaným v horní části tohoto formuláře.

Příloha č. 2: Skóre jednotlivých zemí ve výzkumu svobody projevu na internetu

Zdroj: Vlastní zpracování podle dat výzkumu Freedom on the Net organizace Freedom House



Index svobody projevu na internetu



Jordánsko	omezena										4
Kambodža	omezena										4
Kanada	bez omezení										0
Kazachstán	striktně omezena										8
Keňa	omezena										2
Kolumbie	omezena										2
Kuba	striktně omezena										6
Kyrgyzstán	omezena										5
Libanon	omezena										3
Libye	omezena										3
Maďarsko	bez omezení										1
Malajsie	omezena										3
Malawi	omezena										3
Maroko	omezena										3
Mexiko	omezena										3
Myanmar	striktně omezena			*							5
Německo	bez omezení										1
Nigérie	omezena										4
Pákistán	striktně omezena								*		6
Rusko	striktně omezena										9
Rwanda	omezena										5
SAE	striktně omezena										7
Saudská Arábie	striktně omezena										6
Singapur	omezena										3
Spojené Království	bez omezení										2
Srí Lanka	omezena										5
Súdán	striktně omezena										6
Sýrie	striktně omezena										6
Thajsko	striktně omezena										6
Tunisko	omezena										2
Turecko	striktně omezena										4
Uganda	omezena										1
Ukrajina	omezena										6
USA	bez omezení										2
Uzbekistán	striktně omezena										7
Venezuela	striktně omezena										6
Vietnam	striktně omezena										7
Zambie	omezena										2
Zimbabwe	omezena										5
	TOTAL (červen 2018 - květen 2019)	20	34	17	38	16	15	47	31	32	
	TOTAL	20	34	18	38	17	15	47	32	32	

Institut komunikačních studií a žurnalistiky FSV UK
Teze BAKALÁŘSKÉ diplomové práce

TUTO ČÁST VYPLŇUJE STUDENT/KA:

Příjmení a jméno diplomantky/diplomanta:
Brišová Jana

Razítko podatelny:

Imatrikulační ročník diplomantky/diplomanta:
2016

E-mail diplomantky/diplomanta:
91349371@fsv.cuni.cz

Studijní obor/forma studia:
Žurnalistika

Předpokládaný název práce v češtině:

Svoboda projevu na internetu a cenzura jako prostředek k ochraně soukromí uživatelů

Předpokládaný název práce v angličtině:

Free speech on the Internet and censorship as a way to protect users' privacy

Předpokládaný termín dokončení (semestr, akademický rok – vzor: ZS 2012/2013):

(diplomovou práci je možné odevzdat nejdříve po dvou semestrech od schválení tezí)

LS 2018/2019

Základní charakteristika tématu a předpokládaný cíl práce (max. 1000 znaků):

Práce má za cíl popsat problematiku svobody projevu na internetu a prozkoumat s ní spojené narušování soukromí a zmapovat možnosti ochrany uživatelů. Dále rozebírá cenzuru a omezování svobody projevu jako prostředek k ochraně soukromí na internetu. Práce se také zkoumá pozitivní i negativní faktory anonymity na internetu jako nástroje k zajištění naprosté svobody v digitálním světě.

Předpokládaná struktura práce (rozdělení do jednotlivých kapitol a podkapitol se stručnou charakteristikou jejich obsahu):

Svoboda projevu na internetu

- Právní úprava v ČR
- Konflikt svobody projevu a práva na soukromí
- Ochrana osobnosti
- Právní úprava ochrany osobnosti a práva na soukromí
- Zveřejňování informací na internetu a možné hrozby pro uživatele
- Privacy paradox
- Ochrana osobnosti na internetu
- Možnosti omezení svobody projevu
- Ochrana osobních údajů
- Jak se mohou uživatelé chránit
- Porovnání se svobodou tisku

Cenzura na internetu

- Nejčastější důvody k zavedení cenzury
- Prostředky, metody a formy cenzury na internetu
- Jak se cenzura dá obcházet
- Cenzura na jednotlivých sociálních sítích
- Aktuální situace cenzury a možný budoucí vývoj

Anonymita

- Nástroj pro absolutní svobodu projevu
- Prostředek k nezákonné či neetické činnosti

Vymezení zpracovávaného materiálu (např. konkrétní titul periodika a období jeho analýzy):

Tato práce analyzuje vědecké články a legislativní vymezení zabývající se právem na svobodu projevu v digitální sféře, právem na vlastní soukromí a ochranu osobnosti a cenzurou jako možným řešením konfliktu těchto dvou práv.

Postup (technika) při zpracování materiálu:

Studium textů, analýza přístupů k ochraně svobody projevu a práva na soukromí a ochranu osobnosti, vyhodnocování relevantnosti důvodů k cenzurování obsahu na internetu a průzkum možností, jak takovou cenzuru provádět, porovnávání pozitivních a negativních faktorů týkajících anonymity na internetu

Základní literatura (nejméně 5 nejdůležitějších titulů k tématu a způsobu jeho zpracování; u všech titulů je nutné uvést stručnou anotaci na 2-5 řádků):

STRYKER, Cole. Hacking the Future: Privacy, Identity, and Anonymity on the Web. ISBN-13: 978-1590209745, The Overlook Press, 2012

Tato kniha zkoumá vliv anonymity na svobodný projev na internetu a možné hrozby v tomto kontextu. Anonymitu rozebírá nejdříve historicky ve sféře politické, literární i kulturní. Autor v knize prozkoumává falešné i reálné on-line identity a prozoumává, zda je vůbec možná absolutní anonymity na internetu v dnešní velmi pokročilé době nových technologií.

KOKOLAKIS, Spyros. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. COMPUTERS [online]. 2017, 64, 122-134 [cit. 2018-05-24]. ISSN 01674048.

Tato práce vysvětluje tzv. privacy paradox, který sleduje rozpor mezi postoji a chování uživatelů sociálních sítí vůči poskytování osobních údajů. Autor poskytuje různé interpretace tohoto fenoménu z hlediska sociální teorie, psychologie či behaviorální ekonomie.

SANGSUVAN, Kitsuron. Balancing Freedom of Speech on the Internet Under International Law. North Carolina Journal of International Law [online]. 2014, 39(3), 701-755 [cit. 2018-05-24]. ISSN 07431759.

Tato práce zkoumá jestli a jak je svoboda projevu na internetu vyvažována za účelem ochrany společnosti a předcházení interkulturních a cross-kulturních konfliktům. Popisuje také mezinárodní právní vymezení svobody projevu, jak je k ní přístupováno a jak je ochraňována v různých státech a jak je s ní zacházeno v internetovém prostředí.

Robert G. Larson III (2013) Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech, Communication Law and Policy, 18:1, 91-120, DOI: 10.1080/10811680.2013.746140

Cílem této práce je prokázat, že právo na soukromí, ochrana osobních údajů a právo na jejich kompletní vymazání v kontextu sociálních sítí je ve fundamentálním rozporu s právem na svobodu projevu.

BARENDT, E. M. Freedom of speech. 2nd ed. New York: Oxford University Press, 2005. ISBN 978-019-9244-515.

Autor v knize zkoumá různé ústavní zvyklosti a právní přístupy k budování rovnováhy mezi svobodou projevu a právem na vlastní soukromí a ochranu osobnosti. Právo na svobodu projevu podporuje argumentací ze sféry filosofie, politiky a práva.

Diplomové práce k tématu (seznam bakalářských, magisterských a doktorských prací, které byly k tématu obhájeny na UK, případně dalších oborově blízkých fakultách či vysokých školách za posledních pět let)
ČERMÁK, Radim. Svoboda vyjadřování a cenzura na internetu a sociálních sítích. Praha, 2016. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Vedoucí práce Jan Reindl.

MATUŠŮ, Hana. Ochrana osobnosti versus svoboda projevu na internetu. Olomouc, 2016. Diplomová práce. Univerzita Palackého v Olomouci, Právnická fakulta. Vedoucí práce Doc. JUDr. Michal Bartoň, Ph.D.

Datum / Podpis studenta/ky

24. 5. 2018

TUTO ČÁST VYPLŇUJE PEDAGOG/PEDAGOŽKA:

Doporučení k tématu, struktuře a technice zpracování materiálu:

Případné doporučení dalších titulů literatury předepsané ke zpracování tématu:

Potvrzuji, že výše uvedené teze jsem s jejich autorem/kou konzultoval(a) a že téma odpovídá mému oborovému zaměření a oblasti odborné práce, kterou na FSV UK vykonávám.

Souhlasím s tím, že budu vedoucí(m) této práce.

.....
Příjmení a jméno pedagožky/pedagoga

.....
Datum / Podpis pedagožky/pedagoga

TEZE JE NUTNO ODEVZDAT VYTIŠTĚNÉ, PODEPSANÉ A VE DVOU VYHOTOVENÍCH DO TERMÍNU UVEDENÉHO V HARMONOGRAMU PŘÍSLUŠNÉHO AKADEMICKÉHO ROKU, A TO PROSTŘEDNICTVÍM PODATELNY FSV UK. PŘIJATÉ TEZE JE NUTNÉ SI VYZVEDNOUT V SEKRETARIÁTU PŘÍSLUŠNÉ KATEDRY A NECHAT VEVÁZAT DO OBOU VÝTISKU DIPLOMOVÉ PRÁCE.

TEZE SCHVALUJE GARANT PŘÍSLUŠNÉHO STUDIJNÍHO PROGRAMU/OBORU.