VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

CENZÚRA NA INTERNETE VO VYBRANÝCH KRAJINÁCH

AUTOR PRÁCE **AUREL STRIGÁČ**

BRNO 2024

Obsah

Kapitola 1

Teoretický úvod

Cenzúra na internete[6] zahrňuje množstvo právnych, etických a technologických aspektov, ktoré majú významný dopad na prístup k informáciám a slobodu prejavu. V tejto časti sa zameriame na rozbor týchto aspektov.

1.1 Právne aspekty

Cenzúra na internete je regulovaná na základe rôznych národných právnych predpisov. V autoritatívnych režimoch sa cenzúra používa na kontrolu politických názorov a obmedzenie prístupu k medzinárodným informačným zdrojom. Na druhej strane, v demokratických krajinách sa právne predpisy, zvyčajne, snažia chrániť slobodu prejavu pri súčasnom zabezpečovaní ochrany pred nelegálnym alebo škodlivým obsahom, ako sú teroristické propagácie alebo nenávistné prejavy.

1.2 Etické aspekty

Etika cenzúry na internete čelí dileme medzi ochranou individuálnych práv na slobodu prejavu a nutnosťou ochrany spoločnosti. Diskusie v tejto oblasti často skúmajú, ako vyvážiť tieto záujmy bez nadmerného zasahovania do osobných slobôd. Výzvy plynúce z technologického pokroku a rozšíreného prístupu k digitálnym médiám ešte viac komplikujú tieto etické otázky.

1.3 Technologické aspekty

Technológie cenzúry na internete zahŕňajú rozsiahle nástroje a metódy, ako sú blokovanie IP adries, filtrovanie kľúčových slov alebo monitorovanie online aktivít. Na druhej strane, techniky ako VPN, Tor a šifrovanie umožňujú užívateľom obísť cenzúru a získavať prístup k obmedzenému obsahu. Tieto technológie predstavujú stálu výzvu pre regulátorov, ktorí sa snažia efektívne monitorovať a regulovať online priestor.

Kapitola 2

Metódy potláčania obsahu na internete

2.1 Metódy technickej cenzúry internetového obsahu

Internetový obsah je predmetom rôznych metód technickej cenzúry, vrátane nasledujúcich prístupov[8]:

2.1.1 Blokovanie IP adries

Prístup na určité IP adresy je, jednoducho, zamietnutý. Ak je cieľová webová stránka hostovaná na zdieľanom serveri, všetky webové stránky na tom istom serveri budú zablokované. Toto ovplyvňuje IP-založené protokoly ako HTTP, FTP a POP. Typickou metódou obchádzania je nájsť proxy servery, ktoré majú prístup k cieľovým webovým stránkam, avšak proxy servery môžu byť tiež zablokované alebo zahltované. Niektoré veľké webové stránky, ako napríklad Google, pridelili ďalšie IP adresy na obchádzanie blokády, no neskôr bolo blokovanie rozšírené tak, aby pokrylo aj tieto nové adresy. Kvôli problémom s geolokáciou je blokovanie založené na geolokácii zvyčajne implementované blokovaním IP adries.

2.1.2 Filtrovanie a presmerovanie systému doménových mien (DNS)

Zablokované doménové mená nie sú rozlúštené, alebo je prostredníctvom DNS únosu alebo iných metód vrátená nesprávna IP adresa. Toto ovplyvňuje všetky IP-založené protokoly ako HTTP, FTP a POP. Typickou metódou obchádzania je nájsť alternatívny DNS resolver, ktorý správne rozlúšti doménové mená, ale aj doménové servery môžu byť predmetom blokovania, najmä blokovania IP adries. Ďalším riešením je obísť DNS, ak je IP adresa dostupná z iných zdrojov a sama nie je zablokovaná. Príklady zahŕňajú úpravu súboru Hosts alebo zadanie IP adresy namiesto doménového mena ako súčasť URL adresy v internetovom prehliadači. Túto metódu cenzúry sa oplatí si zapamätať, pretože sa k nej vrátime v kapitole *3.1: The Great Firewall of China.*

2.1.3 Filtrovanie URL

Reťazce URL sú skenované na cieľové kľúčové slová bez ohľadu na špecifikované doménové meno v URL. Toto ovplyvňuje protokol HTTP. Typické metódy obchádzania zahŕňajú použitie escape znakov v URL alebo použitie šifrovaných protokolov ako VPN a TLS/SSL.

2.1.4 Filtrovanie paketov

Prebieha ukončenie prenosov TCP paketov, keď je zistený určitý počet kontroverzných kľúčových slov. Toto ovplyvňuje všetky TCP-založené protokoly ako HTTP, FTP a POP, avšak vyhľadávanie výsledkov na vyhľadávačoch je pravdepodobnejšie cenzurované. Typické metódy obchádzania zahŕňajú použitie šifrovaných spojení – ako VPN a TLS/SSL – na maskovanie obsahu HTML, alebo zmenšenie MTU/MSS v TCP/IP zásobníku na zníženie množstva textu obsiahnutého v danom pakete.

2.1.5 Reset spojenia

Ak je predchádzajúce TCP spojenie zablokované filtrom, budúce pokusy o spojenie z oboch strán môžu byť tiež zablokované na určitý čas. V závislosti od miesta blokovania môžu byť blokovaní aj iní používatelia alebo webové stránky, ak je komunikácia smerovaná cez blokované miesto. Metódou obchádzania je ignorovať resetovací paket poslaný firewallom.

2.1.6 Odpojenie siete

Technicky jednoduchšou metódou cenzúry internetu je úplné odpojenie všetkých routerov, buď softvérovo, alebo hardvérovo (vypnutím strojov, vytrhnutím káblov). Metódou obchádzania by mohlo byť použitie satelitného ISP na prístup k internetu.

2.1.7 Cenzúra portálov a odstraňovanie výsledkov vyhľadávania

Hlavné portály, vrátane vyhľadávačov, môžu vylúčiť webové stránky, ktoré by inak zahrnuli. Tým sa stránka stáva neviditeľnou pre ľudí, ktorí nevedia, kde ju nájsť. Keď to robí hlavný portál, má to podobný efekt ako cenzúra. Niekedy sa toto vylúčenie deje na splnenie právneho alebo iného požiadavku, inokedy je to čisto na uvážení portálu. Napríklad Google.de a Google.fr odstraňujú zoznamy neo-nacistov a iných v súlade s nemeckým a francúzskym právom.

2.1.8 Útoky na počítačové siete

Útoky odmietnutia služby a útoky, ktoré poškodzujú webové stránky opozície, môžu produkovať rovnaký výsledok ako iné blokovacie techniky, obmedzujúc alebo limitujúc prístup k určitým webovým stránkam alebo iným online službám, hoci iba na obmedzený čas. Táto technika môže byť použitá počas obdobia pred voľbami alebo iným citlivým obdobím. Častejšie ju využívajú neštátne aktéry, ktorí sa snažia narušiť služby.

2.2 Metódy netechnickej cenzúry internetového obsahu

Cenzúra internetového obsahu podlieha metódam podobným tým, ktoré sa používajú pri tradičných médiách[8]. Príklady zahŕňajú:

- Zákony a predpisy môžu zakazovať rôzne typy obsahu alebo vyžadovať, aby bol obsah odstránený alebo blokovaný buď proaktívne, alebo na základe žiadostí.

- Vydavatelia, autori a poskytovatelia internetových služieb (ISP) môžu dostávať formálne a neformálne žiadosti o odstránenie, úpravu, skreslenie alebo blokovanie prístupu k určitým stránkam alebo obsahu.
- Vydavatelia a autori môžu prijať úplatky za zaradenie, odstránenie alebo skreslenie prezentovanej informácie.
- Vydavatelia, autori a poskytovatelia internetových služieb môžu čeliť zatknutiu, trestnému stíhaniu, pokutám a väzeniu.
- Vydavatelia, autori a poskytovatelia internetových služieb môžu byť predmetom občianskoprávnych žalôb.
- Zariadenia môžu byť skonfiškované a/alebo zničené.
- Vydavatelia a poskytovatelia internetových služieb môžu byť zatvorení alebo im môže byť odopretá alebo odňatá potrebná licencia.
- Vydavatelia, autori a poskytovatelia internetových služieb môžu čeliť bojkotom.
- Vydavatelia, autori a ich rodiny môžu byť vystavení hrozbám, útokom, bitkám a dokonca vraždám.
- Vydavatelia, autori a ich rodiny môžu byť vyhrážkami alebo stratiť pracovné miesta.
- Jednotlivci môžu byť platení za písanie článkov a komentárov podporujúcich určité pozície alebo útočiacich na opozičné pozície, zvyčajne bez uznania tejto skutočnosti čitateľom a divákom.
- Cenzori môžu vytvárať vlastné online publikácie a webové stránky s cieľom ovplyvniť online názory.
- Prístup k internetu môže byť obmedzený kvôli reštriktívnym licenčným politikám alebo vysokým nákladom.
- Prístup k internetu môže byť obmedzený kvôli nedostatku potrebnej infraštruktúry, či už úmyselne alebo nie.
- Prístup k výsledkom vyhľadávania môže byť obmedzený kvôli zapojeniu vlády do cenzúry konkrétnych vyhľadávacích termínov; obsah môže byť vylúčený na základe podmienok stanovených s vyhľadávačmi. Aby bolo vyhľadávačom umožnené pôsobiť na novom území, musia súhlasiť s dodržiavaním cenzúrnych štandardov stanovených vládou v danej krajine.

Kapitola 3

Potláčanie obsahu na internete v jednotlivých krajinách

3.1 The Great Firewall of China

3.1.1 Úvod

Jedným z primárnych filtrovacích mechanizmov, na ktorý sa spolieha *The Great Firewall of China* (GFW)[2], je manipulácia s DNS odpoveďami určených domén. Keď GFW manipuluje s DNS požiadavkou, používateľ prijme viaceré DNS odpovede – ako legitímne, tak manipulované.

3.1.2 Technické pozadie

Internetová infraštruktúra v Číne je podrobne monitorovaná a regulovaná prostredníctvom GFW, ktorý implementuje viacero cenzúrnych metód, vrátane manipulácie DNS odpovedí[1]. GFW aktívne sleduje DNS požiadavky na určité domény a reaguje zasielaním manipulovanej DNS odpovede DNS resolveru, ktorý požiadavku inicioval. Táto manipulovaná odpoveď zvyčajne dorazí do resolveru pred legitímnou odpoveďou od príslušného DNS servera, čo vedie k tomu, že resolver uchováva manipulovanú odpoveď v svojej cache a ignoruje pravú odpoveď od DNS servera[1].

3.1.3 Význam a dôsledky DNS manipulácie

Rôzne štúdie a analýzy ukazujú[4], že nielen samotné manipulované odpovede sú problémom, ale aj legitímne odpovede od DNS serverov môžu byť kontaminované. Toto naznačuje, že cieľom útokov GFW môže byť nielen priamo užívateľ, ale aj základná infraštruktúra DNS serverov v rámci Číny. Jedno štúdium[4] napríklad identifikovalo deväť IP adries, ktoré sú často vracané ako výsledok pre mnohé rôzne kontaminované domény. Tento nález podporuje hypotézu, že GFW nejedná arbitrárne, ale sústredene cieľuje na špecifické domény a IP adresy, čo má za následok zámerne skreslené a manipulované odpovede.

[1] Prezentácia funkčnosti DNS cenzúry v Číne: https://www.youtube.com/watch?v=TeYFPirvhv8

3.2 Spojené Štáty Americké

3.2.1 Právne základy a regulačné snahy

Prvý dodatok k Ústave Spojených štátov amerických[7] chráni slobodu prejavu a vyjadrovania proti akýmkoľvek úrovňam vládnej cenzúry. Táto ochrana sa rozširuje aj do kybernetického priestoru, a preto je vládne technické filtrovanie online obsahu v Spojených štátoch relatívne minimálne. Avšak kvôli komplexným právnym a súkromným predpisom je internet napriek tomu regulovaný.

3.2.2 Implementácia a dôsledky

Priame cenzurovanie internetu je zakázané Prvým dodatkom s výnimkou obscénnosti, ako je detská pornografia. Boli pokusy prijať niekoľko zákonov na ďalšiu reguláciu takýchto obscénností a schopnosti detí pristupovať k takémuto materiálu, ale potom boli zistené ako neústavné, pretože prekročili svoje hranice. Dva takéto zákony boli Communications Decency Act z roku 1996 a Child Online Protection Act z roku 1998. Ďalšie podobné akty boli prijaté, vrátane Children's Online Privacy Protection Act z roku 2000 a Children's Internet Protection Act z roku 2000, ktoré chránia súkromie maloletých na internete a zároveň vyžadujú, aby školy K-12 a knižnice, ktoré prijímajú federálnu pomoc pre prístup na internet, obmedzili prístup maloletých k nevhodnému materiálu.

Okrem škôl K-12 a knižníc, ktoré prijímajú federálnu pomoc, majú vlastné filtrovanie aj iné subjekty v Spojených štátoch. Mnohé veľké korporácie ako Google a Microsoft praktizujú samocenzúru. Vojenské inštitúcie tiež zavádzajú filtrovanie pre svoj personál z rôznych bezpečnostných dôvodov.

Ďalším hlavným zdrojom internetovej cenzúry, ktorý bol legalizovaný podľa Digital Millennium Copyright Act z roku 1998, umožňuje jednoduchšie právne kroky proti porušovaniu autorských práv online. Napríklad rýchle vyhľadávanie na Google pre "Hangover 2 download"viedlo k odstráneniu niekoľkých záznamov kvôli sťažnostiam súvisiacim s DMCA.

3.3 Európska Únia

3.3.1 Návrh čiernej listiny

V roku 2011 navrhla Pracovná skupina pre presadzovanie práva Európskej únie (LEWP) nápad, ktorý viedol mnohých ľudí k extrémnym obavám o budúcnosť internetu v EÚ. Skupina navrhla drastické opatrenia na riešenie nelegálnych stránok. Ich návrh zahŕňal vytvorenie čiernej listiny stránok udržiavanej poskytovateľmi internetových služieb (ISP)[5], ktoré boli považované za nevhodné.

3.3.2 Morálna dilema

Táto čierna listina bola vnímaná ako mimoriadne nebezpečná a autoritatívna. Hoci v rôznych krajinách EÚ, vrátane Francúzska a Nemecka[3], došlo k prípadom cenzúry v malom meradle, nič takéhoto rozsahu v Európe doteraz nebolo vidieť. Jej cieľom bolo poskytnúť jednotný bezpečný európsky kybernetický priestor pre jej občanov. Mnohí však poznamenávajú, že aj keby takýto firewall existoval, ľudia by našli spôsoby, ako ho obísť. Koncept firewallu by umožňoval voľný pohyb vnútri firewallu, ale poskytoval by len určité virtuálne

vstupné body, kde by ISP mohli filtrovať a blokovať stránky, ktoré považuje za nelegálne. Takýto firewall by vyžadoval obrovské zdroje na jeho vytvorenie a udržiavanie.

Európski ISP argumentujú, že bremeno blokovania a udržiavania týchto čiernych listín a blokovanie týchto stránok by nemalo byť kladené na nich. Taký firewall by nielenže stál ISP milióny eur na filtrovanie všetkého obsahu, ale tiež by nemali byť zodpovední za riešenie nelegálneho obsahu. ISP tvrdia, že nelegálny obsah by mal byť jednoducho odstránený pri zdroji, pretože bloky siete možno obísť. Je zaujímavé poznamenať, že tieto stránky môžu ľahko získať nové IP adresy od svojich poskytovateľov webového hostingu. S čoraz obmedzenejšou zásobou adries IPv4 nie je ekonomicky realizovateľné plytvať IP adresami a mať IP adresy, ktoré sú na čiernej listine a nepoužiteľné.

Existuje mnoho problémov súvisiacich s firewallom. Na začiatok, kto rozhoduje, čo sa považuje za, takzvane, nelegálny obsah. Hoci nelegálny obsah môže byť zdieľaný aj inými spôsobmi než cez internet, u iných komunikačných foriem, ako je telefón, neexistuje cenzúra. Okrem toho by mal byť vyžadovaný súdny preskum na určenie, či by mal byť web právoplatne blokovaný. Inak, kto zabráni tomu, aby sa táto čierna listina používala na potlačenie slobody prejavu alebo iných ľudských práv? S takýmto mechanizmom by EÚ mohla ľahko začať blokovať stránky jednoducho na základe toho, že stránky zverejňujú informácie, ktoré členské štáty považujú za politicky nepríjemné.

Kapitola 4

Záver

Cenzúra na internete predstavuje multidimenzionálnu výzvu, ktorá vyžaduje premyslený prístup k zákonodarným, etickým a technologickým aspektom. Internet, ako významný dar modernej doby, priniesol revolučné zmeny vo vzdelávaní, komunikácii a obchode. Avšak s veľkou silou prichádza veľká zodpovednosť, a preto je dôležité, aby spoločnosť a zákonodarcovia našli rovnováhu medzi využívaním tohto nástroja a ochranou základných ľudských práv.

4.1 Význam internetu a jeho zodpovedné využívanie

Internet sa stal neoddeliteľnou súčasťou každodenného života, poskytuje nekonečné možnosti na získavanie a šírenie informácií. Avšak, s týmito možnosťami prichádzajú aj riziká, ako sú dezinformácie, nezákonný obsah a zneužívanie digitálneho priestoru. Práve tieto riziká sa v dnešnej dobe preukazujú čím ďalej, tým viac. Je nevyhnutné, aby sme našli rovnováhu, ktorá umožní využívať potenciál internetu, zatiaľ čo sa zároveň minimalizujú jeho negatívne dôsledky.

4.2 Ochrana spoločnosti versus sloboda na internete

Cenzúra, ak je vykonávaná zodpovedne, môže slúžiť ako nástroj na ochranu verejnosti pred škodlivým obsahom, bez toho, aby sa obmedzovali základné slobody. Je dôležité, aby cenzúrne opatrenia boli transparentné, zákonné a spravodlivé, zabezpečujúce ochranu spoločnosti, kým zároveň udržujú dôležitý princíp slobody prejavu. Tento jemný balans vyžaduje neustálu revíziu a adaptáciu pravidiel, aby držali krok s technologickým vývojom a meniacimi sa sociálnymi normami.

4.3 Etické a právne rámce v digitálnom veku

Ako sa technológie vyvíjajú, musia sa takisto vyvíjať aj etické a právne rámce, ktoré ich regulujú. Spoločnosť musí spolupracovať s technologickými firmami a právnymi odborníkmi, aby definovala, čo je prijateľné a čo prekračuje hranice zákona a morálky. Vytváranie silných, avšak flexibilných právnych noriem, ktoré umožňujú inovácie a zároveň poskytujú nevyhnutnú ochranu, je kľúčové pre správne fungovanie digitálneho priestoru.

Literatúra

[1] Anonymous. The collateral damage of internet censorship by DNS injection. jún 2012, s. pp 21–27. DOI: 10.1145/2317307.2317311. Dostupné z: https://dl.acm.org/doi/10.1145/2317307.2317311.

[2] BARME, G. R. a YE, S. The Great Firewall of China. [https://www.wired.com/1997/06/china-3/]. jún 1997. Otvorené 01.05.2024.

[3] European Digital Rights (EDRi). France and Germany demand more censorship from internet companies. [https://edri.org/our-work/leak-france-germany-demand-more-censorship-from-internet-companies/]. 2018. Otvorené 01.05.2024.

[4] Farnan, O., Darer, A. a Wright, J. Poisoning the Well: Exploring the Great Firewall's Poisoned DNS Responses. október 2016, s. pp 95–98. DOI: 10.1145/2994620.2994636. Dostupné z: https://dl.acm.org/doi/10.1145/2994620.2994636.

[5] Gillis, A. S. ISP (Internet Service Provider). [https://www.techtarget.com/whatis/definition/ISP-Internet-service-provider]. 2022. Otvorené 01.05.2024.

[6] IPLocation.net. Internet Censorship. [https://www.iplocation.net/internet-censorship]. 2023. Otvorené 01.05.2024.

[7] The White House. The Constitution. [https://www.whitehouse.gov/about-the-white-house/our-government/the-constitution/#:~:text=The%20First%20Amendment%20provides%20that,for%20a%20redress%20of%20grievances.]. 2024. Otvorené 01.05.2024.

[8] Wikipedia.org. Internet censorship. [https://en.wikipedia.org/wiki/Internet_censorship]. 2024. Otvorené 01.05.2024.