Kam kráčí svoboda internetu?

Jakub Rejzek
Šimon Zajíček

Svoboda internetu

svoboda internetu se v roce 2022 celosvětově znovu propadla a to již po dvanácté za sebou

nejhůře je na tom Čínská lidová republika, Ruská federace a Severní Korea

nejsvobodnější internet mají na Islandu a v Estonsku

Freedom House 2022

Evropská unie

Česká republika

Technický problém

Etický problém

Evropská unie

Legislativa

Nařízení Rady Evropské unie č. 833/2014

- reakce na vpád ruských vojsk na Ukrajinu (Donbas)
- pozastavení vysílání některých televizních stanic
- označení vybraných společností za šiřitele dezinformací
- v letech 2022 a 2023 rozšířeno o další televizní stanice
- v České republice provádí dohled nad dodržováním povinností Český telekomunikační úřad (ČTÚ)

- efektivita je diskutabilní - televize jsou k dispozic na webových portálech
- nereálný požadavek na zablokování obsahu na jiných než oficiálních webech
- neexistuje specifický seznam URL adres

Nařízení Evropského parlamentu a Rady EU č. 2022/2065

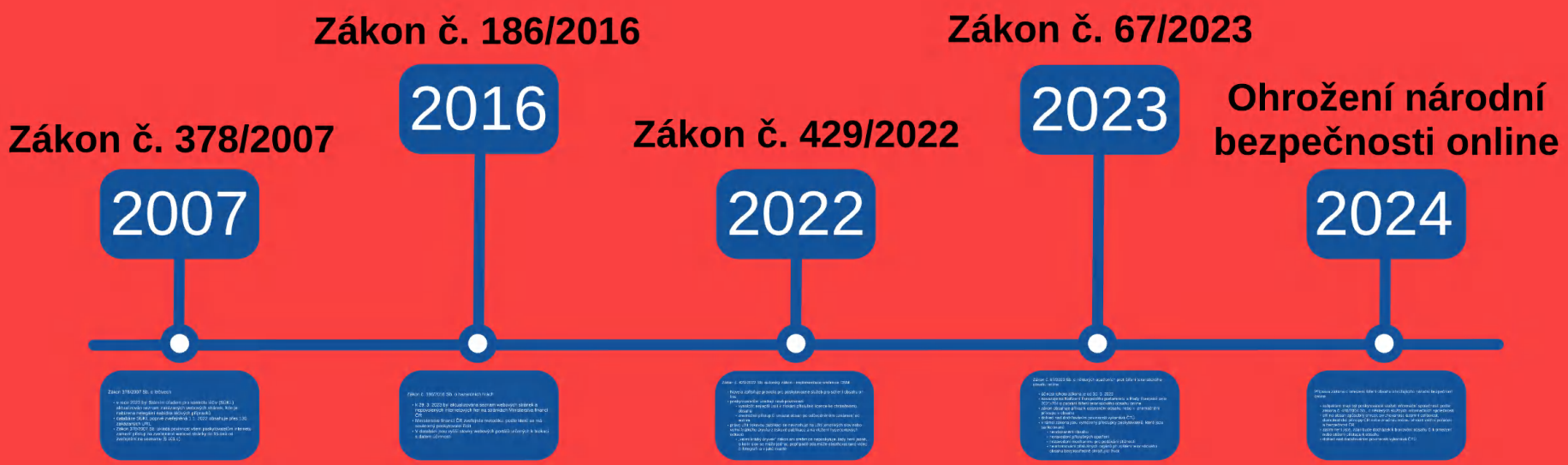
- upravuje odpovědnost poskytovatele zprostředkovatelských služeb
  - služba prostého přenosu
  - služba ukládání do mezipaměti
  - hostingová služba
- cílem je blokovat nelegální obsah chráněný autorským právem a šíření dezinformací
- při zjištění protiprávní činnosti nebo nezákonného obsahu, má poskytovatel povinnost urychleně přijmout opatření k odstranění nezákonného obsahu nebo ke znemožnění přístupu k němu
- nejednotná definice nelegálního obsahu napříč členskými státy
- povinnost vyhodnocovat nelegální obsah je na poskytovatelých služby

Návrh Evropské komise pro boj se sexuálním zneužíváním dětí COM/2022/209

- cílem legislativy má být větší pravomoce státu při blokování a mazání obsahu s dětskou pornografií
- navrhovaným řešením je implementace softwarového nástroje používající umělou inteligenci (AI) schopného monitorovat obsah na sítích a vyhodnocovat obsah s dětskou pornografií (instalace softwaru pouze po nařízení soudem)
- součástí řešení má být kapacita kontrolních orgánů prolomit šifrování soukromých komunikací, kde se dětská pornografie často šíří
- problémem je nepřesné rozpoznávání ilegálních aktivit od legálních soukromých zpráv - zásah do soukromí

Česká republika

Legislativa



Zákon 378/2007 Sb. o léčivech

- v roce 2023 byl Státním úřadem pro kontrolu léčiv (SÚKL) aktualizován seznam zakázaných webových stránek, kde je nabízena nelegální nabídka léčivých přípravků
- databáze SÚKL poprvé zveřejněná 1.1. 2022 obsahuje přes 130 zakázaných URL
- Zákon 378/2007 Sb. ukládá povinnost všem poskytovatelům internetu zamezit přístup na zveřejněné webové stránky do 15 dnů od zveřejnění na seznamu (§ 101 c)

Zákon č. 186/2016 Sb. o hazardních hrách

- k 29. 3. 2023 byl aktualizována seznam webových stránek a nepovolených internetových her na stránkách Ministerstva financí ČR
- Ministerstvo financí ČR zveřejnilo metodiku, podle které se má soukromý poskytovatel řídit
- V databázi jsou vyšší stovky webových portálů určených k blokaci s datem účinnosti

Zákon č. 429/2022 Sb. autorský zákon - implementace směrnice DSM

- Novela zpřísňuje pravidla pro poskytovatele služeb pro sdílení obsahu on-line
- poskytovatelům vznikají nové povinnosti:
  - vynaložit nejlepší úsilí k získání příslušné licence ke chráněnému obsahu
  - znemožnit přístup či smazat obsah po odůvodněném oznámení od autora
- právo užít tiskovou publikaci se nevztahuje na užití jenotlivých slov nebo *velmi krátkého úryvku* z tiskové publikace a na vložení hypertextových odkazů
  - „velmi krátký úryvek“ zákon ani směrnice neposkytuje, tedy není jasné, o kolik slov se může jednat, popřípadě zda může obsahovat také video či fotografii a v jaké kvalitě

Zákon č. 67/2023 Sb. o některých opatřeních proti šíření teroristického obsahu online

- účinost tohoto zákona je od 30. 3. 2023
- navazuje na Nařízení Evropského parlamentu a Rady Evropské unie 2021/784 o potírání šíření teroristického obsahu online
- zákon obsahuje příkaz k odstranění obsahu nebo k znemožnění přístupu k obsahu
- dohled nad dodržováním povinností vykonává ČTÚ
- v rámci zákona jsou vymezeny přestupky poskytovatelů, které jsou sankciované
    - neodstranění obsahu
    - nezavedení příslušných opatření
    - nezavedení mechanimu pro podávání stížností
    - neinformování příslušných orgánů při zjištění teroristického obsahu bezprostředně ohrožující život

Příprava zákona o omezení šíření obsahu ohrožujícího národní bezpečnost online

- subjektem mají být poskytovatelé služeb informační společnosti podle zákona č. 480/2004 Sb., o některých službých informačních společností
- cílí na obsah způsobilý ohrozit svrchovanost, územní celistvost, demokratické principy ČR nebo značnou měrou ohrozit vnitřní pořádek a bezpečnost ČR
- zatím není jisté, zdali bude docházek k blokování obsahu či k omezení nebo stížení přístupu k obsahu
- dohled nad dodržováním povinností vykonává ČTÚ

Technický problém

Technicky možné ne vždy znaméná reálné

Nařízení vyžadují technicky možná, ale prakticky nereálná či neúčinná řešení

Poskytnutí šifrovacích klíčů povede k jejich obměně

Nedostatek specifikací a prováděcích předpisů

Blokace obsahu není samospásná, lze ji jednoduše obejít

Využití AI zvýší schopnosti ISP, ale také sníží kontrolu

Data retention
provozní a lokalizační údaje

- Ukládají se plošně informace o uskutečněné komunikaci, ovšem bez znalosti jejího obsahu (na rozdíl od odposlechu).
- Data uchovávají poskytovatelé po dobu 6 měsíců. Jde jak o telefonní hovory, SMS/MMS, tak připojení k internetu

```
Date first seen          Event  XEvent Proto      Src IP Addr:Port          Dst IP
Addr:Port     X-Src IP Addr:Port        X-Dst IP Addr:Port   In Byte Out Byte
2023-04-22 18:45:00.013 DELETE  Ignore UDP       10.14.132.13:43060 ->
8.8.8.8:53       xx.xx.xx.32:43060 ->          8.8.8.8:53           0        0
2023-04-22 18:45:00.015 DELETE  Ignore TCP       10.14.142.11:65364 ->
8.8.8.8:443      xx.xx.xx.32:65364 ->          8.8.8.8:443          0        0
2023-04-22 18:45:00.015 CREATE  Ignore UDP       10.51.144.10:9401  ->
8.8.8.8:53      xx.xx.xx.196:9401  ->          8.8.8.8:53           0        0
2023-04-22 18:45:00.016 CREATE  Ignore UDP         10.65.5.16:57109 ->
8.8.8.8:53       xx.xx.xx.66:47392 ->          8.8.8.8:53           0        0
```

- DNS
- protok
  webo
  (čísel
  jmé
- Pos
  důvo
  rámci
- Co te
  např.

Data retention a DNS

- DNS = Domain Name System
- protokol zajišťující překlad názvů domén webových stránek z nepřehledné (číselné) podoby na tzv. „doménové jméno“
- Poskytovatel má možnost z technických důvodů sledovat či ovlivňovat provoz v rámci DNS
- Co tedy řeší? 10.x.x.x požaduje spojení např. na email.seznam.cz (77.75.78.196)

domén

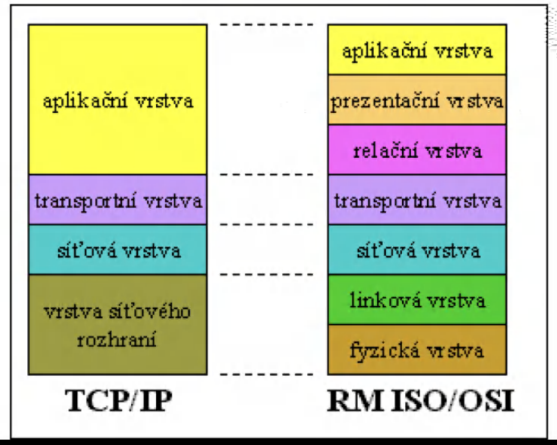
ové

nických
voz v

spojení
.78.196)

V praxi se nejčastěji ukládají

- zdrojové a cílové IP adresy spojení, ty jednoznačně identifikují koncové stanice
- zdrojový a cílový port komunikace spolu s typem komunikačního protokolu, což pomáhá identifikovat aplikaci, která komunikaci iniciovala
- datum a čas a množství dat, které spojením proteklo
- ostatní požadovaná data se pak odvozují z dalších databází jako jsou zákaznické databáze a registry IP adres



- HTTPS
- pro
komu

- HTT
dův

- Přesto
zabezp
být v

s typem

iciovala
ním

í z
tabáze

Šifrování provozu

- HTTPS (Hypertext Transfer Protocol Secure)
  - protokol používaný pro zabezpečenou komunikaci mezi webovým prohlížečem a webovým serverem
  - HTTPS využívá šifrování, které zajišťuje důvěrnost, integritu a autentizaci dat při přenosu
- Přestože HTTPS poskytuje zvýšenou úroveň zabezpečení, některé informace stále mohou být vysledovány během provozu HTTPS.

- Dom
  - F
    s
    j
    T
    z
    i
    r
- Čas
  - I
    s
    s
    c
    p
    c

Secure)
enou
čem a

išťuje
at při

úroveň
mohou
TTPS.

Mezi tyto informace patří

- Doménové jméno a IP adresa
  - Při komunikaci mezi prohlížečem a serverem je stále viditelné doménové jméno a IP adresa webové stránky Tato informace může být zaznamenána poskytovatelem internetových služeb (ISP) nebo monitorována na firemních sítích.
- Čas a délka spojení
  - ISP nebo síťový správce mohou sledovat čas, kdy bylo navázáno spojení s konkrétním serverem, a jak dlouho toto spojení trvalo. To může poskytnout určitý náznak o tom, jaký obsah uživatel prohlížel

- Veli
  -
- Čas
  -

Mezi tyto informace patří

- Velikost dat
  - Velikost přenášených dat mezi prohlížečem a serverem je také viditelná. I když nelze zjistit konkrétní obsah, velikost dat může poskytnout informace o tom, jaký typ obsahu byl přenášen (např. text, obrázky, video)
- Čas a délka spojení
  - ISP nebo síťový správce mohou sledovat čas, kdy bylo navázáno spojení s konkrétním serverem, a jak dlouho toto spojení trvalo. To může poskytnout určitý náznak o tom, jaký obsah uživatel prohlížel

Mezi tyto informace patří

- Typ šifrování
  - Informace o použitém šifrování a protokolu pro zabezpečení spojení (např. TLS 1.3) je viditelná. Tato informace nemusí být citlivá, ale může sloužit k analýze bezpečnosti spojení.
- Samotný obsah komunikace (konkrétní stránky, e-maily, zprávy, hesla) je díky šifrování chráněn a nelze jej během provozu HTTPS snadno vysledovat. HTTPS zvyšuje úroveň soukromí a zabezpečení při používání internetu, ale není absolutní ochranou proti všem formám sledování.

Šifrování DNS

- Secure DNS
  - označení pro technologie a protokoly, které zvyšují bezpečnost a soukromí DNS dotazů a odpovědí
  - DNS je základní služba internetu, která převádí lidsky čitelné názvy domén (např. example.com) na IP adresy (např. 192.0.2.1), které počítače používají k navázání spojení
  - tradiční DNS komunikace jsou nešifrované a náchylné k útokům a sledování. Secure DNS technologie zahrnují několik protokolů a přístupů, které chrání DNS komunikaci

koly,
omí DNS

, která
én (např.
ř.
ají k

a
gie
upů,

Šifrování DNS

- DNS over HTTPS (DoH)
  - DoH šifruje DNS dotazy/odpovědi pomocí HTTPS, což zajišťuje důvěrnost, autentizaci a integritu dat.
  - DoH chrání DNS komunikaci před odposlechy a útoky typu "man-in-the-middle", které mohou změnit DNS odpovědi a odkazovat uživatele na škodlivé weby.

- DNS o
  - Do
    pro
    pro
  - Do
    uto
  - Do
    že
    pro
    sta
    Do
    ope
    na

ědi

tu dat.
řed
-in-the-
)NS
e na

Šifrování DNS

- DNS over TLS (DoT)
  - DoT je podobný DoH, ale používá protokol TLS (Transport Layer Security) pro šifrování DNS komunikace
  - DoT chrání také před odposlechy a útoky typu "man-in-the-middle"
  - Rozdíl mezi DoH a DoT spočívá v tom, že DoH je zaměřen na použití v prohlížečích a provozuje se přes standardní HTTPS port (443), zatímco DoT je navržen pro použití v operačních systémech a provozuje se na dedikovaném portu (853)

Šifrování DNS

- DNSSEC (Domain Name System Security Extensions)
- DNSSEC je sada rozšíření pro DNS, která zavádí digitální podpisy a autentizaci pro DNS záznamy
- DNSSEC chrání uživatele před útoky typu "cache poisoning" a "man-in-the-middle" tím, že ověřuje pravost a integritu DNS záznamů.
- DNSSEC ovšem nešifruje DNS komunikaci, takže dotazy a odpovědi jsou stále viditelné pro odposlouchávání

Šifrování DNS

- Tyto technologie mohou být použity samostatně nebo v kombinaci, aby se zvýšila bezpečnost a soukromí DNS komunikace
- Pro použití Secure DNS je třeba mít podporu na straně klienta (operační systém nebo prohlížeč) a na straně DNS serveru (resolver)
- Některé operační systémy a prohlížeče již podporují DoH a DoT, a existuje mnoho veřejných DNS resolverů, které podporují tyto protokoly

Šifrování DNS

- Tyto technologie mohou být použity samostatně nebo v kombinaci, aby se zvýšila bezpečnost a soukromí DNS komunikace
- Pro použití Secure DNS je třeba mít podporu na straně klienta (operační systém nebo prohlížeč) a na straně DNS serveru (resolver)
- Některé operační systémy a prohlížeče již podporují DoH a DoT, a existuje mnoho veřejných DNS resolverů, které podporují tyto protokoly

ity
y se
NS

mít
ční
DNS

eče již
noho
porují

DNS?

Jakýkoliv DNS mimo ČR jednoduše obejde blokování v ČR.
Jakýkoliv DNS mimo EU jednoduše obejde blokování v EU.
Jakákoliv VPN kamkoliv jednoduše obejde blokování kdekoliv.

Vše na dvě kliknutí.

Google? 8.8.8.8
CloudFlare? 1.1.1.1

Složité? Dva kroky podle návodu na Youtube…

Etický problém

technicky možné ne vždy znamená etické

Hranice osobní svobody je stále posouvána na úkor bezpečí

Prolamování šifrování naruší důvěru a integritu internetu

Nařízení vyžadují po poskytovatelých nerálné schopnosti

Nedostatečná schopnost diskriminace uživatelů

Zneužitelnost softwarových a hardwarových kapacit

Proporcionalita a teorie kluzkého svahu

Kam kráčí svoboda internetu?

Jakub Rejzek
Šimon Zajíček