2022

SBĚR A VYUŽITÍ DAT UŽIVATELŮ INTERNETU

SÁRA SOVIČKOVÁ

VÝZKUMNÁ ZPRÁVA

KONGRESU

SBĚR A VYUŽITÍ DAT UŽIVATELŮ INTERNETU

AUTOR: SÁRA SOVIČKOVÁ

1. ÚVOD – O ČEM TATO VZK JE

Internet dnes využívá přibližně 62,5 % světové populace, aktivními uživateli sociálních sítí je pak 58,4 % všech obyvatel.[1] Není proto překvapivé, že se data těchto uživatelů a jejich využití staly velkým tématem. Výhody internetu a sociálních sítí jsou založeny na prvotních myšlenkách jejich zakladatelů a jsou jimi zejména možnost spojit se s lidmi po celém světě, rozvoj globálních komunit a obrovská efektivita při předávání jakýchkoliv informací, což nám často a v mnoha oblastech usnadňuje život. Kvůli kombinaci těchto skvělých vlastností a rychlosti, s jakou se internet stal součástí naší reality, si mnozí uživatelé nestihli uvědomit, co všechno se dá z dat, která běžně generují, vyčíst, a tudíž jak moc jsou cenná a pro koho.

Tato výzkumná zpráva uvádí v první části některé příklady zneužití uživatelských dat a ilustruje na nich zranitelnost současného systému. Dále rozebírá aktuální legislativu ve Spojených státech, která řeší soukromí uživatelů internetu, regulaci sběru a využití jejich dat. Zároveň upozorňuje na její nedostatky a ukazuje jejich dopady ve světle mezinárodní spolupráce i individuálních škod způsobených uživatelům. Shrnuje také některé klíčové body, které by v budoucích zákonech mohly být žádoucí.

2. VYBRANÉ KAUZY

2.1 CAMBRIDGE ANALYTICA

Kauza týkající se společnosti Cambridge Analytica (dále jen „***CA***“) ve spojení s Facebookem z roku 2018 se stala slavným a strašidelným příkladem toho, k čemu se dají získaná data využít. Díky ní si mnozí běžní uživatelé i zákonodárci uvědomili, že mezi hlavní a velmi cenné komodity, se kterými se nyní obchoduje, jsou právě uživatelská data.

V březnu 2018 média uvedla, že CA za účelem profilování voličů porušila zásady používání dat Facebooku a sbírala údaje o milionech jeho uživatelů. CA to provedla ve spolupráci s Aleksandrem Koganem, tvůrcem aplikace *thisisyourdigitallife app*, která umožňovala uživatelům Facebooku vyplňovat osobnostní kvízy. Aplikace následně získávala od uživatelů data z jejich profilů a profilů jejich přátel. Díky tomu byla vytvořena rozsáhlá sada dat, která byla následně bez vědomí uživatelů předána CA. S těmito informacemi CA vytvořila profily potenciálních voličů pro cílení reklam i celkového obsahu. Kromě reklam na Facebooku totiž mohla být optimalizace pro vyhledávače použita k nasměrování uživatelů k reklamám a dalšímu obsahu (např. blogům nebo alternativním zpravodajským zdrojům) mimo Facebook.[2] Takto byla společnost schopna

ovlivňovat veřejné mínění se zaměřením na voliče, kteří si nebyli jisti, kam se přiklonit a (v případě Spojených států) na obyvatele tzv. swing states.

CA se měla úspěšně podílet na mnoha kampaních po celém světě, například v Keni, Nigérii, Mexiku, Brazílii nebo Indii.[3] Jejími nejznámějšími projekty jsou ale bezpochyby Leave.EU, čili kampaň pro Brexit a Trumpova prezidentská kampaň. Poté, co vypluly na povrch detaily o tom, jak CA data získala, jací aktéři tuto společnost financovali a jaké měla jejich práce dopady na proces demokratických voleb, se strhla obrovská mediální bouře a společnost zanikla.[4] Facebook pak čelil mnoha obviněním kvůli zneužití dat jeho uživatelů a nestalo se tak naposledy. [5]

2.2 TWITTER

Federální obchodní komise (FTC) uvedla koncem května roku 2022, že podniká kroky proti společnosti Twitter, Inc. pro klamavé používání údajů na zabezpečení účtu pro cílenou reklamu. V letech 2014 až 2019 totiž poskytlo více než 140 milionů uživatelů Twitteru svá telefonní čísla nebo e-mailové adresy poté, co jim společnost řekla, že tyto informace pomohou zabezpečit jejich účty. Firma ale vydělávala na tom, že umožnila inzerentům používat tato data k cílení na konkrétní uživatele, aniž by o tom uživatele informovala. Tato činnost však porušila příkaz FTC z roku 2011, který společnosti výslovně zakázal zkreslovat její postupy v oblasti soukromí a zabezpečení. Podle navrhovaného příkazu FTC a Ministerstva spravedlnosti by musel Twitter zaplatit pokutu 150 milionů dolarů a měl by zakázáno finančně těžit ze svých podvodně shromážděných dat. Ke dni uzavření této výzkumné zprávy však ještě nerozhodl federální distriktní soud o návrhu příkazu.

Klamavé používání telefonních čísel a e-mailových adres uživatelů Twitterem pro cílenou reklamu také porušilo dohody EU-U.S. Privacy Shield a Swiss-U.S. Privacy Shield, které vyžadovaly, aby zúčastněné společnosti dodržovaly určité zásady ochrany osobních údajů k tomu, aby mohly legálně přenášet data ze zemí EU a Švýcarska.[6]

3. SOUČASNÁ SITUACE

3.1 JAK TO VIDÍ BĚŽNÍ AMERIČANÉ

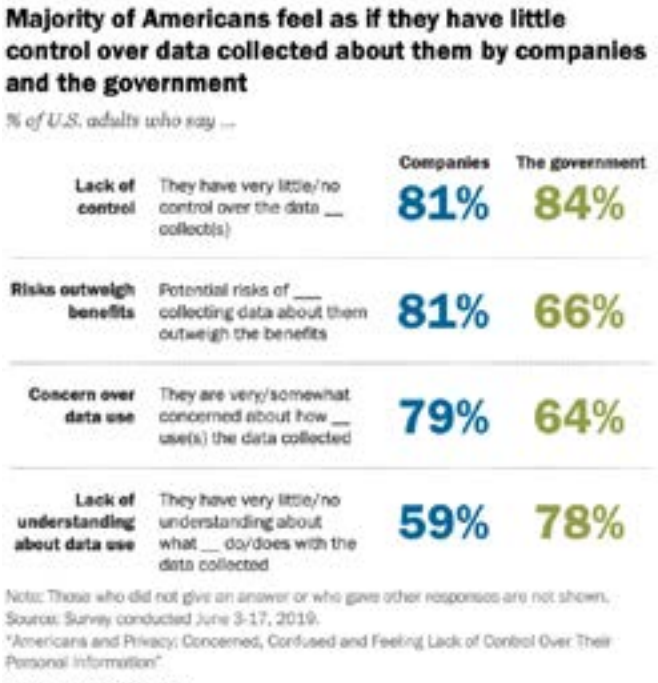
Otázka uživatelských dat se právě díky těmto a dalším kauzám z minulých let začala řešit důrazněji. Způsobily totiž, že veřejnost pochopila možná rizika a o téma se více zajímá a pohlíží na něj s většími obavami o svoje soukromí.

Tlak veřejnosti se tak stal jedním z několika faktorů, které přispívají k větší snaze soukromých společností a zákonodárců změnit praktiky v odvětví osobních údajů. Myšlenka „surveillance capitalism“, kterou její autorka Shoshana Zuboff popisuje jako „ekonomický systém vybudovaný na tajném získávání a manipulaci s lidskými daty“, se stala součástí obecného diskurzu a zachytila rostoucí povědomí spotřebitelů o tom, že jejich data se kupují, prodávají a používají bez jejich souhlasu, a jejich rostoucí neochotu se s tím smířit. Lidé to začínají dávat najevo: na hlavním severoamerickém trhu čelí Facebook i Twitter úbytku svých každodenních aktivních uživatelů.[7]

Podle **výzkumu Pew Research Center z června 2019** se většina Američanů domnívá, že jejich online i offline aktivity jsou pravidelně sledovány a monitorovány společnostmi a vládou. Je to tak běžná součást moderního života, že zhruba šest z deseti dospělých Američanů tvr-

dí, že si nemyslí, že je možné prožít jeden den, aniž by o nich společnosti nebo vláda shromažďovaly údaje. Produkty a služby založené na datech jsou často uváděny na trh s potenciálem ušetřit uživatelům čas a peníze nebo dokonce vést k lepšímu zdraví a spokojenosti. Přesto velká část dospělých v USA není přesvědčena o tom, že jim tento systém rozsáhlého shromažďování dat přináší výhody.

I když však veřejnost vyjadřuje obavy z různých aspektů svého digitálního soukromí, mnoho Američanů přiznává, že ne vždy pečlivě dbají na zásady ochrany osobních údajů a podmínky služeb, se kterými se pravidelně setkávají. Široká veřejnost také obecně nerozumí zákonům o ochraně osobních údajů: 63 % Američanů tvrdí, že zákonům a předpisům, které v současné době platí na ochranu soukromí jejich údajů, rozumí jen velmi málo, nebo vůbec.

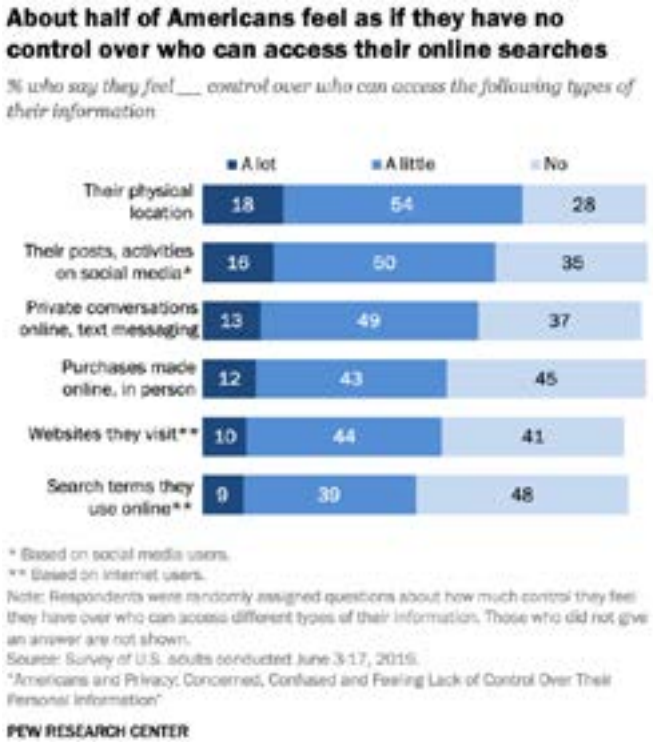


Graf 1: Průzkum veřejného mínění Američanů o kontrole nad daty, která o nich shromažďuje vláda a soukromé společnosti[23]

Pew Research Center uvádí také hlavní poznatky zveřejněného výzkumu:

- **Rozšířenost sledování**: 72 % Američanů uvádí, že mají pocit, že všechno, téměř všechno, nebo většinu toho, co dělají online nebo při používání mobilního telefonu, sledují inzerenti, technologické firmy nebo jiné společnosti. Téměř polovina (47 %) dospělých se domnívá, že alespoň většinu jejich online aktivit sleduje vláda.

- **Ztráta kontroly nad osobními údaji**: Zhruba osm z deseti nebo více dospělých Američanů tvrdí, že mají velmi malou nebo žádnou kontrolu nad údaji, které o nich shromažďuje vláda (84 %) nebo společnosti (81 %).



Graf 2: Průzkum veřejného mínění Američanů o kontrole nad historií jejich vyhledávání na internetu[24]

- **Rizika a přínosy sběru dat a profilování**: 81 % Američanů si myslí, že potenciální rizika sběru dat o nich ze strany společností převažují nad přínosy, a 66 % si myslí totéž o sběru dat o nich ze strany vlády.

- **Nedostatek porozumění**: 78 % dospělých Američanů tvrdí, že velmi málo nebo vůbec nerozumí tomu, co vláda dělá s údaji, které shromažďuje, a 59 % tvrdí totéž o údajích, které shromažďují společnosti.[8]

Podle **ankety CBS News** z dubna roku 2018 si šest z deseti Američanů myslí, že vláda by měla zpřísnit regulaci technologických společností a společností působících v oblasti sociálních médií, aby se pokusila zabránit zneužívání údajů uživatelů. Tento

názor jde napříč stranami a sdílí ho většina demokratů i republikánů. Téměř čtyři z deseti Američanů s tím ale nesouhlasí a tvrdí, že regulace by mohly omezit inovace a růst. Anketa také ukázala, že 81 % uživatelů se obává, že „ostatní“ lidé příliš rychle věří všemu, co vidí na Facebooku. Uživatelé uvádějí, že oni sami věří jen velmi malé části toho, co vidí na Facebooku. Třetina z nich věří pouze tomu, co se dozví od přátel a rodiny.[9]

Z těchto výsledků samozřejmě vyvstává tradiční téma pro diskuzi - regulace. Odpůrci regulace předpokládají, že lidé jsou schopni ve vlastním zájmu rozhodovat o sdělování či nesdělování informací. Zastánci tohoto názoru mají tendenci vidět ochranu soukromí skrze regulaci jako zásah do v zásadě příznivé trajektorie vývoje informačních technologií a výhod, které tyto technologie přinášejí.

Příznivci regulace se naopak obávají o schopnost jednotlivců starat se o své soukromí v prostředí stále složitějších kompromisů. Tradiční nástroje pro rozhodování o ochraně soukromí, jako jsou např. volba a souhlas, podle tohoto pohledu již neposkytují dostatečnou ochranu. Namísto spoléhání se na individuální odpovědnost je proto zapotřebí regulační zásah, aby se vyvážily zájmy uživatelů proti moci komerčních subjektů a vlád, které drží tato data.[10]

3.2 LEGISLATIVA

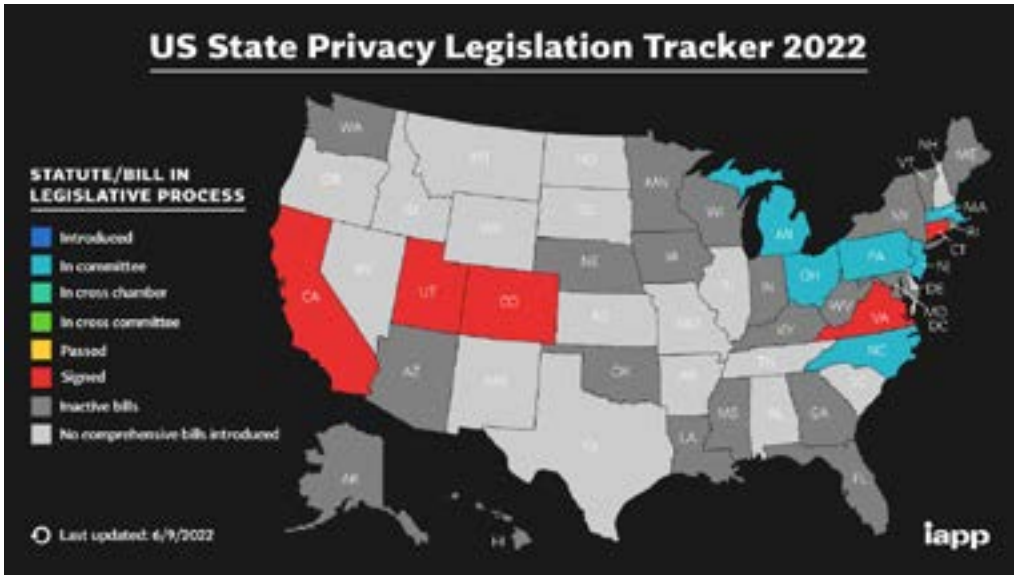
Bezpečnost dat není pro sektor informačních technologií obecně zákonem předepsána. Místo toho firmy investují do bezpečnosti IT jako součást řízení podnikových rizik. Zmírnění tohoto rizika může být podstatné pro jejich investory nebo přínosné pro jejich uživatele.

V americkém systému platí pravidla ochrany osobních údajů, která zajišťují soukromí jednotlivce vzhledem k vládě. Nicméně ochrana soukromí jednotlivců před jinými subjekty (např. jednotlivci nebo korporacemi) je záležitostí státního práva a soukromých dohod (tj. smluv). To vytváří větší zátěž pro uživatele, neboť se po nich požaduje, aby porozuměli riziku generování a sdílení dat a zároveň byli schopni revidovat a rozumět jednotlivým dohodám s různými poskytovateli služeb, které využívají.[11]

Kongres přijal řadu federálních zákonů, jejichž cílem je zajistit právní ochranu osobních údajů jednotlivců. Na rozdíl od systému převládajícího v Evropě a některých dalších zemích mají Spojené státy spíše než jeden komplexní zákon „mozaiku“ federálních zákonů, které upravují postupy společností v oblasti ochrany údajů. Tyto zákony se značně liší svým účelem a rozsahem. Většina z nich ukládá povinnosti v oblasti ochrany údajů buď konkrétním subjektům v některých odvětvích jako například finančním institucím, zdravotnickým subjektům a běžným telekomunikačním operátorům nebo stanovuje obecně druhy údajů, jako jsou například údaje o dětech. Jiné zákony však doplňují omezenou ochranu soukromí stanovenou ústavou a uplatňují podobné zásady na soukromé subjekty. Například zákon o uchovávaných komunikacích (Stored Communications Act - SCA) obecně zakazuje neoprávněný přístup k určitým elektronickým komunikacím uchovávaných poskytovateli internetových služeb nebo jejich zveřejňování.

Konečně některé zákony zakazují široké kategorie jednání, které sice nejsou omezeny na ochranu údajů, ale omezují způsob, jakým mohou společnosti nakládat s osobními údaji. Především zákon o Federální obchodní komisi (FTC Act) zakazuje „nekalé nebo klamavé jednání nebo praktiky“[12] a zmocňuje FTC k postihu aplikace nebo webové stránky, která porušuje své vlastní zásady ochrany osobních údajů. FTC může také vyšetřovat porušení marketingových formulací týkajících se ochrany soukromí, jako tomu bylo v případě stížnosti na společnost Zoom, která klamala uživatele tvrzením, že videochaty jsou šifrovány end-to-end (nebo u výše zmíněného Twitteru).

Vzhledem k širokému spektru různých zákonů je snadné pochopit, že lidé jsou zmateni tím, jaká práva mají a jaká ne. K tomu je třeba dodat, že vedle těchto federálních zákonů existuje také několik zákonů státních.



Obrázek 1: Mapa států podle stavu přijaté legislativy o ochraně soukromí[25]

Tyto zákony mají podobná ustanovení, která uživatelům obvykle zaručují poskytnutí určitého oznámení a možnosti, jak ovládat svá data. Ve zkratce společnost, která vykonává činnost regulovanou těmito předpisy, musí uživatelům oznámit, zda údaje prodává, a uživatelé mají také možnost volby, zda s tím souhlasí, či nikoliv, a mají právo k údajům přistupovat, mazat je, opravovat nebo přesouvat. [13] Mezi nejrozsáhlejší a nejambicióznější z těchto zákonů patří CCPA.

Kalifornský zákon z roku 2018 (dále jen "**CCPA**") se narozdíl od „mozaiky" na federální úrovni neomezuje na konkrétní odvětví společností nebo skupinu uživatelů, místo toho se vztahuje na všechny společnosti, které shromažďují osobní údaje Kaliforňanů, jsou ziskové, podnikají v Kalifornii a splňují základní prahové hodnoty. Analytici naznačují, že tyto prahové hodnoty jsou dostatečně nízké, aby se zákon mohl vztahovat na značný počet „relativně malých" podniků s webovými stránkami přístupnými v Kalifornii.[14] Spotřebitelům dává větší kontrolu nad osobními údaji, které o nich podniky shromažďují, a nařízení k provedení CCPA poskytují návod pro společnosti, jak tento zákon implementovat. CCPA zajišťuje kalifornským spotřebitelům nová práva na ochranu soukromí včetně:

- práva na informace o osobních údajích, které o nich podnik shromažďuje, a o tom, jak jsou používány a sdíleny;
- práva na vymazání osobních údajů, které o nich byly shromážděny (s některými výjimkami);
- práva odmítnout prodej svých osobních údajů;
- práva na nediskriminaci při uplatňování jejich práv podle CCPA.

Podniky jsou povinny poskytnout spotřebitelům určitá oznámení vysvětlující jejich postupy v oblasti ochrany osobních údajů. CCPA se vztahuje na mnoho podniků včetně zprostředkovatelů údajů.[15]

Žádný jiný zákon na státní ani federální úrovni nemá tak široké pole působnosti, ani nezajišťuje právo na soukromoprávní žalobu, což bude dále zmíněno jako jeden z potenciálních klíčových bodů pro budoucí legislativu. Zároveň se v Kalifornii dbá na schopnost vymáhat tento zákon.

V listopadu 2020 byla schválena CPRA, volební iniciativa, která mění zákon CCPA a zahrnuje další ochranu soukromí spotřebitelů. Zákonem CPRA pak byla zřízena Kalifornská agentura pro ochranu soukromí (CPPA), jejímž úkolem je implementovat a prosazovat tento zákon.[16]

3.3 MEZINÁRODNÍ SITUACE

Neexistence robustního a rozšířeného režimu, který by omezoval moderní sledování a zneužívání údajů, je stále častěji také problémem zahraniční politiky. Slabost amerického práva na ochranu soukromí poškozuje národní bezpečnost USA tím, že umožňuje široký prodej citlivých údajů občanů a jejich sdílení s třetími stranami, a to s malou nebo žádnou transparentností či zárukami. Dále je tato situace příčinou nedůvěry v americké technologické firmy v zahraničí. Existuje nespočet legitimních důvodů, proč mají američtí technologičtí giganti problémy s pověstí, od samotné tržní síly a rozsáhlého lobbingu až po umožnění šíření nenávisti na internetu a masivního zneužívání údajů. K charakteristice tohoto jevu se používají výrazy jako například „datový kolonialismus“ a „digitální kolonialismus“ zejména v kontextu, kdy velké technologické firmy vstupují do zemí s nižšími zdroji (např. Venezuela, Uganda, Indie), sledují občany a čerpají veškerou hodnotu zpět do svého sídla, přičemž utvrzují další problémy, jako je například nerovná dělba práce.[17]

Otázky soukromí a ochrany údajů jsou již po desetiletí spornými body ve vztazích mezi USA a EU. EU považuje soukromí komunikací a ochranu osobních údajů za základní práva kodifikovaná v zákonech EU, zatímco federální politika USA chrání některé údaje pouze na základě sektoru. V průběhu let uzavřely Spojené státy a EU několik dohod o předávání údajů (v oblasti obchodních vztahů i v oblasti vymáhání práva), které se snažily řešit obavy EU ohledně postupů USA v oblasti ochrany údajů. Navzdory ujištěním ze strany USA zůstalo mnoho obyvatel EU znepokojeno americkými zákony o zpravodajských službách a dohledu, dále pak možným přístupem vlády USA k osobním údajům občanů EU. Výsledné napětí a právní problémy ovlivnily dohody mezi USA a EU o předávání údajů, ohrozily dvoustranný obchod pro podniky USA a EU a vyvolaly obavy kongresu.[18]

3. 3. 1 CÍLE A PRINCIPY GDPR

GDPR staví na 7 cílech, které pravděpodobně budou inspirací pro budoucí legislativu ve Spojených státech.

- **Legalita, spravedlnost a transparentnost.** Osobní údaje musí být ve vztahu k jednotlivcům zpracovávány zákonným, spravedlivým a transparentním způsobem.
- **Omezení účelu.** Osobní údaje by měly být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely, avšak zpracování pro účely archivace ve veřejném zájmu, vědecký či historický výzkum nebo statistické účely mohou být v souladu s touto zásadou.
- **Minimalizace údajů.** Osobní údaje musí být přiměřené, relevantní a omezené na to, co je nezbytné ve vztahu k účelům, pro které jsou údaje zpracovávány.
- **Přesnost.** Osobní údaje uchovávané zpracovateli a správci by měly být přesné, aktuální a měly by být vymazány nebo opraveny bezodkladně.
- **Omezení ukládání.** Osobní údaje musí být uchovávány ve formě, která umožňuje identifikaci subjektů údajů po dobu ne delší, než je nezbytné, ale mohou být archivovány, pokud je to ve veřejném zájmu nebo pro účely vědeckého a historického výzkumu či statistické účely.

- **Integrita a důvěrnost** (tj. bezpečnost údajů). Osobní údaje musí být zpracovávány způsobem, který zajišťuje bezpečnost a chrání před neoprávněným zpracováním, náhodnou ztrátou, zničením nebo poškozením.

- **Odpovědnost.** Správci údajů musí být odpovědní za dodržování zásad GDPR a musí být schopni je prokázat.

A zároveň poskytuje jednotlivcům několik práv.

- **Právo na informace.** Fyzické osoby mají právo být informovány o shromažďování a používání svých osobních údajů. Správci musí jednotlivcům poskytnout určité informace, včetně účelů zpracování, doby uchovávání a toho, s kým budou údaje sdíleny. Informace musí být stručné, transparentní, srozumitelné, snadno dostupné a podané jednoduchým jazykem.

- **Právo na přístup** (tj. právo na kopii). Fyzické osoby mají právo na přístup ke svým osobním údajům a na získání jejich kopií a správci musí na žádost o přístup odpovědět do jednoho měsíce.

- **Právo na opravu.** GDPR poskytuje fyzickým osobám právo požadovat od správců osobních údajů opravu nepřesných informací nebo doplnění neúplných údajů.

- **Právo na výmaz** (známé také jako „právo být zapomenut“). Fyzické osoby mají v některých případech právo na vymazání svých osobních údajů.

- **Právo na přenositelnost údajů.** Právo na přenositelnost údajů umožňuje fyzickým osobám získat osobní údaje, které poskytly správci, v běžně používaném, strojově čitelném formátu, který lze předat jinému správci, aniž by byla ovlivněna použitelnost údajů.

- **Právo vznést námitku.** Nařízení GDPR dává fyzickým osobám právo vznést námitku proti zpracování jejich osobních údajů v několika případech. Fyzické osoby mají absolutní právo vznést námitku proti zpracování údajů pro účely přímého marketingu.[19]

4. ZÁVĚR – JAKÁ JE BUDOUCNOST TOHOTO TÉMATU

4.1 NA CO SE ZAMĚŘIT

Práva vztahující se k shromažďování a sdílení údajů: stejně, jako je tomu u GDPR, by zákony měly lidem dávat právo zjistit, jaké údaje o nich různé společnosti shromáždily, právo požadovat, aby společnosti shromážděné údaje vymazaly, a právo snadno přenášet údaje z jedné služby do druhé.

Dalším kritickým a často kontroverzním bodem je „opt-in“ souhlas: společnost by se uživatelů měla zeptat, zda může jejich údaje sdílet nebo prodávat třetím stranám. Neměli by trávit hodiny tím, že se budou muset odhlašovat ze shromažďování svých soukromých údajů prostřednictvím každé služby, kterou používají. Alternativou, kterou implementuje například CCPA, je globální opt-out pomocí nastavení v prohlížeči nebo přímo na úrovni zařízení.[20]

Obecně je vhodné čerpat především z GDPR nebo CCPA a zamyslet se nad mírou regulace, kterou by měl zákon zavést. Je přitom vhodné brát v potaz současné obavy i schopnosti amerických občanů, případně si osobně vyzkoušet získat údaje, které o vás nashromáždila některá společnost (např. Facebook).

4.2 REÁLNÁ PŘEDLOHA

Dne 3. června 2022 zveřejnil Výbor pro energetiku a obchod bipartitní návrh zákona s názvem American Data Privacy and Protection Act. Záměrem návrhu zákona je poskytnout komplexní právní předpisy o ochraně osobních údajů včetně vytvoření jednotného národního rámce ochrany osobních údajů a robustního souboru práv na ochranu soukromí spotřebitelů.[21]

Jedná se o vcelku ambiciózní, ale zatím nadějný pokus o komplexní federální zákon, který Spojeným státům tak chybí. Jde ale o kompromis a některé jeho body jsou proto kritizovány. Návrh zákona sice předpokládá výhradní pravomoc federálního práva upravovat ochranu osobních údajů a soukromí, ale obsahuje dlouhý seznam výjimek, kdy právní úprava jednotlivých států bude nadále přetrvávat a tudíž mírně podkopává původní cíl federálního zákona (tj. mít jednotné právní předpisy, aby se snížily náklady na jejich dodržování a zjednodušila se pravidla pro spotřebitele).

4.3 VYMAHATELNOST NOVÝCH ZÁKONŮ

Jednou z hlavních otázek, které vyvolává každý návrh zákona o ochraně osobních údajů, je způsob prosazování nových federálních práv nebo povinností, které by daný návrh zákona ukládal. Jedním z tradičních způsobů vymáhání by byla federální agentura, například Federální obchodní komise nebo Ministerstvo spravedlnosti, a to prostřednictvím občanskoprávních sankcí nebo trestní odpovědnosti. Návrh zákona by také mohl stanovit vymáhání prostřednictvím občanskoprávních žalob podaných ministry spravedlnosti států, případně federálními státními zástupci či státními zástupci jednotlivých států. Vedle těchto metod několik externích komentátorů nedávno vyzvalo k tomu, aby veškeré nové federální právní předpisy o ochraně soukromí zahrnovaly federální právo na soukromou žalobu - právo, které by umožnilo jednotlivcům poškozeným porušením zákona podat žalobu proti narušitelům s cílem získat peněžní odškodnění u federálního soudu.[22]

5. OTÁZKY PRO STANOVISKO

- Jak by tvoje strana/frakce zajistila, aby se běžní uživatelé lépe orientovali v této otázce?
- Podpořila by tvoje strana/frakce spolupráci s EU za účelem zachování toku dat mezi kontinenty (i za cenu přísnějších pravidel pro americké společnosti)?
- Přiklonila by se tvoje strana/frakce spíše k větší regulaci („pro vlastní dobro občanů“), nebo byste se spoléhali na jejich vlastní zodpovědnost?
- Podpořila by tvoje strana/frakce možnost soukromé žaloby, „opt-in“ (také „privacy by default“ přístup) nebo globální „opt-out“?
- Ke které variantě vymáhání zákona by tvoje strana/frakce přiklonila?
- Jaký má tvoje strana/frakce postoj k regulaci velkých korporací?

6. DOPORUČENÉ A ROZŠIŘUJÍCÍ ZDROJE

Články k dalšímu aspektu tohoto tématu
https://www.propublica.org/series/machine-bias

Cambridge Analytica - co nabízela pro vylepšení kampaně Leave.EU https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/BK-Background--paper-CA-proposals-to-LeaveEU.pdf

Cambridge Analytica Scandal
https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you--need-to-know.html

Vliv cílené reklamy
https://www.fastcompany.com/90656170/targeted-ads-arent-just-annoying-they-can-be-harmful-heres-how-to-fight-back,
https://theconversation.com/targeted-ads-isolate-and-divide-us-even-when-theyre-not-political-new-research-163669

7. POUŽITÉ ZDROJE

Context ke Cambridge Analytica
https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and--sport/dr-emma-briant-explanatory-essays2.pdf

US State Privacy Legislation Tracker https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

filmy The Great Hack a The Social Dilemma

EU and U.S. agree to new data-sharing pact
https://www.cnbc.com/2022/03/25/eu-and-us-agree-new-data-transfer-pact-to-replace-privacy-shield.html

American Data Privacy and Protection Act Draft Legislation (Section by Section Summary)
https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E-2B3E50

Inspirace ke zneužívání dat
https://www.invisibly.com/learn-blog/data-misuse-7-examples

7. ZDROJE Z POZNÁMEK V DOKUMENTU

1 DIGITAL AROUND THE WORLD. In: DATAREPORTAL [online]. 2022 [cit. 2022-03-27]. Dostupné z: https://datareportal.com/global-digital-overview#:~:text=4.95%20billion%20people%20around%20the, of%20the%20world%27s%20total%20population

2 JAIKARAN, Chris. Data, Social Media, and Users: Can We All Get Along?. In: Congressional Research Service [online]. 2018-04-04 [cit. 2022-06-29]. Dostupné z: https://crsreports.congress.gov/product/pdf/IN/IN10879

3 Cambridge Analytica: The data firm's global influence. In: BBC News [online]. 2018-03-22 [cit. 2022-06-29]. Dostupné z: https://www.bbc.com/news/world-43476762

4 CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. In: The Guardian [online]. 2017-05-07 [cit. 2022-06-29]. Dostupné z: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

5 Facebook data privacy scandal: A cheat sheet. In: TechRepublic [online]. 2020-07-30 [cit. 2022-06-29]. Dostupné z: https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/

6 FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads. In: Federal Trade Commission [online]. 2022-05-25 [cit. 2022-06-29]. Dostupné z: https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using--account-security-data-sell-targeted-ads

7 RAHNAMA, Hossein a Alex PENTLAND. The New Rules of Data Privacy. In: Harward Bussiness Review [online]. 2022-02-25 [cit. 2022-06-29]. Dostupné z: https://hbr.org/2022/02/the-new-rules-of-data-privacy

8 AUXIER, Brooke, Lee RAINIE a Monica ANDERSON. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. In: Pew Research Center [online]. 2019-11-15 [cit. 2022-07-01]. Dostupné z: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over--their-personal-information/

9 DE PINTO, Jennifer, Fred BACKUS a Kabir KHANNA. POLITICS Americans are skeptical Facebook can protect user data - CBS News poll. In: CBS News [online]. 2018-04-10 [cit. 2022-07-01]. Dostupné z: https://www.cbsnews.com/news/americans-are-skeptical-facebook--can-protect-user-data-cbs-news-poll/

10 ACQUISTI, Alessandro, Laura BRANDIMARTE a George LOEWENSTEIN. Privacy and human behavior in the age of information. In: Science [online]. 2015-01-30 [cit. 2022-07-01]. Dostupné z: https://www.heinz.cmu.edu/~acquisti/papers/AcquistiBrandimarteLoewenstein--S-2015.pdf

11 pozn. 2

12 MULLIGAN, Stephen, Wilson FREEMAN a Chris LINEBAUGH. Data Protection Law: An Overview. In: Congressional Research Service [online]. 2019-03-25 [cit. 2022-07-01]. Dostupné z: https://sgp.fas.org/crs/misc/R45631.pdf

13 KLOSOWSKI, Thorin. The State of Consumer Data Privacy Laws in the US (And Why It

Matters). In: The New York Times: Wirecutter [online]. 2021-09-06 [cit. 2022-07-01]. Dostupné z: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

14 pozn. 12

15 California Consumer Privacy Act (CCPA). In: State of California Department of Justice: Office of the Attorney General [online]. [cit. 2022-07-01]. Dostupné z: https://www.oag.ca.gov/privacy/ccpa

16 CCPA and CPRA. In: International Association of Privacy Professionals [online]. [cit. 2022-07-01]. Dostupné z: https://iapp.org/resources/topics/ccpa-and-cpra/

17 SHERMAN, Justin. Weak US Privacy Law Hurts America's Global Standing. In: Wired [online]. 2021-07-20 [cit. 2022-07-01]. Dostupné z: https://www.wired.com/story/weak-us-privacy-law-hurts-americas-global-standing/

18 FEFER, Rachel a Kristin ARCHICK. U.S.-EU Trans-Atlantic Data Privacy Framework. In: Congressional Research Service [online]. 2022-06-02 [cit. 2022-07-01]. Dostupné z: https://crsreports.congress.gov/product/pdf/IF/IF11613

19 pozn. 12

20 pozn. 13

21 LEWIS, Jackson. Congress Releases Draft Federal Privacy Law with Potential Traction To Pass. In: The National Law Review [online]. 2022-06-21 [cit. 2022-07-01]. Dostupné z: https://www.natlawreview.com/article/congress-releases-draft-federal-privacy-law-potential-traction-to-pass

22 LINEBAUGH, Chris. Enforcing Federal Privacy Law— Constitutional Limitations on Private Rights of Action. In: Congressional Research Service [online]. 2019-05-31 [cit. 2022-07-01]. Dostupné z: https://crsreports.congress.gov/product/pdf/LSB/LSB10303

23 AUXIER, Brooke, Lee RAINIE a Monica ANDERSON. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. In: Pew Research Center [online]. 2019-11-15 [cit. 2022-07-01]. Dostupné z: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over--their-personal-information/

24 Tamtéž

25 CCPA and CPRA. In: International Association of Privacy Professionals [online]. [cit. 2022-07-01]. Dostupné z: https://iapp.org/resources/topics/ccpa-and-cpra/

ČESKÝ MODEL AMERICKÉHO KONGRESU 2022

CENTRUM POLITICKÝCH STUDIÍ, Z. S.
NÁMĚSTÍ JANA PALACHA 2
110 00 PRAHA 1