Ochrana osobních údajů v digitálním světě

Milena Mücková
milena.muckova@amo.cz

JMÉNO: [redacted]

ADRESA: [redacted]

VĚK: [redacted]

RODNÉ ČÍSLO: [redacted]

AMO.CZ

1 ÚVOD

Informační a komunikační technologie jsou v dnešní době nedílnou součástí života každého z nás. Sdílení našeho jména, data narození a dalších údajů na internetu již považujeme za samozřejmost. Méně samozřejmý je však fakt, že pro jiné subjekty není složité získat naše osobní data a nakládat s nimi způsobem, se kterým bychom častokrát nesouhlasili. Díky málo regulované manipulaci s daty jsou například různé firmy schopny získat obrovské množství dat, které mohou využívat dle svých vlastních zájmů. I přes to, že osobní údaje jsou součástí naší identity, jejich význam byl v minulosti častokrát podceňován. Události posledních let však potvrdily, že ochrana osobních údajů v digitálním světě nabírá na důležitosti a je třeba ji neustále přizpůsobovat technickému pokroku.[1]

Tento *background report* si klade za cíl poskytnout delegátům základní přehled v oblasti zpracování osobních údajů a seznámit je se způsoby, kterými mohou být zneužity. Věnuje se legislativě, která je upravuje, a v neposlední řadě nastiňuje situaci v jednotlivých částech světa. Na úplném konci se nachází *Seznam doporučených zdrojů*, které mohou být prvním stavebním kamenem pro psaní stanovisek k jednání.

2 CO JSOU TO OSOBNÍ ÚDAJE?

Definice osobních údajů se často liší, v současnosti je nejvíce rozšířená definice dle evropské legislativy, konkrétně dle *Obecného nařízení o ochraně osobních údajů* (GDPR, podrobněji viz 4.2), podle níž je osobní údaj každá informace, která umožňuje identifikovat konkrétní fyzickou osobu.[2] Samotné určení ale záleží také na šíři kontextu, v němž je daný údaj uveden. Mezi nejčastěji uváděné osobní údaje patří jméno, adresa, trvalé bydliště, věk, pohlaví, datum narození, rodné číslo, e-mailová či IP adresa, telefonní číslo a další.[3] Zvláštní kategorií podle *Obecného nařízení o ochraně osobních údajů* jsou pak citlivé osobní údaje, jejichž zpracování podléhá mnohem přísnějším pravidlům. Patří mezi ně například rasový původ občana, příslušnost k náboženství, biometrické údaje (otisk prstu, snímek obličeje), politické názory nebo sexuální orientace – tedy údaje, jejichž zneužití může občanovi uškodit např. v zaměstnání nebo ve škole, či způsobit jeho diskriminaci.[4]

Profilování je účelové zpracování informací o dané osobě, díky čemuž mohou firmy či jiné subjekty dále předvídat její chování. Například dlouhodobým sledováním polohy mobilního telefonu lze vysledovat bydliště či zaměstnání jeho uživatele.[29]

Ochrana osobních údajů je žádoucí především z důvodu zachování soukromí každého jedince. Snaží se předcházet například profilování, které může odhalit informace, jež bychom nechtěli sdílet. Jedná se o dnes už běžnou metodu používanou v marketingu, především k zacílení reklamy, nicméně nemůžeme vyloučit také například krádež identity, při níž se pachatel pomocí získaných informací vydává za někoho jiného, a jednoduše si tak na jméno dané osoby například půjčí peníze. Obecně se pohybujeme na velmi tenkém ledě v otázce, do kdy je profilování klasifikovatelné jako právo na informace, a kdy už se jedná o zásah do soukromí jedince.[5]

Mezi nejčastěji uváděné osobní údaje patří jméno, adresa, trvalé bydliště, věk, pohlaví, datum narození, rodné číslo, e-mailová či IP adresa, telefonní číslo a další.[30]

Nesmíme zapomínat na fakt, že v každé kultuře je na roli jedince pohlíženo jinak. Mravní, politické i právní standardy každé země jsou utvářeny zejména historickými zkušenostmi a tradicemi, a tudíž se častokrát diametrálně liší. Právě to je pak jedním z důvodů, proč je těžké najít všeobecný konsenzus v definici osobních údajů.

3 ZNEUŽÍVÁNÍ OSOBNÍCH ÚDAJŮ

Zneužívání osobních údajů můžeme obecně rozdělit na dva typy podle toho, kdo s daty pracuje. Buď se může jednat o soukromé firmy, které často nakládají s daty bez vědomí jejich vlastníků, nebo je poskytují třetím stranám. Toto chování by mělo být regulováno státem, avšak ne vždy se tak děje. Na druhou stranu jsou to právě státy, kdo mnohdy narušuje právo na soukromí svých občanů, například monitorováním lidí na soukromých místech nebo pracovištích.

Následující kapitola je věnována dvěma různým případům rozsáhlé manipulace s osobními údaji, které ilustrují, jakým způsobem mohou být data shromažďována a použita z obou pohledů.

3.1 Kauza Cambridge Analytica

Hromadný sběr údajů skrze chytrá zařízení (mobily, notebooky, chytré hodinky, fitness náramky, aj.) se stal trendem poslední doby. Správce údajů získává osobní údaje uživatelů skrze služby, kterých lidé zdarma využívají. Ve skutečnosti tak uživatelé platí svým soukromím, neboť nevědomky umožňují cizím osobám získat jejich údaje. Tyto osoby následně využijí osobní údaje uživatelů k vytvoření dokonale cílené a zpeněžitelné reklamy na míru. Tento postup není nelegální, nicméně je důležité si uvědomit, jaký proces vede k obsahu, který se nám např. na sociálních sítích zobrazuje.[6]

Právě tohoto postupu využila britská společnost Cambridge Analytica, která před americkými prezidentskými volbami v roce 2016 vedla cílenou kampaň na téměř každého amerického občana. Jak něčeho takového mohla dosáhnout? Použila algoritmus, který identifikoval povahu uživatelů Facebooku na základě jejich aktivity. Byl založen na psychologickém testu, který klasifikoval každého Američana v pěti ohledech – míře jeho otevřenosti, extroverzi, pečlivosti, ochoty a neuroticismu. Díky tomuto hodnocení mohla společnost Cambridge Analytica profilovat uživatele velmi přesně. V průměru stačilo 10 „lajků" na odhadnutí člověka lépe, než jej znají jeho kolegové; 150 lajků pro poznání člověka lépe, než jej znají jeho rodiče; a 300 lajků stačilo, aby Cambridge Analytica znala daného uživatele lépe než jeho životní partner. Na základě výsledků byla vytvořena reklama pro více druhů osobností, která pak mohla působit lépe než všeobecně adresovaná propagace.[7]

Samotný postup by byl legální, kdyby společnost získala údaje se souhlasem všech uživatelů, to se však nestalo. Cambridge Analytica získala většinu dat skrz aplikace, které uživatelé používali na základě souhlasu s uložením osobních údajů. Zásadní problém nastal ve chvíli, kdy se nejednalo pouze o jejich vlastní data, ale i o informace jejich přátel na Facebooku, jejichž data byla tím pádem zpracována bez souhlasu. Pomocí této sítě kontaktů mohla společnost zpracovat rozsáhlou škálu informací bez souhlasu většiny jejich majitelů.[8]

3.2 Čínský kreditový systém

Dalším aktuálním příkladem manipulace s osobními daty je tzv. čínský kreditový systém, za nímž (narozdíl od kauzy s firmou Cambridge Analytica) stojí samotná čínská vláda. Sběr dat se stal účinným prostředkem, který umožňuje Čínské lidové republice neustále monitorovat své občany v reálném čase.

Tamější vláda už od roku 2014 postupně vyvíjí automatizovaný mechanismus pro kontrolu svých občanů, který je založen na masivním sběru a analýze osobních údajů.[9] Ty jsou zajišťovány především 170 miliony kamer (do roku 2020 jich Čína plánuje instalovat o dalších 400 milionů více), jež automaticky identifikují tváře.[10] Automaticky generované skóre založené na chování občanů pak má okamžitý vliv na sociální a ekonomický status příslušných osob. Při nízkém kreditu si například nemohou půjčit peníze z banky nebo platí vyšší daně. Naopak vysoký počet bodů je odměněn nízkými úroky a nízkými daněmi. Sankce jdou až do takových extrémů, že při velmi nízkém hodnocení člověk ztrácí právo koupit si například lístek na vlak nebo letenku. Hodnota skóre se odvíjí od čtyř faktorů – dodržování legislativy, ekonomického a sociálního chování a v neposlední řadě také chování v digitálním světě.[11]

Nicméně je třeba si uvědomit, že čínský kreditový systém doposud nefunguje ve svém plném rozsahu a jeho funkce se budou rozšiřovat až do roku 2020, kdy bude spuštěn celoplošně. Navzdory obavám, které potenciální dopady tohoto nařízení vyvolávají v zahraničí, jej čínská vláda popisuje jako efektivní nástroj pro kontrolu trhu. I přes toto tvrzení zneužívání dat čínských občanů představuje obrovské riziko.

4 LEGISLATIVA UPRAVUJÍCÍ OCHRANU OSOBNÍCH ÚDAJŮ

Technický pokrok posledních let přináší neustále nové výzvy v oblasti kybernetické bezpečnosti a pro právo jakožto konzervativní vědu je těžké dostatečně rychle reagovat. Právní normy týkající se ochrany osobních údajů nemají takovou historii jako jiné oblasti lidských práv, a proto je jejich vznik a aplikace časově náročnější.[12]

Právo na ochranu proti zasahování do soukromého života je zakotveno nejen ve *Všeobecné deklaraci lidských práv a svobod* (čl. 12), ale i v *Mezinárodním paktu o občanských a politických právech* (čl. 17), který je narozdíl od *Deklarace* právně závazný. Tyto úpravy jsou však velmi obecné a pro současnou dobu nedostačující. Přestože je míra ochrany osobních dat důležitým faktorem pro mezinárodní spolupráci, její výše se v různých částech světa liší. Pozitivní skutečností je fakt, že v současné době má již 134 států světa nějakou formu ochrany osobních údajů.[13] Žijeme však v globalizované době, kdy je transport dat mezi státy běžnou záležitostí, a právě v tom spočívá problém. I když žijete v zemi, která vaše data chrání dostatečně, neznamená to, že je nemůže zneužít zahraniční firma, které byla poskytnuta. Naše osobní data jsou cennou komoditou, jejíž manipulace stále nemá stanovena žádná plošná pravidla.

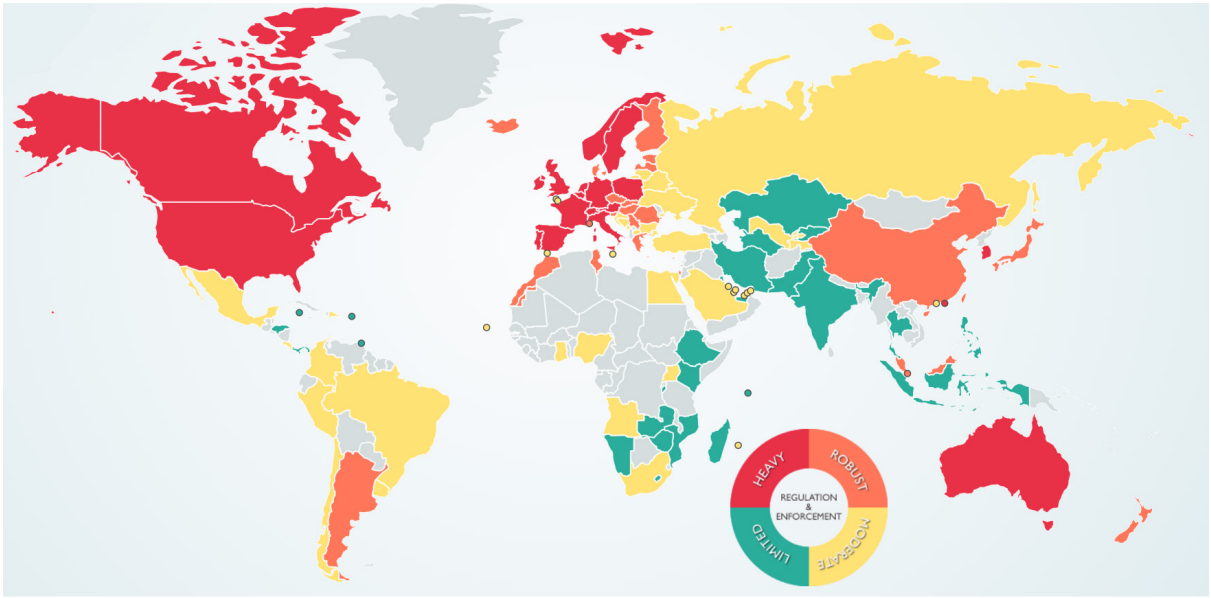
Další problém nastává v situacích, kdy legislativa v daném státě sice existuje, nicméně není správně aplikována a vymáhána – orgány veřejné moci (soudy, policie apod.) ani široká veřejnost nejsou v tomto ohledu dostatečně informováni.

4.1 Úmluva 108

První dokument, který nastínil principy ochrany osobních údajů, byl čl. 8 *Evropské úmluvy o ochraně lidských práv a základních svobod* (1950). Právě na něm staví první ucelený (a pro signatáře závazný) dokument upravující ochranu dat – Úmluva o ochraně osob se zřetelem na automatizované zpracování dat (dále jen Úmluva 108), jež byla schválena Radou Evropy v roce 1981.[14] Doposud ji ratifikovalo již 55 států světa.[15] K úmluvě mohou přistoupit i nečlenské státy Rady Evropy, tudíž mezi jejími signatáři nalezneme i státy jako Senegal či Tunisko.

první ucelený (a pro signatáře závazný) dokument upravující ochranu dat – Úmluva o ochraně osob se zřetelem na automatizované zpracování dat

Úmluva 108 se tak stala odrazovým můstkem nejen pro evropskou legislativu, ale i pro globální šíření digitálních práv. Původní znění Úmluvy 108 definuje základní zásady pro ochranu osobních údajů. Definuje, co lze považovat za osobní údaje a jejich zvláštní skupiny, pro které platí jiná pravidla uchování. Definice těchto základních pojmů jsou obsahově stejné jako v *GDPR* (viz dále). Je důležité zmínit, že Úmluva 108 zavazuje k zavedení pravidel automatizovaného zpracování státy, nikoli právnické osoby. Dále nařizuje státům zřídit úřad, který by se zabýval dodržováním vni-



Obr. 1: Míra ochrany osobních údajů ve světě[31]

Nařízení je jednou z forem právních aktů Evropské unie. Narozdíl od **směrnice** je účinné přímo, členské státy tedy již nepřijímají žádné vlastní tzv. prováděcí zákony. To také znamená, že nařízení platí na celém území Unie jednotně, neliší se ani v detailech.[32]

trostátního právního řádu a sledoval tok informací přes hranice.

V průběhu posledních 10 let tento dokument prošel modernizací. Aby vyhovoval současné době, byl přidán *dodatkový protokol*. Celkově se svým zněním velmi přiblížil *GDPR*, rozšířil práva osob, jejichž údaje jsou zpracovávány – například byla přidána možnost podat stížnost proti automatizovanému zpracování údajů. Důležitým bodem je i posílení kompetencí dozorových úřadů a posílení jejich mezinárodní spolupráce. Mimo to byla odstraněna výjimka, která dovolovala signatářům vynechat některé body Úmluvy při vnitrostátní aplikaci.[16] Kompletní Úmluvu 108 naleznete v doporučených zdrojích.

4.2 GDPR

Obecné nařízení o ochraně osobních údajů (General data protection regulation, GDPR) je nařízení Evropské unie účinné od 25. května 2018, které v současné době poskytuje nejucelenější rámec ochrany osobních údajů na světě.[17] Jeho cílem je co nejkomplexnější ochrana osobních dat občanů EU. Nastavuje pravidla pro všechny firmy, instituce i jedince, které tyto informace zpracovávají, ať už jsou součástí členských států či nikoliv.

GDPR zavádí mnoho nových práv pro občany (tzv. subjekty údajů). Ti mají možnost být informováni nejen o délce a způsobu zpracování svých dat, ale také o jejich příjemci. V praxi to znamená například komplexní online přístup k vlastní zdravotní dokumentaci, posudkům lékařů atd. Nařízení ovšem myslí i na duševní vlastnictví či obchodní tajemství, kterým jsou uděleny výjimky. Občané mají rovněž právo na tzv. „výmaz", které jim umožňuje vznést námitku proti zpracování nebo odvolat svůj souhlas, nebo na přenositelnost údajů, díky které lze převést osobní údaje od jednoho poskytovatele k druhému, a vyhnout se tak vyplňování nových formulářů.[18]

Mezi výhody *GDPR* patří rozhodně vymahatelné sankce (velmi často likvidační pokuty), větší informovanost občanů či kontrola vlastních údajů. V praxi pak dochází například ke zredukování nevyžádaných telefonátů nebo reklamních newsletterů od společností, pro něž nebylo složité získat kontaktní údaje velké masy lidí. Na druhou stranu hlavní negativní dopady pociťují především malé firmy, pro které mohou být náklady spojené s administrativní stránkou nařízení neúnosné. Pokud firma zpracovává data na základě souhlasu subjektů, musí být schopna dostatečně informovat své zaměstnance i klienty a zároveň tyto souhlasy uchovávat pro pozdější doložení.[19]

Význam *GDPR* ovšem přesahuje hranice Evropy. EU jakožto největší obchodní blok na světě změnou vlastních pravidel fungování digitálního trhu nepřímo ovlivňuje i způsob ochrany osobních údajů v jiných státech. Na jedné straně se tak děje přímo: EU nyní podmiňuje nové obchodní dohody dorovnáním standardu ochrany osobních údajů. Druhou klíčovou cestou je vlastní rozhodnutí globálních firem fungujících na digitálním trhu. Ty jsou tlačeny k úpravě svých pravidel, aby nepřišly o významné evropské zákazníky.[20]

4.3 Situace v dalších částech světa

Jižní Amerika

Ve většině zemí Jižní Ameriky existovaly různé formy ochrany dat už před *GDPR*. První zemí, která schválila komplexní předpisy, bylo Chile, které již v roce 1999 zahrnulo ochranu osobních údajů do individuálních práv ve své ústavě.[21] I přes to, že byl tento článek ústavy v roce 2018 pozměněn, stále nedefinuje pojem osobní údaje, formy jejich zpracování, ani nezavádí žádné kontrolní mechanismy.

Nejvýznamnější kroky doposud učinila Brazílie, kde byl loni schválen nový zákon upravující 40 předešlých předpisů týkající se ochrany dat, *Lei Geral de Proteção de Dados (Obecný zákon o ochraně údajů)*.[22] Tento zákon v základu vychází z *GDPR*, nicméně rozšiřuje svou působnost i na všechny právnické osoby, které nakládají s údaji obyvatel Brazílie. Ti musí být seznámeni s tím, jak jsou jejich údaje shromažďovány, na jak dlouho a proč. Kromě toho musí být informace zničeny, pokud je společnost dále nepotřebuje. Sankce za porušení jsou stanoveny na 2 % ročního obratu firmy.[23]

Asie

Státy jihovýchodní Asie (např. Singapur, Malajsie, Thajsko) patří mezi nejrychleji se vyvíjející region v oblasti digitálních inovací a s rozvojem digitálního obchodu se mnohonásobně zvýšilo i množství dat, se kterými mohou místní firmy nakládat. Většina států tak začala po vzoru Evropské unie implementovat zákony vycházející z *GDPR*, snažíce se zajistit přetrvání obchodních styků. Například v Japonsku se podařilo dosáhnout reciproční smlouvy s Evropskou unií, která umožňuje volný tok informací mezi těmito státy.[24]

Nedávné aféry úniků dat ve světě však vedly k tomu, že některé země jdou v ochraně osobních údajů svých občanů ještě dál. Například Vietnam schválil velice kontroverzní zákon, který vyžaduje, aby technologické firmy jako Google nebo Facebook uchovávaly data o občanech na území Vietnamu a zároveň je byly schopny předat Ministerstvu veřejné bezpečnosti, pokud o ně požádá.[25] Obdobná legislativa se postupně rozšiřuje do stále více států.

Afrika

Klíčovým právním dokumentem na území Afriky je v současné době Úmluva o kybernetické bezpečnosti a ochraně osobních údajů schválená Africkou unií v roce

2014, která reaguje na rozvoj mezinárodního obchodu a šíření dostupnosti internetu v afrických státech.[26] Signatáři se zavazují ke zřízení závazných regulačních opatření v oblasti kybernetické bezpečnosti a mimo jiné tato Úmluva navrhuje vytvoření regionálního monitorovacího mechanismu. Doposud však tento dokument podepsalo pouze 14 států a ratifikovalo jen 5.[27]

5 DOSAVADNÍ KROKY HRC

Rada pro lidská práva se tématem práva na soukromí v digitálním světě zaobírá dlouhodobě. Významným krokem posledních let bylo stanovení tříletého mandátu Zvláštního zpravodaje v oblasti práva na soukromí v roce 2015, který byl rezolucí z roku 2018 prodloužen. Do náplně jeho práce patří shromažďování informací o aktuálním dění a jejich předávání Radě pro lidská práva. Dále zajišťuje prostor pro diskuzi mezi soukromými firmami a vládami, v neposlední řadě identifikuje problémy v jednotlivých státech a navrhuje možná řešení a doporučení. Jeho komentáře k situaci v různých zemích jsou pak pro HRC klíčovým zdrojem. Příkladem jeho práce může být otevřený dopis adresovaný Indii, v němž komentoval vývoj tamější legislativy, nebo kritika aktivit národních agentur na území Jižní Koreje.[28] Jednou za rok pak předkládá obsáhlou výroční zprávu Valnému shromáždění OSN, ve které jmenuje konkrétní problémy a výstupy ze své činnosti.

6 SHRNUTÍ BACKGROUNDU A VÝSTUP Z JEDNÁNÍ

Manipulace s osobními údaji se v posledních letech stala velmi frekventovanou praktikou, jejíž regulace stále nebyla jasně stanovena. Mezinárodní tok informací je v digitálním světě běžnou praxí, ale jejich ochrana se může napříč zeměmi výrazně lišit, a proto je třeba apelovat na členské státy Organizace spojených národů, aby pracovaly na jejím sjednocení.

Radu pro lidská práva na XXV. ročníku Pražského studentského summitu čeká nelehký úkol. Je zapotřebí, aby vypracovala a schválila rezoluci, která bude reflektovat aktuální situaci v digitálním světě. Výsledný dokument by měl nastavit stejná kritéria pro chování všech členských států a určit, jak by měly s daty svých občanů nakládat. Mimo to může definovat pojmy, které byly zmíněny v background reportu, nebo pracovat s náplní mandátu Zvláštního zpravodaje, jehož dosavadní aktivity mohou být inspirací pro další body rezoluce. Naskýtá se zde rovněž příležitost zaměřit se na státy, které porušují základní lidská práva svých občanů, a cílit některé body přímo na ně.

8 DOPORUČENÉ A ROZŠIŘUJÍCÍ ZDROJE

https://www.dlapiperdataprotection.com/index.html

– přehled ochrany dat v jednotlivých státech, ideální pro první seznámení se se situací v zastupovaném státě

https://privacyinternational.org/type-resource/explainers

– videa od neziskové organizace Privacy International přehledně vysvětlující klíčové pojmy

https://www.gdpr.cz/

– průvodce GDPR

https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

– stránky Zvláštního zpravodaje pro právo na soukromí

dokument The Great Hack

– režie Karim Amer, Jehane Noujaim. USA. 2019

7 OTÁZKY PRO JEDNÁNÍ

1. V čem se liší právo na ochranu osobních údajů od jiných, všeobecných lidských práv?
2. Chrání váš stát osobní údaje svých občanů? Jak?
3. Jak by měla vypadat přiměřená regulace zpracování dat soukromými firmami?
4. S jakou definicí osobních údajů jste ochotni souhlasit?

SEZNAM POUŽITÝCH ZDROJŮ

1 Proč potřebuje Evropa lepší ochranu osobních dat. Obecné nařízení o ochraně osobních údajů—prakticky. [online]. [cit. 2019-07-10]. Dostupné z: https://www.gdpr.cz/gdpr/proc/

2 What is personal data? European Commission. [online]. [cit.2019-07-10]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

3 Tamtéž

4 Co jsou to dle GDPR osobní údaje? GDPR Solutions. [online]. [cit. 2019-07-10]. Dostupné z: https://www.gdprsolutions.cz/narizeni-gdpr/osobni-udaje/

5 2.8 Ochrana osobních údajů. Základy IT gramotnosti. [online]. [cit. 2019-07-11]. Dostupné z: https://is.muni.cz/do/1492/el/sitmu/law/html/ochrana-osobnich-udaju.html

6 Tamtéž

7 BBC: Facebook data: How it was used by Cambridge Analytica [online]. 9. 4. 2018. [cit. 2019-7-30]. Dostupné z: https://www.bbc.com/news/av/technology-43674480/facebook-data-how-it-was-used-by-cambridge-analytica

8 What is Cambridge Analytica scandal? YouTube [online]. 20. 3. 2018. [cit. 2019-07-30]. Dostupné z: https://www.youtube.com/watch?v=Q91nvbJSmS4

9 BOTSMAN, Rachel. Big data meets Big Brother as China moves to rate its citizens. WIRED UK [online]. 21. 10. 2017 [cit. 2019-09-06]. Dostupné z: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

10 LIU, Joyce. In Your Face: China's all-seeing state. BBC [online]. 10. 12. 2017 [cit. 2019-9-6]. Dostupné z: https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state

11 MEISSNER, Mirjam. China's social credit system [online]. 2017. [cit. 2019-07-30]. Dostupné z: https://www.merics.org/sites/default/files/2017-09/China%20Monitor_39_SOCS_EN.pdf

12 SPÁČIL, Michal. Svět hardware [online]. 6. 9. 2013. [cit. 2019-07-30]. Dostupné z: https://www.svethardware.cz/internet-a-ochrana-osobnich-udaju-1-cast/38179

13 GREENLEAF, Graham. Countries with Data Privacy Laws - By Year 1973-2019. [online]. 3. 6. 2019. [cit. 2019-08-10]. Dostupné z: https://ssrn.com/abstract=3386510

14 Rada Evropy. Úřad pro ochranu osobních údajů [online]. [cit. 2019-07-31]. Dostupné z: https://www.uoou.cz/rada-evropy/ds-1797/archiv=0 & p1=1659

15 Chart of signatures and ratifications of Treaty 108. Council of Europe [online]. [cit. 2019-07-30]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

16 NONNENMANN, František. Modernizace Úmluvy 108, základního nástroje Rady Evropy pro ochranu osobních údajů. Epravo.cz [online]. [cit. 2019-07-31]. Dostupné z: https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html

17 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. [cit. 2019-

07-31]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679 & from=CS

18 Jaká práva dává GDPR nám jako občanům

Obecné nařízení o ochraně osobních údajů prakticky. [online]. [cit. 2019-07-30]. Dostupné z: https://www.gdpr.cz/gdpr/prava/.

19 Jaké zásadní změny GDPR přinese.

Obecné nařízení o ochraně osobních údajů prakticky. [online]. [cit. 2019-07-31]. Dostupné z: https://www.gdpr.cz/gdpr/zmeny/.

20 SCOTT, Mark a Laurens CERELUS. Europe's new data protection rules export privacy standards worldwide. Politico [online]. [cit. 2019-09-26]. Dostupné z: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/

21 State of Privacy Chile. Privacy International [online]. 2019 [cit. 2019-09-06]. Dostupné z: https://privacyinternational.org/state-privacy/28/state-privacy-chile

22 State of Privacy Brazil. Privacy International [online]. 2019 [cit. 2019-09-06]. Dostupné z: https://privacyinternational.org/state-privacy/42/state-privacy-brazil

23 Tamtéž

24 The European Union and Japan agreed to create the world's largest area of safe data flows. European Union. 17. 8. 2018. [online]. [cit. 2019-08-10]. Dostupné z: https://europa.eu/rapid/press-release_IP-18-4501_en.htm

25 HIEBERT, Murray. Vietnam's New Cyber Law Could Hobble Foreign Investors and Limit Basic Freedoms. CSIS [online]. 2. 7. 2018 [cit. 2019-09-06]. Dostupné z: https://www.csis.org/analysis/vietnams-new-cyber-law-could-hobble-foreign-investors-and-limit-basic-freedoms

26 African Union Convention on Cyber Security and Personal Data Protection. African Union[online]. [cit. 2019-08-10]. Dostupné z: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

27 Tamtéž

28 Special Rapporteur on the right to privacy. OHCHR [online]. [cit. 2019-08-10]. Dostupné z: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

29 2.8 Ochrana osobních údajů. Základy IT gramotnosti. [online]. [cit. 2019-07-11]. Dostupné z: https://is.muni.cz/do/1492/el/sitmu/law/html/ochrana-osobnich-udaju.html

30 What is personal data? European Commission. [online]. [cit.2019-07-10]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

31 DLA Piper [online]. [cit. 2. 8. 2019]. Dostupné z: https://www.dlapiperdataprotection.com/index.html?t=world-map & c=AO

32 Druhy právních předpisů EU. Evropská komise [online]. [cit. 2019-09-26]. Dostupné z: https://ec.europa.eu/info/law/law-making-process/types-eu-law_cs

Pražský studentský summit

Pražský studentský summit je unikátní vzdělávací projekt existující od roku 1995. Každoročně vzdělává přes 300 studentů středních i vysokých škol o současných globálních tématech, a to především prostřednictvím simulace jednání tří klíčových mezinárodních organizací – OSN, NATO a EU.

studentsummit.cz
summit@amo.cz
facebook.com/studentsummit
instagram.com/praguestudentsummit
twitter.com/studentsummit
youtube.com/studentsummit

Asociace pro mezinárodní otázky (AMO)

AMO je nevládní nezisková organizace založená v roce 1997 za účelem výzkumu avzdělávání v oblasti mezinárodních vztahů. Tento přední český zahraničně politický think-tank není spjat s žádnou politickou stranou ani ideologií. Svou činností podporuje aktivní přístup k zahraniční politice, poskytuje nestrannou analýzu mezinárodního dění a otevírá prostor k fundované diskusi.

Milena Mücková

Autorka je spolupracovnicí Asociace pro mezinárodní otázky a členem přípravného týmu Pražského studentského summitu.

POŘADATEL

AMO.CZ

GENERÁLNÍ PARTNER

The Kellner Family Foundation

TOP PARTNEŘI

Ministerstvo zahraničních věcí České republiky

PRAHA PRAGUE PRAGA PRAG

VŠE Vysoká škola ekonomická v Praze

Evropská komise
Zastoupení v České republice

METROPOLITNÍ UNIVERZITA PRAHA

US embassy

PARTNEŘI

UNIVERZITA KARLOVA V PRAZE

SCIO

Embassy of Canada
Ambassade du Canada

AUTO ZRUCKÝ
DEALER NISSAN

Městská část Praha 6

PRAGUE
CONGRESS CENTRE

UNITED NATIONS
Informační centrum OSN v Praze

T · ·

leo express

Microsoft

OSCE

MEDIÁLNÍ PARTNEŘI

HOSPODÁŘSKÉ NOVINY

RESPEKT

Autor: Milena Mücková
Imprimatur: František Novotný, Tomáš Rezek
Jazyková úprava: Karolína Oškerová, Tereza Novotná, Anna Zadražilová, Jakub Drahorád
Sazba: Michaela Nováková
Grafická úprava: Jaroslav Kopřiva

Vydala Asociace pro mezinárodní otázky (AMO) pro potřeby XXV. ročníku Pražského studentského summitu.

Asociace pro mezinárodní otázky (AMO)
Žitná 27, 110 00 Praha 1
Tel.: +420 224 813 460, e-mail: summit@amo.cz
IČ : 65 99 95 33

www.amo.cz
www.studentsummit.cz