https://doi.org/10.5817/RPT2024-1-1

FLUKTUACE UŽIVATELSKÝCH DAT JAKO RIZIKO PRO SOUKROMÍ

JAKUB KLODWIG[1]

ABSTRAKT

Článek přistupuje ke koncovým zařízením jako k bráně propojující uživatele a kyberprostor, přičemž analyzuje a kategorizuje relevantní datové toky. Jednotlivé kategorie dat jsou diskutovány a klasifikovány v kontextu ochrany osobních údajů a práva na ochranu soukromí v elektronických komunikacích. Autor na příkladech demonstruje rizika spojená s jednotlivými druhy dat a konkrétní praxi jejich šíření z koncového zařízení mimo dispozice koncových uživatelů.

KLÍČOVÁ SLOVA

Koncové zařízení; koncový uživatel; soukromí; osobní údaje; uživatelská data; aplikace; trackery; třetí strana; cookies; předávání osobních údajů

ABSTRACT

The paper approaches end-user devices as a gateway connecting users and cyberspace, analyzing and categorizing relevant data flows. The different categories of data are discussed and classified in the context of eprivacy and personal data protection. The author uses examples to demonstrate the risks associated with each type of data category and the specific practice of disseminating it from end-user devices beyond the control of end-users.

[1] JUDr. Jakub Klodwig je doktorandem Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a koncipientem v advokátní kanceláři HAVEL & PARTNERS. Kontaktní email: klodax@gmail.com

KEY WORDS

Terminal device; end user; privacy; personal data; user data; apps; trackers; third party; cookies; transfer of personal data

1. ÚVOD

Tendence integrování informačních technologií do různých sfér života v 21. století přináší jejich uživatelům mnoho nových funkcí a výhod, ale nese s sebou také nové hrozby, kterým je nezbytné věnovat pozornost. Jednou z nich je také stále se zvyšující množství produkovaných dat, které vzniká ve stále vyšší kvalitě. Odhaduje se, že jen za poslední dva roky bylo vygenerováno 90 % světových dat a od roku 2010, kdy byly globálně vytvořeny zhruba 2 zettabyty dat, se toto číslo zvýšilo odhadem 60krát.[2] Obdobně například podle studie Dell Technologies Global Data Protection Index z roku 2021 soukromé společnosti spravují desetinásobný objem dat, než jakým disponovaly v roce 2016.[3]

Ačkoliv jsou data vytvářena primárně za účelem uspokojování potřeb jejich adresátů, jsou data také něčím, co může člověka omezovat ba i ohrožovat. Na rozdíl od světa fyzického, v kyberprostoru a ve všech elektronických zařízeních vznikají data o činnosti uživatelů. Tzv. digitální stopa[4] zůstává po téměř jakékoliv interakci s koncovým zařízením[5] někde elektronicky zaznamenána. Na rozdíl od fyzického světa tak koncová za-

[2] DUARTE, Fabio. Amount of Data Created Daily (2024). In: *Exploding Topics* [online] [cit. 27. 3. 2024]. Dostupné z: https://explodingtopics.com/blog/data-generated-per-day

[3] DELL TECHNOLOGIES. *Global Data Protection Index 2021: Key Findings*. 2021, s. 30. [online]. [cit. 28. 3. 2024]. Dostupné z: www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-keyfindings.pdf

[4] SEDLÁČEK, Jakub. Digitální stopa: Konec empirické sociologie? In: *Czech Sociological Review*. [online]. 2020, roč. 56, č. 4, s. 472. Dostupné z: https://search.ebscohost.com/login.aspx?authtype=ip&custid=s8431878&profile=eds

[5] Pojem „*koncové zařízení*“ je definován v čl. 1 písm. a) Směrnice Komise 2008/63/ES ze dne 20. 6. 2008 o hospodářské soutěži na trhu s telekomunikačními koncovými zařízeními jako „*zařízení přímo nebo nepřímo připojené k rozhraní veřejné telekomunikační sítě, které může vysílat, zpracovávat nebo přijímat informace; připojení přímé či nepřímé může být provedeno kabelově, za použití optického paprsku nebo elektromagnetických vln; připojení je nepřímé, jestliže je mezi rozhraní sítě a koncové zařízení připojeno další zařízení*“. Jakkoliv byla tato definice prvotně vytvořena pro prostředí telekomunikační sítě, lze ji dnes použít pro koncová zařízení v internetové síti.

řízení, prostřednictvím nichž v kyberprostoru lidé interagují do jisté míry permanentně, vytvářejí potenciál ke sledování nebo analyzování jejich činnosti. Tento datový potenciál ale může být snadno zneužit.

Cílem tohoto článku je proto analyzovat datové toky v osobních koncových zařízeních uživatelů a navrhnout kategorizaci těchto dat. Popsání a rozřazení dat vznikajících v koncových zařízeních pomůže identifikovat potenciální hrozby z pohledu ochrany osobních údajů a ochrany soukromí v elektronických komunikacích a bude sloužit pro další výzkum ochrany soukromí v koncových zařízeních.

2. ZDROJE DAT

S rozvojem smartphonů, wearables a obecně osobních koncových zařízení[6] rychle roste množství a také druhy dat, které jsou o uživatelích shromažďovány.[7] Data jsou často generována například měřením sensorů a čidel, jiná data uživatelé do koncových zařízení sami dobrovolně zadávají a další data vznikají při samotném používání zařízení. Je však třeba si uvědomit, že ne všechna data vytvořená aktivitou uživatele prostřednictvím koncového zařízení v koncovém zařízení zůstávají. Existuje totiž velké množství dat, které fyzicky vznikají mimo koncové zařízení, ačkoliv je k nim přistupováno prostřednictvím koncového zařízení. Tuto distinkci je nezbytné udělat a rozlišit tak různé druhy dat, aby nebyly opomenuty jejich specifické aspekty a mohly být pak také řádně právně subsumovány.

Koncová zařízení již dávno nefungují jen samostatně[8] natož izolovaně, ale jsou denně nástrojem mnoha interakcí uživatele na webových stánkách, sociálních sítích anebo v řadě jiných aplikací, pro které koncové zařízení

[6] Osobními koncovými zařízeními pro účely tohoto článku rozumíme taková koncová zařízení, která jsou vytvořena primárně pro používání jedním uživatelem, jakými jsou typicky smartphony nebo wearables.

[7] CENA, Federica. RAPP, Amon. LIKAVEC, Silvia. MARCENGO, Alessandro. Envisioning the future of personalization through personal informatics: A user study. *International Journal of Mobile Human Computer Interaction* [online]. 2018. roč. 10. č. 1, s. 52. ISSN 1942-390X. [cit. 27. 3. 2024]. Doi:10.4018/IJMHCI.2018010104

[8] Samostatnost je v tomto kontextu uvažována jako překonaná, jelikož je dnes běžné, že si uživatelé stahují do svých koncových zařízení řadu aplikací, doplňků či rozšíření expandujících paletu funkcionalit. Je tedy běžné, že jsou koncová zařízení doplňována a propojována s dalšími produkty třetích stran.

(potažmo jeho software) slouží jako platforma. Koncové zařízení pro uživatele představuje pomyslnou bránu do kyberprostoru a k řadě dalším cílům, které zde může uživatel chtít realizovat, zjistit či využít. Veškerá aktivita uživatele prostřednictvím koncového zařízení může být zaznamenávána a dále zpracovávána, zejména při využití softwaru třetích stran.[9] Data a aktivity uživatele totiž přesahují rámec koncového zařízení a velké skupiny dat jsou generovány prostřednictvím aktivity uživatele na koncovém zařízení v prostředí třetích stran. Je proto nutné rozlišovat zdroj, povahu a také právní režim dat, které díky koncovému zařízení vznikají.

Stejně jako koncové zařízení může být chápáno jejich uživateli jako vstupní brána do kyberprostoru, je i z perspektivy dalších subjektů koncové zařízením využíváno jako klíč k monitorování, získávání a analyzování konkrétních lidí. Proto je nezbytné rozlišovat data v koncovém zařízení podle jejich původu, a tedy rozlišovat následující zdroje dat:

1. Data vytvořená uživatelem
2. Data vytvořená koncovým zařízením
3. Data vytvořená aplikací nainstalovanou v koncovém zařízení
4. Data vytvořená webovou stránkou, načtenou z koncového zařízení[10]

První skupinou dat, která se na koncovém zařízení vyskytují jsou data, která uživatel do koncového zařízení sám vloží. Vstup od uživatele přitom může mít více forem, a to jak manuální (ruční uložení telefonního čísla a jména), verbální (namluvení záznamu do mikrofonu), tak i například data do zařízení uživatelem importovaná ze zařízení jiného. Nemusí se tedy jednat o data původně vytvořená samotným uživatelem, ale může se jednat také o data, která již dříve existovala v jiném zařízení. I ta mají totiž z pohledu koncového zařízení svůj původ odvozený právě od samotného uživatele a jeho aktivity mimo dané koncové zařízení.

[9] Uživatelé běžně spouštějí a využívají počítačové programy a software třetích stran, který neprovozují a který je pro ně neznámý. Tím může docházet k produkci nových dat o používání softwaru tímto uživatelem v prostředí třetích stran.

[10] KLODWIG, Jakub. Wearables a právo na informační sebeurčení. In: *CyberCon 2023*. Vyžádaná přednáška. Brno.

Data vytvořená uživatelem jsou typicky ta zadaná při prvním spuštění koncového zařízení a jeho nastavování. Může se však jednat i o běžné vyplňování formulářů, registraci či přidávání kontaktů na jiné uživatele. Tyto vstupy uživatele zahrnují také psaní zpráv, natáčení videí a další různá data, které uživatel vědomě vytváří.

Druhá skupina dat zahrnuje všechna data, vytvořená v koncovém zařízení. Jedná se tedy o data, která zařízení vytvoří při činnosti uživatele (data o uživatelově aktivitě jako je záznam EKG, počet kroků uživatele, monitoring jeho spánku, metadata vyfocených fotografií etc.), ale zahrnuje také data, která zařízení vytvoří samo prostřednictvím vlastních čidel a sensorů (gyroskop, lokalizační údaje, aktuální stav baterie, přítomnost paměťové karty etc).

Třetí skupina dat není tvořena ani uživatelem, ani koncovým zařízením, ale jinou třetí stranou, jejíž software byl do koncového zařízení přidán. Data jsou sice vytvořená také v koncovém zařízení, ale nikoliv v samotném softwaru vlastního koncového zařízení. Jejich vznik je iniciován a řízen externím kódem aplikace, vyvinuté často jiným subjektem, která byla do koncového zařízení přidána. Aplikace jsou na koncová zařízení instalovány zpravidla z online obchodů typu App Store či Google Play. Uživatel při jejich instalaci uzavírá s daným subjektem smlouvu zpravidla akceptací obchodních podmínek. Smlouva a přídatná dokumentace pak upravuje pravidla spolupráce, užívání aplikace uživatelem a také slouží k předání informací uživateli, včetně informací o rozsahu zpracování osobních údajů.

Poslední, čtvrtá skupina zahrnuje data, která vzniknou, pokud se koncové zařízení připojí prostřednictvím webového prohlížeče na webové stránky. Surfování na internetu je tak z pohledu koncového zařízení specifické v tom, že prostřednictvím aplikačního programu druhé strany (tzn. webového prohlížeče) je přistupováno do prostředí dalšího, třetího subjektu. Při přistupování na webovou stránku vznikají technická data, která jsou nezbytná pro uskutečnění samotného načtení webové stránky. Velmi podstatné jsou ale data, která vytvoří načtená webová stránka po tom, co se k nim koncové zařízení připojí. Zde je totiž největší potenciál pro získávání dat o koncovém zařízení a potažmo o koncovém uživateli samotném.

Uživatel se totiž pohybuje v prostředí třetí strany, která má mnoho možností, jak své prostředí nastavit, tak aby z přistoupivšího koncového zařízení získala co nejvíce dat. Může se přitom jednat jak o data již dostupná v koncovém zařízení, tak i data, která si webová stránka vytvoří na základě interakcí uživatele na webové stránce. Množství, charakter i použití těchto dat je pak fakticky v rukou provozovatele webové stránky.

V porovnání s předchozí skupinou dat však v tomto případě není uzavírána mezi uživatelem a provozovatelem webu žádná smlouva, která by podmínky takového zpracování dat upravovala. Uživatel nemusí znát subjekt provozující danou webovou stránku a často si ani nemusí být samotné technické interakce při načtení webové stránky na pozadí vědom. V případě vytvoření dat ze čtvrté skupiny je tak obecně nižší oprávněné očekávání uživatele, že bude do jeho soukromí třetím subjektem zasahováno.

Z tohoto důvodu zůstává stanovování pravidel pro webové stránky a jejich snahy o vytěžení dat uživatele prostřednictvím jeho koncového zařízení převážně na právní úpravě ochrany soukromí v elektronických komunikacích,[11] potažmo na právní úpravě ochrany osobních údajů.[12] Uživatel totiž nemusí být fakticky se čtením a ukládáním dat do jeho koncového zařízení srozuměn, nemusí znát subjekt, který tak činí, nedochází k žádné kontraktaci a zpravidla není tato nevyváženost ani jinak kompenzována.[13]

---

[11] Konkrétně tuto problematiku upravuje § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Prodrobněji viz KLODWIG, Jakub. Pokročilé metody identifikace koncových zařízení. In: *COFOLA 2020*: *Sborník příspěvků mladých právníků, doktorandů a právních vědců* [online]. Brno: Muni Press, s. 1092. ISBN 978-80-210-9670-7. [cit. 28. 3. 2024]. Dostupné z: https://www.law.muni.cz/sborniky/cofola/2020/cofola2020.pdf

[12] Osobní údaje jsou definovány dle čl. 4 odst. 1 GDPR jako *„informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*. Rozsah tohoto pojmu byl vyložen v rozsudku *(Anon. 2016)* a podrobněji o této problematice např. v KLODWIG, Jakub. Wearables a ochrana soukromí. In: *Obchodněprávní revue*. 2021, Nakladatelství C.H. Beck, roč. 13, č. 3, s. 230-236. ISSN 1803-6554. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpw64s7gnpxgxzsgeza&groupIndex=3&rowIndex=0&refSource=search

3. DATA V KONCOVÉM ZAŘÍZENÍ

Digitální stopa, která se vytváří při používání koncového zařízení uživatelem má velký potenciál uživatele identifikovat. To je významné zejména proto, že osobním údajem podle čl. 4 odst. 1 GDPR je *„informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*.

Podle uvedené definice se o zpracování osobních údajů nebude jednat například při zpracování dat ze silničního senzoru pro měření rychlosti větru a jejich předávání elektronické dopravní tabuli, která zobrazí řidičům upozornění v případě překročení určité hodnoty. Není totiž možné za pomoci těchto dat v koncovém zařízení ani nepřímo za pomoci jiných dat identifikovat fyzickou osobu. Naopak záznam kamerového systému sloužícího ke kontrole SPZ nebo data o použití firemní čipové karty pro otevírání dveří v kancelářské budově osobními údaji pravděpodobně budou.[14] Není přitom jediným kritériem, zda je na základě těchto dat konkrétní osoba schopná subjekt osobních údajů identifikovat, ale, jak již bylo dovozeno judikaturou Soudního dvora Evropské unie, pro splnění definice osobního údaje stačí, pokud existují jiné prostředky díky nimž lze konkrétní osobu identifikovat při vynaložení přiměřených prostředků nepřímo.[15] Tento výklad definice osobních údajů je přitom značně extenzivní, jelikož často

[13] Příkladem takového opatření ke zvýšení ochrany soukromí a informovanosti uživatelů je například povinnost aplikací vytvářet Politiku soukromí, aby mohly být uživatelům nabízeny ke stažení na online tržištích jako jsou zejména App Store nebo Google Play. Viz APPLE INC. App Privacy Details in the App Store. In: *Apple Developer*. [online] [cit. 28. 3. 2024]. Dostupné z: https://developer.apple.com/app-store/app-privacy-details/ a GOOGLE, INC. Play Console Help - User Data - Privacy Policy [online]. *Policy center*. 2024 [cit. 28. 3. 2024]. Dostupné z: https://support.google.com/googleplay/android-

[14] Obdobně tak i identifikátor koncového zařízení jako je identifikační číslo vozidla (VIN) lze považovat za osobní údaj. Viz Rozsudek SDEU ze dne 9. listopadu 2023, ve věci C-319/22, Gesamtverband Autoteile-Handel eV proti SCANIA CV AB. ECLI:EU:C:2023:837. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=279492&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=746319

může nutit subjekty nakládat „z opatrnosti“ jako s osobními údaji nejen s daty, ze kterých oni sami nejsou schopni konkrétní fyzickou osobu identifikovat, ale také s daty, u nichž není jisté, zda skutečně osobními údaji jsou.[16]

Nicméně i osobní koncová zařízení mohou generovat data, která nebudou mít povahu osobních údajů. Zda se jedná o osobní údaj je nutné vždy posoudit v kontextu konkrétní situace. Příkladem lze ale zmínit statistické údaje o průměrné době využívání zařízení po delší časový úsek, nebo také data o střední hodnotě využívaného jasu od výroby zařízení. Tyto statistické údaje nemají téměř žádný potenciál v různých situacích uživatele identifikovat. Údaj totiž během daného období integruje data o dílčích interakcích a může průměrovat údaje za dobu užívání zařízení i několika po sobě následujícími majiteli zařízení. Identifikovatelnost konkrétní osoby v těchto případech tak může být u dat generovaných osobním koncovým zařízením vyloučena.

Také při zpracování dat systémem koncových zařízení typu chytré domácnosti, ve kterých žije větší množství osob, bude méně pravděpodobné, že budou generovaná data identifikovat konkrétní fyzickou osobu. Produkovaná data totiž budou převážně referenční k celé skupině osob žijících v dané domácnosti jako celku, a nikoliv jen k jedné fyzické osobě. Naopak koncová zařízení, která běžně používá jediná osoba, osobní údaje pravděpodobně generovat budou. Zpravidla totiž bude existovat nějaký subjekt, který bude disponovat daty o tom, kdo vlastní či užívá dané koncové zařízení. Tím může být například výrobce dané značky elektroniky, mobilní operátor či poskytovatel služeb internetového připojení. Ačkoliv

[15] Po rozsudku *SDEU ze dne 24. listopadu 2011, ve věci C-70/10 Scarlet Extended SA. [online]. ECLI:EU:C:2011:771. Dostupné z: https://hudoc.echr.coe.int/eng?i=001-58497*, který označil statické IP adresy jako osobní údaje, jelikož umožňují určení totožnosti uživatele, bylo v případu viz Rozsudek SDEU ze dne 19. října 2016, ve věci C-582/14, Patrick Breyer proti Bundesrepublik Deutschland. [online]. ECLI:EU:C:2016:779. Dostupné z: https://hudoc.echr.coe.int/eng?i=001-58497 dovozeno, že i dynamické IP adresy jsou osobními údaji. Podmínkou ale je, že poskytovatel internetového připojení nebo správci místních sítí mohou tohoto uživatele při vynaložení přiměřených prostředků identifikovat díky použití dalších informací potřebných k identifikaci uživatele internetové stránky.

[16] WP29, 2007. *Opinion 4/2007 on the concept of personal data* [online]. 20. červen 2007. [cit. 28. 3. 2024]. Dostupné z: http://ec.europa.eu/justice_home/fsj/privacy/index_en.html

tedy identifikátory koncových zařízení nemají apriori osobní povahu, získávají tuto povahu ve vztahu k jakékoli osobě, která má k dispozici prostředky, jež jí rozumně umožňují spojit tento údaj s konkrétní osobou.

V praxi tak lze mobilní telefon identifikovat prostřednictvím telefonního čísla, laptop díky http cookies, nebo chytré hodinky díky úvodní tapetě s fotkou.[17] Regulace osobních údajů tak dopadá na každou z výše uvedených skupin dat, ačkoliv na každou z nich jiným způsobem.

4. SPECIFIKA JEDNOTLIVÝCH SKUPIN DAT V KONCOVÉM ZAŘÍZENÍ

Na první skupinu dat vytvořených uživatelem v koncovém zařízení se při zpracování uživatelem často uplatní výjimka pro fyzické osoby zpracovávající osobní údaje v průběhu výlučně osobních či domácích činností dle čl. 2 odst. 2 písm. c) 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 (dále jen „**GDPR**“). Za domácí se přitom považuje činnost prováděná v soukromí jako je například nahrání si vlastního zpěvu uživatele za účelem následného zhodnocení vlastního projevu a jeho zlepšování. Pod zmíněnou výjimku ale lze v určitých situacích podřadit také činnost prováděnou na veřejnosti nebo dokonce v rámci výkonu povolání.[18] V každém případě se však musí jednat o činnost ve prospěch uživate-

[17] Navíc pokud budou dvě koncová zařízení, která vlastní a využívá jeden uživatel, komunikovat a integrovat data, jež tato zařízení vyprodukují, budou velice pravděpodobně identifikovat právě činnost této osoby, a budou tudíž osobními údaji. KLODWIG, Jakub. Wearables a ochrana soukromí. In: *Obchodněprávní revue*. 2021, Nakladatelství C.H. Beck, roč. 13, č. 3, s. 230-236. ISSN 1803-6554. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpw64s7gnpxgxzsgeza&groupIndex=3&rowIndex=0&refSource=search

[18] Rozsudek ESLP ze dne 16. února 2000, ve věci Amann V. Switzerland. [online]. Dostupné z: https://hudoc.echr.coe.int/eng?i=001-58497; RÁMIŠ, Vladan. Článek 2 Věcná působnost. In: *Obecné nařízení o ochraně osobních údajů* [online]. Praha: C. H. Beck, s. 66–68 [cit. 28. 3. 2024]. Dostupné z: https://www.beck-online.cz/bo/document-view.seam?documentId=nnptembsgbpwk232ge3tqltdnqza#

le, a nikoliv jakékoliv jiné třetí osoby. Tato výjimka se tak neuplatní pro zpracování osobních údajů provozovateli aplikací a webových stránek.

Vzhledem k tomu, že první skupina vzniká v koncovém zařízení z vůle uživatele, jedná se o data, která jsou vytvářena transparentně a pod dohledem uživatele. Existence těchto dat, stejně jako míra jejich citlivosti je uživatelům (na rozdíl od ostatních skupin dat) zcela zřejmá a mohou tomu přizpůsobit i nakládání s nimi. Ačkoliv se citlivost těchto dat může velmi různit v závislosti na jejich povaze, lze předpokládat, že se bude často jednat o velmi citlivé osobní údaje. Kromě samotného uživatele a softwaru v koncovém zařízení ale nejsou tyto údaje apriori zpracovávány žádným dalším subjektem, a proto nejsou ze své povahy významně ohrožovány.

Druhá skupina dat, vytvořených osobním koncovým zařízením má podobný režim jako první skupina dat s tím rozdílem, že existuje ještě vyšší pravděpodobnost, že se bude jednat o osobní údaje, ba dokonce o zvláštní kategorie osobních údajů podle čl. 9 GDPR. Data vytvářená osobním koncovým zařízením totiž často vznikají v souvislosti s aktivitou uživatele, což může vést k jeho minimálně nepřímé identifikaci. Pokud tedy koncové zařízení zaznamenává pohybovou aktivitu uživatele, lze z času a místa uskutečněné aktivity uživatele snadno identifikovat. Navíc jakékoliv údaje získané z těla uživatele typu tepové frekvence, délky nebo rozboru spánku jsou všechno údaje pevně spjaty s osobou uživatele a mohou mít obecně vyšší citlivost než první skupina dat.

Tento závěr podporuje také skutečnost, že osobní údaje v druhé skupině dat mohou vznikat automatizovaně, bez aktivního vstupu či vědomí uživatele, a to pravidelně a dlouhodobě. Po uživateli tak může zůstávat například kompletní záznam jeho polohy, podrobnosti o jeho spánku, nebo údaje o jeho uskutečněných hovorech, včetně jejich délky a příjemců. Může se tak jednat o relativně velké množství komplexních údajů, které jsou v osobním koncovém zařízení shromažďovány, a to včetně osobních údajů,

které by za jiných okolností lékaři zapisovali do zdravotní dokumentace.[19] To vytváří relativně velké riziko pro soukromí uživatele a potenciál pro zneužití. Výhodou této skupiny dat je, že se na jejich tvorbě apriori nepodílí žádná třetí strana. Absence třetí strany při tvorbě dat umožňuje uživateli tyto data lépe chránit a bránit jejich zpracování před externími subjekty.

To však platí o poznání méně u třetí skupiny dat, která vznikají prostřednictvím aplikací nainstalovaných na koncovém zařízení.[20] Aplikace totiž dle zjištění průzkumů dosud ve velké míře sdílejí data včetně citlivých osobních údajů se třetími subjekty[21] a často nedodržují regulaci ochrany soukromí a osobních údajů, na což upozorňují některé neziskové organizace, včetně NOYB – European Center for Digital Rights.[22] Častým nedostatkem je například zpracování osobních údajů uživatelů bez toho, aniž by aplikace měly nějaký zákonný důvod pro zpracování osobních údajů nebo se i pokusily získat jejich souhlas.[23] Získaná data navíc aplikace sdílejí

[19] Zda se jedná o běžné koncové zařízení, na které dopadá obecná právní úprava, nebo o zdravotnický prostředek, který musí naplňovat podstatně vyšší sektorové požadavky medicínského práva, závisí zejména na účelu, k jakému je dané zařízení určeno. Nezávisí tak na tom, kolik funkcí dané zařízení má, zda je softwarem či hardwarem nebo jaká data zpracovává, jako spíše na marketingové strategii prodejce a prezentaci zařízení jeho výrobcem.

[20] V průzkumu aplikací na jednotlivých operačních systémem včetně různých verzí Androidu bylo zjištěno, že i při minimální konfiguraci a nečinnosti, předinstalované aplikace z koncového zařízení zasílají značné množství dat třetím stranám jako je např. Google, Microsoft, LinkedIn nebo Facebook Viz. HANDSETS, Realme. LIU, Haoyu. PATRAS, Paul a LEITH, Douglas. Android Mobile OS Snooping By Samsung, Xiaomi, Huawei and Realme Handsets. In: *semanticscholar.org* [online]. [cit. 28. 3. 2024]. s. 12. Dostupné z: https://www.semanticscholar.org/paper/Android-Mobile-OS-Snooping-By-Samsung%2C-Xiaomi%2C-and-Handsets-Liu/993c4e5cbe8151fd426d08ac606ea5daa6c78605

[21] JIN, Haojian. LIU, Minyi. DODHIA, Kevan. LI, Yuanchun. SRIVASTAVA, Gaurav. FREDRIKSON, Matthew. AGARWAL Yuvraj a HONG, Jason. Why Are They Collecting My Data?: Inferring the Purposes of Network Traffic in Mobile Apps. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* [online]. Roč. 2. č. 4, s. 2. ISSN 2474-9567. Doi:10.1145/3287051

[22] NOYB – EUROPEAN CENTER FOR DIGITAL RIGHTS, 2023. How mobile apps illegally share your personal data. *NOYB* [online] [cit. 28. 3. 2024]. Dostupné z: https://noyb.eu/en/how-mobile-apps-illegally-share-your-personal-data

[23] BINNS, Reuben. ZHAO, Jun. VAN KLEEK, Max. SHADBOLT, Nigel. Measuring third party tracker power across web and mobile. *ACM Transactions on Internet Technology*. 2018. roč. 18. č. 4; ZIMMECK, Sebastian. STORY, Peter. SMULLEN, Daniel. RAVICHANDER, Abhilasha. WANG, Ziqi. REIDENBERG, Joel. RUSSELL, Cameron a SADEH, Norman. MAPS: Scaling Privacy Compliance Analysis to a Million Apps. *Proceedings on Privacy Enhancing Technologies* [online]. 2019, s. 66–86. Doi:10.2478/popets-2019-0037

se třetími stranami, a to v nikoliv zanedbatelném rozsahu. Průzkum švýcarské společnosti pCloud International AG z roku 2021 například odhalil, že 52 % ze vzorku aplikací vybraných v Apple Store[24] sdílí získaná data se třetími stranami.[25] Takto sdílená data, která často zahrnují i osobní údaje se tak snadno šíří mimo koncové zařízení a dostávají se do dispozice dalších subjektů. Tato zjištění poukazují na riziko pojící se s třetí skupinou dat. Na rozdíl od prvních dvou skupin, které nejsou bez dalšího v dispozici třetí strany, jsou výše uvedené průzkumy důkazem, jak flagrantně provozovatelé aplikací porušují soukromí uživatelů a data z třetí skupiny šíří mimo koncové zařízení, a tedy i faktické dispozice uživatele.

Nejedná se přitom o problém pouze aplikací dostupných v Apple Store, ale podle jiného průzkumu reprezentativního vzorku celkem 1297 aplikací, které jsou zdarma dostupné i na britském Google Play, průměrná aplikace zkontaktuje již při svém spuštění 4,7 dalších subjektů, a to ještě před jakoukoliv interakcí s uživatelem.[26] Přičemž 10 % ze vzorku nejpoužívanějších aplikací na tom bylo ještě hůře a kontaktovalo průměrně alespoň 7 různých subjektů. Nejčastěji kontaktovaným subjektem byla společnost Alphabet Inc. (mateřská společnost Google LLC IPA) a to celkem od 58,6 % aplikací.[27]

Obecně zaznamenaný trend ukazuje, že aplikace velice často kontaktovaly své provozovatele, tedy přímo společnosti, které aplikace vyvíjejí a udržují. Takových aplikací bylo 856, což odpovídá více než 71 %. Tato

[24] Aplikace byly v Apple Store vybírány na základě štítků ochrany osobních údajů, přičemž byly zkoumány tyto kategorie: „Reklama třetích stran“ a „Reklama a marketing vývojáře“.

[25] DIMITROV, Ivan. Invasive apps. In: *pcloud.com* [online] 2021. [cit. 28. 3. 2024]. Dostupné z: https://www.pcloud.com/invasive-apps

[26] Vzhledem k tomu, že v průzkumu byly zkoumány identifikátory koncových zařízení (tzv. trackers), tak se dokonce velmi pravděpodobně jednalo o zpracování osobních údajů. Viz KOLLNIG, Konrad. BINNS, Reuben. DEWITTE, Pierre. VAN KLEEK, Max. WANG, Ge. OMEIZA, Daniel. WEBB, Helena. SHADBOLT, Nigel. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. *Seventeenth Symposium on Usable Privacy and Security*. 2021. ISSN 978-1-939133-25-0. s. 187.

[27] KOLLNIG, Konrad. BINNS, Reuben. DEWITTE, Pierre. VAN KLEEK, Max. WANG, Ge. OMEIZA, Daniel. WEBB, Helena. SHADBOLT, Nigel. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. *Seventeenth Symposium on Usable Privacy and Security*. 2021. s. 187. ISSN 978-1-939133-25-0.

statistika tak ukazuje na vysoce pravděpodobně úmyslnou non-compliance provozovatelů aplikací, kteří nastavují své aplikace tak, aby z nich vytěžily co nejvíce informací o jejich uživatelích a mohli je dále zužitkovat nebo potenciálně také zpeněžit.

Pouze 9,9 % aplikací v daném průzkumu nějakým způsobem žádalo uživatele o udělení souhlasu s použitím identifikační metody a 12,2 % aplikací alespoň v nějakém rozsahu plnila svoji informační povinnost.[28] Selhávání celého systému pak dokresluje, že většina aplikací, které souhlas sbíraly tak činily pod nátlakem na uživatele. Konkrétně 43,7 % z aplikací, které souhlas sbíraly, tak nedávaly uživateli jinou možnost než zaškrtnout souhlas, bez alternativy pro odmítnutí. Dalších 20,2 % aplikací sice možnost souhlas neudělit poskytovaly, ale v případě neudělení se okamžitě ukončily. Pouze 42 aplikací (odpovídajících 3,5 % z posuzovaného celku) umožňovalo uživateli použít aplikaci i bez udělení souhlasu s použitím identifikační metody.[29]

Uvedené průzkumy ukazují rizika, která se s používáním aplikací a tvorbou třetí skupiny dat pojí. Prezentovaná míra porušování soukromí koncových uživatelů je nanejvýš vážná a uživatelé by o ni měli být informováni. Bez povědomí uživatelů a širší veřejnosti o tom, jak provozovatelé aplikací nakládají s daty totiž lze jen stěží očekávat, že by se mohla situaci vyvíjet ve prospěch ochrany soukromí uživatelů nebo se alespoň přestala dále zhoršovat.

Dalším vypozorovaným trendem při pozorování ochrany soukromí a osobních údajů v koncových zařízeních je totiž zhoršování situace jednotlivých aplikací v čase. Bylo prokázáno, že při porovnávání jednotlivých aplikací v čase a zaznamenaných úniků dat, kdy jsou zohledňovány druhy dat, počet míst, na nichž se uniklá data objevila a zda byla zašifrována, tak je vypozorovaná tendence výrazně negativní. Pouze 26,3 % z celkových více než 500 pozorovaných aplikací zlepšilo své zabezpečení uživatelských

[28] Ibidem.

[29] Ibidem s. 188.

dat. V téměř dvojnásobku aplikací (konkrétně 51,1 % z nich) se ochrana soukromí jejich uživatel zhoršila.[30]

Při vytváření, čtení a dalším zpracování uživatelských dat aplikacemi tedy snadno dochází k ventilování dat z koncového zařízení dalším subjektům. Jakákoliv data zpracovaná aplikací tak mohou být analyzována a sdílena často bez dodržení zákonných parametrů. Aplikace tak sbírají a sdílejí osobní údaje včetně uživatelského obsahu, historie zadaných hesel ve vyhledávání nebo například dat o navštěvovaných webových stránkách. Průzkum porovnávající rozsah sdílených dat o uživatelích mezi aplikacemi, za tímto účelem vymezil následující kategorie dat:

1. Údaje o nákupech
2. Lokalizační údaje
3. Kontaktní údaje
4. Adresář kontaktů
5. Uživatelský obsah
6. Historie vyhledávání
7. Navštívené webové stránky
8. Identifikátory
9. Metadata o používání aplikace
10. Diagnostická data
11. Citlivé osobní údaje
12. Údaje o finančních transakcích
13. Zdravotní osobní údaje
14. Další údaje[31]

[30] REN, Jingjing. LINDORFER, Martina. DUBOIS, Daniel. RAO, Ashwin. CHOFFNES, David a VALLINA-RODRIGUEZ, Narseo. Bug Fixes, Improvements, ... and Privacy Leaks - A Longitudinal Study of PII Leaks Across Android App Versions. In: *Network and Distributed System Security Symposium*: *Proceedings 2018 Network and Distributed System Security Symposium* [online]. 2018. San Diego, CA: Internet Society [cit. 28. 3. 2024]. s. 2. ISBN 978-1-891562-49-5. Doi:10.14722/ndss.2018.23143

[31] Volný překlad názvu kategorií autorem. Originální znění v angličtině viz DIMITROV, Ivan. Invasive apps. In: *pcloud.com* [online] 2021. [cit. 28. 3. 2024]. Dostupné z: https://www.pcloud.com/invasive-apps

Co se pak týče počtu kategorií osobních údajů, tak nejvíce kategorií sdílí se třetími stranami aplikace sociálních sítí jako je Instagram (11 ze 14 kategorií), Facebook (8 ze 14 kategorií), nebo LinkedIn (7 ze 14 kategorií). Mezi deseti nejinvazivnějšími aplikacemi se pak kromě těchto tří aplikací umístily postupně ještě Uber Eats, Trainline, Youtube, Youtube Music, Deliveroo, Duolingo a eBay.[32]

V praxi se tak například při každém spuštění videa přes aplikaci Youtube sdílí se třetími stranami lokalizační údaje, kontaktní údaje, historie vyhledávání, údaje o navštívených webových stránkách, identifikátory a metadata o užívání aplikace. Tyto data jsou využívány k cílení reklam, které se před, během nebo po přehrání videa uživateli zobrazí, ale také mohou být předány či prodány jiným subjektům, které pak na uživatele lépe zacílí svoji reklamu na dalších stránkách, platformách a na sociálních sítích.[33] Některé aplikace dokonce umožňují sledovat činnost uživatelů i mimo vlastní aplikaci a obohacují tak shromážděné údaje o ještě více informací o chování a o zájmech uživatelů.[34]

Vzhledem k odvozenosti dat vznikajících v aplikaci koncového zařízení od jejího uživatele, bude i třetí skupina dat často obsahovat osobní údaje. Data ale nebudou zpravidla odvozena od hodnot naměřených na těle uživatele, jako spíše vzniknou jeho interakcí s aplikací, a tudíž se nebude pravděpodobně tak často jednat o zvláštní kategorie osobních údajů dle čl. 9 GDPR, jako u předchozí skupiny dat. Vzhledem k tomu, že jejich vznik je určen provozovatelem aplikace, neuplatní se na jejich zpracování provozovatelem výjimka z GDPR. Zásadním rozdílem oproti dvojici předchozích skupin dat je ale vznik těchto dat v rámci dispozice třetí strany, která dle dostupných průzkumů překvapivě často neplní své zákonné povinnosti. Ačkoliv tedy data z třetí skupiny dat nemusí být tak citlivá jako druhá skupina dat, jsou tato data snadno zneužívána provozovateli aplikací a dochází

[32] DIMITROV, Ivan. Invasive apps. In: *pcloud.com* [online] 2021. [cit. 28. 3. 2024]. Dostupné z: https://www.pcloud.com/invasive-apps

[33] Ibidem.

[34] NOYB – EUROPEAN CENTER FOR DIGITAL RIGHTS, 2023. How mobile apps illegally share your personal data. *NOYB* [online] [cit. 28. 3. 2024]. Dostupné z: https://noyb.eu/en/how-mobile-apps-illegally-share-your-personal-data

k jejich unikání mimo koncové zařízení a faktické dispozice jejich uživatelů.

Poslední z vymezených zdrojů je skupina dat, vytvořená webovou stránkou, načtenou z koncového zařízení. Aby mohl uživatel z koncového zařízení na web přistupovat, potřebuje použít webový prohlížeč. Provozovatel webového prohlížeče na koncovém zařízení je v pozici provozovatele aplikace a tedy tzv. druhé strany. Provozovatel webových stránek, na které se koncové zařízení prostřednictvím prohlížeče připojí je pak vůči uživateli koncového zařízení v pozici třetího subjektu, který nemá s uživatelem apriori žádný přímý právní vztah. Přesto však díky aktivitě uživatele na webové stránce může o uživateli za určitých podmínek vytvářet a zpracovávat nové osobní údaje, ale také přistupovat k údajům již uloženým v koncovém zařízení.

Obecně lze tak rozlišit dva druhy dat a sice data interní (pocházející z prvních dvou zdrojů, uvedených výše), která vznikají nebo jsou zpracovávána v koncovém zařízení uživatele (dále jen „**interní data**“) a data externí, která o uživateli vytváří jiné subjekty včetně provozovatelů nainstalovaných aplikací a provozovatelů webových stránek, které koncové zařízení načetlo (dále jen „**externí data**“).

Obdobně jako aplikace jsou webové stránky zpravidla pod správou jiného subjektu, který její prostředí vytváří, přizpůsobuje a spravuje tak i její technické nastavení. Situace je ve vztahu ke koncovým zařízením stejná v tom smyslu, že se aktivita uživatele realizuje v prostředí jiného subjektu, který tuto aktivitu může snadno monitorovat a vytvářet na základě ní cenná externí data. Odlišnost naopak spočívá v tom, že zatímco při užívání aplikace je software stažený a nainstalovaný do samotného koncového zařízení, obsah webové stránky je uložený a spuštěný na jiném zařízení a koncové zařízení si jeho obsah prostřednictvím webového prohlížeče a internetové sítě pouze načte a zobrazí.

Webové stránky mají také na rozdíl od aplikací, které má uživatel nainstalované v koncovém zařízení zpravidla za jedním konkrétním účelem, širší pole využití. Jak aplikace, tak i webové stránky mají možnost vytvářet vlastní externí data v závislosti na různých aspektech interakce s uživate-

lem. Právě variabilnější obsah webových stránek, zahrnující zpravidla řadu různých podstránek s různými tématy, nebo texty v rámci jedné domény protkané hypertextovými odkazy, umožňují vytvářet širší škálu údajů o uživateli.

Tento potenciál je navíc podpořený volnějším vztahem mezi provozovatelem a uživatelem. K instalaci aplikace do koncového zařízení uživatele bývá nutné, aby spolu provozovatel aplikace a uživatel uzavřeli smlouvu (např. akceptací obchodních podmínek). Jinak je tomu při pouhém surfování na webových stránkách, kdy k podpisu smlouvy nebo jiné formální interakci mezi provozovatelem webu a uživatelem není apriori důvod.[35] Provozovatel webu a uživatel tak spolu mají volnější vztah, který lze za normálních okolností přirovnat ke vztahu nakladatelství, které vydává denní tisk a kolemjdoucími, kteří si mohou jeho výtisky zdarma rozebrat. Kolemjdoucí si může a nemusí vzít a přečíst výtisk, stejně jako si uživatel může a nemusí načíst a přečíst obsah webové stránky.

Platformy jako je App Store nebo Google Play navíc stanovují vlastní požadavky pro aplikace, aby pro uživatele vytvořily Politiky soukromí, v nichž uživatele povinně informují nejen o identitě správce, ale také o zpracování osobních údajů, jejich předávání a o právech subjektů údajů. Přičemž není možné, aby aplikace politiku soukromí neměla, jelikož pokud aplikace Politiku soukromí do Google Play či App Store nenahraje, nemůže být aplikace přes tato globálně rozšířená tržiště aplikací vůbec nabízená.[36]

Zatímco provozovatelé aplikací jsou fakticky nuceni vytvářet Politiky soukromí a uživatele informovat o nezbytných parametrech zpracování, tak provozovatelé webových stránek čistě fakticky tuto podmínku ze strany prohlížečů nemají. Právní úprava jim sice povinnost informovat své uživatele za určitých okolností stanovuje,[37] ale mnoho provozovatelů webových

[35] Smlouvy mohou být uzavírány pak v návaznosti na obsah webové stránky a například nákup zboží na daném e-shopu. Nikoliv však apriori pro přístup na webovou stránku.

[36] COOKIE-SCRIPT. Privacy Laws for Apps: How to Protect User Data? In: *Cookie-script.com* [online]. [cit. 28. 3. 2024]. Dostupné z: https://cookie-script.com/blog/privacy-laws-for-apps-how-to-protect-user-data

[37] Viz čl. 13 GDPR a § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů.

stránek tuto povinnost stejně neplní.[38] Téměř 40 % oblíbených webových stránek v Evropě ještě v roce 2019 nezobrazovala[39] požadavek na udělení souhlasu, a i z těchto webových stránek dalších 8 % stránek neobsahovalo odkaz na Privacy policy.[40] V praxi se tak ukazuje být efektivnější požadavek tržišť s aplikacemi jakožto norma definiční autority,[41] která nemůže být na dané platformě nesplněna.

Na rozdíl od aplikací tak uživatel nemusí ani vědět, kdo je provozovatelem webové stránky, kterou si načetl, a přesto je to právě provozovatel webové stránky, kdo má nejlepší pozici pro získávání dat o uživateli. Existuje totiž velké množství způsobů, jak načtení webové stránky nastavit tak, aby bylo o přistupujícím koncovém zařízení (a potažmo také o jeho uživateli), zjištěno co nejvíce údajů.[42] Díky dispozici s technickým nastavením webové stránky a s jejím načítáním mohou provozovatelé docílit automatického čtení dat z přistupujících koncových zařízení, ukládání dat do koncových zařízení a vytváření mnoha různých identifikátorů, které podrobně zmapují pohyb uživatele na webové stránce a vytvoří velké množství dat

[38] Z obchodní analýzy společnosti consentmanager.net mapující pomocí crawleru 100 000 nejnavštěvovanějších webových stránek v Evropě vyplývá, že cookies používá 96 % webových stránek. Průměrně webová stránka ukládá 17 různých cookies, z čehož jsou pouze 4 cookies z kategorie nezbytně nutných cookies. I přesto používá profesionální cookies banner pouze 27 % z nich, přičemž toto číslo se významně liší mezi jednotlivými státy (DE 36 %, DK 50 %, FR 35 %, UK 41 %, PL 32 %, SE 38 %). Reálné procento stránek, které používá cookie banner bude ovšem vyšší o stránky, které používají cookie banner, který si sami navrhly, nebo použily některý z open source řešení. Je však otázkou, zda jsou tyto online zdarma dostupná řešení souladná se zákonnými požadavky a nakolik reflektují správné rozřazení cookies do jednotlivých kategorií. Viz WINKER, Jan, Competition Analysis of Consentmanager.net 2023.

[39] UTZ, Christine. DEGELING, Martin. FAHL, Sascha. SCHAUB, Florian a HOLZ, Thorsten. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: *Conference on Computer and Communications Security*: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [online]. 2019. New York, NY, USA: Association for Computing Machinery, s. 973. [cit. 28. 3. 2024]. ISBN 978-1-4503-6747-9. Dostupné z: doi:10.1145/3319535.3354212

[40] Ibidem, s. 976.

[41] Více o fakticitě definičních norem viz LESSIG, Lawrence. *Code: Version 2.0*. New York: Basic Books. 2006. ISBN 978-0-465-03914-2.

[42] TOMÍŠEK, Jan, Jak regulovat cookies v nařízení ePrivacy. *Revue pro právo a technologie* [online]. 2023. roč. 14, č. 27, s. 243. ISSN 1805-2797. Doi:10.5817/RPT2023-1-5

o interakcích uživatele na webové stránce aniž by si toho musel být uživatel vědom.[43]

Tomuto ztotožňování je nutné se dále věnovat, jelikož jak uživatel přesouvá svoji aktivitu do kyberprostoru v čím dál větším rozsahu, nabývá i jeho online aktivita a její analýza stále většího významu. Výhodné pro provozovatele webových stránek také je, že výsledky této analýzy mohou být v reálném čase rovnou zužitkovány k zobrazování obsahu na webové stránce. Obsah tak může být pro každého uživatele vybírán, aby byl relevantní a stránka tak více atraktivní.

Motivaci pro poskytovatele webových stránek zvyšuje i možnost interaktivity webové stránky, kdy zobrazený obsah nebo reklama může uživatele prostřednictvím hypertextového odkazu rovnou přenést na kýženou webovou stránku a tam svůj zájem projevit, tzn. realizovat nákup, přečíst si daný obsah nebo se například přihlásit k odběru newsletteru. Možností využití dat vytvořených webovou stránkou je celá řada a neustále se rozvíjí.

Zásadní v kontextu ochrany soukromí je, že data vytvořená webovou stránkou a mnoho dalších dat získaných z koncového zařízení provozovatelé webových stránek užívají nejen sami pro své vlastní účely, ale také k jejich masivnímu šíření a vzájemnému sdílení s řadou dalších třetích stran. Britský průzkum z roku 2021 tak například odhalil, že medián počtu identifikátorů třetích stran na jedné webové stránce byl 315.[44] Stačil tedy jediný průchod webovou stránkou, aby byla vytvořena data o uživatelově aktivitě a rozšířena k dalším více než třem stovkám subjektů, přičemž uživatel nemusí znát provozovatele webové stránky a ani si nemusí být samotného sledování vědom. O to spíše je alarmující, jestliže budou na této webové stránce ukládány identifikátory stovek jiných třetích stran a data o uživatelově aktivitě jim budou předávána. Kombinace těchto faktorů

[43] Povinnost provozovateli webové stránky uživatele informovat přidává až právní úprava, avšak technicky lze identifikátory do koncového zařízení nahrát naprosto bez vědomí uživatele.

[44] Číslo přitom vychází pouze z počtu stran, o kterých webové stránky samy informují. Viz NOUWENS, Midas. LICCARDI, Ilaria. VEALE, Michael. KARGER, David a KAGAL, Lalana. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* [online]. 2020. [cit. 28. 3. 2024]. Doi:10.1145/3313831.3376321

a velkého potenciálu komercializace získaných dat způsobuje enormní hrozbu pro ochranu soukromí v koncovém zařízení.

Ačkoliv tedy ani čtvrtá skupina dat co do citlivosti zřejmě nepřekoná druhou skupinu dat, je tato skupina výjimečná širokou paletou různých dat, která může obsahovat a nízkou transparentností pro samotné uživatele. Obdobně jako provozovatelé aplikací také provozovatelé webových stránek nezřídka nedodržují své povinnosti plynoucí z regulace ochrany soukromí a osobních údajů. Data od provozovatelů webových stránek jsou ale také rozsáhle sdílena s řadou dalších subjektů. Vzhledem k tomu, že provozovatelé mohou za určitých okolností získat i interní data z prvních dvou skupin, je tento potenciál fluktuace dat z koncových zařízení velkou hrozbou pro ochranu soukromí.

5. ZÁVĚR

V tomto článku bylo koncové zařízení označeno za pomyslnou vstupní bránu propojující uživatele s obsahem a službami ať již přímo v koncovém zařízení, v aplikacích nebo na webových stránkách, na které může uživatel prostřednictvím koncového zařízení přistupovat. Ačkoliv je tento vztah n zírán řadou uživatelů jako jednostranný, kdy uživatelé takto získávají informace, služby a produkty, jsou to i provozovatelé aplikací a webových stránek, kteří skrze koncové zařízení přicházejí na své.

Data v koncovém zařízení byla proto rozdělena podle jejich původu na čtyři základní skupiny. První skupinou jsou data, která vytváří sám uživatel a do koncového zařízení je například importuje či nahrává. Jedná se o transparentní skupinu dat, která má sice přímou výpověď o soukromých záležitostech uživatele, ale uživatel má o jejím zpracování dobrý přehled a může tomu přizpůsobit i své jednání. Druhou kategorií jsou data vytvořená koncovým zařízením zpravidla při interakci s uživatelem, která mají velký potenciál nebýt „jen“ osobními údaji jako ostatní skupiny, ale velice často také některou ze zvláštních skupin dle čl. 9 GDPR. Vznikají totiž pravidelně, automatizovaně a dlouhodobě, často bez vědomí nebo dohledu uživatele např. ve formě snímání tepové frekvence chytrými hodin-

kami. Jejich častá odvozenost od těla samotného uživatele a dlouhodobost jejich snímání vede k velké citlivosti této skupiny dat.

První dvě skupiny dat mají společné homogenní prostředí koncového zařízení bez apriorního přístupu programových prostředků jiného subjektu, což se ukázalo jako velmi významné pro možnost jejich ochrany. Díky tomu, že takto vzniklá data jsou uložena a zpracována v samotném koncovém zařízení, jedná se o interní data, na jejichž zpracování uživatelem se často může použít výjimka z věcné působnosti GDPR pro zpracování osobních údajů pro výlučně osobní či domácí činnosti.

Třetí skupinou jsou pak data vytvořená aplikací, která byla do koncového zařízení nainstalována a jedná se tedy o program cizího subjektu přidaný do koncového zařízení na základě smlouvy. Aplikace přistupují jak k interním datům, tak i vytvářejí vlastní externí data. Jak bylo zjištěno, aplikace ale také nadměrně komunikují externí data z koncového zařízení. Data jsou skrze aplikace sdíleny nejen s vlastními provozovateli aplikace, ale také s řadou třetích stran, a to dokonce i při minimální konfiguraci a nečinnosti koncového zařízení. To vytváří velké riziko pro soukromí koncových uživatelů, kteří tak často nevědomky o soukromí svých dat nezvratně přichází.

Posledním druhem dat v tomto kontextu jsou data vytvořená webovými stránkami, na které uživatel přistupuje přes webový prohlížeč. Tento vztah, ačkoliv může být pro běžného uživatele nejčastější, je poměrně komplikovaný, jelikož do něj vstupují další dva aktéři. Koncové zařízení totiž prostřednictvím softwaru webového prohlížeče (pod správou druhé strany) načítá webové stránky třetích stran. Data vytvořená webovou stránkou na základě aktivity uživatele prostřednictvím koncového zařízení jsou vytvářena a ukládána na serverech provozovatele webové stránky mimo koncové zařízení. Interakce mezi provozovatelem webové stránky a koncovým zařízením jsou navíc fakticky pod správou provozovatele webového prohlížeče. Tento druh vzniku externích dat byl při uvážení absence kontraktu mezi uživatelem a provozovatelem webové stránky, množství dat, které o uživateli vzniká mimo koncové zařízení, častém nedostatku informací o jejich zpracování, vlivu dalšího subjektu spravujícího nastavení interakcí

mezi uživatelem a webovou stránkou, a zejména velmi snadné využitelnosti pro další zpracování, šíření a zužitkování, označen za pravděpodobně nejrizikovější ze všech čtyř analyzovaných druhů.

Na základě zjištěných skutečností lze také konstatovat, že provozovatelé aplikací a provozovatelé webových stránek jsou subjekty s velkým potenciálem pro narušování soukromí uživatelů v koncovém zařízení. Díky interakci s uživateli mohou vytvářet velké množství externích dat, ale mohou často získávat přístup i k citlivým interním datům, uloženým v koncových zařízeních. To je velice znepokojivé vzhledem k analyzovaným průzkumům, dle kterých provozovatelé aplikací a webových stránek navzdory platné právní úpravě využívají relativně často tato data pro vlastní účely. Multiplikátorem takového zásahu pak je sdílení získaných dat o uživatelích s řadou dalších subjektů. V kontextu výše uvedeného lze tak počínání některých provozovatelů aplikací a webových stránek, kterým narušují ochranu soukromí uživatelů, označit za alarmující. Zejména třetí a čtvrtá skupina dat je významně ohrožena zásahem třetích stran. Právě prostřednictvím neoprávněného zpracování externích dat provozovateli aplikací a webových stránek se osobní údaje uživatelů koncových zařízení šíří do kyberprostoru.

Tyto poznatky budou podkladem pro další výzkum a podporu ochrany soukromí v koncových zařízeních.

6. SEZNAM ZDROJŮ

[1] APPLE INC. App Privacy Details in the App Store. In: *Apple Developer*. [online] [cit. 28. 3. 2024]. Dostupné z: https://developer.apple.com/app-store/app-privacy-details/

[2] BINNS, Reuben. ZHAO, Jun. VAN KLEEK, Max. SHADBOLT, Nigel. Measuring third party tracker power across web and mobile. *ACM Transactions on Internet Technology*. 2018. roč. 18. č. 4, s. 1–22.

[3] CENA, Federica. RAPP, Amon. LIKAVEC, Silvia. MARCENGO, Alessandro. Envisioning the future of personalization through personal informatics: A user study. *International Journal of Mobile Human Computer Interaction* [online]. 2018. roč. 10. č. 1, s. 52–66. ISSN 1942-390X. [cit. 27. 3. 2024]. Doi:10.4018/IJMHCI.2018010104

[4] COOKIE-SCRIPT. Privacy Laws for Apps: How to Protect User Data? In: *Cookie-script.com* [online]. [cit. 28. 3. 2024]. Dostupné z: https://cookie-script.com/blog/privacy-laws-for-apps-how-to-protect-user-data

[5] DELL TECHNOLOGIES. *Global Data Protection Index 2021: Key Findings*. 2021, [online]. [cit. 28. 3. 2024]. Dostupné z: www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-keyfindings.pdf

[6] DIMITROV, Ivan. Invasive apps. In: *pcloud.com* [online] 2021. [cit. 28. 3. 2024]. Dostupné z: https://www.pcloud.com/invasive-apps

[7] DUARTE, Fabio. Amount of Data Created Daily (2024). In: *Exploding Topics* [online] [cit. 28. 3. 2024]. Dostupné z: https://explodingtopics.com/blog/data-generated-per-day

[8] GOOGLE, INC. Play Console Help - User Data - Privacy Policy [online]. *Policy center*. 2024 [cit. 28. 3. 2024]. Dostupné z: https://support.google.com/googleplay/android-

[9] HANDSETS, Realme. LIU, Haoyu. PATRAS, Paul a LEITH, Douglas. Android Mobile OS Snooping By Samsung, Xiaomi, Huawei and Realme Handsets. In: *semanticscholar.org* [online]. [cit. 28. 3. 2024]. Dostupné z: https://www.semanticscholar.org/paper/Android-Mobile-OS-Snooping-By-Samsung%2C-Xiaomi%2C-and-Handsets-Liu/993c4e5cbe8151fd426d08ac606ea5daa6c78605

[10] JIN, Haojian. LIU, Minyi. DODHIA, Kevan. LI, Yuanchun. SRIVASTAVA, Gaurav. FREDRIKSON, Matthew. AGARWAL Yuvraj a HONG, Jason. Why Are They Collecting My Data?: Inferring the Purposes of Network Traffic in Mobile Apps. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* [online]. Roč. 2. č. 4, s. 1–27. ISSN 2474-9567. Doi:10.1145/3287051

[11] KLODWIG, Jakub. *Ochrana soukromí v kontextu koncových zařízení uživatelů* [online]. Diplomová práce. Brno: Masarykova univerzita, Právnická fakulta. [cit. 28. 3. 2024]. Dostupné z: https://is.muni.cz/th/u6bwf/

[12] KLODWIG, Jakub. Pokročilé metody identifikace koncových zařízení. In: *COFOLA 2020*: *Sborník příspěvků mladých právníků, doktorandů a právních vědců* [online]. Brno: Muni Press, s. 1091–1108. ISBN 978-80-210-9670-7. [cit. 28. 3. 2024]. Dostupné z: https://www.law.muni.cz/sborniky/cofola/2020/cofola2020.pdf

[13] KLODWIG, Jakub. Wearables a právo na informační sebeurčení. In: *CyberCon 2023*. Vyžádaná přednáška. Brno.

[14] KLODWIG, Jakub. Wearables a ochrana soukromí. In: *Obchodněprávní revue*. 2021, Nakladatelství C.H. Beck, roč. 13, č. 3, s. 230-236. ISSN 1803-6554. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpw64s7gnpxgxzsgeza&groupIndex=3&rowIndex=0&refSource=search

[15] KOLLNIG, Konrad. BINNS, Reuben. DEWITTE, Pierre. VAN KLEEK, Max. WANG, Ge. OMEIZA, Daniel. WEBB, Helena. SHADBOLT, Nigel. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. *Seventeenth Symposium on Usable Privacy and Security*. 2021. ISSN 978-1-939133-25-0.

[16] LESSIG, Lawrence. *Code: Version 2.0*. New York: Basic Books. 2006. ISBN 978-0-465-03914-2.

[17] NOUWENS, Midas. LICCARDI, Ilaria.VEALE, Michael. KARGER, David a KAGAL, Lalana. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* [online]. 2020. [cit. 28. 3. 2024]. Doi:10.1145/3313831.3376321

[18] NOYB – EUROPEAN CENTER FOR DIGITAL RIGHTS, 2023. How mobile apps illegally share your personal data. *NOYB* [online] [cit. 28. 3. 2024]. Dostupné z: https://noyb.eu/en/how-mobile-apps-illegally-share-your-personal-data

[19] RÁMIŠ, Vladan. Článek 2 Věcná působnost. In: *Obecné nařízení o ochraně osobních údajů* [online]. Praha: C. H. Beck, s. 66–68 [cit. 28. 3. 2024]. Dostupné z: https://www.beck-online.cz/bo/document-view.seam?documentId=nnptembsgbpwk232ge3tqltdnqza#

[20] REN, Jingjing. LINDORFER, Martina. DUBOIS, Daniel. RAO, Ashwin. CHOFFNES, David a VALLINA-RODRIGUEZ, Narseo. Bug Fixes, Improvements, ... and Privacy Leaks - A Longitudinal Study of PII Leaks Across Android App Versions. In: *Network and Distributed System Security Symposium*: *Proceedings 2018 Network and Distributed System Security Symposium* [online]. 2018. San Diego, CA: Internet Society [cit. 28. 3. 2024]. ISBN 978-1-891562-49-5. Doi:10.14722/ndss.2018.23143

[21] Rozsudek ESLP ze dne 16. února 2000, ve věci Amann V. Switzerland. [online]. Dostupné z: https://hudoc.echr.coe.int/eng?i=001-58497

[22] Rozsudek SDEU ze dne 24. listopadu 2011, ve věci C-70/10 Scarlet Extended SA. [online]. ECLI:EU:C:2011:771. Dostupné z: https://hudoc.echr.coe.int/eng?i=001-58497

[23] Rozsudek SDEU ze dne 19. října 2016, ve věci C-582/14, Patrick Breyer proti Bundesrepublik Deutschland. [online]. ECLI:EU:C:2016:779. Dostupné z: https://hudoc.echr.coe.int/eng?i=001-58497

[24] Rozsudek SDEU ze dne 9. listopadu 2023, ve věci C-319/22, Gesamtverband Autoteile-Handel eV proti SCANIA CV AB. ECLI:EU:C:2023:837. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=279492&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=746319

[25] SEDLÁČEK, Jakub. Digitální stopa: Konec empirické sociologie? In: *Czech Sociological Review*. [online]. 2020, roč. 56, č. 4, s. 471-490. Dostupné z: https://search.ebscohost.com/login.aspx?authtype=ip&custid=s8431878&profile=eds

[26] TOMÍŠEK, Jan, Jak regulovat cookies v nařízení ePrivacy. *Revue pro právo a technologie* [online]. 2023. roč. 14, č. 27, s. 235–332. ISSN 1805-2797. Doi:10.5817/RPT2023-1-5

[27] UTZ, Christine. DEGELING, Martin. FAHL, Sascha. SCHAUB, Florian a HOLZ, Thorsten. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: *Conference on Computer and Communications Security*: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [online]. 2019. New York, NY, USA: Association for Computing Machinery, s. 973–990 [cit. 28. 3. 2024]. ISBN 978-1-4503-6747-9. Dostupné z: doi:10.1145/3319535.3354212

[28] WINKER, Jan, Competition Analysis of Consentmanager.net 2023.

[29] WP29, 2007. *Opinion 4/2007 on the concept of personal data* [online]. 20. červen 2007. [cit. 28. 3. 2024]. Dostupné z: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

[30] ZIMMECK, Sebastian. STORY, Peter. SMULLEN, Daniel. RAVICHANDER, Abhilasha. WANG, Ziqi. REIDENBERG, Joel. RUSSELL, Cameron a SADEH, Norman. MAPS: Scaling Privacy Compliance Analysis to a Million Apps. *Proceedings on Privacy Enhancing Technologies* [online]. 2019, s. 66–86. Doi:10.2478/popets-2019-0037
