https://doi.org/10.5817/RPT2023-1-5

JAK REGULOVAT COOKIES V NAŘÍZENÍ EPRIVACY[1]

JAN TOMÍŠEK[2]

ABSTRAKT

Cílem tohoto článku je představit návrh, jak by připravované nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích (tzv. nařízení ePrivacy) mělo upravovat použití cookies a podobných technologií. Současná směrnice 2002/58/ES řeší rizika spojená s použitím cookies a podobných technologií především požadavkem na informovaný souhlas uživatele. Toto řešení však klade nepřiměřený důraz na kontrolu ze strany uživatele, kterou však není v možnostech uživatele při běžném používání internetu efektivně vykonávat. Výsledkem je tak snížená úroveň ochrany soukromí uživatele před sledováním a současně komplikace pro stránky nabízející bezplatný obsah, financovaný pomocí cílené reklamy. Článek proto popisuje, jak fungují cookies a podobné technologie, co přinese blokace tzv. cookies třetích stran v nejrozšířenějších prohlížečích, jaká je historie právní úpravy soukromí v elektronických komunikacích, jaká je platná právní úprava použití cookies a podobných technologií a jak se tato úprava vyvíjela v různých verzích návrhu nařízení ePrivacy. Následně představuje návrh, jak by podle použití cookies a podobných technologií mělo být v nařízení ePrivacy upraveno de lege ferenda.

[1] Tento článek vznikl v rámci projektu "Právo a technologie XI“, MUNI/A/1293/2022.

[2] Mgr. et Mgr. Ing. Jan Tomíšek je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a partnerem v advokátní kanceláři ROWAN LEGAL, kontaktní e-mail: jantomisek@gmail.com. Autor by rád poděkoval Matěji Myškovi, Jakubu Míškovi, Valdanu Rámišovi, Františku Nonnemannovi a dvěma anonymním recenzentům za jejich podnětné připomínky k tomuto článku. Veškeré chyby jdou výhradně na vrub autora.

KLÍČOVÁ SLOVA

Cookies, soukromí, osobní údaje, GDPR, ePrivacy

ABSTRACT

The aim of this article is to present a proposal on how the forthcoming Regulation of the European Parliament and of the Council on respect for privacy and the protection of personal data in electronic communications (ePrivacy Regulation) should regulate the use of cookies and similar technologies. The current Directive 2002/58/EC addresses the risks associated with the use of cookies and similar technologies primarily by requiring the informed consent of the user. However, this solution places undue emphasis on user control, which is not effectively within the user's ability to exercise in the normal course of internet use. The result is a reduced level of protection of the user's privacy from tracking and, at the same time, complications for sites offering free content financed by targeted advertising. The article therefore describes how cookies and similar technologies work, what blocking third-party cookies in the most widely used browsers will bring, the history of the legal regulation of privacy in electronic communications, what the current legal regulation of the use of cookies and similar technologies is, and how this regulation has evolved in the different versions of the draft ePrivacy Directive. It then presents a de lege ferenda proposal for how the use of cookies and similar technologies should be regulated in the ePrivacy Regulation.

KEY WORDS

Cookies; Privacy; Personal Data; GDPR; ePrivacy

1. ÚVOD

Použití cookies a podobných technologií je v právu Evropské unie řešeno především právní úpravou soukromí v elektronických komunikacích.[3] Návrh nové podoby této právní úpravy, tzv. nařízení ePrivacy, představila Ev-

[3] Viz směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích).

ropská komise v lednu 2017.[4] Ani po 5 letech však nedošlo k jejímu přijetí a konec legislativního procesu zatím není v dohledu, jak je blíže objasněno v tomto článku. To otevírá prostor k hlubšímu zamyšlení, jak by nová právní úprava měla regulovat použití cookies a podobných technologií.

Cookies a podobné technologie v rámci webových stránek lze (vedle řady jiných účelů) využít ke sledování uživatelů ve smyslu sběru údajů o jejich chování.[5] Tyto údaje pak lze využít k odvozování osobnostních a dalších charakteristik uživatelů – profilování.[6] Informace z profilu uživatele lze pak využít pro cílení reklamy.[7] Důsledkem tohoto sledování mohou být diskriminace,[8] manipulace[9] a odrazující efekty (*chilling effects*).[10]

---

[4] Viz návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) COM/2017/010 final – 2017/03 (COD) (dále jen „návrh Komise“).

[5] Viz BARTH, Adam. HTTP State Management Mechanism - Request for Comments. RFC 6265. In: *Internet Engineering Task Force* [online]. 2011 [cit. 20. 7. 2022], s. 4. LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*. Boca Raton: CRC Press, 2020, s. 120.

[6] 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 ve svém čl. 4 bod 4 definuje profilování jako jakoukoli formu „automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu“.

[7] Viz LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 120.

[8] Viz ANGWIN, Julia, PARRIS, Terry. Facebook Lets Advertisers Exclude Users by Race. In: *ProPublica* [online]. 28. 10. 2016 [cit. 6. 3. 2022]. Dostupné z: https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race. SPEICHER, Till et al. Potential for Discrimination in Online Targeted Advertising. In: *Conference on Fairness, Accountability and Transparency*: *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* [online]. PMLR, 2018 [cit. 6. 3. 2022], s. 9, 10.

[9] Viz např. CALO, Ryan. Digital market manipulation. *George Washington Law Review* [online]. 2013, roč. 82, č. 4 [cit. 12. 2. 2023], s. 996. CRAIN, Matthew, NADLER, Anthony. Political Manipulation and Internet Advertising Infrastructure. *Journal of Information Policy* [online]. 2019, roč. 9 [cit. 10. 9. 2022], s. 374.

[10] Viz RICHARDS, Neil. *Intellectual privacy: rethinking civil liberties in the digital age*. Oxford: Oxford University Press, 2015, s. 101.

Současná směrnice 2002/58/ES řeší rizika spojená s použitím cookies a podobných technologií především požadavkem na informovaný souhlas uživatele.[11] Souhlas je však v kontextu webových stránek problematickým nástrojem ochrany soukromí. Podstatou požadavku na souhlas je snaha o dosažení kontroly uživatele nad nakládáním s informacemi o jeho osobě.[12] To je však v kontextu množství webových stránek a mobilních aplikací, které s takovými informacemi pracují a se kterými uživatel běžně interaguje, neproveditelné.[13] Poznatky z behaviorální ekonomie ukazují, že uživatelé kontrolu nejsou v tomto měřítku schopni efektivně vykonávat.[14] Důsledkem je zahlcení uživatelů žádostmi o souhlas téměř na každé webové stránce, kterou navštíví. Žádosti o souhlas jsou pro uživatele obtěžující, přitom nezvyšují povědomí uživatelů o rizicích, která jsou s použitím cookies a podobných technologií spojena – naopak často vedou k mechanickému udělení souhlasu.[15]

Cílem tohoto článku je představit návrh, jak by použití cookies a podobných technologií mělo být v nařízení ePrivacy upraveno, aby tyto problémy institutu souhlasu byly alespoň částečně překonány. Návrh spočívá ve vyloučení použití specifického druhu cookies (tzv. vlastních cookies)

[11] Viz čl. 5 odst. 3 směrnice 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích).

[12] Viz RICHARDS, Neil M., HARTZOG, Woodrow. Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review* [online]. 2016, roč. 19, č. 3, [cit. 30. 1. 2021], s. 444.

[13] Slovy Woodrowa Hartzoga, kontrola není „bezedná studna". Srov. HARTZOG, Woodrow. *Privacy's blueprint*. Cambridge, Massachusetts: Harvard University Press, 2018, s. 63.

[14] Viz CAROLAN, Eoin, CASTILLO-MAYEN, M. Rosario. Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws. *Virginia Journal of Law & Technology*. 2014, roč. 19, č. 2, s. 362. COFONE, Ignacio N. The way the cookie crumbles: online tracking meets behavioural economics. *International Journal of Law and Information Technology* [online]. 2017, roč. 25, č. 1 [cit. 2. 2. 2022], s. 51. DOUGHERTY, Christie. Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation. *Northeastern University Law Review* [online]. 2020, roč. 12, č. 2 [cit. 2. 2. 2023], s. 638.

[15] Viz KULYK, Oksana et al. Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity* [online]. 2020, roč. 6, č. 1 [cit. 2. 2. 2022], s. 4. Dále viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics*, s. 44. CRANOR, Lorrie Faith. Cookie monster. *Communications of the ACM* [online]. 2022, roč. 65, č. 7 [cit. 2. 2. 2022], s. 32.

a podobných technologií a dále technologií nahrazujících tzv. cookies třetích stran z působnosti právní úpravy ochrany soukromí v elektronických komunikacích a ponechání jejich použití pouze v režimu GDPR, s doplněním povinností pro tvůrce webových prohlížečů o povinnost cookies třetích stran a podobné technologie blokovat ve výchozím nastavení těchto prohlížečů.

Článek proto popisuje, jak cookies a podobné technologie fungují a co přinese blokace cookies třetích stran v nejrozšířenějších prohlížečích. Dále popisuje historii právní úpravy soukromí v elektronických komunikacích a platnou právní úpravu použití cookies a podobných technologií. Následně popisuje vývoj textu nařízení ePrivacy a představuje výše nastíněný návrh. Závěr článku shrnuje provedené úvahy.

2. COOKIES A PODOBNÉ TECHNOLOGIE

Cookies jsou krátké textové řetězce, které může webová stránka uložit do webového prohlížeče uživatele.[16] Při dalším požadavku na zobrazení webové stránky internetový prohlížeč ověří, jestli má pro tuto webovou stránku uložené nějaké cookies, a pokud ano, zašle je na server jako součást hlavičky požadavku.[17] Vedle hodnoty lze cookies nastavit i další parametry. Jedním z nich je platnost (exspirace), která určuje dobu, po kterou bude od svého uložení příslušná cookie zasílána spolu s požadavky na stránky z dané domény.[18]

Cookies jsou z hlediska uložení ve webovém prohlížeči a zpřístupnění webovým stránkám vázány na doménu.[19] Pokud tedy byla cookie do prohlí-

[16] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online]. Konkrétně může webový server do hlavičky odpovědi na požadavek zaslání obsahu konkrétní webové stránky vložit pole Set-Cookie, které může obsahovat páry klíč–hodnota, například „Set-Cookie: PHPSESSID = r2t5uvjq435r4q7ib3vtdjq120; language = cs“. Na základě tohoto pokynu si internetový prohlížeč uloží cookie „PHPSESSID“ s hodnotou „r2t5uvjq435r4q7ib3vtdjq120“ a cookie „language“ s hodnotou „cs“.

[17] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online]. Ve výše popsaném příkladu tak součástí hlavičky požadavku na zobrazení další stránky ze stejné domény bude také pole „Cookie: PHPSESSID = r2t5uvjq435r4q7ib3vtdjq120; language = cs“.

[18] Viz tamtéž.

[19] Viz tamtéž.

žeče uložena v rámci přístupu k webové stránce na doméně „priklad.cz“, odešle se pouze v rámci požadavků na webové stránky ze stejné domény (např. „priklad.cz/ukázka“) nebo z jejích subdomén (např. „dobry.priklad.cz“).[20]

Cookies slouží primárně k zajištění stavové komunikace v rámci *World Wide Webu*. Komunikační protokol HTTP, který je využíván pro přenos webových stránek ze serveru do webového prohlížeče, je totiž tzv. bezstavový,[21] což znamená, že mezi jednotlivými požadavky na zobrazení webové stránky není v rámci HTTP protokolu přenášena žádná informace (tzv. stav).

Cookies umožňují mezi jednotlivými zobrazeními webové stránky přenášet např. preference uživatele, jako je jazyková verze webové stránky, kterou si uživatel zvolil (pokud stránka umožňuje výběr jazyka). Současně cookies umožňují také na straně serveru udržovat mezi návštěvami webové stránky tzv. sezení (*sesssion*) nesoucí stav komunikace. Toto udržování stavu se realizuje tak, že se do cookie zapíše unikátní identifikátor daného sezení (*session ID*), který je pak při následujících požadavcích zaslán příslušné webové stránce. Ta podle něj rozpozná, že určitý požadavek navazuje na požadavky již dříve realizované.[22]

Vedle zajištění stavové komunikace jako nástroje k zajištění funkcionality webové stránky však cookies mohou sloužit mnoha dalším účelům. Identifikace uživatele mezi jednotlivými přístupy je užitečná i pro měření návštěvnosti určité webové stránky a analýzu chování jejích návštěvníků – díky cookies je možné vedle počtu zobrazení jednotlivých stránek sledovat počet návštěvníků, kteří si zobrazili více stránek, sledovat opakované návštěvy (pokud je cookie nastavena delší platnost než do ukončení běhu in-

[20] Při přístupu na webovou stránku na adrese „jiny-priklad.cz“ tak tyto cookies z domény „priklad.cz“ na server odeslány nebudou.

[21] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online].

[22] Viz tamtéž. Například, že stránku s určitým zbožím v internetovém obchodě požaduje internetový prohlížeč uživatele, který v předchozím spojení vložil jiné zboží do svého košíku – webová stránka tak může např. zobrazit uživateli indikátor, že už má nějaké zboží v košíku.

ternetového prohlížeče) a zkoumat, jak uživatelé web používají (v jakém pořadí stránky zobrazují, pomocí kterých odkazů se přesouvají, apod.).[23]

Možnosti použití cookies jsou dále rozšířeny tím, jak jsou dnes webové stránky po technické stránce obvykle strukturovány. V počátcích *World Wide Webu* byla přenosová rychlost a propustnost připojení k internetu nízká a bylo žádoucí, aby se na základě jediného HTTP požadavku načetla celá webová stránka. V současnosti jsou však přenosová rychlost a propustnost běžného připojení k internetu výrazně vyšší a před úsporou počtu požadavků má přednost bohatost obsahu a interaktivita webové stránky. Z toho důvodu se do webové stránky vkládá řada dalších prvků, které se načítají samostatnými požadavky. Nejjednodušším příkladem jsou obrázky, které jsou do webové stránky vloženy tak, že v kódu webové stránky je obsažena zvláštní značka, která pro internetový prohlížeč znamená pokyn, aby si ze stanovené adresy pomocí protokolu HTTP vyžádal obrázek a vložil ho do zobrazované webové stránky. Obdobně lze do webové stránky vkládat styly, které upravují její vizuální aspekty, nebo skripty, což jsou spustitelné počítačové programy. Takto vkládaných položek jsou dnes v rámci webové stránky běžně desítky.

Vkládání obsahu přitom není omezeno pouze na doménu, ze které se načítá příslušná webová stránka – např. webová stránka „priklad.cz“ může obsahovat značku dávající internetovému prohlížeči pokyn k vložení obrázku z adresy „databaze-obrazku.cz/priklad.png“. Jelikož je vkládaný obsah získáván opět pomocí protokolu HTTP, doména, ze které je obsah získáván, může v rámci požadavku na zaslání obsahu číst a v rámci odpovědi zapisovat cookies ve webovém prohlížeči uživatele. Ve výše uvedeném příkladu tedy webový server na adrese „databaze-obrazku.cz“ může z internetového prohlížeče číst, resp. do něj zapisovat cookies, i když uživatel aktuálně prohlíží webovou stránku na doméně „priklad.cz“.

[23] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online]. LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 120; ZHENG, Guangzhi; PELTSVERGER, Svetlana. Web analytics overview. In: *Encyclopedia of Information Science and Technology, Third Edition* [cit. 6. 2. 2023]. IGI Global, 2015 [cit. 6. 2. 2023], s. 3.

Cookies vložené z domény, na které se nachází webová stránka, již uživatel aktuálně prohlíží, se označují jako vlastní cookies (cookies první strany, *first-party cookies*). Cookies vložené z jiných domén se v daném kontextu označují jako cookies třetích stran (*third-party cookies*).[24] Ve výše uvedeném příkladu tedy cookies z domény „priklad.cz" budou vlastní cookies, cookies z domény „databaze-obrazku.cz" budou cookies třetí strany. Stále však platí, že cookies jsou ukládány a zpřístupňovány odděleně, server na adrese „databaze-obrazku.cz" tedy obdrží pouze cookies nastavené z této domény, nikoli cookies, které zapsal server s adresou „priklad.cz".

Podobně jako cookies lze ke sledování chování uživatelů použít i další technologie. Podstatou části z nich je ukládání dat do webového prohlížeče uživatele, jiné pracují s údaji, které lze získat z koncového zařízení a vypovídají o jeho hardwaru či softwaru.[25] Ukládání do webového prohlížeče využívají *ETags*, které fungují na bázi vyrovnávací paměti (*cache)* webového prohlížeče. Do této paměti se ukládají prvky webové stránky, aby nebylo třeba je opakovaně načítat při její další návštěvě. Těmto ukládaným prvkům jsou přidělovány identifikátory, které může webová stránka měnit. To lze využít k uložení jedinečného identifikátoru, podobně jako se ukládá do cookie.[26]

Standard pro kódování webových stránek HTML5 přinesl novou funkcionalitu prohlížeče označovanou webové úložiště (*web storage)*. Podobně jako cookies umožňuje ukládání párů klíč–hodnota, kapacita úložiště je však výrazně větší (5 MB na každou webovou stránku oproti 4kB na jednu cookie). Webové úložiště se dělí na dvě části – úložiště sezení (*session storage*), které

[24] Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies. In: *Evropská komise* [online]. 7. 6. 2012, s. 5. [cit. 23. 1. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf (dále jen „WP194")

[25] Viz HOOFNAGLE, Chris Jay et al. Behavioral advertising: The offer you can't refuse. *Harvard Law & Policy Review*. 2012, roč. 6, s. 286.

[26] Viz HINTERNESCH, Nicolas. No Cookies, No Problem — Using ETags For User Tracking. In: *Medium* [online]. 17. 5. 2021 [cit. 18. 1. 2023]. Dostupné z: https://levelup.gitconnected.com/no-cookies-no-problem-using-etags-for-user-tracking-3e745544176b HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 281.

se vymaže po zavření záložky v prohlížeči, a místní úložiště, které nemá žádnou exspiraci (chová se tedy jako cookies bez nastavené doby exspirace).[27]

Spíše za historickou technologii lze považovat Flash cookies spojené se zásuvným modulem do webových prohlížečů označovaným Flash.[28] Tyto Flash cookies byly historicky využívány také pro obnovení cookies, které uživatel ze svého prohlížeče vymazal.[29]

Údaje o softwaru nebo hardwaru koncového zařízení využívá technika označovaná jako *device fingerprinting* nebo *browser fingerprinting*.[30] Webové stránky mají pro své fungování přístup k rozsáhlým informacím o webovém prohlížeči uživatele a jeho zařízení, jako jsou typ a verze prohlížeče, typ a verze operačního systému nebo rozlišení obrazovky. Tyto údaje jsou pro zařízení uživatele do jisté míry unikátní, a mohou tak vytvářet jeho unikátní „otisk" použitelný pro sledování.[31] Webové prohlížeče mají také dynamické funkcionality, které mohou být ovládány prostřednictvím skriptů vložených do webových stránek, a chování těchto funkcionalit se může na různých zařízeních a v různých prohlížečích i v různých verzích stejného prohlížeče lišit.[32] Využití údajů, které o sobě zařízení aktivně vysílá, lze

---

[27] Viz HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse,* s. 283. HTML Web Storage API In: *W3 schools* [online]. [cit. 18. 1. 2023]. Dostupné z: https://www.w3schools.com/html/html5_webstorage.asp

[28] Viz HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 282.

[29] Viz HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 283.

[30] Do češtiny lze název přeložit jako snímání otisků zařízení, resp. prohlížeče. Viz CAO, Yinzhi, LI, Song, WIJMANS, Erik. (Cross-)Browser Fingerprinting via OS and Hardware Level Features. In: *Network and Distributed System Security Symposium*: *Proceedings 2017 Network and Distributed System Security Symposium* [online]. San Diego, CA: Internet Society, 2017, [cit. 28. 10. 2022], s. 1. HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 285. Viz také Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29. Stanovisko č. 9/2014 k uplatňování směrnice 2002/58/ES na otisky zařízení. In: *Evropská komise* [online]. 25. 11. 2014, s. 3. [cit. 1. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf (dále jen „WP224")

[31] K přehledu relevantních údajů viz WP224, s. 5.

[32] CAO, Yinzhi; LI, Song; WIJMANS, Erik. (Cross-)Browser Fingerprinting via OS and Hardware Level Features. s. 2.

označit jako pasivní fingerprinting, využití údajů, které je třeba získat aktivně pomocí skriptu, pak jako aktivní fingerprinting.[33]

Jednou z takových funkcionalit je tzv. *HTML canvas* (plátno) – funkcionalita určená ke kreslení grafických prvků na obrazovky zařízení, například pro animace, herní grafiku nebo vizualizaci dat. HTML canvas lze použít pro vykreslení konkrétního obrázku mimo oblast viditelnou uživateli prohlížeče a následné zkoumání vykresleného obrázku (např. jeho rozměrů a dalších vlastností). Protože existují drobné rozdíly ve způsobu vykreslování obrázku v různých prohlížečích a na různých zařízeních, poskytuje zkoumání údaje, které lze rovněž využít k vytvoření otisku konkrétního prohlížeče.[34] Podle studie Acara a kol. z roku 2014 ze 100 000 nejnavštěvovanějších webových stránek na internetu podle portálu Alexa obsahovalo 5,5 % skripty pro snímání otisků HTML canvas.[35]

3. KONEC COOKIES TŘETÍCH STRAN

Protože cookies (zejména cookies třetích stran) lze využít ke sledování chování uživatele, obsahují některé moderní prohlížeče funkcionality, které toto sledování a uložení nebo čtení cookies v některých případech blokují.[36] V srpnu roku 2019 oznámil Google v tomto směru zahájení iniciativy nazvané *Privacy Sandbox*. Cílem této inciativy je vytvoření sady otevřených standardů, které posílí ochranu soukromí na webu.[37]

---

[33] Viz MAYER, Jonathan R., MITCHELL, John C. Third-party web tracking: Policy and technology. In: 2012 *IEEE symposium on security and privacy* [online]. IEEE, 2012 [cit. 27. 5. 2023]. s. 421.

[34] Viz KONIK, James. How Does Canvas Fingerprinting Work? In: *Fingerprint* [online]. 11. 7. 2021 [cit. 28. 10. 2022]. Dostupné z: https://fingerprint.com/blog/canvas-fingerprinting/

[35] Viz ACAR, Gunes, et al. The web never forgets: Persistent tracking mechanisms in the wild. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* [online]. 2014. [cit. 12. 2. 2023], s. 678.

[36] Viz Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era. In: *Interactive Advertising Bureau* [online]. Březen 2022, s. 18. [cit. 31. 1. 2023]. Dostupné z: https://iabeurope.eu/wp-content/uploads/2022/03/IAB-Europe-Guide-to-a-Post-Third-Party-Cookie-Era-March-2022.pptx.pdf

[37] Viz SCHUH, Justin. Building a more private web. In: *Google* [online]. 22. 8. 2019 [cit. 26. 2. 2022]. Dostupné z: https://blog.google/products/chrome/building-a-more-private-web/

Google tak nejspíše reagoval na dřívější kroky zejména ze strany Apple, nadace Mozilla vyvíjející internetový prohlížeč Firefox a také na některé úvahy ze strany Microsoftu.[38] Apple ve svém internetovém prohlížeči Safari od roku 2017 uplatňuje opatření proti sběru údajů o chování uživatele.[39] Podobná opatření v červnu 2019 oznámila nadace Mozilla[40] a Microsoft je ve stejnou dobu přidal v experimentálním režimu do prohlížeče Edge.[41] Význam oznámení tohoto kroku ze strany Googlu je dán tím, že jeho webový prohlížeč Chrome je nejrozšířenějším prohlížečem na světě.[42]

Inciativa *Privacy Sandbox* ve své prvotní verzi neobsahovala záměr blokovat cookies třetích stran. Google toto pojetí odůvodňoval tak, že rozsáhlé blokování cookies by poškodilo zájmy uživatelů podporováním použití technik, jako je fingerprinting, a dále tím, že blokování cookies bez náhradního řešení, jak zajistit zobrazování relevantních (personalizovaných) reklam, by poškodilo financování médií a webových služeb.[43] Zdrženlivý přístup Googlu k blokování cookies třetích stran není překvapivý, když jeho příjmy pochází především z internetové reklamy.[44]

---

[38] Viz LEE, Timothy B. Google defends tracking cookies—some experts aren't buying it. In: *Ars Technica* [online]. 26. 8. 2019 [cit. 26. 2. 2022]. Dostupné z: https://arstechnica.com/tech-policy/2019/08/why-some-experts-are-skeptical-of-googles-new-web-privacy-strategy/

[39] Viz WILANDER, John. Intelligent Tracking Prevention. In: *WebKit* [online]. 5. 6. 2017 [cit. 26. 2. 2022]. Dostupné z: https://webkit.org/blog/7675/intelligent-tracking-prevention/

[40] Viz CAMP, Dave. Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise In: *The Mozilla Blog* [online].]. 4. 6. 2019 [cit. 26. 2. 2022]. Dostupné z: https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/

[41] Viz BRINKMANN, Martin. A look at Microsoft Edge's Tracking Prevention feature.. In: *gHacks Technology News* [online]. 28. 6. 2019 [cit. 26. 2. 2022]. Dostupné z: https://www.ghacks.net/2019/06/28/a-look-at-microsoft-edges-tracking-prevention-feature/

[42] Podle statistik za leden roku 2022 byl tržní podíl prohlížeče Google Chrome 64,68 %. Z hlediska velikosti podílu za ním následovaly prohlížeče Safari (18,29 %) a Microsoft Edge (4,23 %). Srov. Browser Market Share Worldwide. In: *StatCounter Global Stats* [online]. 31. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://gs.statcounter.com/browser-market-share

[43] Viz SCHUH, Justin. Building a more private web: A path towards making third party cookies obsolete. In: *Chromium Blog* [online]. 14. 1. 2020 [cit. 30. 5. 2023]. Dostupné z: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

[44] Viz LEE, Timothy B. Google defends tracking cookies—some experts aren't buying it. In: *Ars Technica* [online]. 26. 8. 2019 [cit. 26. 2. 2022]. Dostupné z: https://arstechnica.com/tech-policy/2019/08/why-some-experts-are-skeptical-of-googles-new-web-privacy-strategy/

Přesto v lednu roku 2020 Google oznámil, že přistoupí k blokování cookies třetích stran v prohlížeči Google Chrome. Změnu postoje odůvodnil tím, že po diskuzi s webovou komunitou nabyl přesvědčení, že nástroje iniciativy *Privacy Sandbox* dokážou zajistit fungující web využívající financování z reklam a nahradit cookies třetích stran. V tomto okamžiku společnost avizovala záměr ukončit podporu cookies třetích stran v prohlížeči Chrome do dvou let.[45]

Inciativa *Privacy Sandbox* obsahuje celou sadu nástrojů pro nahrazení cookies třetích stran v oblastech, jako je cílení nebo měření výkonnosti reklamy. Jako klíčovou náhradu cookies třetích stran pro účely cílené internetové reklamy společnost Google původně navrhovala technologii *Federated Learning of Cohorts* (FLoC)[46] založenou na zařazování uživatelů do skupin podle jejich aktivity na internetu (sdružování uživatelů, kteří prochází podobný obsah). V rámci této technologie měl internetový prohlížeč uživatele zpracovat údaje o webových stránkách, které uživatel v poslední době procházel, a na základě matematického modelování přidělit uživateli identifikátor „kohorty" uživatelů, kteří v poslední době procházeli podobnou skladbu webových stránek. Modelování mělo být založené na technice strojového učení označované jako sdružené učení (*federated learning*), která umožňuje souběžné zlepšování modelů v jednotlivých prohlížečích, aniž by údaje o aktivitách jednotlivého uživatele musely jeho prohlížeč opustit. Identifikátor kohorty měl pak následně být z prohlížeče předáván webovým stránkám inzerentů, aby věděli, na jaké kohorty mají své reklamy cílit, a médiím, aby mohla podle preferencí zvolených inzerenty zobrazit uživateli z určité kohorty cílenou reklamu.[47] Ochranu uživatelů měla zajistit především minimální velikost kohorty, kdy by centrální administrátor systému

[45] Viz SCHUH, Justin. Building a more private web: A path towards making third party cookies obsolete [online].

[46] Název je zřejmě slovní hříčkou – anglické slovo *flock* lze přeložit jako hejno či (v tomto kontextu poněkud pejorativněji) stádo.

[47] Viz DUTTON, Sam. FLoC. In: *Chrome Developers* [online]. 18. 5. 2021 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/floc/

zajišťoval, aby nebyl předáván identifikátor takové kohorty, která zahrnuje nízký počet osob (méně než tisíce).[48]

Tato technologie se stala terčem kritiky s ohledem na úroveň ochrany, kterou měla poskytnout uživatelům, a také z pohledu ochrany hospodářské soutěže. Z pohledu ochrany uživatelů byl kritizován potenciál identifikátoru kohorty usnadnit fingerprinting – v případě zařazení uživatele pomocí identifikátoru do kohorty o velikosti několik tisíc uživatelů by mohla být identifikace jednotlivce na základě jiných atributů jeho prohlížeče a zařízení výrazně jednodušší.[49] Dále bylo kritizováno riziko odhalení informací napříč kontexty – webové stránky, disponující komplexnější identitou uživatele (např. takové služby, do kterých se uživatel přihlašuje e-mailovou adresou), by mohly pomocí identifikátoru kohorty odvodit o uživateli dodatečné údaje, pokud by dokázaly zpětně odvodit vlastnosti dané kohorty.[50] Kohorty by také přitom mohly vymezovat skupiny uživatelů se specifickými vlastnostmi, jako příslušníky národnostních menšin apod. Tato vlastnost kohort by také mohla otevírat cestu ke zneužití identifikátoru kohorty pro účely diskriminace.[51]

Z pohledu hospodářské soutěže pak koncept vyvolal kritiku, že ze společnosti Google vytváří nezbytného prostředníka pro jakékoli cílení reklamy ve vztahu k uživatelům prohlížeče Google Chrome. To vedlo k zahrnutí inciativy Privacy Sandbox mezi tvrzená porušení soutěžního práva v rámci řízení vedeného generálními advokáty 15 států USA proti společnosti Google.[52] Vyšetřování této iniciativy zahájil také britský dozorový úřad pro oblast hospodářské soutěže *Competition and Markets Authority* (dále jen „CMA“).

---

[48] Viz CYPHERS, Bennett. Google's FLoC Is a Terrible Idea. In: *Electronic Frontier Foundation* [online]. 3. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[49] Viz tamtéž.

[50] Viz tamtéž.

[51] Viz tamtéž.

[52] Viz ROBERTSON, Adi. Google antitrust suit takes aim at Chrome's Privacy Sandbox. In: *The Verge* [online]. 16. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy

Po více než roce vyšetřování a jednání přijal v únoru roku 2022 CMA závazky společnosti Google. Ta se mimo jiné zavázala, že podporu cookies třetích stran neukončí dříve, než CMA potvrdí, že jeho obavy z narušení hospodářské soutěže byly dostatečně ošetřeny.[53] Dle aktuálního harmonogramu je ukončení podpory plánováno od poloviny roku 2024,[54] zda se tento termín nebude posouvat, však zatím není jasné. Společnost Apple v prohlížeči Safari mezitím již k úplnému blokování cookies třetích stran přistoupila.[55]

V mezičase přitom společnost Google ukončila testování FLoC a tuto technologii opustila.[56] V lednu 2022 zveřejnila podrobnosti technologie Topics API, která má pro účely cílené reklamy nahradit cookies třetích stran namísto FLoC.[57] Podstatou technologie Topics API je přiřazení tematických štítků webovým stránkám, určení nejvýznamnějších tematických štítků pro konkrétního uživatele na základě jeho nedávné historie procházení webových stránek a zpřístupnění těchto štítků webovým stránkám skrze programové rozhraní (API) internetového prohlížeče.[58]

V rámci tohoto konceptu přitom společnost Google plánuje, že seznam dostupných štítků bude předem stanovený a omezený tak, aby nezahrnoval citlivé kategorie, jako např. zdraví či etnickou příslušnost. Přiřazení štítku webové stránce bude probíhat na základě části URL adresy (části před určením domény vyššího řádu, tzv. *hostname*, tj. např. „priklad“ u domény „priklad.cz“) pomocí strojového učení s využitím modelu předem vloženého do internetového prohlížeče. Rozhraní prohlížeče pak poskytne webové

[53] Viz Competition and Markets Authority. CMA to keep ‘close eye’ on Google as it secures final Privacy Sandbox commitments. In: *GOV.UK* [online]. [cit. 26. 2. 2022]. Dostupné z: https://www.gov.uk/government/news/cma-to-keep-close-eye-on-google-as-it-secures-final-privacy-sandbox-commitments

[54] Viz *How We’re Protecting Your Online Privacy* [online].

[55] Viz WILANDER, John. Full Third-Party Cookie Blocking and More. In: *WebKit* [online]. 24. 3. 2020 [cit. 26. 2. 2022]. Dostupné z: https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

[56] Viz *How We’re Protecting Your Online Privacy* [online].

[57] Viz DUTTON, Sam. The Topics API. In: *Chrome Developers* [online]. 25. 1. 2022 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/topics/

[58] Viz tamtéž.

stránce tři nejčastější tematické štítky pro daného uživatele, každé za jeden ze tří předcházejících týdnů.[59]

Tematické štítky si budou moci na webové stránce vyžádat i skripty třetích stran, obecně však platí, že štítek obdrží pouze taková stránka nebo skript, které se s daným štítkem pro daného uživatele již setkaly. Pokud je tedy jedním z tematických štítků za poslední období pro daného uživatele „sport“, pak jej skript reklamní sítě vložený do webu „priklad.cz“ z domény „reklamni-sit.cz“ obdrží pouze v případě, že byl v minulosti skript z domény „reklamni-sit.cz“ načten do prohlížeče tohoto uživatele na jiném webu, kterému internetový prohlížeč přiřadil štítek „sport“, například na sportovním zpravodajském serveru nebo internetovém obchodu se sportovním vybavením. Toto opatření by mělo bránit tomu, aby pomocí tematických štítků webové stránky odvozovaly o uživatelích více informací, než mohou aktuálně odvodit pomocí cookies třetích stran.[60]

Vedle konceptu Topics API představil Google v lednu 2022 také koncept technologie FLEDGE umožňující cílení na uživatele, kteří navštívili určitou internetovou stránku.[61] Podstatou této technologie je provádění reklamních aukcí nikoli v systému reklamní burzy,[62] ale přímo ve webovém prohlížeči uživatele. Technologie by měla být používána tak, že pokud uživatel navštíví webovou stránku a její provozovatel chce takovému uživateli později zobrazit cílenou reklamu související s touto návštěvou, zapíše do internetového prohlížeče uživatele skutečnost, že uživatel spadá do zájmové skupiny definované tímto provozovatelem webové stránky.[63]

Následně při návštěvě webové stránky zobrazující reklamu by měl provozovatel takové webové stránky mít možnost zahájit v zařízení uživatele aukci, pro kterou by poskytl data o potenciálních účastnících (inze-

[59] Viz tamtéž.

[60] Viz tamtéž.

[61] Viz DUTTON, Sam, LEE, Kevin K. FLEDGE. In: *Chrome Developers* [online]. 27. 1. 2021 [cit. 22. 1. 2023]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/fledge/. K významu zkratky srov. Intent to Experiment: First "Locally-Executed Decision over Groups" Experiment (FLEDGE) In: *Google Groups* [online]. 25. 3. 2022 [cit. 22. 1. 2023]. Dostupné z: https://groups.google.com/a/chromium.org/g/blink-dev/c/0VmMSsDWsFg

[62] Viz blíže část 7.2 .

[63] Viz DUTTON, Sam, LEE, Kevin K. *FLEDGE* [online].

rentech) a zájmových skupinách, kterým tito inzerenti mají zájem zobrazit reklamu. Prohlížeč uživatele by pak oslovil ty inzerenty, jejichž zájmová skupina je v prohlížeči již zapsána, a podle jejich nabídek vyhodnotil vítěznou nabídku v aukci a zobrazil uživateli reklamu příslušného inzerenta.[64]

Vedle snah o nahrazení cookies třetích stran méně invazivními technologiemi zahrnuje inciativa *Privacy Sandbox* také další technologie, které by měly zabránit sledování chování uživatelů pomocí fingerprintingu. Jednou z nich je *Privacy Budget*, jejíž podstatou je sledování objemu informací, které si konkrétní webová stránka vyžaduje o internetovém prohlížeči a zařízení uživatele, a stanovení maximálního stropu pro objem poskytnutých informací tak, aby z těchto informací nebylo možné sestavit unikátní otisk zařízení.[65] Harmonogram jejího nasazení však Google zatím neuvádí.[66]

4. VÝVOJ PRÁVNÍ ÚPRAVY

Právní úprava ochrany soukromí v elektronických komunikacích má v evropském právu dlouhou historii. První směrnice upravující tuto oblast byla přijata v roce 1997 jako součást tzv. prvního telekomunikačního balíčku.[67] Tato směrnice ještě neobsahovala právní úpravu cookies, resp. ochrany koncového zařízení uživatele služeb elektronických komunikací.

V roce 2000 byla zahájena příprava nového legislativního rámce, později označovaného jako druhý telekomunikační balíček, jehož součástí se stala i současná směrnice 2002/58/ES.[68] Ta ve svém čl. 5 odst. 3 upravuje uchovávání informací a získávání přístupu k již uchovávaným informacím

[64] Viz tamtéž.

[65] Vit LASSEY, Brad. Combating Fingerprinting with a Privacy Budget. In: *GitHub* [online]. 25. 2. 2022 [cit. 6. 3. 2022]. Dostupné z: https://github.com/mikewest/privacy-budget WHITE, Alexandra. Privacy Budget. In: *Chrome Developers* [online]. 4. 3. 2022 [cit. 28. 10. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/privacy-budget/

[66] Viz *How We're Protecting Your Online Privacy* [online].

[67] Viz směrnici Evropského parlamentu a Rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví telekomunikací. Viz též PAPAKONSTANTINOU, Vagelis; DE HERT, Paul. The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights. *John Marshall Journal of Computer and Information Law* [online]. 2011, roč. 29, č. 1, [cit. 2. 2. 2023], s. 38.

v koncovém zařízení účastníka nebo uživatele služeb elektronických komunikací. Návrh směrnice z pera Evropské komise však tuto právní úpravu neobsahoval[69] – poprvé se objevila až v návrhu vzešlém z prvního čtení v Evropském parlamentu.[70] Evropský parlament přitom navrhl úpravu, která pro uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení účastníka nebo uživatele služeb elektronických komunikací (jako jsou například cookies) vyžadovala „předchozí výslovný souhlas".[71]

Tento návrh se setkal se silnou negativní reakcí organizací zastupujících reklamní sektor a podnikatele obecně.[72] Zřejmě s ohledem na tuto opozici Rada Evropské unie ve své společné pozici nahradila požadavek na souhlas požadavkem na informování a poskytnutí možnosti uchovávání a získávání přístupu odmítnout.[73] Tento protinávrh se nakonec promítl i do schváleného znění čl. 5 odst. 3 směrnice, které bylo následující:

> *Členské státy zajistí, aby užívání sítí elektronických komunikací k uchovávání informací nebo získávání přístupu k informacím uchovávaným v koncovém zařízení účastníka nebo uživatele bylo povoleno pouze za podmínky, že dotčený účastník či uživatel byl jasně a úplně informován v souladu se směrnicí 95/46/ES, mimo jiné o úče-*

---

[68] Viz PAPAKONSTANTINOU, Vagelis; DE HERT, Paul. *The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights*, s. 38.

[69] Viz návrh směrnice Evropského parlamentu a Rady o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací KOM/2000/0385 final – COD 2000/0189.

[70] Viz návrh směrnice Evropského parlamentu a Rady o zpracovávání osobních údajů a ochraně soukromí v odvětví elektronických komunikací KOM(2000) 385 final – C5-0439/2000 * 2000/0189(COD)), pozměňovací návrh 26.

[71] Tamtéž.

[72] Viz KOSTA, Eleni. Peeking into the cookie jar: the European approach towards the regulation of cookies. *International Journal of Law and Information Technology* [online]. 2013, roč. 21, č. 4 [cit. 11. 1. 2023], s. 387. MERCADO KIERKEGAARD, Sylvia. How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law & Security Review* [online]. 2005, roč. 21, č. 4 [cit. 11. 1. 2023].

[73] Viz společnou pozici (ES) č. 26/2002 přijatou Radou dne 28. ledna 2002 s ohledem na přijetí směrnice 2002/ES Evropského parlamentu a Rady ze dne 22. prosince 2002 o změně směrnice Evropského parlamentu a Rady (ES) č. …/…. … o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, (2002/C 113 E/03).

> *lech zpracování, a že je mu správcem údajů nabídnuto právo odmítnout takové zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení nebo usnadnění přenosu sdělení prostřednictvím sítí elektronických komunikací nebo, je-li to nezbytně nutné pro poskytování služeb informační společnosti, které si účastník nebo uživatel výslovně vyžádal.*[74]

Do českého právního řádu bylo ustanovení transponováno s účinností od 1. 5. 2005 prostřednictvím § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích (dále jen „ZEK“).

Další vývoj právní úpravy ovlivnil případ hudebního vydavatelství Sony/BMG. Některá hudební CD tohoto vydavatelství musela být na počítači přehrávána pomocí zvláštního softwarového přehrávače, který byl obsažen přímo na daném CD. V roce 2005 expert na bezpečnost Mark Russinovich odhalil, že při přehrávání příslušných CD nedojde na počítači pouze ke spuštění tohoto přehrávače, ale také k instalaci softwaru eXtended Copy Protection (XCP) společnosti First 4 Internet.[75]

Tento software sloužil jako technický prostředek ochrany autorských práv (nástroj pro tzv. *Digital Rights Management*, zkráceně DRM). Jeho cílem bylo omezit počet kopií hudebních CD, které bude možné pořídit, a zabránit tak jejich neoprávněnému rozmnožování. Software se však instaloval skrytě po vložení CD do počítače, bez upozornění uživatele (tomu bylo k akceptaci předloženo pouze licenční ujednání k vestavěnému hudebnímu přehrávači, které tento software nezmiňovalo), nastavoval sám pro sebe zvýšená oprávnění a kvůli nevhodnému návrhu zvyšoval zranitelnost počítače proti malwaru. Současně k němu nebyl poskytován žádný nástroj pro odinstalaci.[76] Následně bylo odhaleno, že jiná CD Sony/BMG obsahují podobný nástroj MediaMax-3, který však trpěl velmi podobnými nedo-

[74] Přestože tento text a jeho pozdější verze pracují se spojením „účastník nebo uživatel“ a návrh nařízení ePrivacy s pojmem „koncový uživatel“, pro zjednodušení v dalším výkladu používám pouze pojem uživatel ve stejném významu.

[75] Viz RUSSINOVICH, Mark. Sony, Rootkits and Digital Rights Management Gone Too Far In: *Mark's Blog* [online]. 17. 3. 2015 [cit. 11. 1. 2023]. Dostupné z: https://web.archive.org/web/20150317040653/http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx

statky.[77] Jednání společnosti Sony/BMG přitom bylo mimo působnost původního znění čl. 5. odst. 3 směrnice 2002/58/ES – nejednalo se totiž o přístup ke koncovému zařízení v souvislosti s užíváním služby elektronických komunikací.

V roce 2007 Evropská komise jako součást třetího telekomunikačního balíčku představila návrh směrnice novelizující směrnici 2002/58/ES.[78] Součástí tohoto návrhu byla také úprava čl. 5 odst. 3 tak, aby působnost ustanovení nebyla vázána na služby elektronických komunikací.[79] Teprve v rámci jednání v Evropském parlamentu byla do návrhu novely doplněna úprava požadující souhlas k uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení.[80] V rámci prvního čtení v Evropském parlamentu byl tento návrh doprovozen formulací „se zohledněním toho, že nastavení prohlížeče představuje předchozí souhlas".[81]

---

[76] Viz SunnComm MediaMax Security Vulnerability FAQ. In: *Electronic Frontier Foundation* [online]. 19. 7. 2007 [cit. 11. 1. 2023]. Dostupné z: https://www.eff.org/pages/sunncomm-mediamax-security-vulnerability-faq

[77] Viz KOSTA, Eleni. *Peeking into the cookie jar: the European approach towards the regulation of cookies*, s. 384.

[78] Viz návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele {SEK(2007) 1472} {SEK(2007) 1473} /* KOM/2007/0698 final – COD 2007/0248 */.

[79] Viz tamtéž.

[80] Viz legislativní usnesení Evropského parlamentu ze dne 24. září 2008 o návrhu směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele (KOM(2007)0698 – C6-0420/2007 – 2007/0248(COD)).

[81] Viz tamtéž.

Po odmítnutí ze strany Evropské komise[82] byl ve druhém čtení v Evropském parlamentu opět navržen souhlasový režim, avšak bez tohoto dovětku.[83]

Jak Evropská komise, tak Rada Evropské unie následně bez zvláštního odůvodnění návrh Evropského parlamentu na souhlasový režim přijaly[84] a novela byla vydána jako směrnice 2009/136/ES. Novelizovaný čl. 5 odst. 3 zní následovně:

> *Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí 95/46/ES, mimo jiné o účelu zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal.*

---

[82] Viz pozměněný návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele ze dne 6. 11. 2008, KOM/2008/0723 final - COD 2007/0248.

[83] Viz legislativní usnesení Evropského parlamentu ze dne 6. května 2009 ke společnému postoji Rady ohledně přijetí směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele (16497/1/2008 – C6-0068/2009 – 2007/0248(COD)).

[84] Viz stanovisko Komise podle čl. 251 odst. 2 třetího pododstavce písm. c) Smlouvy o ES ke změnám navrženým Evropským parlamentem týkajícím se společného postoje Rady v souvislosti s návrhem směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, kterým/kterou se mění návrh Komise podle čl. 250 odst. 2 Smlouvy o ES ze dne 29. 7. 2009, KOM/2009/0421 final – COD 2007/0248.Viz též KOSTA, Eleni. op. cit., s. 390.

Za zmínku stojí také to, že ještě před finálním schválením směrnice Evropským parlamentem a Radou vydalo 13 členských států (nezahrnujících Českou republiku) stanovisko, že článek 5 odst. 3 není míněn jako změna stávajícího požadavku, kdy může být souhlas vykonán jako právo odmítnout cookies nebo podobné technologie používané pro legitimní účely.[85] V tomto stanovisku se opírají o bod 66 odůvodnění směrnice 2009/136/ES, který se vztahuje k uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, nehovoří však překvapivě o souhlasu, ale o právu takové činnosti odmítnout.[86]

Poněkud překvapivá byla také reakce České republiky na směrnici 2009/136/ES. Tato směrnice byla sice do ZEK transponována zákonem č. 468/2011 Sb.,[87] § 89 odst. 3 však tímto zákonem novelizován nebyl.[88] Ke korektní transpozici tak došlo až zákonem č. 374/2021 Sb. s účinností od 1. 1. 2022.

5. PLATNÁ PRÁVNÍ ÚPRAVA

Platná právní úprava uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení je obsažena v § 89 odst. 3 ZEK, který stanoví:

---

[85] Viz Dodatek k poznámce „I/A“ Přijetí návrhu směrnice Evropského parlamentu a Rady (ES) č. 1308/2006 Rady, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, 2002/19/ES o přístupu a propojení k sítím a službám elektronických komunikací a 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (LA + S) (třetí čtení) ze dne 18. 11. 2009, 2007/0247 (COD), 15864/09 ADD 1 REV 1, změněno Opravou dodatku k poznámce „I/A“ Přijetí návrhu směrnice Evropského parlamentu a Rady (ES) č. 1308/2006 Rady, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, 2002/19/ES o přístupu a propojení k sítím a službám elektronických komunikací a 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (LA + S) (třetí čtení) ze dne 19. 11. 2009, 2007/0247 (COD), 15864/09 ADD 1 REV 1 COR 1.

[86] Viz tamtéž.

[87] Viz důvodovou zprávu k zákonu č. 468/2011 Sb.

[88] K chybné transpozici čl. 5 odst. 3 viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie* [online]. 2014, roč. 5, č. 9 [cit. 23. 1. 2023], s. 60. TOMÍŠEK, Jan. Cookies a GDPR. *Právní rozhledy* [online]. 2018, roč. 26, č. 20 [cit. 6. 2. 2023], s. 688.

> *Každý, kdo hodlá používat nebo používá sítě elektronických komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních účastníků nebo uživatelů, získá od těchto účastníků nebo uživatelů předem prokazatelný souhlas s rozsahem a účelem jejich zpracování. Tato povinnost neplatí pro technické ukládání nebo přístup výhradně pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací nebo je-li to nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem.*

Z pohledu cookies a podobných technologií umožňujících ukládání údajů v zařízení uživatele, jak jsou ETrackers a webové úložiště, tato úprava znamená požadavek na získání souhlasu s ukládáním cookies do koncového zařízení a jejich následným čtením, vyjma případů, kdy jsou tyto cookies nebo podobné technologie nezbytné k fungování webové stránky, např. košíku v internetovém obchodě.[89]

Aplikace právní úpravy na techniky využívající údaje o zařízení uživatele (fingerprinting) je méně jasná. Dle stanoviska Pracovní skupiny pro ochranu osobních údajů zřízené podle článku 29 (dále jen „WP29“)[90] se čl. 5 odst. 3 směrnice 2002/58/ES na tyto techniky vztahuje „[j]e-li otisk vytvořen uchováváním informací nebo získáním přístupu k informacím uchovávaným v koncovém zařízení uživatele.“[91] Stanovisko bohužel neobjasňuje, které údaje se z pohledu Pracovní skupiny získávají přístupem k informacím uchovávaným v koncovém zařízení uživatele a které nikoli.

Domnívám se, že tuto otázku je třeba posuzovat ve světle bodu 24 odůvodnění směrnice 2002/58/ES, který uvádí, že koncové zařízení je součástí soukromí uživatele, v anglickém znění součástí jeho privátní sféry (*private sphere)*. Bylo by podle mě příliš extenzivní dovozovat, že součástí této

[89] K tomu, jaké cookies lze považovat za nezbytné a jaké nikoli, viz WP194, s. 6. Pro shrnutí a diskuzi viz TOMÍŠEK, Jan. *Cookies a GDPR*, s. 691. Viz také KOSTA, Eleni. *Peeking into the cookie jar: the European approach towards the regulation of cookies*, s. 393.

[90] WP29 byla orgánem, který sdružoval jednotlivé dozorové úřady členských států podle právní úpravy předcházející GDPR, tedy podle směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

privátní sféry jsou rovněž údaje, které o sobě zařízení aktivně vysílá v hlavičce požadavku na získání webové stránky v rámci protokolu HTTP.[92] Naopak součástí této privátní sféry jsou podle mého názoru údaje, které musí být zjišťovány pomocí skriptu spuštěného na koncovém zařízení. Tyto údaje nejsou sice v úzkém slova smyslu uchovávány v koncovém zařízení podobně, jako jsou strukturovaně uchovávány např. cookies nebo údaje ve webovém úložišti, jsou však jako atributy v zařízení uloženy, proto je mohou spuštěné skripty zjišťovat. Současně jak uvádí WP29, pojem přístup k údajům uloženým v koncovém zařízení se nevztahuje pouze na údaje, které do zařízení uložila konkrétní webová stránka , ale i na údaje dříve uložené.[93] Dovozuji tedy, že se čl. 5 odst. 3 neaplikuje na pasivní fingerprinting, ale pouze na fingerprinting aktivní.

---

[91] Viz WP224, s. 7. Tento závěr potvrzuje rovněž Prohlášení Evropského sboru pro ochranu osobních údajů k revizi nařízení o soukromí a elektronických komunikacích a jeho dopad na ochranu jednotlivců s ohledem na soukromí a důvěrnost jejich komunikací, které uvádí, že „nejen cookies, ale každá sledovací technologie již podléhá souhlasu uživatele nebo podléhá některé z výjimek uvedených v ePrivacy směrnici“ (viz Evropský sbor pro ochranu osobních údajů. Prohlášení Evropského sboru pro ochranu osobních údajů o revizi nařízení o soukromí a elektronických komunikacích a jejím dopadu na ochranu fyzických osob v souvislosti se soukromím a důvěrným charakterem jejich komunikace. In: *European Data Protection Board*. [online]. 5. 5. 2018 [cit. 16. 7. 2018]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_cs_0.pdf), a také návrh Doporučení k zpracovaní cookies a obdobných prostředků sledovaní od 25. května 2018 vydané Úřadem pro ochranu osobních údajů, které v bodě 2 hovoří o „používání cookies, počítačových souborů, které mimo jiné umožňují jednoznačně rozpoznat přístroj, a jiných obdobných prostředků používaných k rozlišení koncových zařízení uživatelů (jedná se například o otisky zařízení, angl. device fingerprinting).“ Viz Úřad pro ochranu osobních údajů. Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018. In: *Úřad pro ochranu osobních údajů* [online]. 25. 6. 2020. [cit. 1. 2. 2023]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=42915

[92] Jde o údaje o internetovém prohlížeči a operačním systému uživatele, včetně jejich verze, obsažené v poli *User-Agent*. Viz Internet Engineering Task Force. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content [online]. červen 2014. Červen 2014 [cit. 1. 2. 2023]. In: *Data Tracker*. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7231#section-5, čl. 5.1. Toto pole může mít například pro zařízení Apple iPhone a internetový prohlížeč Safari tvar „Mozilla/5.0 (iPhone; CPU iPhone OS 12_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1“ nebo pro počítač s operačním systémem Microsoft Windows 10 a internetovým prohlížečem Chrome „Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36“.

[93] Viz WP224, s. 8.

Samotný požadavek na souhlas je pak třeba vykládat v souladu s požadavky na souhlas stanovené GDPR – směrnice 2002/58/ES ve svém čl. 2 písm. f) stanoví, že „souhlas uživatele či účastníka odpovídá souhlasu subjektu údajů podle směrnice 95/46/ES“, která byla zrušena a nahrazena GDPR. GDPR ve svém článku 94 odst. 2 pak stanoví, že odkazy na směrnici 95/46/ES se považují za odkazy na GDPR.[94] To znamená, že souhlas musí být v souladu s čl. 4 bodem 11 GDPR „svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“.

Podrobnostem získávání souhlasu se věnují stanoviska řady dozorových úřadů členských států EU.[95] Svobodnost souhlasu v kontextu cookies znamená především, že souhlas nemůže být vynucován znemožněním přístupu k webové stránce či mobilní aplikaci při jeho neudělení (tzv. *cookie walls*

[94] Ke vztahu směrnice 2002/58/ES a GDPR blíže viz Evropský sbor pro ochranu osobních údajů. Stanovisko č. 5/2019 ke vzájemnému působení mezi směrnicí o soukromí a elektronických komunikacích a obecným nařízením o ochraně osobních údajů (GDPR), zejména pokud jde o příslušnost, úkoly a pravomoci úřadů pro ochranu údajů. In: *European Data Protection Board* [online]. 12. 3. 2019. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_cs.pdf ETTELDORF, Christina. EDPB on the Interplay between the ePrivacy Directive and the GDPR Reports: European Union. *European Data Protection Law Review* [online]. 2019, roč. 5, č. 2 [cit. 2. 2. 2023].

[95] Například viz Commission nationale de l'informatique et des libertés. Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ». In: *Commission nationale de l'informatique et des libertés* [online]. [cit. 1. 2. 2023]. Str. 7. Dostupné z: https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf. Information Commissioner's Office. How do we comply with the cookie rules? In: *Information Commissioner's Office* [online]. [cit. 1. 2. 2023]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/. Na další stanoviska odkazuje Spolek pro ochranu osobních údajů. Viz Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022. In: *Spolek pro ochranu osobních údajů* [online]. 15. 12. 2021. [cit. 1. 2. 2023]. Dostupné z: https://www.ochranaudaju.cz/wp-content/uploads/2021/12/Stanovisko_cookies_2021_final.pdf. S politováním je třeba konstatovat, že mezi úřady, které ke cookies vydaly stanovisko, se neřadí český Úřad pro ochranu osobních údajů, který pouze v roce 2018 vydal návrh svého doporučení k veřejné konzultaci, finální stanovisko však vydáno nebylo. Viz Úřad pro ochranu osobních údajů. Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018 [online]. Ke kritice doporučení viz TOMÍŠEK, Jan. *Cookies a GDPR*.

nebo *tracking walls*).[96] Konkrétnost se promítá do požadavku na uvedení účelů, ke kterým budou cookies použity, přičemž uživatel musí mít možnost rozhodovat o udělení či neudělení souhlasu k jednotlivým účelům.[97] Informovanost souhlasu pak znamená zejména povinnost uvedení informací o totožnosti subjektu žádajícího souhlas, rozsahu a účelech zpracování a o právu souhlas kdykoliv odvolat.[98] Ve vztahu ke cookies je významná informace o době exspirace cookies[99] a třetích stranách, které případně budou cookies na základě souhlasu do zařízení uživatele ukládat, resp. je číst.[100] Požadavek na jednoznačnost projevu vůle vylučuje udělen

[96] Viz Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022 [online], s. 3; Evropský sbor pro ochranu osobních údajů. Pokyny č. 05/2020 k souhlasu podle nařízení 2016/679 ze dne 4. května 2020. In: *European Data Protection Board* [online]. 4. 5. 2020. [cit. 1. 2. 2023]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=47474t. Dále viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. Adtech and real-time bidding under European data protection law. *German Law Journal* [online]. 2022, roč. 23, č. 2, [cit. 6. 2. 2023] s. 236.

[97] Viz Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022 [online], s. 3 a 5. Dále viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 236.

[98] Viz bod 42 odůvodnění GDPR.

[99] Viz rozsudek SDEU (velkého senátu) ze dne 1. října 2019 ve věci C-673/17, Planet49, bod 75.

[100] Blíže k informační povinnosti viz také Evropský sbor pro ochranu osobních údajů. Pokyny č. 8/2020 k cílení na uživatele sociálních médií ze dne 13. dubna 2021. In: *European Data Protection Board* [online]. 13. 4. 2021. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2021- 11/edpb_guidelines_082020_on_the_c_cs_0.pdf. Bod 72 a násl. Dále viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 236.

souhlasu např. prostým pokračováním v prohlížení webové stránky.[101] Při sběru souhlasu je také třeba se vyhnout klamavým praktikám.[102]

6. NAŘÍZENÍ EPRIVACY

Návrh nařízení ePrivacy představila Evropská komise v lednu 2017.[103] Příslušný výbor Evropského parlamentu k němu v říjnu 2017 schválil řadu pozměňovacích návrhů, které se staly oficiální pozicí Evropského parlamentu pro jednání s Evropskou komisí a Radou Evropské unie.[104] Souběžně probíhaly diskuze v Radě,[105] které v únoru 2021 vyústily ve společnou pozici Rady pro jednání s Evropským parlamentem.[106]

Ochraně informací uchovávaných v koncových zařízeních uživatelů a souvisejících s těmito zařízeními ve vztahu ke cookies se návrh Evropské komise věnuje v čl. 8 odst. 1. Čl. 10 pak stanovuje požadavky na nastavení webových prohlížečů týkající se cookies a podobných technologií.[107]

Působnost čl. 8 odst. 1 je vztažena k „využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z kon-

[101] Podle SDEU GDPR „výslovně vylučuje považovat za souhlas ‚[m]lčení, předem zaškrtnutá políčka nebo nečinnost'". Viz rozsudek SDEU ze dne 1. října 2019 ve věci C-673/17 (Planet49), bod 62. Dále viz Spolek pro ochranu osobních údajů. op.cit. s. 4. VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 236. Úvahu o „udělení souhlasu jednoznačnou akcí uživatele na webu, např. kliknutím na libovolný odkaz, pokud je uživatel předem poučen (např. v informační liště), že taková akce se považuje za souhlas, a je mu dána možnost souhlas neudělit (např. vypnutím příslušné funkce zahrnující zpracování osobních údajů v nastavení stránky předtím, než je příslušné zpracování osobních údajů zahájeno)" vyjádřenou v TOMÍŠEK, Jan. Cookies a GDPR. *Právní rozhledy*. 2018, roč. 26, č. 20, s. 693. lze ve světle stanovisek dozorových úřadů považovat za překonanou. Pro historickou perspektivu viz BORGESIUS, Frederik J. Zuiderveen. *Personal data processing for behavioural targeting: which legal basis?* [online]. 2015, roč. 5, č. 3, [cit. 1. 2. 2023]., s. 170.

[102] Evropský sbor pro ochranu osobních údajů. Report of the work undertaken by the Cookie Banner Taskforce, Adopted on 17 January 2023. In: *European Data Protection Board* [online]. 17. 1. 2023. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

[103] Viz návrh Komise.

[104] LAURISTIN, Marju. Zpráva o návrhu nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES. A8-0324/2017. In: *European Parliament* [online]. 20. 10. 2017 [cit. 11. leden 2023]. Dostupné z: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html (dále jen „pozice Evropského parlamentu").

cových zařízení koncových uživatelů, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení koncoví uživatelé“. Z této formulace oproti čl. 5 odst. 3 směrnice 2002/58/ES jednoznačně plyne, že se právní úprava vztahuje nejen na technologie spočívající v ukládání dat do webového prohlížeče uživatele jako cookies nebo webové úložiště, ale také techniky pracující s údaji, které lze z koncového zařízení získat a vypovídají o jeho hardwaru či softwaru, jako je fingerprinting. Současně jsem však toho názoru, že stejně jako čl. 5 odst. 3 směrnice 2002/58/ES se úprava čl. 8 odst. 1 nevztahuje na pasivní fingerprinting, tj. na použití údajů, které o sobě zařízení aktivně vysílá, jako jsou údaje z hlaviček požadavků protokolu HTTP.[108]

Tituly k využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z koncových zařízení uživatelů, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení uživatelé, jsou shodně se současnou úpravou technická nezbytnost dle písmen a)

[105] Pro shrnutí vývoje v různých fázích viz např. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Progress report. 2017/0003(COD), 13106/20. In: *EUR-Lex* [online]. 23. 11. 2020 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-13106-2020-INIT/en/pdf Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 5008/2. In: *EUR-Lex* [online]. 5. 1. 2021 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf Pro přehled všech verzí viz návrh Úřad pro publikace Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 52017PC0010. In: *EUR-Lex* [online]. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010

[106] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP. 2017/0003(COD), 6087/21. In: *EUR-Lex* [online]. 10. 2. 2021 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT (dále jen „pozice Rady“).

[107] Viz návrh Komise.

a c) a souhlas uživatele dle písmene b). Doplněno bylo pouze písmeno d) umožňující tyto činnosti ve vztahu k „měření návštěvnosti internetových stránek, za předpokladu, že toto měření je prováděno poskytovatelem služby informační společnosti požadované koncovým uživatelem“.[109]

Novinkou v návrhu je především uložení povinností tvůrcům internetových prohlížečů v čl. 10. Tyto povinnosti však byly navrženy poměrně mírně – příslušný software by pouze musel „nabízet možnost zabránit třetím stranám v uchovávání informací v koncovém zařízení koncového uživatele nebo ve zpracovávání informací, které jsou v tomto zařízení již uchovávané“ (tj. možnost blokovat cookies a podobné technologie), a při instalaci informovat koncového uživatele o možnostech nastavení ochrany soukromí a k tomu, aby mohla instalace pokračovat, vyžadovat souhlas koncového uživatele s nastavením.[110]

Pozice Evropského parlamentu oproti návrhu Komise zúžila formulaci titulů pro přístup k zařízení koncového uživatele předložených Komisí (např. požadavkem na „striktní“ technickou nezbytnost nebo požadavkem na „určitý souhlas“).[111] Dále rozpracovala podmínky pro uplatnění titulu měření návštěvnosti webu a doplnila nové tituly bezpečnostních aktualizací softwaru a nezbytného přístupu zaměstnavatele k pracovnímu zařízení.[112] Doplněno rovněž bylo ustanovení specificky zakazující *cookie walls* bránící v přístupu k webové stránce při neudělení souhlasu.[113]

---

[108] Na pasivní fingerprinting lze aplikovat čl. 8 odst. 2 návrhu Komise, který se vztahuje na „[s]hromažďování informací vysílaných koncovým zařízením za účelem umožnění připojení tohoto zařízení k jinému zařízení“. Dle písmene b) tohoto ustanovení však lze takový fingerprinting realizovat, pokud „je zobrazeno jasné a nápadné oznámení informující alespoň o způsobech shromažďování, jeho účelu a osobě, která je za ně odpovědná, a podávající další informace požadované podle článku 13 nařízení (EU) 2016/679, pokud jsou shromažďovány osobní údaje, jakož i o případných opatřeních, která může koncový uživatel koncového zařízení učinit, aby shromažďování minimalizoval nebo zastavil“ a současně za podmínky použití vhodných technických a organizačních opatření podle čl. 32 GDPR.

[109] Viz čl. 8 odst. 1 návrhu Komise. Překlad autor.

[110] Viz čl. 10 odst. 1 a 2 návrhu Komise.

[111] Viz pozměňovací návrhy č. 84 až 88 pozice Evropského parlamentu.

[112] Viz pozměňovací návrhy č. 89 až 91 tamtéž. Úpravu měření návštěvnosti doplňuje rovněž pozměňovací návrh č. 99 tamtéž.

[113] Viz pozměňovací návrh č. 92 tamtéž.

Významně byly v pozici Evropského parlamentu přepracovány povinnosti tvůrců internetových prohlížečů. Nově by internetové prohlížeče musely ve výchozím nastavení blokovat cookies a podobné technologie s výjimkou takových, které jsou technicky nezbytné, při instalaci uživateli nabídnout možnost toto výchozí nastavení odsouhlasit nebo změnit, nabídnout též možnost rozhodnout o blokaci cookies a podobných technologií pro měření návštěvnosti a nabízet možnost udělení určitého souhlasu nastavením prohlížeče.[114]

Pro účely tohoto určitého souhlasu má uživatel být před prvním použitím prohlížeče informován o možnosti nastavit souhlasy pro každou webovou stránku samostatně a tato možnost nastavení má být neustále snadno dostupná.[115] Toto individuální nastavení by zřejmě měla mít možnost iniciovat i jednotlivá webová stránka.[116] Tato nastavení souhlasů a námitek proti zpracování ve smyslu čl. 21 GDPR by se současně měla promítnout do technicky specifikovaných signálů odesílaných webovým stránkám. Tyto signály by pak měly být pro příslušné webové stránky závazné.[117] Pozice Evropského parlamentu také rozšiřuje požadavek na souhlas na pasivní fingerprinting, pokud slouží jiným než technickým nebo statistickým účelům.[118]

Souběžné diskuze v Radě Evropské unie byly komplikované – trvaly více než 4 roky a ve vztahu k článku 8 a souvisejícím bodům odůvodnění při nich vzniklo nejméně 12 různých verzí návrhu obsahujících dílčí změny.[119] V úvodu diskuzí vyjádřily některé členské státy potřebu nalézt vyvážené řešení reagující na problém „souhlasového vyčerpání“ (*consent fatigue*), tedy

[114] Viz pozměňovací návrhy č. 106 až 109 tamtéž.

[115] Viz pozměňovací návrh č. 110 tamtéž.

[116] Viz pozměňovací návrh č. 116 tamtéž.

[117] Viz pozměňovací návrhy č. 103 a 111 až 115 tamtéž.

[118] Viz pozměňovací návrhy č. 95 až 99 tamtéž.

[119] Viz Úřad pro publikace Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 52017PC0010. In: *EUR-Lex* [online]. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010.

přetížení uživatelů četnými požadavky na souhlas.[120] Významným tématem diskuzí byly také technické a ekonomické vlastnosti ekosystému internetové reklamy.[121]

K prvním změnám v návrhu začalo docházet v průběhu estonského předsednictví během podzimu 2017. Článek 9 upravující souhlasy byl z důvodu obecnosti přesunut do kapitoly I jako článek 4a[122] – tato změna přetrvala až do finální pozice Rady.[123] Podobně jako v Evropském parlamentu bylo navrženo doplnění titulu pro aktualizace softwaru,[124] následně také pro lokalizaci volajícího v případě nouzového volání.[125]

[120] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Discussion on possible compromise solutions. 2017/0003(COD), 5934/19. In: *EUR-Lex* [online]. 4. 2. 2019, s. 3. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5934_2019_INIT

[121] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Presidency note. 2017/0003 (COD), 10866/17. In: *EUR-Lex* [online]. 3. 7. 2017, s. 4. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10866_2017_INIT

[122] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003 (COD), 11995/17. In: *EUR-Lex* [online]. 8. 9. 2017, čl. 4a. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11995_2017_INIT

[123] Viz pozice Rady, čl. 4a.

[124] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003 (COD), 11995/17. čl. 8.

[125] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency. 2017/0003 (COD), 15333/17. In: *EUR-Lex* [online]. 5. 12. 2017, čl. 8. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15333_2017_INIT

Přestože v říjnu 2017 schválil svůj návrh Evropský parlament, do návrhů diskutovaných v Radě se viditelným způsobem nepromítl,[126] předmětem diskuze však byla mimo jiné otázka, zda by prohlížeče měly umožňovat udělení souhlasu pro konkrétní webové stránky.[127] K diskuzi byla také předložena možnost zahrnout do textu titul pro přístup ke koncovému zařízení v podobě oprávněného zájmu.[128] Ani jeden z těchto návrhů se v danou chvíli nepromítl do diskutovaného textu,[129] předmětem diskuze se však stala otázka *cookie walls a* do bodu 21 odůvodnění byla doplněna věta deklarující, že přijetí cookies může být podmínkou přístupu k webové stránce.[130]

Problematika souhlasu jako podmínky přístupu pak byla v rámci odůvodnění postupně rozpracovávána i v dalších verzích návrhu.[131] Nejprve byla textace formulována tak, že souhlas může být vyžadován pro přístup k obsahu poskytovanému bez přímé platby, pokud je uživateli současně nabídnuta ekvivalentní možnost, jak k obsahu přistupovat bez udělení souhlasu.[132] V návrhu rakouského předsednictví Rady pak byla tato formulace doplněna deklarací, že použití cookies může být nezbytné v případě webové

[126] Viz tamtéž. Pouze zmínka o zařízeních zaměstnavatele se později promítla do bodu 20a odůvodnění návrhu viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions. 2017/0003(COD), 5934/19. s. 4.

[127] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper 2017/0003(COD), 5165/18. In: *EUR-Lex* [online]. 11. 1. 2018, s. 22. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5165_2018_INIT

[128] Viz tamtéž, s. 21.

[129] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion. 2017/0003(COD), 7207/18. In: *EUR-Lex* [online]. 22. 3. 2018, čl. 8 a 10. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7207_2018_INIT

[130] Viz tamtéž, bod 21 odůvodnění.

stránky, která je převážně financována z reklamy, pokud je uživatel vhodným způsobem informován o účelech použití cookies a toto užití přijal,[133] toto doplnění však bylo finským předsednictvím vypuštěno.[134]

Současně byl po diskuzi vypuštěn celý čl. 10 upravující funkcionality webových prohlížečů, a to s ohledem na obavy o dopady na zátěž pro prohlížeče a aplikace, otázky hospodářské soutěže a také schopnosti tohoto ustanovení řešit problém „souhlasového vyčerpání" (*consent fatigue*).[135] Ma-

[131] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency. 2017/0003(COD), 10975/18. In: *EUR-Lex* [online]. 10. 7. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT bod odůvodnění 20. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 13256/18. In: *EUR-Lex* [online]. 19. 10. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT bod odůvodnění 21. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions. 2017/0003(COD), 5934/19. s. 3.

[132] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 10975/18. bod odůvodnění 20.

[133] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 13256/18. bod odůvodnění 21. Tato formulace se zdá být vnitřně rozporná, protože odkazuje z hlediska titulu pro přístup k zařízení jak na nezbytnost pro poskytování služby, tak na souhlas.

[134] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 11291/19. In: *EUR-Lex* [online]. 26. 7. 2019, bod 21 odůvodnění. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11291_2019_INIT

terie byla v pozdější verzi částečně doplněna do bodu 21a odůvodnění návrhu.[136]

Za významný považuji návrh chorvatského předsednictví, který v návaznosti na dřívější diskuze[137] do čl. 8 vkládá jako právní titul pro přístup ke koncovému zařízení oprávněný zájem.[138] Navržená formulace byla obdobná čl. 6 odst. 1 písm. f) GDPR – přístup ke koncovému zařízení by byl možný, pokud by to bylo nezbytné pro účely oprávněných zájmů poskytovatele, s výjimkou případů, kdy by nad takovým zájmem převažovaly zájmy nebo základní práva a svobody koncového uživatele.[139] Návrh byl doplněn ustanovením stanovícím domněnku, že zájmy koncového uživatele převažují nad zájmy poskytovatele služby mj. v případě, kdy poskytovatel služby shromažďuje nebo zpracovává informace za účelem profilování uživatele.[140] Vedle toho byl doprovozen zákazem takto získané informace v neanonymizované podobě sdílet s jinými subjekty, vyjma zpracovatelů zavázaných podle čl. 28 GDPR. Podmínkou jeho využití bylo také předchozí posouzení vlivu zamýšlené činnosti na důvěrnost komunikací a soukromí koncových uživatelů podle čl. 35 GDPR, informování uživatele o zamýšleném přístupu a jeho právu tento přístup odmítnout a přijetí přiměřených technických a organizačních opatření.[141]

---

[135] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 017/0003(COD), 10975/18. s. 3

[136] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions 2017/0003(COD), 5934/19. s. 3.

[137] Viz tamtéž, s. 21.

[138] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003(COD), 5979/20. čl. 8 odst. 1 písm. g) a odst. 1a.

[139] Viz tamtéž, čl. 8 odst. 1 písm. g).

[140] Viz tamtéž.

[141] Viz tamtéž, čl. 8 odst. 1a a bod odůvodnění 21b.

Tento návrh byl podroben diskuzi v Radě, přičemž z podkladu německého předsednictví, které následovalo po předsednictví chorvatském, vyplývá obava, že by tento přístup „výrazně usnadnil instalaci softwaru, který je často považován za hlavní vstupní bránu pro škodlivý software.“[142] Německé předsednictví proto navrhlo buď zachovat chorvatský návrh a diskutovat, jak zajistit bezpečnost koncových zařízení, nebo se vrátit k předchozí textaci finského předsednictví, která oprávněný zájem jako titul pro přístup ke koncovému zařízení nepřipouštěla.[143] Druhý navrhovaný přístup v Radě převládl a oprávněný zájem byl jako titul nakonec z textace vypuštěn.[144]

Ve finálním znění pozice Rady se tak samotný čl. 8 odst. 1 od původní textace navržené Evropskou komisí liší výčtem titulů pro přístup ke koncovému zařízení, ne však koncepčně.[145] Zpřesněn je titul pro měření návštěvnosti[146] a doplněn titul pro zajištění bezpečnosti služby informační společnosti, předcházení podvodům a detekci technických chyb,[147] titul pro bezpečnostní aktualizace softwaru[148] a titul pro přístup k zařízení v případě nouzového volání.[149] Dále je doplněno nové ustanovení upravující okolnosti, které by měly být zohledněny při posuzování, zda je zpracování informací získaných ze zařízení koncového uživatele k jiným účelům slučitelné s původním účelem, pro který byly informace získány, a podmínky ta-

[142] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications) – Presidency discussion paper 2017/0003(COD), 9243/20. In: *EUR-Lex* [online]. 6. 6. 2020, s. 6, překlad autor. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT

[143] Viz tamtéž.

[144] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications). 2017/0003(COD), 9931/20. In: *EUR-Lex* [online]. 4. 11. 2020, s. 4 a čl. 8. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT

[145] Viz pozici Rady.

[146] Viz čl. 8 odst. 1 písm. d a bod 21a odůvodnění pozice Rady.

[147] Viz tamtéž, čl. 8 odst. 1 písm. da).

[148] Viz tamtéž, čl. 8 odst. 1 písm. e) a bod 21b odůvodnění.

[149] Viz tamtéž, čl. 8 odst. 1 písm. f).

kového dalších zpracování vč. zákazu sdílet takové informace s jinými subjekty než zpracovateli zavázanými podle čl. 28 GDPR nebo v anonymizované podobě.[150] Do čl. 8 odst. 2 pak byl podobně jako v pozici Evropského parlamentu doplněn požadavek na souhlas s pasivním fingerprintingem, pokud slouží jiným než statistickým účelům.[151]

Významné změny se dotýkají odůvodnění návrhu a čl. 9 a 10. V bodu odůvodnění 20aaaa bylo doplněno, že přístup k webové stránce bez přímé úhrady může být podmíněn souhlasem s ukládáním a čtením cookies, aniž by uživatel byl zbaven svobodné volby, a to za předpokladu, že jsou uživateli poskytovány srozumitelné informace o používání cookies a může si volit mezi variantou služby s udělením souhlasu a ekvivalentní nabídkou, která udělení souhlasu nevyžaduje.[152] Toto pravidlo přitom nemá být možné aplikovat v případě významné nerovnováhy mezi koncovým uživatelem a poskytovatelem služby, například u služeb veřejných institucí a poskytovatelů služeb v dominantním postavení na trhu.[153] Současně však bod 21aa odůvodnění uvádí, že použití cookies může být nezbytné v případě webové stránky, která je převážně financována z reklamy, pokud je uživatel vhodným způsobem informován o účelech použití cookies a toto užití přijal.[154]

Články 9 a 10 pak byly přetvořeny do čl. 4a, který však z hlediska požadavků na funkce webových prohlížečů obsahuje minimum z původního návrhu Evropské komise. V článku je tak pouze stanoveno, že souhlas je možné vyjádřit pomocí internetového prohlížeče.[155] Nově je přitom doplněno, že takto udělený souhlas má převážit nad nastavením softwaru, a pokud je uživatelem udělen pro konkrétní službu, má být okamžitě promítnut.[156]

Materie původního čl. 10 je pak přesunuta do bodu 20a odůvodnění, který uvádí, že koncoví uživatelé čelí častým žádostem o souhlas s použitím

[150] Viz tamtéž, čl. 8 odst. 1 písm. g) až i).

[151] Viz tamtéž, čl. 8 odst. 2.

[152] Viz tamtéž, bod 20aaaa odůvodnění.

[153] Viz tamtéž.

[154] Viz tamtéž, bod 21aa odůvodnění.

[155] Viz tamtéž, čl. 4a odst. 2.

[156] Viz tamtéž, čl. 4a odst. 2aa.

cookies, což může vést k přetížení koncových uživatelů a k tomu, že žádosti o souhlas nečtou, a to může v důsledku vést ke snížení úrovně poskytované ochrany. Proto by bylo užitečné, aby určitý a informovaný souhlas k jednomu či více účelům bylo možné vyjádřit pomocí nastavení internetového prohlížeče, například formou seznamu poskytovatelů, jimž bude použití cookies určitých typů dovoleno. Odůvodnění vyzývá tvůrce internetových prohlížečů k vytvoření takových možností, nejde však o právně závaznou povinnost. Vedle toho odůvodnění doplňuje, že „přímo vyjádřený" souhlas (patrně je tím myšlen souhlas ve vztahu ke konkrétní webové stránce) by měl mít vždy přednost.[157]

Návrh tedy prodělal v průběhu jednání v Radě významný vývoj, a to směrem odlišným, než se ubírá návrh Evropského parlamentu, který klade důraz na souhlas koncového uživatele a jeho povinnou a komplexní implementaci na úrovni nastavení webových prohlížečů. S ohledem na tuto rozdílnost vyjednávacích pozic Evropského parlamentu a Rady lze očekávat dlouhou diskuzi v rámci trialogu a také je namístě diskutovat, jaké řešení úpravy přístupu ke koncovému zařízení by bylo *de lege ferenda* nejvhodnější.

7. POŽADAVKY NA NOVOU PRÁVNÍ ÚPRAVU

Pro účely diskuze je vhodné shrnout, že platná právní úprava pro ukládání a čtení cookies a použití podobných technologií včetně použití údajů o koncovém zařízení vyžaduje ve většině případů souhlas – ten není třeba pouze pro cookies a podobné technologie nezbytné k fungování příslušné webové stránky. Souhlas musí splňovat požadavky GDPR, tedy být svobodný, konkrétní, informovaný a mít formu jednoznačného projevu vůle.

Návrh nařízení ePrivacy tento základní požadavek zachovává. Výslovně rozšiřuje působnost právní úpravy na využití funkcí koncového zařízení pro zpracování dat na shromažďování informací z koncových zařízení.[158] Jak ve znění předloženém Evropskou komisí, tak v rámci pozic Evropského parlamentu a Rady pak zavádí některé další úzce vymezené výjimky z poža-

[157] Viz tamtéž, bod 20a odůvodnění.

[158] Viz čl. 8 odst. 1 a bod 20 odůvodnění návrhu Komise.

davku na souhlas – z pohledu cookies je relevantní zejména výjimka pro měření návštěvnosti webových stránek.[159]

Evropský parlament a Rada se však významně rozchází v přístupu k udělování souhlasu. Evropský parlament klade důraz na svobodnost souhlasu (vč. zákazu cookie walls),[160] možnost udělování velmi specifických souhlasů prostřednictvím nastavení internetového prohlížeče[161] a povinnost webových stránek příslušné signály internetového prohlížeče respektovat.[162] Naopak Rada připouští, že pro přístup k webové stránce poskytované bezplatně může být souhlas s použitím cookies za definovaných podmínek vyžadován[163] a navrhuje, aby poskytnutí možnosti udělovat souhlasy prostřednictvím nastavení webového prohlížeče bylo pro tvůrce těchto prohlížečů dobrovolné.[164]

Tato rozdílnost pozic ukazuje na dva hlavní problémy, se kterými by se nová právní úprava měla vyrovnat. Na jedné straně je to problematika přetížení uživatelů žádostmi o souhlas. Na druhé straně pak potřeba zajistit přiměřené podmínky pro realizaci cílené reklamy, která je zdrojem financování pro některé webové stránky, které nabízejí uživatelům obsah či služby zdarma.

Současně je potřeba vnímat, že právní úprava čtení a ukládání cookies a použití podobných technologií jako součást právní úpravy soukromí v elektronických komunikacích je nástrojem ochrany práva na soukromí, které je základním právem chráněným čl. 7 odst. 1 a čl. 10 odst. 2 a 3 Listiny základních práva a svobod,[165] čl. 7 Listiny základních práv Evropské unie a čl. 8 Úmluvy o ochraně lidských práv a základních svobod Rady Evropy.[166] Toto pojetí vyplývá z bodů 1, 4, 5, 6 a 24 odůvodnění směrnice

[159] Viz přehled v části 6. výše.

[160] Viz pozměňovací návrh č. 92 pozice Evropského parlamentu.

[161] Viz pozměňovací návrhy č. 106 až 109 tamtéž.

[162] Viz pozměňovací návrhy č. 103 a 111 až 115 tamtéž.

[163] Viz bod 20aaaa odůvodnění pozice Rady.

[164] Viz bod 20a odůvodnění pozice Rady.

[165] Viz ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.

2002/58/ES, bodu 66 odůvodnění směrnice 2009/136/ES a z bodů 1 a 20 odůvodnění návrhu nařízení ePrivacy.

Nová právní úprava čtení a ukládání cookies a použití podobných technologií by tedy měla snížit zátěž uživatelů četnými žádostmi o souhlas, vytvořit přiměřené podmínky pro realizaci cílené reklamy jako zdroje financování pro některé webové stránky, a přitom zachovat nebo zvýšit úroveň ochrany soukromí jednotlivců v tomto kontextu.

7.1 PŘETÍŽENÍ ŽÁDOSTMI O SOUHLAS

Problém přetížení uživatelů četnými žádostmi o souhlas s použitím cookies je dle mého názoru spojen s přístupem k ochraně soukromí jako kontrole nad informacemi.[167] Ten vychází z historického pojetí soukromí jako práva jednotlivce „rozhodovat o tom, v jakém rozsahu budou jeho myšlenky a pocity komunikovány jiným,“[168] které v roce 1890 formulovali Warren a Brandeis a které se promítá se do pojetí soukromí řady moderních autorů, jako je Westin,[169] Moore[170] nebo Clarke.[171]

Přístup nastavený v roce 1890 však neobstojí tváří v tvář současným technologiím. Množství webových stránek, které pracují s informacemi relevantními pro soukromí uživatele a které běžný uživatel může za jediný den navštívit, je tak vysoké, že kvalifikované vykonání kontroly nad nakládáním s takovými informacemi (typicky rozhodnutí o udělení či neudělení souhlasu) není reálné.

Takové kvalifikované rozhodnutí by zpravidla vyžadovalo posouzení podrobných podmínek ochrany soukromí všech takových webových stránek.

---

[166] Viz sdělení č. 209/1992 Sb. federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

[167] Viz RICHARDS, Neil M.; HARTZOG, Woodrow. *Taking Trust Seriously in Privacy Law*, s. 444.

[168] Viz WARREN, Samuel D.; BRANDEIS, Louis D. Right to privacy. *Harvard Law Review* [online]. 1890, roč. 4, č. 5 [cit. 6. 2. 2023], s. 198.

[169] Viz WESTIN, A. *Privacy and Freedom*. New York: Ig Publishing, 2018, s. 24.

[170] Viz MOORE, Adam D. *Privacy rights: Moral and legal foundations*. Pennsylvania: Penn State Press, 2010, s.16.

[171] Viz CLARKE, R. Introduction to Dataveillance and Information Privacy, and Definitions of Terms In: *Roger Clarke's Web-Site* [online]. 24. 7. 2016 [cit. 3. 8. 2021]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html#Priv.

Podle výzkumu z roku 2008 by přitom průměrný Američan musel strávit v průměru 201 hodin tím, aby si rychle prošel všechny zásady ochrany soukromí, se kterými se za rok setká.[172] Domnívám se, že v současnosti by počet hodin byl výrazně vyšší s ohledem na intenzivnější používání internetu i vzhledem k tomu, že s rostoucími požadavky na transparentnost[173] rozsah těchto zásad spíše vzrostl.

Podle studie z roku 2020 zkoumající pět nejčastěji používaných nástrojů pro shromažďování souhlasů na 10 000 nejnavštěvovanějších webových stránkách ve Velké Británii byl medián počtu třetích stran uvedených v souhlasovém dialogu 315. Text popisující tyto třetí strany měl v průměru 7985 slov, což by znamenalo, že čtenář čtoucí 250 slov za minutu na každé webové stránce stráví průměrně více než 31 minut čtením o třetích stranách, na které se vztahuje souhlas, o který byl požádán.[174]

I při prostudování všech příslušných zásad a informací by přitom uživatel nejspíše čelil informační asymetrii, protože procesy zpracování dat navazující na použití cookies a podobných technologií jsou zpravidla komplexní a zásady ochrany soukromí tak nemohou obsahovat veškeré informace, které o nich má provozovatel webové stránky k dispozici.[175] S komplexností těchto procesů je také spojena komplexnost předkládaných voleb. Souhlas s použitím cookies a podobných technologií musí splňovat požadavky GDPR, proto se musí žádost o souhlas vztahovat ke všem účelům zpracování a uživatel musí mít možnost o účelech rozhodovat jednot-

[172] Viz MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* [online]. 2008, roč. 4, č. 3 [cit. 6. 3. 2022], s. 565.

[173] Zejména viz čl. 12 GDPR.

[174] Viz NOUWENS, Midas et al. 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]. New York, NY, USA: Association for Computing Machinery, 2020, [cit. 2. 2. 2023]. s. 4 a 6.

[175] Viz ACQUISTI, Alessandro et al. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys* [online]. 2017, roč. 50, č. 3 [cit. 2. 2. 2023] s. 4. CAROLAN, Eoin CASTILLO-MAYEN, M. Rosario. *Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws*, s. 380. COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics*, s. 51.

livě.[176] Ohledně jedné webové stránky tak nestačí učinit jedno rozhodnutí, ale je třeba takových rozhodnutí několik (jakkoli se nakonec mohou projevit jedinou akcí směřující k udělení souhlasu pro všechny účely).[177]

Zpracování takového množství informací naráží na kognitivní limity uživatele – behaviorální ekonomie v tomto směru používá pojem limitovaná racionalita.[178] Rozhodnutí v tomto směru jsou také ovlivňována zkresleními v úsudku a chování, které mohou vést k rozhodnutím, jež nejsou v souladu se skutečnými preferencemi uživatele.[179] K tomu mohou vést také úmyslné či neúmyslné manipulace ze strany provozovatelů webových stránek, kteří mají tendenci směřovat uživatele k volbě, která je pro provozovatele výhodnější (typicky udělení souhlasu), např. zvýrazněním příslušných tlačítek.[180]

Praktická implementace žádostí webových stránek o souhlas tak nevede k vyšší informovanosti uživatelů o cookies nebo podobných technologií nebo větší motivaci informace získávat.[181] Naopak tyto žádosti mohou v uživatelích vyvolávat (ne nutně podložený) pocit lepší ochrany soukromí

[176] Viz bod 43 odůvodnění GDPR. Dále viz Spolek pro ochranu osobních údajů. op. cit., s. 5.

[177] Nemluvě o případech, kdy provozovatel webové stránky proaktivně umožňuje rozhodování o jednotlivých třetích stranách, jak to například vyžaduje standard IAB TCF 2.0. Viz Interactive advertising bureau. IAB Europe Transparency & Consent Framework Policies. In: *Interactive advertising bureau* [online]. 21. 6. 2022 [cit. 22. 1. 2023]. Dostupné z: https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/ příloha B, část C, bod c.iii. V takových případech mohou být voleb desítky.

[178] Viz ACQUISTI, Alessandro et al. *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online,* s. 5.

[179] Viz ACQUISTI, Alessandro et al. *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online* s. 6. ; DOUGHERTY, Christie. *Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation*, s. 640.

[180] Viz UTZ, Christine et al. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [online]. New York, NY, USA: Association for Computing Machinery, 2019, [cit. 2. 1. 2022] s. 976. noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints. In: *noyb* [online]. 31. 5. 202 [cit. 24. 1. 2023]. Dostupné z: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints. Obdobně viz Evropský sbor pro ochranu osobních údajů. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them Version 1.0 Adopted on 14 March 2022. In: European Data Protection Board [online]. 14. 3. 2022 [cit. 1. 2. 2023] Dostupné z: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

a motivovat je k rozsáhlejšímu sdílení informací.[182] Současně uživatelé považují žádosti často za obtěžující.[183]

Jak tedy správně uvádí citovaný bod 20a odůvodnění návrhu nařízení ePrivacy ve znění pozice Rady Evropské unie, uživatelé internetu čelí častým žádostem o souhlas s použitím cookies, což může vést k přetížení koncových uživatelů a k tomu, že žádosti o souhlas nečtou,[184] a to může v důsledku vést ke snížení úrovně poskytované ochrany.

Řešením tohoto problému je snížení důrazu na kontrolu uživatele jako prostředku ochrany jeho soukromí. Aby toto snížení důrazu na kontrolu však současně neznamenalo snížení úrovně poskytované ochrany, je třeba najít alternativní řešení, které tuto ochranu zajistí. Východiskem dle mého názoru může být přístup k ochraně soukromí založený na důvěře, přebírající prvky z práva fiduciárních vztahů.[185]

Jak poznamenává von Lewinski, právní úprava ochrany osobních údajů je soubor pravidel, který upravuje asymetrii vznikající při zpracování

---

[181] Viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics,* s. 51.

[182] Viz CAROLAN, Eoin; CASTILLO-MAYEN, M. Rosario. Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws. *Virginia Journal of Law & Technology*. 2014, roč. 19, č. 2, s. 378.

[183] Viz KULYK, Oksana et al. Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity* [online]. 2020, roč. 6, č. 1, [cit. 1. 2. 2023], s. 4. Dále viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics,* s. 32.

[184] Viz KULYK, Oksana et al. tamtéž., s. 11.

[185] Viz RICHARDS, Neil M.; HARTZOG, Woodrow. *Taking Trust Seriously in Privacy Law*, s. 458. Samotná myšlenka přenesení poznatků z oblasti fiduciárních vztahů do oblasti ochrany soukromí byla poprvé formulována Jackem Balkinem. Viz BALKIN, Jack M. Information Fiduciaries in the Digital Age. In: *Balkinization.* [online] 5. 3. 2014 [cit. 3. 1. 2022]. Dostupné z: https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html_BALKIN, Jack M. Information fiduciaries and the first amendment. *UC Davis Law Review* [online]. 2015, roč. 49, č. 4 [cit. 12. 2. 2023]. K této myšlence viz ZITTRAIN, Jonathan. How to Exercise the Power You Didn't Ask For. *Harvard Business Review* [online]. 19. 9. 2018 [cit. 30. 10. 2022]. Ke kritice viz KHAN, Lina M.; POZEN, David E. A skeptical view of information fiduciaries. *Harvard Law Review* [online]. 2019, roč. 133, č. 2 [cit. 2. 2. 2023], s. 516. K diskuzi z českého prostředí viz TOMÍŠEK, Jan. Souhlasy s cookies a přístupy k ochraně osobních údajů. *Právník* [online]. 2022, roč. 161, č. 6 [cit. 6. 2. 2023], s. 571 a násl.

osobních údajů.[186] Tuto asymetrii lze podle mého názoru vyvážit nejen tím, že se slabší straně poskytne určitá kontrola nad zpracováním (přístup založený na kontrole), ale také tak, že se omezí jednání dominantní strany tak, aby se snížilo riziko, že zneužije svého postavení nebo bude jednat nedbale na úkor slabší strany. Domnívám se tedy, že nová právní úprava čtení a ukládání cookies a použití podobných technologií by měla namísto kontroly uložit subjektům, které činnosti provádí, takové povinnosti, které zajistí, že v souvislosti s těmito činnostmi nebudou jednat na úkor uživatele.

7.2 FINANCOVÁNÍ BEZPLATNÉHO OBSAHU A SLUŽEB

Problém financování webových stránek nabízejících bezplatný obsah a služby je podobně komplexní jako problém kontroly uživatele. Komentáře reprezentantů reklamního průmyslu budí dojem, že bez možnosti podmiňovat přístup k obsahu souhlasem s cookies se evropský mediální prostor zhroutí.[187] Takový pohled by byl patrně zjednodušující, na druhou stranu nelze podceňovat význam cílené reklamy pro financování médií a dalšího bezplatného obsahu.[188] Nezávislá média jsou přitom důležitá pro demokracii.[189] Z toho důvodu je namístě vést diskuzi, jak umožnit realizaci internetové reklamy způsobem, který by představoval zásah do práva na soukromí

[186] Viz VON LEWINSKI, Kai. Geschichte des Datenschutzrechts von 1600 bis 1977. In: *Freiheit-Sicherheit-Öffentlichkeit*. Heidelberg: Nomos Verlagsgesellschaft mbH & Co. KG, 2009, s. 200.

[187] Viz Interactive advertising bureau. ePrivacy Regulation. In: *Interactive advertising bureau* [online]. [cit. 20. 1. 2023]. Dostupné z: https://iabeurope.eu/proposed-eprivacy-regulation/. Podobně viz HÄRTING, Niko, GÖSSLING, Patrick. Study on the Impact of the Proposed Draft of the ePrivacy Regulation. *Computer Law Review International* [online]. 2018, roč. 19, č. 1 [cit. 20. 1. 2023].

[188] Viz Online platforms and digital advertising. In *Competition and Markets Authority*. [online]. 1. 7. 2020. Dostupné z: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, s. 6. Evropská komise. Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. In: *Evropská komise* [online]. 30. 1. 203 [cit. 2. 2. 2023]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en s. 97.

[189] Viz MCNAIR, Brian. Journalism and Democracy. In: *Journalism and Democracy* [online]. New York: Routledge, 2009, [cit. 20. 1. 2023], s. 248.

v rozsahu proporcionálním k přínosu pro právo na svobodu projevu, právo na přístup k informacím a demokratický právní stát jako veřejný statek.

Současný ekosystém internetové reklamy je ve velké míře založen na sdílení osobních údajů.[190] Tyto osobní údaje jsou sbírány jak inzerenty (např. internetovými obchody), tak provozovateli webových stránek zobrazujícími reklamu (např. online médii), resp. provozovatelé webových stránek zobrazujících reklamu umožňují tato data sbírat třetím stranám, jako jsou platformy poptávky (DSP),[191] platformy nabídky (SSP)[192] a platformy pro správu dat (DMP).[193] Tyto subjekty údaje sbírají, ukládají a budují z nich profil uživatele,[194] který využívají k tomu, aby se v reálném čase rozhodovali, jak je pro ně atraktivní zobrazení reklamy v konkrétní ploše na konkrétní webové stránce, kterou uživatel aktuálně prohlíží.[195] Současně si tyto subjekty údaje sdílí.[196]

---

[190] Ke zdůvodnění, proč jsou sdílená data osobními údaji viz Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29. Stanovisko 2/2010 k internetové reklamě zaměřené na chování. In: *Evropská komise* [online]. 22. 6. 2010. [cit. 2. 2. 2023] Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_cs.pdf s. 9. Dále srov. VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 233; Z BORGESIUS, Frederik J. Zuiderveen. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, [cit. 2. 2. 2023] s. 270.

[191] Srov. LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization,* s. 106.

[192] Viz LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 96, 345. YUAN, Shuai et al. Internet Advertising: An Interplay among Advertisers, Online Publishers, Ad Exchanges and Web Uses. In: *arXiv* [online]. 2. 7. 2012 [cit. 18. 11. 2022], s. 7.

[193] Viz LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 96, 124.

[194] Ve smyslu čl. 4 bod 4 GDPR.

[195] Viz LIU, Peng; CHAO, Wang. tamtéž, s. 18. YUAN, Shuai; WANG, Jun; ZHAO, Xiaoxue. Real-time bidding for online advertising: measurement and analysis. In: *Proceedings of the Seventh International Workshop on Data Mining for Online Advertising* [online]. 2013 [cit. 18. 11. 2022], s. 3.

[196] Viz LIU, Peng; CHAO, Wang. tamtéž s. 124. YUAN, Shuai et al. *Internet Advertising: An Interplay among Advertisers, Online Publishers, Ad Exchanges and Web Users* [online], s. 7.

Subjekty v tomto ekosystému legitimizují svoji činnost složitě konstruovanými souhlasy.[197] Podrobná diskuze platnosti těchto souhlasů z pohledu GDPR přesahuje rámec tohoto článku.[198] I kdybychom však předpokládali, že tyto souhlasy jsou platné, nelze ignorovat zásady ochrany osobních údajů stanovené v čl. 5 GDPR.[199] Jednou z těchto zásad je zásada korektnosti zpracování osobních údajů (v anglickém znění *fairness)*, která vchází z čl. 8 Listiny základních práv Evropské unie a která vyžaduje, „aby nebyly osobní údaje zpracovány způsobem, který je pro subjekt údajů neoprávněně škodlivý, nezákonně diskriminační, neočekávaný nebo zavádějící".[200] Klíčovými prvky korektnosti jsou mimo jiné očekávání, interakce, zákaz diskriminace a zákaz vykořisťování.[201]

---

[197] Viz Interactive advertising bureau. IAB Europe Transparency & Consent Framework Policies [online], příloha B, část C.

[198] Analýzu v tomto směru předkládají VEALE, Michael, BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 243.

[199] Tyto zásady mohou být porušeny, a to bez nutnosti porušení některého dalšího ustanovení GDPR. Viz Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022. In: *European Data Protection Board* [online]. 5. 12. 2022, bod 223. [31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf s odkazem na Evropský sbor pro ochranu osobních údajů. Závazné rozhodnutí 1/2021 ve věci sporu ohledně návrhu rozhodnutí irského dozorového úřadu týkajícího se společnosti WhatsApp Ireland podle čl. 65 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů. In: *European Data Protection Board* [online]. 28. 7. 2021, bod 191. [31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2022-03/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_cs.pdf

[200] Viz Evropský sbor pro ochranu osobních údajů. Pokyny 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů Verze 2.0 Přijato dne 20. října 2020. In: *European Data Protection Board.* [online]. 20. 10. 2020, bod 69. [cit. 31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_cs.pdf Též viz Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022 [online], bod 226.

[201] Viz Evropský sbor pro ochranu osobních údajů. Pokyny 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů Verze 2.0 [online], bod 70. Též viz Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022 [online], bod 227.

Výše popsaná struktura ekosystému internetové reklamy je vzdálená chápání běžných uživatelů internetu.[202] Lze tedy těžko dovozovat, že toky jejich osobních údajů v této struktuře jsou v souladu s jejich rozumným očekáváním. Důsledkem je to, že uživatelé neznají jednotlivé subjekty zapojené do tohoto systému a jejich postavení a nejsou schopni vykonávat vůči nim svá práva – chybí tedy element interakce. Systémy internetové reklamy také umožňují diskriminující praktiky[203] a využití zranitelnosti uživatelů pro manipulaci.[204]

Tyto dílčí rozpory podle mého názoru znamenají, že zpracování osobních údajů ve stávající struktuře ekosystému internetové reklamy představuje ze strany zapojených správců osobních údajů porušení zásady korektnosti. Při důsledné revizi ze strany dozorových úřadů v oblasti ochrany osobních údajů by tedy stávající struktura ekosystému internetové reklamy neměla obstát.

Navzdory řadě podaných stížností[205] je jediným dostupným rozhodnutím dozorového úřadu v této souvislosti rozhodnutí belgického dozorového úřadu z února 2022,[206] které se však vztahuje zejména k rámci pro souhlasy

---

[202] Viz SMIT, Edith G., VAN NOORT, Guda, VOORVELD, Hilde A. M. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior* [online]. 2014, roč. 32, s. 21. Viz též vyjádření vedoucí britského dozorového úřadu Elizabeth Denham Information Commissioner's Office ICO calls on Google and other companies to eliminate existing privacy risks posed by adtech industry [online]. 29. 11. 2021 [cit. 23. 1. 2023]. Dostupné z: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-calls-on-google-and-other-companies-to-eliminate-existing-privacy-risks-posed-by-adtech-industry/

[203] Viz např. ANGWIN, Julia, PARRIS, Terry. Facebook Lets Advertisers Exclude Users by Race [online]. SPEICHER, Till et al. Potential for Discrimination in Online Targeted Advertising [online], s. 9, 10.

[204] Viz např. CALO, Ryan. *Digital market manipulation*, s 996. CRAIN, Matthew, NADLER, Anthony. *Political Manipulation and Internet Advertising Infrastructure*, s. 374.

[205] Viz RYAN, Johnny. Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR. In: brave [online] 12. 9. 2018 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/adtech-data-breach-complaint/ RYAN, Johnny. Update on GDPR complaint (RTB ad auctions). In: *brave* [online] 28. 1. 2019 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/update-rtb-ad-auction-gdpr/

[206] Autorité de protection des données. *The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR* [online]. [cit. 23. leden 1. 2023]. Dostupné z: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

IAB TCF a nakládání s daty při předávání souhlasů udělovaných pomocí tohoto rámce, nikoli samotnému zpracování osobních údajů v systémech internetové reklamy a nezabývá se aplikací zásady korektnosti.[207] Nedávné odvážné rozhodnutí Evropského sboru pro ochranu osobních údajů (dále jen „EDPB“) ve věci služby Instagram[208] však naznačuje, že bychom se v dohledné době mohli dočkat důslednějšího zásahu dozorových úřadů proti ekosystému internetové reklamy. Takový zásah by pak patrně vedl k podstatné transformaci celého ekosystému.

Současně je třeba vnímat, že ekosystém internetové reklamy prodělává významnou transformaci spojenou s výše popsanou postupně končící podporou cookies třetích stran ve webových prohlížečích.[209] Společnosti jako Google, který je zároveň významným hráčem na poli internetové reklamy, na tento trend reagují snahou nalézt technologie, které zmenší zásah do soukromí spojený s použitím cookies třetích stran, ale zachovají stávající obchodní modely a strukturu ekosystému internetové reklamy.[210]

Tyto trendy jdou ruku v ruce, je však otázkou, jak by je měla reflektovat právní úprava přístupu ke koncovému zařízení. Na jednu stranu je patrné, že podpora cookies třetích stran v nejvýznamnějších internetových prohlížečích nebude mít dlouhý život a právní úprava, která by směřovala k jejich povinné blokaci, by tedy neměla pro ekosystém internetové reklamy znamenat podstatnější zásah. Na druhou stranu o dopadech technologií, které je mají nahradit, jako je Topics API a FLEDGE, na ochranu sou-

[207] Tamtéž.

[208] Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era [online], s. 17 a násl. Podrobně viz část 3. tohoto článku.

[209] Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era [online], s. 17 a násl. Podrobně viz část 3. tohoto článku.

[210] Viz části 3. tohoto článku. Některé open source alternativy uvádí CINAR, Naim; ATEŞ, Sezgin. Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era [online]. *SSRN Scholarly Paper*. 24. 2. 2022 [cit. 4. 1. 2023]. Viz též Evropská komise. Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. In: *Evropská komise* [online]. 30. 1. 2023, s. 177 a násl. [cit. 2. 2. 2023]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en Změna také může mít dopady z pohledu hospodářské soutěže v podobě posílení dominantního postavení některých subjektů, diskuze těchto dopadů přesahuje záběr tohoto článku.

kromí a jejich současném přínosu pro webové stránky s bezplatným obsahem financovaným z reklamy zatím nemáme jednoznačná data.[211]

Přístup právní úpravy k těmto technologiím by tedy měl být opatrný – je namístě, aby poskytoval vyšší míru flexibility, avšak pouze po důsledném zvážení a přezkoumání konkrétní technologie a se zachováním přiměřené míry kontroly ze strany uživatele.

7.3 OCHRANA SOUKROMÍ

Otázku zajištění stejné nebo vyšší úrovně ochrany soukromí je podle mého názoru třeba vykládat ve světle již citovaných bodů odůvodnění právních předpisů chránících soukromí v elektronických komunikacích a ve světle jejich vývoje.

Bod 24 odůvodnění směrnice 2002/58/ES hovoří o špionážním softwaru (*spyware*), webových štěnicích (*web bugs*), skrytých identifikátorech a jiných podobných nástrojích, které mohou pronikat do koncového zařízení uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele. Bod 66 odůvodnění směrnice 2009/136/ES o softwaru, který tajně sleduje činnost uživatele nebo podvrací provoz koncového zařízení uživatele ve prospěch třetí strany (*spyware*), a virech.[212]

Návrh nařízení ePrivacy v podobě předložené Evropskou komisí jde v tomto směru dále a v bodu 20 odůvodnění hovoří ve stejném kontextu o špionážním softwaru (*spyware*), webových štěnicích (*web bugs*), skrytých identifikátorech, sledovacích cookies a jiných podobných nežádoucích ná-

[211] Ke kritice viz GUY, Amy. Early design review for the Topics API #726. Komentář uživatele rhiaro z 12. 1. 2023. In: github [online]. 12. 1. 2023 [cit. 30. 1. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459

[212] Bod 25 odůvodnění směrnice 2002/58/ES pak zdůrazňuje, že informování o cookies je „obzvláště důležité v případě, kdy uživatelé odlišní od původního uživatele mají přístup ke koncovému zařízení, a tudíž i k veškerým údajům uchovávaným v takovém zařízení, které obsahují i citlivé informace o soukromí," a proto požaduje, aby informace a právo odmítnout byly „poskytnuty jednorázově pro použití různých nástrojů, které mohou být instalovány do koncového zařízení uživatele v průběhu téhož připojení, jakož i pro další použití těchto nástrojů v průběhu následných připojení." Jakkoli je však tento záměr legitimní, stopy v zařízení uživatele zanechávají i technicky nezbytné cookies, které jsou z nastaveného režimu vyňaty.

strojích pro sledování, které mohou pronikat do koncového zařízení koncového uživatele.

Z toho lze dovodit, že právní úprava soukromí v elektronických komunikacích sleduje v rámci ochrany práva na soukromí při přístupu ke koncovému zařízení uživatele dva dílčí cíle – ochranu bezpečnosti koncového zařízení a ochranu uživatele před skrytým či neoprávněným sledováním.

Ochrana bezpečnosti koncového zařízení v tomto kontextu znamená jednak ochranu před instalací softwaru, který může být považován za malware, ale také instalací softwaru či nastavení, které mohou otevírat cestu kompromitaci koncového zařízení jiným způsobem, přičemž hranice mezi těmito dvěma skupinami může být neostrá. Cíl je ilustrován případem Sony/BMG. Software této společnosti měnil nastavení počítače takovým způsobem, který usnadňoval proniknutí malwaru do počítače, a sám byl tak později některými antivirovými programy klasifikován jako malware.

Ochrana před skrytým nebo neoprávněným sledováním se pak vztahuje jednak k softwaru, který může uživatele sledovat (*spyware*), ale také ke sledování pomocí cookies a podobných technologií. Ani v jednom případě přitom nemá ochrana formu absolutního zákazu použití těchto technologií, protože v některých případech je může uživatel do svého zařízení instalovat vědomě a cíleně.

Oba tyto cíle považuji za legitimní a stále aktuální a právní úprava ochrany soukromí v elektronických komunikacích by měla i v budoucnu směřovat k jejich plnění.

7.4 DÍLČÍ ZÁVĚR

Ve světle výše provedené diskuze by nová právní úprava přístupu ke koncovému zařízení uživatele měla ve vztahu ke cookies a podobným technologiím méně spoléhat na kontrolu ze strany koncového uživatele. Současně by však měla umožnit rozumnou míru kontroly uživatele nad novými technologiemi, které by v budoucnu měly nahradit cookies třetích stran, protože o jejich dopadech na soukromí zatím nemáme přesvědčivá data. Konečně by měla zachovat nebo zvýšit úroveň ochrany bezpečnosti koncové-

ho zařízení a ochrany uživatele před skrytým nebo neoprávněným sledováním.

8. MOŽNÉ PŘÍSTUPY K NOVÉ PRÁVNÍ ÚPRAVĚ

K realizaci výše zmíněných cílů lze podle mého názoru přistoupit třemi základními způsoby – definováním titulů, resp. výjimek pro různé scénáře použití cookies, definicí jednoho obecného titulu s určitou formou korektivu nebo kombinací těchto způsobů.

První přístup byl zvolen v návrhu nařízení ePrivacy z pera Evropské komise, a nakonec převládl i v konečné pozici Rady. Ilustruje ho nově definovaný titul pro použití cookies k měření návštěvnosti,[213] který byl košatě rozpracován Evropským parlamentem[214] i Radou.[215] Problém tohoto přístupu je jeho kazuistický charakter. Existuje řada dalších scénářů použití cookies a podobných technologií, které jsou vůči soukromí uživatele minimálně invazivní (nepředstavují skryté či neoprávněné sledování, jemuž má právní úprava zabránit), současně se však nevejdou pod základní titul technické nezbytnosti. Jde například o technické cookies spojené s některými prvky dodatečné funkcionality webové stránky, jako je přehrávání videí nebo chatovací okna.[216]

Ukázkou druhého přístupu je návrh chorvatského předsednictví doplnit mezi tituly oprávněný zájem s dodatečnými podmínkami.[217] Těmito bylo provedení balančního testu – poměřování zájmu provozovatele webové stránky a zájmů a základních práv uživatele – a splnění dalších podmínek, jako je posouzení dopadů na soukromí, informování uživatele a zabezpe-

[213] Viz čl. 8 odst. 1 návrhu Komise.

[214] Viz pozměňovací návrhy č. 89 a 99 pozice Evropského parlamentu.

[215] Viz čl. 8 odst. 1 písm. d) a bod 21a odůvodnění pozice Rady.

[216] Blíže viz příklad v části 9.3 níže.

[217] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003(COD), 5979/20. In: *EUR-Lex* [online]. 21. 2. 2020, čl. 8 odst. 1 písm. g) a odst. 1a. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT

čení.[218] Problémem tohoto přístupu je aplikovatelnost navrhovaného širokého titulu i mimo oblast použití cookies a podobných technologií. Vedle minimálně invazivních scénářů ukládání a čtení cookies by tak tento titul mohl legitimizovat, nebo být zneužit k legitimizaci invazivních praktik, jako je instalace sledovacího softwaru nebo softwaru ohrožujícího bezpečnost koncového zařízení, kterým má právní úprava ochrany koncového zařízení zabránit.[219]

Kombinace těchto přístupů může podle mého názoru spočívat ve stanovení obecného titulu, resp. výjimky,[220] která by se však vztahovala pouze na použití vlastních cookies (tj. těch cookies, které do zařízení ukládá webová stránka, kterou uživatel prohlíží, nikoli jiná webová stránka), podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a dále technologií nahrazujících cookies třetích stran, u těchto nových technologií však pouze v rozsahu, v jakém jejich konkrétní specifikace budou schváleny EDPB. Korektivem této výjimky by pak podle mého názoru mohla být aplikace GDPR na procesy, které do působnosti výjimky spadnou. Jak bude dále vysvětleno, tuto aplikaci není třeba zvláště uzákoňovat, protože plyne z působnosti GDPR.

Tento přístup podle mého názoru nejlépe naplňuje vytyčené cíle. Vyloučení vlastních cookies, podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a vybraných technologií nahrazujících cookies třetích stran by znamenalo posun od důrazu na kontrolu v podobě souhlasu, jak jej regulují pravidla přístupu ke koncovému zařízení, k flexibilnějšímu režimu GDPR, ve kterém lze zpracování osobních údajů opřít o různé právní základy podle čl. 6 odst. 1.

---

[218] Viz tamtéž, čl. 8 odst. 1a a bod 21b odůvodnění.

[219] V tomto směru sdílím výše citovanou obavu německého předsednictví. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications) – Presidency discussion paper 2017/0003(COD), 9243/20. In: *EUR-Lex* [online]. 6. 6. 2020, s. 6. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT

[220] K diskuzi variant titulu a výjimky viz část 9.6 .

Flexibilnější režim by zároveň znamenal otevření cesty pro realizaci cílené reklamy, pokud bude založena na vybraných technologiích nahrazujících cookies stran, u jejichž technické specifikace EDPB dospěje k závěru, že jejich dopady na soukromí jsou dostatečně malé.

Z hlediska ochrany bezpečnosti koncového zařízení by takové řešení nepředstavovalo žádný ústupek, protože by se neaplikovalo na spustitelný software ani na změny konfigurace koncového zařízení. Z hlediska ochrany před skrytým nebo neoprávněným sledováním by se rovněž nejednalo o ústupek, protože tyto činnosti by byly dále regulovány GDPR, ze kterého plyne požadavek na právní titul a řadu konkrétních opatření k zajištění ochrany práv dotčené fyzické osoby.

Ochrana před skrytým nebo neoprávněným sledováním by naopak mohla být posílena, pokud by se zvolený přístup promítl do povinností tvůrců webových prohlížečů. Výše byla popsána rizika spojená s předáváním dat ve stávající podobě ekosystému internetové reklamy. Toto předávání je primárně založeno na využití cookies třetích stran. Některé webové prohlížeče ukládání a čtení cookies třetích stran ve výchozím nastavení blokují již nyní. Jiné tuto funkcionalitu připravují.[221] Tento postupný trend založený na dobrovolnosti však patrně v dohledné době nezajistí, aby veškerý software, který uživatelé k procházení webu v Evropské unii používají, cookies třetích stran ve výchozím nastavení blokoval. Tvůrcům webových prohlížečů by proto měla být uložena povinnost k takovému výchozímu blokování.

Tato povinnost blokace ve výchozím nastavení by se mohla vztahovat i na technologie nahrazující cookies třetích stran, a to včetně těch, u nichž bude technická specifikace schválena EDPB. U těchto vybraných technologií by však bylo namístě, aby toto výchozí nastavení uživatel při prvním spuštění webového prohlížeče odsouhlasil, resp. dostal možnost jej změnit a tyto technologie povolit. Takové řešení by zachovávalo vysokou míru ochrany před skrytým či neoprávněným sledováním a také přiměřenou míru kontroly uživatele.

[221] Blíže viz část 3.

Zároveň webové prohlížeče mohou pro ochranu uživatelů udělat i více než blokovat cookies třetích stran. Jak ukazuje současná praxe popsaná v části 3. , prohlížeče mohou obsahovat technologie, které aktivně brání sledování uživatelů jinými technikami, jako je fingerprinting. Tyto techniky budou umožňovat sledování uživatelů, i když budou cookies třetích stran ve webových prohlížečích blokovány, proto je namístě uložit tvůrcům webových prohlížečů povinnost přijmout technická opatření, která tomuto sledování budou bránit.

Pokud by tvůrcům webových prohlížečů byla uložena povinnost ve výchozím nastavení blokovat cookies třetích stran a současně přijmout opatření odpovídající stavu techniky, která budou bránit skrytému nebo neoprávněnému sledování uživatele, šlo by dle mého názoru o významné posílení ochrany uživatele před skrytým nebo neoprávněným sledováním. Takové opatření by přitom nezvyšovalo nároky na kontrolu ze strany uživatelů a nijak neomezovalo limitované formy internetové reklamy.

9. ROZBOR A ZHODNOCENÍ NAVRŽENÉHO ŘEŠENÍ

9.1 APLIKACE GDPR

Výše předložený návrh výjimky, která by se však vztahovala na použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení, vychází z předpokladu, že na použití těchto technologií, které může představovat zásah do soukromí ve smyslu neoprávněného nebo skrytého sledování, se aplikuje GDPR, které nepřiměřenému zásahu do soukromí brání.

GDPR se aplikuje na zcela nebo částečně automatizované zpracování osobních údajů.[222] Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě.[223] Identifikovatelnou fyzickou osobou se pak rozumí fyzická osoba, kterou lze přímo či nepřímo identifikovat.[224] Fyzickou osobu lze „považovat za ‚identifikovanou', jestliže je ve

[222] Viz čl. 2 odst. 1 GDPR. Také na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Viz tamtéž.

[223] Viz čl. 4 bod 1 GDPR.

[224] Viz tamtéž.

skupině osob ‚odlišena' ode všech ostatních příslušníků této skupiny."[225] Identifikovatelná je tehdy, pokud ji lze odlišit od všech ostatních příslušníků této skupiny,[226] tedy pokud dostupné informace umožňují na konkrétního člověka „zaostřit".[227]

Leens rozlišuje čtyři formy identifikace – vyhledání (pomocí identifikátoru v registru či tabulce), rozpoznání (pomocí znaků, jako je fyzický vzhled), klasifikaci (označení jednotlivce jako příslušníka určité skupiny) a identifikaci sezení (sledování jednotlivce během interakce).[228] Purtova k této klasifikaci přidává pátou formu – cílení, tedy „výběr jednotlivce ze skupiny jako objektu pozornosti nebo zacházení v určitém časovém okamžiku".[229]

S výjimkou klasifikace všechny tyto formy identifikace přestavují identifikaci ve smyslu GDPR.[230] Ve vztahu k cílení tento závěr plyne zejména z bodu 26 odůvodnění GDPR, který výslovně hovoří o tom, že možnost výběru vyčleněním (*singling out*) je třeba brát v úvahu jako způsob identifikace. Tento přístup zaujímá také judikatura.[231] Přitom pokud výběr jednotlivce ze skupiny jako objektu pozornosti považujeme za formu identifikace ve smyslu GDPR, pak jakákoli forma sledování (včetně sledování skrytého

[225] Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2007 k pojmu osobní údaje In: *Evropská komise* [online]. 20. 6. 2007, s. 12. [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf

[226] Viz tamtéž.

[227] Viz tamtéž, s. 13.

[228] Viz LEENES, Ronald E. Do They Know Me? Decomposing Identifiability *University of Ottawa Law and Technology Journal* [online]. 2007, roč. 4, č. 1-2 [cit. 6. 1. 2023], s. 146 a násl.

[229] Viz PURTOVA, Nadezhda. From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law* [online]. 2022, roč. 12, č. 3 [cit. 2. 2. 2023], s. 170.

[230] Viz PURTOVA, Nadezhda. *From knowing by name to targeting: the meaning of identification under the GDPR*, s. 177.

[231] Viz rozsudek Court of Appeal (Civil Division) ze dne 27. 3. 2015, A2/2014/0403, [2015] EWCA Civ 311, bod 114 a násl. Pro rozbor viz PURTOVA, Nadezhda. *From knowing by name to targeting: the meaning of identification under the GDPR,* s. 176. BORGESIUS, Frederik J. Zuiderveen. *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation,* s. 267.

nebo neoprávněného) představuje zpracování informací o fyzické osobě, která je v tomto smyslu identifikovatelná.[232]

Z hlediska ochrany soukromí uživatele by tento závěr nemusel být dostatečný ve vztahu k vymáhaní právní úpravy v případě softwaru, jako např. spyware. U něj totiž může být obtížné určit, která osoba v konkrétním případě určila účel a prostředky sledování jako formy zpracování osobních údajů a která je tedy správcem osobních údajů ve smyslu GDPR,[233] který je za zpracování osobních údajů odpovědný. Proto je namístě v případě softwaru regulovat samotný akt jeho uložení do koncového zařízení. V případě použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a využití údajů, které koncové zařízení vysílá, však tato nejasnost odpadá.

Cookies a podobné technologie jsou vždy uloženy ve vztahu ke konkrétní doméně a určení webové stránky, resp. provozovatele webové stránky, která je do koncového zařízení uložila, je snadnější než určení původce určitého softwaru.[234] Požadavek na souhlas ve vztahu k některým scénářům použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení tak podle mého názoru nepřináší pro soukromí uživatelů žádnou dodatečnou ochranu. K té postačí ponechat tyto činnosti v působnosti GDPR, do které v případě sledování uživatele spadají.

Ochrana poskytovaná GDPR je přitom komplexnější než ochrana poskytovaná právní úpravou přístupu ke koncovému zařízení. Vedle požadavku na právní titul ke zpracování osobních údajů jako činnosti zahrnující použití cookies a podobných technologií nebo využití údajů, které koncové zařízení vysílá,[235] se na jednu stranu jako ochranný „deštník“ uplatní základní

[232] Např. Nadezhda Purtova uvádí, že identifikace ve smyslu GDPR zahrnuje „také spornější, ale stále populárnější případy tzv. přechodného zpracování údajů, které se k subjektům údajů vztahuje pouze v krátkém okamžiku interakce s technologií, jako … inteligentní kamerový dohled.“ Viz PURTOVA, Nadezhda. *From knowing by name to targeting: the meaning of identification under the GDPR,* s. 181. Překlad autor.

[233] Viz čl. 4 bod 7 GDPR.

[234] Viz blíže část 2.

[235] Viz čl. 6 odst. 1 GDPR.

zásady zpracování osobních údajů uvedené v čl. 5 GDPR a na druhou stranu řada konkrétních práv dotčených fyzických osob (subjektů údajů ve smyslu čl. 4 bod 1 GDPR)[236] a povinností subjektu vykonávajícího danou činnost (správce osobních údajů ve smyslu čl. 4 bod 7 GDPR).[237]

Současně je však právní úprava v GDPR flexibilnější a kontrola subjektu údajů v ní není jediným nástrojem ochrany. Kontrola hraje v GDPR významnou roli – to je patrné jak z bodu 7 odůvodnění GDPR,[238] tak z katalogu právních základů pro zpracování osobních údajů (kde je na prvním místě uveden souhlas)[239] nebo z úpravy práv dotčených fyzických osob.[240] Zpracování osobních údajů je však možné opřít o jiné právní tituly, než je souhlas subjektu údajů, a tedy je možné zpracování legitimizovat, aniž by nad ním musela dotčená fyzická osoba předem vykonat kontrolu (v podobě udělení souhlasu). Pro použití cookies a podobných technologií je relevantní zejména právní základ oprávněného zájmu správce osobních údajů nebo třetí osoby.[241]

Oprávněný zájem lze jako právní základ uplatnit v případě, kdy je zpracování osobních údajů nezbytné pro realizaci oprávněného zájmu správce osobních údajů nebo třetí osoby a tento zájem převažuje nad zájmy a právy a svobodami dotčené osoby (subjektu údajů).[242] Tyto tři podmínky – existence oprávněného zájmu správce nebo třetí osoby, nezbytnost zpracování pro realizaci tohoto zájmu a převaha zájmu nad právy a svobodami subjektu údajů – musí být splněny kumulativně.[243]

---

[236] Viz kapitolu III GDPR.

[237] Viz kapitolu IV GDPR.

[238] Ten výslovně uvádí: „Fyzické osoby by měly mít možnost kontrolovat své vlastní osobní údaje."

[239] Viz čl. 6 odst. 1 GDPR.

[240] Viz kapitolu III GDPR.

[241] Viz čl. 6 odst. 1 písm. f) GDPR.

[242] Viz tamtéž.

[243] Viz KAMARA, Irene, DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach [online]. 8. 8. 2018 [cit. 8. 1. 2023], s. 11. Viz také Rozsudek SDEU (druhého senátu) ze dne 4. 5. 2017 ve věci C-13/16, Rïgas satiksme, bod 28.

Oprávněný zájem správce nebo třetí osoby nemusí být zájmem, který vyplývá z právního předpisu. Může jít o jakýkoli zájem, který právu neodporuje, včetně zájmu komerčního.[244] Podmínka nezbytnosti bude naplněna, pokud je zpracování cestou k naplnění posuzovaného oprávněného zájmu správce, která je nejméně invazivní k zájmům a právům subjektu údajů.[245] Porovnání oprávněného zájmu správce nebo třetí osoby a zájmů a základních práv a svobod subjektu údajů je nejkomplexnější podmínkou. Hraje v něm roli povaha oprávněného zájmu na jedné straně a velikost zásahu do zájmů a základních práv a svobod subjektu údajů na straně druhé. Tu určuje zejména rozsah zpracovávaných osobních údajů, jejich povaha, způsob zpracování a doba zpracování. Význam má také postavení správce osobních údajů a subjektu údajů, resp. jejich vztah.[246] Podle bodu 47 odůvodnění GDPR je významným faktorem také to, „zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít".[247] Roli hrají rovněž dodatečné záruky přijaté správcem k ochraně zájmů a základních práv subjektu údajů, jako např. dodatečné omezení rozsahu údajů, dodatečné informování nebo dodatečné zabezpečení.[248]

Příkladem zpracování, které zahrnuje použití cookies a mohlo by se opírat o oprávněný zájem, je měření návštěvnosti a sledování chování uživatelů za účelem optimalizace fungování webové stránky, pro které návrh nařízení ePrivacy (ve všech jeho podobách) obsahuje zvláštní titul. Zjištění,

[244] Viz KAMARA, Irene; DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, s. 13. Obdobně viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. In: *Evropská komise* [online]. 9. 4. 2014, s. 25. [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf (dále jen „WP217")

[245] Viz KAMARA, Irene, DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 14. Obdobně viz WP127, s. 29.

[246] Viz KAMARA, Irene, DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 14. Obdobně viz WP17, s. 33.

[247] Viz KAMARA, Irene, DE HERT, Paul. KAMARA, Irene; DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 16.

[248] Viz WP217, s. 42.

jak uživatelé používají webovou stránku, a její následná úprava za účelem snadnějšího používání pro uživatele, příp. lepšího dosahování obchodních nebo jiných cílů provozovatele webové stránky (např. většího počtu dokončených objednávek v internetovém obchodě), je zájmem, který neodporuje svou podstatou unijnímu právu ani právu České republiky. Tento zájem není možné realizovat bez údajů o tom, jak uživatelé webovou stránku používají – např. v jakém kroku zadávání objednávky nejčastěji proces nedokončí a na jaké narážejí překážky. Diskutabilní je pouze rozsah údajů, který je k realizaci tohoto zájmu nezbytný.

Pro účely měření návštěvnosti a sledování chování uživatelů za účelem optimalizace fungování webové stránky lze sbírat údaje s různou mírou podrobnosti, od počtu návštěv jednotlivé webové stránky,[249] až po podrobný záznam pohybů kurzoru uživatele na stránce, který lze rekonstruovat prakticky do podoby videozáznamu.[250] Za nezbytný rozsah zpracování lze dle mého názoru zpravidla považovat zpracování údajů na úrovni interakce uživatele s webovou stránkou (doba setrvání na stránce, stránka, ze které uživatel přišel, stránka, na kterou odešel) a s jejími jednotlivými prvky, např. počty kliknutí, způsoby vyplňování formulářových polí apod. Naopak sběr údajů v podrobnosti umožňující rekonstrukci v podstatě odpovídající videozáznamu průchodu webovou stránkou bych zpravidla za nezbytný nepovažoval (při vyšším počtu návštěv webové stránky by takové údaje patrně bylo problematické vůbec smysluplně využít). Míra nezbytnosti však bude záležet na okolnostech konkrétního případu.

Rozsah zpracovávaných údajů také významně ovlivňuje poměřování zájmu provozovatele webové stránky se zájmy a základními právy a svobodami subjektu údajů – s rostoucím rozsahem údajů totiž roste velikost zásahu do těchto zájmů, práv a svobod, zejména práva na soukromí. Ve výše popsaném případě zpracování údajů na úrovni interakce uživatele s jednotlivými prvky webové stránky bych zásah považoval za přiměřený a zájem provozovatele webové stránky by dle mého názoru nad zájmy subjektu

[249] Viz ZHENG, Guangzhi, PELTSVERGER, Svetlana. *Web analytics overview* [online].

[250] Viz What Are Session Recordings (Session Replays) + How to Use Them In: *hotjar* [online]. [cit. 23. 1. 2023]. Dostupné z: https://www.hotjar.com/session-recordings/

údajů převažoval, mj. proto, že takové zpracování lze podle mého názoru ze strany uživatele předvídat. Naopak v případě zpracování údajů v podrobnosti umožňující rekonstrukci v podstatě odpovídající videozáznamu bych zásah zejména do práva na soukromí považoval za nepřiměřený, mimo jiné s ohledem na nízkou předvídatelnost takového zpracování.[251]

Předpokladem závěru o přiměřenosti zásahu a převaze zájmu správce by ve výše popsaném případě byla podle mého názoru implementace minimální sady vhodných (a dnes běžných) záruk, jako např. nastavení vhodně krátké doby uchování s následnou agregací a anonymizací dat, neukládání IP adres uživatelů (které by umožňovaly údaje ve spojení se záznamy, např. poskytovatele služeb elektronických komunikací spojit s uživatelem identifikovaným občanským jménem, příjmením a dalšími údaji)[252] nebo neukládání údajů, které uživatelé zadávají do formulářů (a které mohou zahrnovat jejich e-mailové adresy, občanská jména a příjmení a další údaje usnadňující identifikaci ve smyslu vyhledání či rozpoznání).[253]

Pro svou flexibilitu byl oprávněný zájem jako právní titul některými autory kritizován jako úniková cesta, kterou lze legitimizovat zpracování, která jsou na újmu subjektu údajů,[254] a pro subjektivní prvek v poměřování zájmů správce a subjektu údajů.[255] Tato volnost je zmírněna tím, že v souladu

[251] Nikoli však za tak zásadní, aby takové zpracování odporovalo zásadě férovosti zpracování ve smyslu čl. 5 odst. 1 písm. a) GDPR. Bylo by tedy možné jej podle mého názoru opřít o vhodně nastavený souhlas uživatelů webové stránky, pokud by byl prezentován např. vybranému náhodnému vzorku uživatelů, od kterých by byl sebrán rozumně zpracovatelný objem dat.

[252] Viz rozsudek SDEU (druhého senátu) ze dne 19. 10. 2016 ve věci C-582/14, Breyer, bod 47.

[253] Jako příklad lze uvést např. šifrování, ať už při přepravě nebo statické, pseudonymizaci, nebo fyzické, organizační a smluvní opatření. Viz např. Google. IP masking in Universal Analytics. In: Analytics Hepl [online]. Nedatováno [cit. 12.2. 2023]. Dostupné z: https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631

[254] Viz FERRETTI, Federico. Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? In: *Common Law Market Review* 2014, r. 51, č. 3, s. 843–868, citováno podle KAMARA, Irene, DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 9.

se zásadou odpovědnosti, zavedenou GDPR,[256] musí správce být schopen svůj oprávněný zájem prokázat. Současně, jak bylo uvedeno výše, bod 47 odůvodnění GDPR blíže specifikuje, jak posuzovat vztah oprávněného zájmu správce a zájmů a základních práv a svobod subjektu údajů.

Na výše navržené řešení se současně podle mého neuplatní výhrada německého předsednictví, že by zavedení oprávněného zájmu do právní úpravy přístupu ke koncovému zařízení výrazně usnadnilo „instalaci softwaru, který je často považován za hlavní vstupní bránu pro škodlivý software.“[257] Oprávněný zájem by totiž jako titul nebylo možné aplikovat na jakýkoli přístup ke koncovému zařízení (např. na instalaci jakéhokoli softwaru), ale pouze na činnosti ukládání a čtení vlastních cookies, použití podobných technologií a využití údajů vysílaných koncovým zařízením, se kterými toto riziko spojeno není.

Řešení by tedy bylo možné konstruovat jako výjimku z aplikace právní úpravy přístupu ke koncovému zařízení na použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a na použití technologií nahrazujících cookies třetích stran. Tyto činnosti by zůstaly v působnosti GDPR, které poskytuje robustní ochranu základním právům a současně větší flexibilitu. Tato flexibilita by se projevila mimo jiné možností aplikovat na výše uvedené činnosti právní základ nezbytnosti zpracování pro oprávněný zájem správce nebo třetí osoby, avšak pouze na tyto vymezené činnosti, nikoli na libovolný přístup ke koncovému zařízení (např. instalaci softwaru).

Takové řešení by podle mého názoru odpovídalo také lidskoprávním základům GDPR a nařízení ePrivacy. Cílem GDPR a obecně práva na ochranu osobních údajů ve smyslu čl. 8 Listiny základních práv Evropské unie je

---

[255] BALBONI, Paolo et al. Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection. *International Data Privacy Law* [online]. 2013, roč. 3, č. 4 [cit. 2. 2. 2023], s. 253.

[256] Viz čl. 5 odst. 2 GDPR.

[257] Viz návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) – Presidency discussion paper ze dne 6. 6. 2020, 2017/0003(COD), 9243/20 s. 6.

chránit základní práva před zásahy v důsledku zpracování osobních údajů.[258] Cílem nařízení ePrivacy je především ochrana soukromí, jak bylo popsáno v části 7.3 . Jakkoli vlastní cookies a podobné technologie lze použít způsobem zasahujícím do soukromí, toto riziko je výrazně nižší než u jiných výše diskutovaných scénářů přístupu ke koncovému zařízení uživatele (např. skryté instalaci softwaru) a vzniká vždy v souvislosti se zpracováním osobních údajů. Právní úprava ochrany osobních údajů je tedy pro případ použití vlastních cookies a podobných technologií přiléhavější.

9.2 ROZSAH VÝJIMKY

Výše navržené řešení předpokládá, že by z působnosti právní úpravy přístupu ke koncovému zařízení bylo vyňato použití vlastních cookies (tj. těch cookies, které do zařízení ukládá webová stránka, kterou uživatel prohlíží, nikoli jiná webová stránka) a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení, a to s argumentem, že na tyto činnosti se v relevantním rozsahu aplikuje GDPR.

Tento závěr by patrně bylo možné učinit i ve vztahu k širšímu rozsahu technologií, které lze použít pro sledování uživatele, zejména ve vztahu ke cookies třetích stran, které rovněž nelze použít např. k instalaci softwaru do koncového zařízení, a tak narušení jeho bezpečnosti, ale pouze k narušení soukromí ve smyslu sledování uživatele. Tato redukce z veškerých cookies na vlastní cookies je však navržena záměrně. Cookies třetích stran jsou totiž klíčovým pilířem současného ekosystému internetové reklamy, protože umožňují sdílení identifikace uživatele (ve smyslu identifikace zařízení, resp. webového prohlížeče pro účely sledování a cílení, nikoli identifikace

[258] Srov. GELLERT, Raphaël. *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press, 2020, s. 18. s odkazem na BENNETT, Colin J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992, s. 33. Viz též recitál 10 GDPR a GELLERT, Raphaël; GUTWIRTH, Serge. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 529. [cit. 30. 5. 2023]. Jakkoli lze dle Gellerta a Gutwirtha z judikatury SDEU dovodit i výklad konstruující právo na ochranu osobních údajů jako autonomní základní právo, tento přístup by podle mého názoru vedl k velmi formální aplikaci tohoto práva a není podle mě správný.

ve smyslu např. občanského jména či příjmení).[259] Toto sdílení přitom považuji za klíčový prvek zásahů do soukromí, které jsou se současnou podobou ekosystému internetové reklamy spojeny.[260] Vynětí těchto cookies pouze do flexibilnějšího režimu GDPR bych proto považoval za nežádoucí. Ze stejného důvodu navrhuji, aby tvůrci webových prohlížečů měli povinnost cookies třetích stran ve výchozím nastavení blokovat.

Otázkou k diskuzi je, zda mírnější režim pro vlastní cookies a výchozí blokace pouze cookies třetích stran je pro ochranu soukromí uživatelů dostatečným řešením. Vedle aspektu subjektu ukládajícího cookies (vlastní cookies oproti cookies třetích stran) mají cookies také časové atributy – jejich platnost může být omezena na dobu do zavření okna webového prohlížeče, resp. konkrétní záložky (tzv. *session cookies*, cookies sezení) nebo na dobu delší.[261] Podobně webové úložiště má část, která se vymaže po zavření okna webového prohlížeče, resp. konkrétní záložky (úložiště sezení), a část sloužící jako trvalé úložiště (místní úložiště).[262] Potenciál použití krátkodobě uchovávaných dat jako cookies sezení a dat v úložišti sezení pro sledování uživatele je přitom výrazně omezenější, protože neumožňuje spojit údaje o chování při dvou různých návštěvách webové stránky, které odděluje zavření okna webového prohlížeče, resp. konkrétní záložky.

Tyto cookies by přitom nemusely být ve výchozím nastavení blokovány absolutně. Namísto toho by se k nim mohly webové prohlížeče chovat tak, jak se chovají prohlížeče mimo mobilní zařízení k požadavkům na otevření nového okna prohlížeče (tzv. vyskakovacího okna, *pop-up window*) – tedy tak, že by uložení jiných dat, než dat platných po dobu sezení zablokovaly, avšak s upozorněním pro uživatele, že k blokaci došlo, aby uživatel mohl blokaci a uložení údaje povolit. Alternativně by nemusely webové prohlížeče uložení jiných dat než dat platných po dobu sezení automaticky blokovat, ale vyžadovat k jejich uložení souhlas, o který by si webová stránka

[259] Ostatně z tohoto důvodu je řada webových prohlížečů ve výchozím nastavení blokuje nebo zamýšlí blokovat.

[260] Blíže viz část 7.2 .

[261] Viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics,* s. 39.

[262] Viz část 2.

mohla požádat přes rozhraní prohlížeče a musel by přes toto rozhraní být udělen.

Ani jedno z těchto řešení by však dle mého názoru nebylo v souladu s výše shrnutými požadavky na ošetření použití cookies a podobných technologií v právní úpravě přístupu ke koncovému zařízení. Je třeba si uvědomit, že data (zejména cookies) s platností delší, než je doba sezení, jsou nutná pro řadu legitimních účelů, jako je zapamatování nastavení webové stránky (např. preferovaného jazyka stránky nebo preferované měny v internetovém obchodě), zapamatování přihlášení apod.[263]

Současně by toto řešení zvýšilo požadavky na kontrolu koncového uživatele, který by musel v legitimních případech uložení data s platností delší, než je doba sezení, aktivně povolovat, nebo u veškerých těchto uložení rozhodovat o souhlasu, přičemž takovým žádostem by mohl čelit téměř na každé webové stránce s ambicí cílit na něj reklamu.

Otázkou také je, zda by se mírnější režim měl vztahovat na technologie nahrazující cookies třetích stran, jako je Topics API a FLEDGE.[264] S ohledem na diskuzi v části 7.2 se domnívám, že s těmito technologiemi nelze zacházet stejně jako s vlastními cookies a podobnými technologiemi, protože jejich dopady na ochranu soukromí a vnímání ze strany uživatelů nejsou dostatečně prozkoumané. Na druhou stranu s ohledem na zachování otevřených cest pro budoucí financování webových stránek nabízejících bezplatný obsah a také prevenci přetížení uživatelů budoucími žádostmi o souhlas by bylo vhodné aplikovat požadavek na kontrolu vůči těmto technologiím v mírnější formě.

Tato mírnější forma kontroly by mohla mít podobu vynětí těchto technologií z požadavku na souhlas spolu s jejich výchozí blokací ve webovém prohlížeči a povinností webového prohlížeče při prvním použití předložit uživateli toto nastavení k odsouhlasení. Tento režim by se však měl vztahovat pouze na takové technologie, jejichž technickou specifikaci posoudí EDPB a schválí ji s ohledem na minimální zásah do soukromí, který tyto technologie vytváří.

[263] Viz WP194, s. 6.

[264] Blíže viz část 3.

Je otázkou, na kolik lze takové řešení považovat za mírnější oproti současné úpravě. Je však třeba vzít v úvahu, že dopady jednotlivých technologií pro ochranu soukromí zatím nejsou některými odborníky hodnoceny jako dostatečné zlepšení oproti aktuálnímu stavu.[265] Současně návrh vychází z předpokladu, že tyto technologie bude možné využít bez zpracování osobních údajů, tj. bez nutnosti získávat souhlas se zpracováním osobních údajů podle GDPR – tento předpoklad může být naplněn u některých technologií, ne však nutně všech.[266]

Za téma pro další zkoumání a případnou diskuzi tedy považuji otázku, zda vedle kladného posouzení technologií EDPB ještě vyžadovat jejich výchozí blokaci a následně odsouhlasení jejich použití uživatelem, případně zda dovolit webovým stránkám podmiňovat přístup k bezplatnému obsahu povolením použití těchto technologií (pozitivně hodnocených EDPB). Tento přístup by uživatele nezbavil možnosti rozhodovat o použití těchto technologií. Současně by se však rozsah kontroly snížil na proveditelnou úroveň a zachoval vysokou míru ochrany soukromí (s ohledem na výchozí nastavení blokující tyto technologie). Na druhou stranu by však mohl znamenat překážku pro financování webových stránek pomocí cílené reklamy a obecně nepřiměřené opatření vzhledem k rizikům pro ochranu soukromí, které by tyto schválené technologie představovaly. Na druhou stranu rezignace na požadavek souhlasu může představovat příliš velký zásah do autonomie uživatele jako aspektu práva na soukromí.[267]

---

[265] Viz výhrady Mozilla Foundation, společnosti Apple a pracovní skupiny World Wide Web Consortium pro architekturu webu (W3C TAG). Request for Position: Topics API #622. In: github [online]. 17. 3. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/mozilla/standards-positions/issues/622 komentář uživatele martinthomson z 6. 1. 2023. The Topics API #111. In: github [online]. 20. 12. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/WebKit/standards-positions/issues/111 komentář uživatele annevk z 20. 12. 2022. Early design review for the Topics API #726. In: github [online]. 25. 3. 2023 [cit. 28. 5. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459 komentář uživatele rhiaro z 12. 1. 2023.

[266] Viz blíže rozbor v části 9.4 .

[267] K autonomii jako složce soukromí viz GELLERT, Raphaël; GUTWIRTH, Serge. *The legal construction of privacy and data protection*. s. 524. Britský ICO požaduje volbu uživatele jako jeden z atributů technologií nahrazujících cookies třetích stran. Viz Information Commissioner's Office. Data protection and privacy expectations for online advertising proposals. s. 43.

Za vhodné proto považuji vázat výjimku na veškeré použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení bez ohledu na dobu platnosti těchto dat a také na použití technologií nahrazujících cookies třetích stran s omezenými dopady na soukromí. K další diskuzi je případná povinnost pro tvůrce internetových prohlížečů blokovat ve výchozím nastavení cookies třetích stran (nikoli jiné druhy cookies) a také technologie nahrazující cookies třetích stran s omezenými dopady na soukromí (s povinností toto dílčí nastavení koncovému uživateli při prvním použití předložit ke schválení či úpravě).

9.3 APLIKACE V SOUČASNÉ PRAXI

V souvislosti s výše předloženým návrhem je také vhodné popsat, jak by se patrně propsal do fungování webových stránek pohledem současného stavu techniky (tj. bez aplikace technologií nahrazujících cookies třetích stran), a to v porovnání se současnou právní úpravou a navrženými podobami nařízení ePrivacy. V současnosti se uživatelé na většině webových stránek setkají se žádostí o souhlas s použitím cookies – liší se především jeho komplexnost a forma. Podkladem pro rozdílnou komplexnost souhlasu je většinou různá míra komplexnosti použití cookies.

Běžná firemní webová prezentace (např. prezentace výrobního podniku či advokátní kanceláře) používá vlastní cookies především pro analýzu chování uživatelů za účelem hodnocení a zlepšování webové prezentace, resp. odvozování obecných trendů. Podle současné právní úpravy je k takovému použití cookies potřeba souhlas. Při případné aplikaci na nařízení ePrivacy jak ve znění návrhu Evropské komise, tak ve znění pozic Evropského parlamentu a Rady by tento souhlas nebyl nezbytný, pokud by analýza nepřekračovala rozsah a splňovala podmínky, které se v různých zněních liší.[268]

Ve znění návrhu Evropské komise by mohla situaci ovlivnit volba zabránit třetím stranám v uchovávání informací v koncovém zařízení, kterou by musel webový prohlížeč při instalaci uživateli nabídnout.[269] Protože by

[268] Viz část 6.

[269] Viz čl. 10 odst. 1 a 2 návrhu Komise.

však tato volba znamenala blokaci všech cookies, tedy volbu s vyznamným negativním dopadem na fungování řady webových stránek, patrně by nešlo o volbu příliš často využívanou.

Znění navržené Evropským parlamentem by změnilo mechanismus udělování souhlasu. Ten by na úrovni jednotlivé webové stránky mělo jít udělit v nastavení prohlížeče. To by se pak mělo promítnout do signálů zasílaných webové stránce, které by se pro tuto stránku staly závaznými. To by v praxi nejspíše znamenalo, že již implementované standardy signálů jako Do Not Track[270] by se staly pro webové stránky závaznými, současně by to však patrně vyžadovalo vývoj zcela nových webových standardů pro udělování souhlasů a vyjadřování námitek, což by byla patrně časově velmi náročná procedura. Pozice Evropského parlamentu sice v jednom pozměňovacím návrhu uvádí, že by některé technologie měly být schvalovány EDPB,[271] ve vztahu k závazným signálům však není taková procedura specificky upravena.

Pozici Rady je ve vztahu k udělování souhlasu nastavením prohlížeče složité interpretovat – pozice sice obsahuje povinnost tento způsob udělování souhlasu umožnit,[272] není však jasné, zda ustanovení cílí na souhlas obecný, či určitý souhlas pro konkrétní webovou stránku. Obecný souhlas by patrně neobstál vůči požadavkům na souhlas popsaným v části 5.

V případě aplikace řešení, které navrhuji, by souhlas rovněž nebyl nezbytný, pokud by analýzu bylo možné opřít o nezbytnost pro oprávněný zájem provozovatele webové stránky – tedy pokud by nepředstavovala nepřiměřený zásah do zájmů a základních práv (zejména práva na soukromí) a při implementaci vhodných záruk. Současně by nebyla vyloučena komplexnější analýza chování na základě souhlasu, pokud by (např. svým rozsahem) neodporovala zásadě férovosti.[273]

---

[270] Viz KAMARA, Irene, KOSTA, Eleni. Do Not Track initiatives: regaining the lost user control. *International Data Privacy Law* [online]. 2016, roč. 6, č. 4 [cit. 2. 2. 2023].

[271] Viz pozměňovací návrh č. 166 pozice Evropského parlamentu.

[272] Viz čl. 4a odst. 2 pozice Rady.

[273] Viz příklad v části 9.3 .

Komplexnější webová aplikace (např. internetový obchod) nebo komplexnější, spotřebitelsky orientovaná webová prezentace (např. webová prezentace banky či pojišťovny) obvykle využívá cookies pro širší paletu účelů. Zpravidla na ní probíhá výše popsaná analýza chování, pro kterou platí závěry uvedené výše. Dále taková webová stránka zpravidla používá vlastní cookies, cookies třetích stran a podobné technologie pro některé dodatečné funkcionality, jako jsou chatovací okna, přehrávání videí, zapamatování preferencí apod.

Při aplikaci současné právní úpravy je třeba u každé takové cookie nebo podobné technologie zvažovat, nakolik je nezbytná „pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací nebo je-li to nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem“.[274] Např. u chatovacích oken a přehrávání videí je toto posouzení problematické a často vede k závěru, že příslušná cookie nezbytná není a může být uložena pouze buď na základě aktivace příslušného prvku (kliknutí na video), nebo na základě souhlasu uživatele.

Ve znění pozice Evropského parlamentu by také musely být ve výchozím nastavení blokovány veškeré cookies vyjma takových, které jsou technicky nezbytné, přičemž uživatel by měl mít při instalaci prohlížeče možnost toto nastavení odsouhlasit nebo změnit.[275] V tomto směru není jasné, jak by měl webový prohlížeč rozpoznat, které cookies jsou pro fungování webové stránky technicky nezbytné – tuto informaci v sobě cookies a další ukládaná data nenesou. Bylo by tedy třeba upravit minimálně internetový protokol HTTP upravující cookies a standard HTML5 definující webové úložiště, aby tato informace byla přenášena, resp. ukládána. Webový prohlížeč by pak musel spoléhat na to, že webová stránka pravdivě označí, které cookies jsou pro ni technicky nezbytné, což by se v praxi nemuselo vždy dít.[276]

[274] Viz § 89 odst. 3 ZEK. Blíže viz WP194.

[275] Pozměňovací návrhy č. 106 až 109 tamtéž.

[276] Nezisková organizace noyb zjistila u 21 % zkoumaných webových stránek, že za nezbytné označují cookies, které pro fungování webové stránky nezbytné nejsou. Viz noyb aims to end “cookie banner terror” and issues more than 500 GDPR complaints [online].

Při aplikaci mnou navrhovaného řešení by pro tyto účely zpravidla nebyl vyžadován souhlas uživatele – ve většině případů by u použití dané technologie bylo možné dovodit nezbytnost pro oprávněný zájem provozovatele webové stránky a převahu nad zájmy a právy uživatele (s ohledem na minimální zásah do těchto práv). Příslušné prvky by však bylo třeba technicky upravit tak, aby nevyužívaly cookies třetích stran, které by byly ve výchozím nastavení ve webových prohlížečích blokovány. Tato změna však bude patrně nutná již v souvislosti s tím, že ve většině webových prohlížečů budou cookies třetích stran ve výchozím nastavení blokovány dobrovolně.

Taková komplexnější webová aplikace či prezentace také často využívá cookies třetích stran pro cílení reklamy provozovatele webové stránky na webových stránkách třetích stran (např. výše popsaný retargeting, tj. zobrazení reklamy na dříve prohlíženou webovou stránku či konkrétní produkt nebo službu).[277] Podle současné právní úpravy je k tomuto použití potřeba souhlas. Tento požadavek zachovává i návrh nařízení ePrivacy ve všech jeho navrhovaných zněních. Mezi těmito zněními by se výše popsaným způsobem odlišoval možný mechanismus udělování souhlasu nastavením prohlížeče a míra blokace cookies ve výchozím nastavení.

V případě aplikace řešení, které navrhuji, by toto cílení nebylo možné s ohledem na výchozí blokaci cookies třetích stran. V souvislosti s dobrovolnou blokací cookies třetích stran ve výchozím nastavení většiny webových prohlížečů by byl dopad podobný, může jej však změnit aplikace nových technologií, diskutovaná níže v části 9.4 . Provozovatel webové stránky by byl motivován případně využít schválené technologie nahrazující cookies třetích stran, pokud by takové retargeting umožňovaly.

[277] Retargeting se běžně projevuje tak, že uživatele na různých webových stránkách, jako jsou např. zpravodajské portály, „pronásleduje“ reklama na zboží nebo službu, které si nedávno prohlížel např. v internetovém obchodě. Blíže viz LAMBRECHT, Anja, TUCKER, Catherine. When does retargeting work? Information specificity in online advertising. *Journal of Marketing research* [online]. 2013, roč. 50, č. 5, s. 562. [cit. 2. 2. 2023], s. 561–576. Dostupné z SagePub: https://journals.sagepub.com/doi/pdf/10.1509/jmr.11.0503

Specifické je použití cookies na webových stránkách, které nabízejí bezplatný obsah nebo služby financované z cílené reklamy.[278] Tyto webové stránky zpravidla do zařízení uživatele pomocí vložených skriptů ukládají desítky cookies různých třetích stran, jako jsou reklamní sítě a burzy a dodavatelé platforem nabídky. K tomu je podle současné právní úpravy potřeba souhlas, přičemž podle standardů aplikovaných v reklamním ekosystému musí mít tento souhlas definovanou strukturu podle účelů, ale také podle třetích stan.[279] Výsledný dialog žádosti o souhlas je tak zpravidla vysoce komplexní, přinejmenším v druhé vrstvě a dalších vrstvách (tj. po kliknutí na tlačítko umožňující podrobnější nastavení).

Podle nařízení ePrivacy by byl požadavek na souhlas zachován, s komplexními dialogy bychom se proto patrně setkávali i nadále. Podle návrhu Evropské komise a pozice Evropského parlamentu by se však opět výše popsaným způsobem odlišoval možný mechanismus udělování souhlasu nastavením prohlížeče a míra blokace cookies ve výchozím nastavení.

Podle návrhu Rady by příslušná webová stránka mohla udělením souhlasu podmiňovat přístup k obsahu, pokud by zároveň nabízela alternativní přístup bez požadavku na souhlas (např. placený přístup k jednotlivému článku nebo předplatné).[280] To by v praxi znamenalo zachování komplexních souhlasových dialogů, avšak proměněných do podoby cookie walls – bez udělení komplexního souhlasu by tedy nebylo možné k obsahu přistoupit.

Řešení, které navrhuji, by znamenalo pro tyto webové stránky podobné omezení jako návrh Komise a pozice Evropského parlamentu s ohledem na výchozí blokaci cookies třetích stran. Bylo by tak motivací pro provozovatele webových stránek k implementaci schválených technologií nahrazujících cookies třetích stran, které by představovaly menší zásah do sou-

[278] Pro účely tohoto příkladu odhlížím od výhrad k reálnosti a udržitelnosti takového řešení diskutovaných v části 7.2 .

[279] Viz Interactive Advertising Bureau. IAB Europe Transparency & Consent Framework Policies [online], příloha B, část C, bod c.iii.

[280] Tamtéž bod 20aaaa odůvodnění.

kromí,[281] popř. k přechodu na jiné formy cílení reklamy, které nevyžadují sledování uživatele, jako je kontextová reklama.[282]

Relevantní je také diskutovat dopad mnou navrhovaného řešení na webové stránky, které by cíleně obcházely (či již dnes obcházejí) blokaci cookies třetích stran za účelem sledování uživatele (ať už pro potřeby cílené reklamy nebo z jiných důvodů). Blokaci cookies třetích stran lze obcházet pomocí technik, jako je fingerprinting, nebo například technickým prezentováním cookies třetích stran jako vlastních cookies.[283]

Současná právní úprava na aktivní fingerprinting aplikuje požadavek souhlasu, jakkoli úprava v tomto směru není výslovná.[284] Stejně tak cookies třetích stran vydávané za cookies vlastní podléhají režimu souhlasu, pokud nejsou technicky nezbytné pro fungování webové stránky (což je nepravděpodobná varianta). Nařízení ePrivacy z pera Komise explicitně rozšiřuje působnost požadavku na souhlas i na aktivní fingerprinting, návrhy Parlamentu a Rady tuto působnost rozšiřují i na fingerprinting pasivní.[285] Podle návrhu Evropské komise a pozice Evropského parlamentu by pak byly některé druhy cookies, vč. vlastních cookies, ve výchozím nastavení webového prohlížeče blokovány (s nutností odsouhlasení nebo změny tohoto úvodního nastavení uživatelem).[286]

Specifická opatření, která by sama o sobě bránila sledování v případě, kdy webová stránka právní předpis poruší a provede např. fingerprinting bez souhlasu, návrh nařízení ePrivacy v žádném znění neobsahuje. Je pouze otázkou, jak by se na fingerprinting měl aplikovat požadavek Evropské-

[281] Blíže viz rozbor v částech 3. a 9.4 .

[282] Viz ZHANG, Kaifu, KATONA, Zsolt. Contextual advertising. *Marketing Science* [online]. 2012, roč. 31, č. 6 [cit. 6. 2. 2023]. K dalším alternativám viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 239.

[283] Tato technika se označuje CNAME cloaking a není na internetu neobvyklá. Viz REN, Tongwei et al. An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections. In: *Workshop on Measurements, Attacks, and Defenses for the Web*: *Proceedings 2021 Workshop on Measurements, Attacks, and Defenses for the Web* [online]. Virtual: Internet Society, 2021, [cit. 4. 1. 2023]. s. 3, 10.

[284] Blíže viz rozbor v části 5.

[285] Blíže viz část 6.

[286] Viz diskuzi v části 9.3 .

ho parlamentu ve výchozím nastavení prohlížeče blokovat ukládání a čtení údajů z koncového zařízení, které není technicky nezbytné. Pokud by tento požadavek byl vykládán jako povinnost blokovat fingerprinting, pak by s ohledem na kategorickou formulaci povinnost nemusela být pro tvůrce webových prohlížečů splnitelná, protože jednoznačně rozpoznat, kdy je čtení údajů o zařízení technicky nezbytné a kdy nikoli, je obtížné.

Mnou navrhované řešení zachovává výše uvedené požadavky na souhlas s fingerprintingem.[287] Ve vztahu ke cookies třetích stran vydávaných za vlastní cookies nestanoví požadavek na souhlas, je však otázkou, zda by takové jednání nešlo kvalifikovat jako obcházení zákona ze strany provozovatele webové stránky. V každém případě by však fingerprintingu i technikám jako vydávání cookies třetích stran za vlastní měla v právní úpravě dle mého návrhu bránit opatření přijatá na úrovni internetového prohlížeče. Internetové prohlížeče jsou obecně ve vhodném postavení, aby bránily soukromí uživatelů před neoprávněným sledováním.[288] Bez využití funkcionalit webového prohlížeče totiž nemůže webová stránka uživatele sledovat. Opatření implementovaná prohlížečem jsou méně náročná pro uživatele – snižují nároky na kontrolu z jeho strany. Internetových prohlížečů, resp. jejich tvůrců, je také výrazně méně než provozovatelů webových stránek, což usnadňuje vymáhání.[289] Současně řadu opatření v tomto směru již internetové prohlížeče implementují.[290]

Aplikace řešení, které navrhuji, na fungování webových stránek pohledem současného stavu techniky ukazuje, že by v praxi přineslo menší počet žádostí o souhlas (nebo alespoň jejich menší komplexnost). Současně by ře-

[287] Resp. požadavku na souhlas s pasivním fingerprintingem podle čl. 8 odst. 2 pozice Parlamentu a pozice Rady se navržené řešení nijak nedotýká. Přesto jsem skeptický ohledně vymahatelnosti tohoto požadavku, protože zda webová stránka provádí pasivní fingerprinting nelze zpravidla zjistit jinak než zkoumáním softwaru používaného k jejímu provozu. Viz MAYER, Jonathan R., MITCHELL, John C. *Third-party web tracking: Policy and technology*, s. 421.

[288] Viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics*, s. 56.

[289] Viz tamtéž.

[290] Pro přehled existujících technologií implementovaných ve webových prohlížečích viz Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era [online], s. 18. [cit. 30. 5. 2023].

šení nezvětšilo možný rozsah zásahů do soukromí uživatelů, ale naopak zvýšilo úroveň jeho ochrany prostřednictvím opatření ve webových prohlížečích, která by nevyžadovala kontrolu ze strany uživatele.

9.4 APLIKACE NA TECHNOLOGIE NAHRAZUJÍCÍ COOKIES TŘETÍCH STRAN

Relevantní je také popsat, jak by se řešení, které navrhuji, aplikovalo na technologie, které mají nahradit cookies třetích stran, a to opět v porovnání se současnou právní úpravou a navrženými podobami nařízení ePrivacy.

Technologie Topics API, popsaná v části 3. , z pohledu právní úpravy spočívá ve čtení údajů z koncového zařízení. Nejde přitom o informace aktivně ukládané webovou stránkou, ale informace generované samotným webovým prohlížečem. Z pohledu přístupu ke koncovému zařízení se tak do jisté míry podobá fingerprintingu, jakkoli fingerprinting spíše pracuje se statickými vlastnostmi zařízení a prohlížeče, nikoli generovanými údaji. Právní důsledky jsou přesto stejné – použití technologie Topics API ze strany webové stránky by podle platné právní úpravy podléhalo souhlasu, stejně tak podle návrhu nařízení ePrivacy. Podle návrhu nařízení ePrivacy ve znění návrhů Evropské komise a Evropského parlamentu by zřejmě mělo být použití technologie Topics API předmětem volby uživatele, resp. by mělo být ve výchozím nastavení blokováno.

Z hlediska GDPR je status Topics API nejednoznačný. Na jednu stranu lze argumentovat, že použití této technologie neposkytuje žádný (byť pseudonymní) identifikátor uživatele. Na druhou stranu Topics API poskytuje údaje pro cílení ve smyslu, který Purtova podřazuje pod identifikaci ve smyslu GDPR, a tedy pod zpracování osobních údajů. Současně údaje poskytované Topics API mohou být do značné míry unikátní.[291] Nelze tedy vyloučit, že použití Topcis API by podléhalo souhlasu podle GDPR.

Technologie FLEDGE se pak svým pojetím více blíží cookies, protože spočívá v ukládání údajů (příslušnosti k zájmové skupině) do prohlížeče uživatele. Tyto údaje nejsou následně čteny přímo webovou stránkou,

[291] Viz THOMSON, Martin. A *Privacy Analysis of Google's Topics Proposal*. In: github [online]. 6. 1. 2023 [cit. 28. 5. 2023]. Dostupné z: https://mozilla.github.io/ppa-docs/topics.pdf s. 12

webová stránka, která je chce využít, však spouští funkci internetového prohlížeče realizující příslušnou akci a zpracovávající tyto zapsané údaje. Uložení údaje o zájmové skupině do prohlížeče by podléhalo souhlasu dle současné právní úpravy i dle nařízení ePrivacy. U spuštění aukce v prohlížeči uživatele je závěr podle současné právní úpravy méně jednoznačný, domnívám se však, že s ohledem na její účel v podobě ochrany soukromé sféry uživatele by mělo i toto spuštění podléhat souhlasu, protože do této sféry zasahuje – využívá výpočetní prostředky zařízení uživatele a vede k vyslání signálů ze zařízení uživatele třetím stranám, přičemž tyto signály vypovídají o zařazení zařízení do zájmové skupiny. Návrh nařízení ePrivacy je v tomto směru explicitní a spuštění akce by podle něj souhlasu podléhalo jednoznačně. Použití FLEDGE by také, podobně jako Topics API, omezovalo výchozí nastavení prohlížeče podle návrhu nařízení ePrivacy ve znění návrhů Evropské komise a Evropského parlamentu.

Z pohledu GDPR by pak použití FLEDGE nemělo představovat zpracování osobních údajů, protože FLEDGE poskytuje webové stránce spouštějící reklamní aukci minimum informací. V podstatě by se měla jen dozvědět, jaká reklama byla zobrazena, který inzerent podal vítěznou nabídku a jakou cenu má za zobrazení zaplatit. Tyto údaje by neměly webové stránce umožňovat cílení na uživatele, které se odehrává mimo její kontrolu v zařízení uživatele.

Řešení, které navrhuji, by tak u Topics API, FLEDGE a podobných technologií (za předpokladu že by jejich použití nebylo považováno za zpracování osobních údajů) upouštělo od souhlasu na úrovni každé jednotlivé webové stránky, pokud by daná technologie odpovídala specifikaci schválené EDPB. Tyto technologie by však mohly být ve výchozím nastavení blokovány a uživateli by bylo toto nastavení mohlo být povinně předkládáno k odsouhlasení při prvním použití webového prohlížeče.[292] Rozhodující by pak bylo vnímání těchto technologií ze strany uživatelů. Pokud by se jejich

[292] Tento přístup by odpovídal doporučením ve stanovisku ICO. Viz Information Commissioner's Office. *Data protection and privacy expectations for online advertising proposals.* In: *Information Commissioner's Office* [online]. 25. 11. 2021, s. 43. [cit. 2. 2. 2023]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pd

tvůrcům podařilo přesvědčit nejen EDPB, ale také uživatele, že tyto technologie nepředstavují významný zásah do jejich soukromí a jsou důležité pro fungování webových stránek nabízejících bezplatný obsah, uživatelé by měli jednoduchou možnost jejich fungování v prohlížeči povolit.

Alternativou by také mohlo být připuštění obdoby cookies walls ve vztahu k těmto technologiím, tj. že by webové stránky mohly podmiňovat přístup k bezplatnému obsahu povolením těchto technologií. Na rozdíl od dnešní podoby cookies walls, které vynucují povolení cookies vč. cookies třetích stran by tyto jejich obdoby vynucovaly použití výrazně méně invazivní technologie a lze zde uvažovat, že volba na straně uživatele by byla reálná a smysluplná – zda snese mírnější formu zásahu do soukromí, nebo upřednostní placený přístup k obsahu.

Dosavadní data přitom naznačují, že postoj uživatelů k cílení reklamy je spíše negativní.[293] Například poté, co Apple na svých zařízeních zavedl možnost jednoduše se rozhodnout o sledování či nesledování za účelem cílené reklamy v konkrétní mobilní aplikaci, po 4 měsících od zavedení této funkce se poměr souhlasů z celkového počtu žádostí pohyboval okolo 20 %.[294] Je tedy otázkou, jaký podíl uživatelů by příslušnou technologii ve svém webovém prohlížeči povolil. Roli by zde mohla hrát dodatečná dobrovolná opatření, která by v tomto směru mohly webové prohlížeče nabídnout, např. možnost na konkrétních webových stránkách tuto funkcionalitu zakázat apod. Na druhou stranu dostupná data nepopisují postoj uživa-

[293] Viz TUROW, J. et al. Americans Reject Tailored Advertising and Three Activities that Enable It. In: *SSRN*. [online]. 29. 9. 2009. [cit. 2. 2. 2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214, s. 3. V Evropě se 7 z 10 lidí obává, že by společnosti mohly využívat data k novým účelům, jako je cílená reklama, aniž by je o tom informovaly. Viz Evropská komise. Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. In: *Evropská komise* [online]. červen 2011, s. 146. [cit. 2. 2. 2023]. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Part%20I%20of%20Special%20Eurobarometer%20359%20-%20Attitudes%20on%20Data%20Protection%20and%20Electronic%20Identity%20in%20the%20European%20Union.pdf

[294] Viz LAZUIK, Estelle. iOS 14 Opt-in Rate - Weekly Updates Since Launch. In: *Flurry*. [online]. 25. 5. 2021. [cit. 2. 2. 2023]. Dostupné z: https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/

telů k cílení v kontextu jiných protihodnot, např. bezplatnému přístupu k obsahu.[295]

9.5 SROVNÁNÍ A ZHODNOCENÍ

Z popisu aplikace navrženého řešení v praxi jsou patrné odlišnosti mezi řešením, které navrhuji, současnou právní úpravou a různými zněními nařízení ePrivacy.

Návrh Evropské komise a pozice Evropského parlamentu výrazně akcentují prvek kontroly uživatele. Ten se projevuje požadavkem na souhlas u většiny případů použití cookies a podobných technologií. Jakkoli se návrh i pozice Evropského parlamentu snaží řešit problém přetížení uživatelů požadavky na souhlas prostřednictvím nastavení webových prohlížečů, toto řešení by podle mě nebylo účinné. Sice by se díky němu pravděpodobně zjednodušil a sjednotil způsob udělování souhlasů (nešlo by o odlišné dialogy na různých webových stránkách, ale jednotný dialog v rozhraní internetového prohlížeče), s ohledem na aplikaci požadavků GDPR na tyto souhlasy by stále bylo však třeba, aby uživatel činil rozhodnutí o udělení souhlasu na úrovni jednotlivých webových stránek.

Toto řešení by tak dle mého názoru významně neposílilo ochranu soukromí uživatelů, ale pouze zmírnilo některé nedostatky současného stavu, a to za cenu podstatné zátěže pro tvůrce internetových prohlížečů, a hlavně tvůrce webových stránek, kteří by své stránky novým nastavením prohlížeče a mechanismům sběru souhlasu museli přizpůsobit.

Pozice Rady Evropské unie pak poměrně kategoricky (na úrovni odůvodnění) deklaruje, že u bezplatných služeb je možné souhlas (za stanovených podmínek) vyžadovat. Toto řešení by však dle mého názoru nesnížilo zátěž uživatelů z hlediska počtu žádostí o souhlas, pouze by snížilo jejich kontrolu skrze odepření bezprostřední možnosti souhlas odmítnout.

Jakkoli se toto řešení může zdát smysluplné u webových stránek, které uživatel navštěvuje pravidelně (např. webový zpravodajský portál, který uživatel navštěvuje denně), a má tak možnost se efektivně rozhodnout, zda

[295] Viz MAYER, Jonathan R., MITCHELL, John C. *Third-party web tracking: Policy and technology*, s. 417.

za službu „zaplatí“ svým soukromím či penězi formou předplatného, v případě jednotlivé návštěvy webové stránky už řešení funguje hůře. Pokud by si tedy uživatel např. na základě sdílení odkazu na sociální síti chtěl přečíst zpravodajský článek na webovém portálu, který běžně nenavštěvuje, stál by před volbou, zda si zaplatit předplatné ve výši nepřiměřené k přínosu přečtení jednoho článku,[296] „zaplatit“ přístup svým soukromím nebo k obsahu nepřistoupit. Jelikož první volba je ekonomicky neracionální, zbydou uživateli fakticky pouze druhá a třetí možnost, kde se však již o „skutečné možnosti volby“ (zmiňované v odůvodnění návrhu ve znění pozice Rady) dá hovořit jen obtížně.

Současně lze takto postavenou možnost volby vykládat tak, že ochrana před zásahy do soukromí má být dostupná jen pro ty, kteří jsou dostatečně finančně vybaveni pro přístup k placenému obsahu. V tomto směru se neztotožňuji s tím, že adekvátní ochrana soukromí jako základního práva by měla být „luxusem“, který si nemůže dovolit každý.

Návrh řešení, který předkládám, spočívá ve stanovení výjimky pro vlastní cookies, podobné technologie a technologie nahrazující cookies třetích stran, pokud by odpovídaly technické specifikaci schválené EDPB. Použití těchto technologií by tak zůstalo pouze v režimu GDPR. Současně by cookies třetích stran byly ve výchozím nastavení blokovány ve webovém prohlížeči.

Obdobně by mohly být blokovány technologie nahrazující cookies třetích stran, blokace by však podléhala odsouhlasení uživatele, který by mohl nastavení změnit. Pokud by použití těchto technologií nepředstavovalo zpracování osobních údajů (přičemž zde závisí na specifikaci konkrétních technologií), nebyl by pro jejich použití nutný souhlas podle GDPR na úrovni každé jednotlivé webové stránky. Řešení by pak doplňovala opatření odpovídající stavu techniky na úrovni prohlížeče, která by bránila skrytému nebo neoprávněnému sledování uživatele.

Toto řešení by podle mě odstranilo výše popsané nedostatky návrhů Evropského parlamentu a Rady. Díky vynětí vlastních cookies, podobných technologií a technologií nahrazujících cookies třetích stran z působnosti

[296] Za předpokladu, že zpravodajský portál neumožňuje přístup pouze k jednotlivému článku.

právní úpravy přístupu ke koncovému zařízení by se pravděpodobně významně snížil počet žádostí o souhlas, kterými by se museli uživatelé zabývat, nebo by se alespoň snížila komplexnost těchto žádostí. K řadě dnes běžných a málo invazivních způsobů zpracování by totiž nebyl potřeba souhlas, ale bylo by možné pro ně najít jiný právní titul podle čl. 6 odst. 1 GDPR, popř. by se GDPR na použití daných technologií neaplikovalo vůbec.

Současně by však nehrozil scénář popsaný německým předsednictvím, tedy výrazné usnadnění instalace „softwaru, který je často považován za hlavní vstupní bránu pro škodlivý software“,[297] neboť instalace jakéhokoli softwaru by stále podléhala právnímu režimu přístupu ke koncovému zařízení, tj. zpravidla požadavku na souhlas.[298]

Vedle toho by navrhovaný přístup mohl přinést větší flexibilitu ve vztahu k financování webových stránek pomocí cílení reklamy s využitím technologií nahrazujících cookies třetích stran. Je přitom k diskuzi, zda použití těchto technologií podmiňovat souhlasem uživatele na úrovni webového prohlížeče, pokud bude daná technologie pozitivně zhodnocena EDPB.

V takovém případě by použití těchto technologií nevyžadovalo souhlas uživatele na úrovni webové stránky, muselo by však být webovém prohlížeči povoleno. Odpadla by tak nutnost sbírat složitě souhlasy technikou podle pozice Evropského parlamentu. Současně by tento přístup znamenal zachování jisté míry kontroly uživatele, která by se realizovala právě skrze nastavení prohlížeče. Na druhou stranu by toto řešení nemuselo být dostatečné z hlediska flexibility pro financování webových stránek pomocí cílené reklamy, pokud by procento uživatelů, kteří by ve svém prohlížeči povolili technologie nahrazující třetích stran, bylo nízké. V takovém případě bychom se pravděpodobně vrátili k úvahám o období cookie walls v duchu pozice Rady, které by blokovaly přístup k bezplatnému obsahu pro uživatele se zakázanými technologiemi nahrazujícími cookies třetích stran. Volby vytvářené těmito obdobami cookies walls by však byly smysluplnější, pro-

[297] Viz návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) – Presidency discussion paper ze dne 6. 6. 2020, 2017/0003(COD), 9243/20, s. 6.

[298] Tím není dotčena možnost přijmout výjimky například pro bezpečnostní aktualizace.

tože potenciální zásah do soukromí by byl u technologií pozitivně hodnocených EDPB nízký.

Ať už však zvolíme variantu s výchozí blokací technologií nahrazujících cookies třetích stran, či nikoli, navrhované řešení podle mého názoru snižuje důraz na kontrolu uživatele, může zvýšit flexibilitu právní úpravy ve vztahu k omezeným formám cílené reklamy a současně zvyšuje úroveň ochrany soukromí uživatele prostřednictvím technických opatření na úrovni internetových prohlížečů.

9.6 NÁVRH ZNĚNÍ

Na základě výše provedené diskuze je namístě také formulovat, jak by navrhované řešení mělo být promítnuto do návrhu nařízení ePrivacy. V návrhu Komise je čl. 8 odst. 1 nařízení formulován jako pravidlo zakazující využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z koncových zařízení, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení uživatelé, s výjimkou využití pro definované důvody. Navrhované řešení nespočívá ve vymezení nového důvodu pro využití funkcí koncového zařízení, ale v úplném vyloučení některých způsobů využití funkcí koncového zařízení z působnosti výše popsaného pravidla. Z toho důvodu by podle mě nemělo být formulováno jako nové písmeno v čl. 8 odst. 1, ale jako nový odstavec čl. 8, stanovící výjimku z odst. 1.

Tato výjimka by pak měla být formulována tak, že se bude vztahovat na vlastní cookies a podobné technologie, tedy na ukládání a čtení informací z koncového zařízení v případě, že tyto informace budou uloženy tak, že je bude moci číst pouze webová stránka, která tyto informace do zařízení uložila. Výjimka by se proto neměla vztahovat na čtení informací v koncovém zařízení, které nebyly do zařízení uloženy příslušnou webovou stránkou. Výjimka by se také neměla vztahovat na počítačové programy (software) podle směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23.

dubna 2009, o právní ochraně počítačových programů.[299] Pro účely zajištění ochrany bezpečnosti koncového zařízení by také ukládané informace neměly měnit bezpečnostní nastavení koncového zařízení.

Tyto požadavky splňuje následující znění, které by mohlo být vloženo do čl. 8 jako nový odstavec 3 (s předpokladem přečíslování stávajících odst. 3 a 4):

> *Odst. 1 se nevztahuje na uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, pokud*
>
> *1. jsou informace do koncového zařízení při poskytování služby informační společnosti vyžádané koncovým uživatelem uloženy poskytovatelem této služby,*
>
> *2. přístup k těmto informacím je omezen na poskytovatele služby informační společnosti, který tyto informace do koncového zařízení uložil,*
>
> *3. tyto informace nejsou počítačovými programy a*
>
> *4. tyto informace nemění bezpečnostní nastavení koncového zařízení.*

Ve vztahu k technologiím nahrazujícím cookies třetích stran by se výjimka měla vztahovat na technologie, jejichž technickou specifikaci schválí EDPB. Taková právní úprava by vyžadovala doplnění nařízení ePrivacy o zcela nová ustanovení upravující příslušnou kompetenci EDPB, postup schvalování technických specifikací a kritéria jejich hodnocení. Není mou ambicí předkládat zde možné komplexní znění takové úpravy,[300] pouze se domnívám, že by mělo směřovat k podrobnému posouzení příslušné technické specifikace z hlediska dopadů dané technologie na soukromí uživatelů.

Do čl. 8 by se pak výjimka mohla promítnout jako nový odstavec 4 následujícího znění.

---

[299] Směrnice 2009/24/ES pojem počítačový program nedefinuje, není tedy podle mě nutné zavádět jeho definici ani do nařízení ePrivacy, jakkoli by patrně bylo vhodné v odůvodnění nařízení uvést, že tento pojem má stejný význam jako ve směrnici 2009/24/ES.

[300] Inspirací obecně může být právní úprava technických požadavků na výroby podle nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a kterým se zrušuje nařízení (EHS) č. 339/9.

Odst. 1 se nevztahuje na využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z koncových zařízení koncových uživatelů, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení koncoví uživatelé, pokud k němu dochází pomocí funkcionality softwaru uváděného na trh, který umožňuje elektronické komunikace včetně získávání a prezentování informací na internetu, a tato funkcionalita odpovídá technické specifikaci schválené Evropským sborem pro ochranu osobních údajů.

Požadavky na funkcionality webových prohlížečů jsou upraveny v čl. 10 návrhu Evropské komise. Odstavce 1 a 2 popisují požadované funkcionality a způsob jejich prezentace koncovému uživateli. Tyto dva odstavce by měla nahradit právní úprava, která tvůrcům internetových prohlížečů uloží ve výchozím nastavení blokaci cookies třetích stran ve webovém prohlížeči a implementaci opatření odpovídajících stavu techniky na úrovni prohlížeče, která budou bránit skrytému nebo neoprávněnému sledování uživatele. Opatření proti sledování koncového uživatele je přitom podle mého názoru třeba formulačně vázat na koncové zařízení, protože to je úroveň, na které je webový prohlížeč schopen sledování bránit. Odstavec 1 by tak mohl znít:

Software uváděný na trh, který umožňuje elektronické komunikace včetně získávání a prezentování informací na internetu, musí ve výchozím nastavení

1. *bránit uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, pokud přístup k těmto informacím není omezen na poskytovatele služby informační společnosti, který tyto informace do koncového zařízení uložil, a*
2. *mít aktivovaná přiměřená opatření odpovídající stavu techniky, která budou bránit skrytému nebo neoprávněnému sledování koncového zařízení.*

Pokud bychom na základě diskuze navržené výše v částech 9.4 a 9.5 dospěli k závěru, že technologie nahrazující cookies třetích stran nemají být ve výchozím nastavení webového prohlížeče blokovány, pak by písmeno a) odst. 1 mělo znít:

1) Bránit uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, pokud přístup k těmto informacím není omezen na poskytovatele služby informační společnosti, který tyto informace do koncového zařízení uložil, a nejde o uchovávání informací nebo získávání přístupu pomocí funkcionality softwaru uváděného na trh, který umožňuje elektronické komunikace včetně získávání a prezentování informací na internetu, odpovídající technické specifikaci schválené Evropským sborem pro ochranu osobních údajů,

Odstavec 2 upravuje odsouhlasení nastavení uživatelem. To podle mého názoru může být (dle výsledků diskuze navržené v částech 9.4 a 9.5) namístě pouze ve vztahu k technologiím nahrazujícím cookies třetích stran, tedy dle výše předloženého návrhu technologií uznaných EDPB. Odstavec 2 by proto mohl znít následovně:

2) Software při prvním spuštění informuje koncového uživatele o nastavení bránícím využití funkcionalit odpovídajících technické specifikaci schválené Evropským sborem pro ochranu osobních údajů a vyžaduje souhlas koncového uživatele s tímto nastavením nebo jeho změnu.

Pokud bychom dospěli k závěru, že technologie nahrazující cookies třetích stran by neměly být ve výchozím nastavení webového prohlížeče blokovány, pak by bylo možné odst. 2 zcela vypustit a následující odstavce přečíslovat.

Odstavec 3 v čl. 10 návrhu Komise obsahuje přechodné ustanovení. Toto ustanovení ukládá v případě softwaru, který bude ke dni účinnosti nařízení již instalován, splnit požadavky podle odstavců 1 a 2 při první aktualizaci softwaru, nejpozději však do tří měsíců od účinnosti. Druhou část požadavku považuji za nesplnitelnou, protože aktualizace softwaru zpravidla není pod kontrolou jeho tvůrce (toho, kdo jej uvádí na trh), ale toho, kdo má pod kontrolou zařízení, na kterém je software instalován. Druhá část požadavku by proto měla být podle mého názoru vypuštěna se zachováním pouze požadavku na splnění povinností při první aktualizaci.

Rovněž v souvislosti s aktualizací softwaru považuji za důležité, aby uživatel byl upozorněn na nové výchozí nastavení prohlížeče a měl možnost jej změnit. Tato povinnost by proto měla být uložena tvůrcům internetových prohlížečů. Odstavec 3 by proto mohl znít následovně:

3) V případě softwaru, který byl ke dni vstupu tohoto nařízení v účinnost již instalován, musí být požadavky podle odstavce splněny při první aktualizaci softwaru. Při instalaci aktualizace software informuje koncového uživatele o výchozím nastavení podle odstavce 1 a umožní mu jeho změnu.

10. ZÁVĚR

Podle platné právní úpravy ochrany soukromí v elektronických komunikacích je pro ukládání a čtení cookies a použití podobných technologií včetně použití údajů o koncovém zařízení nezbytný souhlas uživatele. Ten není vyžadován pouze pro použití cookies a podobných technologií v rozsahu nezbytném k fungování příslušné webové stránky. Souhlas musí splňovat požadavky GDPR, tedy být svobodný, konkrétní, informovaný a mít formu jednoznačného projevu vůle.

Široce formulovaný požadavek na souhlas je projevem přístupu k ochraně soukromí založeného na kontrole a jeho důsledkem je přetížení uživatelů žádostmi o jejich souhlas. V důsledku množství a složitosti procesů využívajících cookies a s nimi související informační asymetrie, složitosti předkládaných voleb, kognitivních limitů uživatelů a manipulativních uživatelských rozhraní není ve vztahu k použití cookies a souvisejících technologií kontrola ze strany uživatele reálná. Snaha o tuto kontrolu naopak vede k frustraci uživatelů. Řešením je podle mého názoru menší důraz na kontrolu a větší důraz na preventivní povinnosti pro ty, kdo relevantní činnosti vykonávají.

Požadavky na souhlas také komplikují realizaci cílené reklamy, která často slouží k financování webových stránek nabízejících bezplatný obsah nebo služby. Jakkoli financování prostřednictvím reklamy není například ve vztahu k médiím jediným možným modelem financování, je třeba počítat s tím, že přechod k jiným modelům financování bude postupný. Proto je

z pohledu významu nezávislých médií pro demokracii žádoucí najít způsob, jak umožnit bez větších komplikací realizaci cílené reklamy ve formě, která by představovala zásah do práva na soukromí v rozsahu proporcionálním k přínosu pro právo na svobodu projevu, právo na přístup k informacím a demokratický právní stát jako veřejný statek.

Návrh nařízení ePrivacy problém přílišného důrazu na kontrolu uživatele ani problém překážek pro omezené formy cílené reklamy neodstraňuje. Pozice Evropské komise pouze zpřesňuje některé pojmy, doplňuje dílčí tituly, o které lze opřít použití cookies bez souhlasu, a přidává požadavky na nastavení souhlasů ve webových prohlížečích. Evropský parlament ve své pozici zvětšuje důraz na souhlas uživatele a zpřesňuje požadavky na možnost jeho udělování prostřednictvím webového prohlížeče, vč. povinnosti webového prohlížeče vysílat signály o nastavení souhlasů a povinnosti webových stránek tyto signály respektovat. Toto řešení sice zmírňuje některé problémy kontroly s ohledem na sjednocení mechanismu udělování souhlasu, nesnižuje však potřebu, aby uživatel rozhodoval o udělení souhlasu ve vztahu k většině webových stránek, které navštíví. Současně nepřináší žádnou flexibilitu ve vztahu k omezeným formám internetové reklamy.

Pozice Rady vypouští závazné požadavky na nastavení webového prohlížeče a umožňuje pro přístup k webové stránce poskytované bezplatně vyžadovat souhlas s použitím cookies (za definovaných podmínek). Toto řešení by sice usnadnilo realizaci cílené reklamy opřené o souhlas, ale zachovalo by stávající problém přílišného důrazu na kontrolu a do jisté míry jej prohloubilo vytvářením neopodstatněného dojmu volby u služeb, které by souhlas mohly vyžadovat.

Východisko spatřuji v zakotvení výjimky z požadavku na souhlas pro použití vlastních cookies (tj. těch cookies, které do zařízení ukládá webová stránka, kterou uživatel prohlíží, nikoli jiná webová stránka), podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a technologií nahrazujících cookies třetích stran. Ve vztahu k technologiím nahrazujícím cookies třetích stran by se tato úprava měla vztahovat pouze na technologie odpovídající technické specifikaci schválené EDPB.

Tato úprava by pak měla být doplněna povinností webových prohlížečů ve výchozím nastavení blokovat cookies třetích stran vč. technologií, které je nahrazují, a přijmout opatření odpovídající stavu techniky, která budou bránit skrytému nebo neoprávněnému sledování uživatele. Nastavení výchozí blokace schválených technologií nahrazujících cookies třetích stran by mělo být uživateli při prvním použití webového prohlížeče předloženo ke schválení.

Pokud by vlastní cookies, podobné technologie spočívající v ukládání dat do koncového zařízení a technologie nahrazující cookies třetích stran nepodléhaly požadavku na souhlas podle právní úpravy přístupu ke koncovému zařízení, jejich použití pro sledování uživatele by i nadále podléhalo GDPR.

Cílem právní úpravy přístupu ke koncovému zařízení je zajištění ochrany před skrytým nebo neoprávněným sledováním uživatele – společně s udržením bezpečnosti koncového zařízení, kterou však cookies a podobné technologie nemohou narušit. GDPR se vztahuje na zpracování informací o fyzické osobě, která je identifikovaná nebo kterou lze přímo či nepřímo identifikovat. Identifikací lze rozumět mimo jiné cílení na danou osobu ve smyslu výběru jednotlivce ze skupiny jako objektu pozornosti (výběr vyčleněním, singling out), tedy i použití cookies a podobných technologií za účelem sledování uživatele.

Právní úprava GDPR je na jednu stranu flexibilnější v rovině právního základu použití cookies a podobných technologií, kterým by nemusel být pouze souhlas nebo jiný úzce definovaný titul, a na druhou stranu poskytuje komplexnější ochranu zahrnující základní zásady zpracování osobních údajů, práva subjektu údajů a povinnosti správce osobních údajů.

Pokud by použití vlastních cookies a podobných technologií podléhalo pouze GDPR, v řadě situací v praxi by odpadla nutnost získávat souhlas uživatele k použití cookies, které nejsou technicky nezbytné k fungování webové stránky, ale zásah do soukromí jimi vyvolaný je minimální. Návrh nařízení ePrivacy v tomto směru zavádí titul pro úzce vymezené způsoby měření návštěvnosti webové stránky, existují však další případy, kdy přísný režim souhlasu není namístě.

Jestliže by z požadavku na souhlas na úrovni každé webové stránky bylo vyňato také použití technologií nahrazujících cookies třetích stran, v rozsahu, v jakém by tyto technologie byly pro minimální zásah do soukromí schváleny EDPB, pak by právní úprava poskytovala také větší flexibilitu pro omezenou formu cílené reklamy jako zdroje financování obsahu, který je na internetu poskytován bezplatně. Je přitom k diskuzi, zda by, s ohledem na zachování přiměřené míry kontroly uživatele, měly být tyto technologie ve výchozím nastavení webového prohlížeče blokovány a toto nastavení mělo být uživateli předloženo ke schválení nebo úpravě.

V případě, že by současně ve webových prohlížečích byly ve výchozím nastavení blokovány cookies třetích stran a byla zavedena opatření odpovídající stavu techniky, která by bránila skrytému nebo neoprávněnému sledování uživatele, uživatel by byl chráněn proti stávajícím formám invazivní cílené reklamy založené na sledování a sdílení osobních údajů pomocí cookies třetích stran. Chráněn by byl také proti technikám, které se snaží blokaci cookies třetích stran obejít, jako je vydávání cookies třetích stran za vlastní a fingerprinting. Toto pojetí právní úpravy by odpovídalo trendu, který již nyní nastavují nejrozšířenější webové prohlížeče.

Výše popsané řešení by tak podle mého názoru oproti současné právní úpravě i návrhu nařízení ePrivacy snížilo důraz na kontrolu uživatele, umožnilo flexibilnější použití omezených forem cílené reklamy a přitom zvýšilo úroveň ochrany soukromí uživatelů před skrytým nebo neoprávněným sledováním.

11. POUŽITÉ PRAMENY

[1] ACAR, Gunes, et al. The web never forgets: Persistent tracking mechanisms in the wild. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security [online]. 2014 [cit. 12. 2. 2023], s. 674-689. Dostupné z ACM Digital Library: https://dl.acm.org/doi/abs/10.1145/2660267.2660347

[2] ACQUISTI, Alessandro et al. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys* [online]. 2017, roč. 50, č. 3, s. 44:1-44:41. ISSN 0360-0300. [cit. 2. 2. 2023]. Dostupné z: DOI:10.1145/3054926

[3] ANGWIN, Julia, PARRIS, Terry. Facebook Lets Advertisers Exclude Users by Race. *ProPublica* [online] 28. 10. 2016 [cit. 6. 3. 2022]. Dostupné z: https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

[4] BALBONI, Paolo et al. Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection. *International Data Privacy Law* [online]. 2013, roč. 3, č. 4, s. 244–261. ISSN 2044-3994. [cit. 2. 2. 2023]. Dostupné z: DOI:10.1093/idpl/ipt019

[5] BALKIN, Jack M. Information Fiduciaries in the Digital Age. In: *Balkinization.* [online] 5. 3. 2014 [cit. 3. 1. 2022]. Dostupné z: https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html

[6] BALKIN, Jack M. Information fiduciaries and the first amendment. *UC Davis Law Review* [online]. 2015, roč. 49, č. 4 [cit. 12. 2. 2023], s. 1183. Dostupné z: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/4692/49_U.C._Davis_Law_Review_1183_2016_.pdf?sequence=2

[7] BARTH, Adam. *HTTP State Management Mechanism* [online]. Request for Comments RFC 6265. B.m.: Internet Engineering Task Force 2011 [cit. 20. 7. 2022]. Dostupné z: DOI:10.17487/RFC6265

[8] BENNETT, Colin J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992, s. 33.

[9] BORGESIUS, Frederik J. Zuiderveen. Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law* [online]. 2015, roč. 5, č. 3, s. 163–176. ISSN 2044-3994. [cit. 2. 2. 2023]. Dostupné z: doi:10.1093/idpl/ipv011

[10] BORGESIUS, Frederik J. Zuiderveen. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, s. 256–271. ISSN 0267-3649. [cit. 2. 2. 2023]. Dostupné z: doi:10.1016/j.clsr.2015.12.013

[11] BRINKMANN, Martin. A look at Microsoft Edge's Tracking Prevention feature - gHacks Tech News. In: *gHacks Technology News* [online] 5. 6. 2017. [cit. 26. 2. 2022]. Dostupné z: https://www.ghacks.net/2019/06/28/a-look-at-microsoft-edges-tracking-prevention-feature/

[12] CALO, Ryan. Digital market manipulation. *George Washington Law Review* [online]. 2013, roč. 82, č. 4 [cit. 12. 2. 2023], s. 995-1051. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gwlr82&section=34&casa_token=oY9YY-cEQUoAAAAAA:1EOMhftCNdkJvbtLXxrwB6X5-eRQXEcSMvUbPKvKCJVf1ta-LiG33fb3rckI-MlflvR2MbcBETw

[13] CAMP, Dave. Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise In: *The Mozilla Blog* [online]. 4. 6. 2019 [cit. 26. 2. 2022]. Získáno z: https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/

[14] CAO, Yinzhi, LI, Song, WIJMANS, Erik. (Cross-)Browser Fingerprinting via OS and Hardware Level Features. In: *Network and Distributed System Security Symposium*: *Proceedings 2017 Network and Distributed System Security Symposium* [online]. San Diego, CA: Internet Society, 2017 [cit. 28. 10. 2022]. ISBN 978-1-891562-46-4. Dostupné z: DOI:10.14722/ndss.2017.23152

[15] CAROLAN, Eoin, CASTILLO-MAYEN, M. Rosario. Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws. *Virginia Journal of Law & Technology* [online]. 2014, roč. 19, č. 2 [cit. 28. 10. 2022], s. 324–388. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/vjolt19&section=6&casa_token=5uomoDkHG_MAAAAA:81N49Z1dJlF_mRM66PAf-KX6bPIlVhCSzc553AzMgr-MU4DYWwtw0J0--phzTGIkm2IApkBKKfg

[16] CINAR, Naim, ATEŞ, Sezgin. Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era. *SSRN Scholarly Paper* [online]. 24. 2. 2022. [cit. 4. 1. 2023]. Dostupné z: DOI:10.2139/ssrn.4041963

[17] CLARKE, Roger. Introduction to Dataveillance and Information Privacy, and Definitions of Terms [online] 24. 7. 2016 [cit. 3. 8. 2021]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html#Priv

[18] COFONE, Ignacio N. The way the cookie crumbles: online tracking meets behavioural economics. *International Journal of Law and Information Technology* [online]. 2017, roč. 25, č. 1 [cit. 2. 2. 2023], s. 38–62. ISSN 0967-0769. Dostupné z: DOI:10.1093/ijlit/eaw013

[19] CRAIN, Matthew, NADLER, Anthony. Political Manipulation and Internet Advertising Infrastructure. *Journal of Information Policy* [online]. 2019, roč. 9 [cit. 10. 9. 2022], s. 370–410. ISSN 2381-5892. Dostupné z: DOI:10.5325/jinfopoli.9.2019.0370

[20] CRANOR, Lorrie Faith. Cookie monster. *Communications of the ACM* [online]. 2022, roč. 65, č. 7 [cit. 2. 2. 2023], s. 30–32. ISSN 0001-0782. Dostupné z: doi:10.1145/3538639

[21] CYPHERS, Bennett. Google's FLoC Is a Terrible Idea. *Electronic Frontier Foundation* [online] 3. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[22] DOUGHERTY, Christie. Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation. *Northeastern University Law Review* [online]. 2020, roč. 12, č. 2 [cit. 2. 2. 2023], s. 629–659. Dostupné z HeinOnline: https://heinonline.org/HOL/Page?handle=hein.journals/norester12&div=23&g_sent=1&casa_token=

[23] DUTTON, Sam, LEE, Kevin K. FLEDGE. In: *Chrome Developers* [online] 27. 1. 2021 [cit. 22. 1. 2023]. Získáno z: https://developer.chrome.com/docs/privacy-sandbox/fledge/

[24] DUTTON, Sam. FLoC. In: *Chrome Developers* [online] 18. 5. 2021 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/floc/

[25] DUTTON, Sam. The Topics API. In: *Chrome Developers.* [online] 25. 1. 2022 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/topics/

[26] ETTELDORF, Christina. EDPB on the Interplay between the ePrivacy Directive and the GDPR. *European Data Protection Law Review* [online]. 2019, roč. 5, č. 2 [cit. 2. 2. 2023], s. 224–231. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/edpl5&section=37

[27] GELLERT, Raphaël; GUTWIRTH, Serge. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 522-530. Dostupné ze ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0267364913001325

[28] GELLERT, Raphaël. *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press, 2020.

[29] GUY, Amy. Early design review for the Topics API #726. Komentář uživatele rhiaro z 12. 1. 2023. In: github [online]. 12. 1. 2023 [cit. 30. 1. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459

[30] HÄRTING, Niko, GÖSSLING, Patrick. Study on the Impact of the Proposed Draft of the ePrivacy Regulation. *Computer Law Review International* [online]. 2018, roč. 19, č. 1 [cit. 20. 1. 2023], s. 6–11. ISSN 2194-4164. Dostupné z: DOI:10.9785/cri-2018-190103

[31] HARTZOG, Woodrow. *Privacy's blueprint*. Cambridge, Massachusetts: Harvard University Press, 2018.

[32] HINTERNESCH, Nicolas. No Cookies, No Problem — Using ETags For User Tracking. *Medium* [online] 2. 7. 2020 [cit. 18. 1. 2023]. Dostupné z: https://levelup.gitconnected.com/no-cookies-no-problem-using-etags-for-user-tracking-3e745544176b

[33] HOOFNAGLE, Chris Jay et al. Behavioral advertising: The offer you can't refuse. *Harvard Law & Policy Review*. 2012, roč. 6, s. 273.

[34] JENSEN, Paul. Intent to Experiment: First „Locally-Executed Decision over Groups" Experiment (FLEDGE) In: *Google Groups*. [online] 25. 3. 2022 [cit. 22. 1. 2023]. Dostupné z: https://groups.google.com/a/chromium.org/g/blink-dev/c/0VmMSsDWsFg

[35] KAMARA, Irene, DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. *SSRN Scholarly Paper* [online]. 8. 8. 2018 [cit. 8. 1. 2023]. Dostupné z: DOI:10.2139/ssrn.3228369

[36] KAMARA, Irene, KOSTA, Eleni. Do Not Track initiatives: regaining the lost user control. *International Data Privacy Law* [online]. 2016, roč. 6, č. 4 [cit. 2. 2. 2023], s. 276–290. ISSN 2044-3994. Dostupné z: DOI:10.1093/idpl/ipw019

[37] KHAN, Lina M.; POZEN, David E. A skeptical view of information fiduciaries. *Harvard Law Review* [online]. 2019, roč. 133, č. 2 [cit. 2. 2. 2023], s. 497-541. Dostupné z JSTOR: https://www.jstor.org/stable/pdf/26868033.pdf

[38] KONIK, James. How Does Canvas Fingerprinting Work – In: *Fingerprint* [online] 11. 6. 2021 [cit. 28. 10. 2022]. Dostupné z: https://fingerprint.com/blog/canvas-fingerprinting/

[39] KOSTA, Eleni. Peeking into the cookie jar: the European approach towards the regulation of cookies. *International Journal of Law and Information Technology* [online]. 2013, roč. 21, č. 4 [cit. 11. 1. 2023], s. 380–406. ISSN 0967-0769. Dostupné z: DOI:10.1093/ijlit/eat011

[40] KULYK, Oksana et al. Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity* [online]. 2020, roč. 6, č. 1 [cit. 2. 2. 2023], s. 1-14. ISSN 2057-2085. Dostupné z: DOI:10.1093/cybsec/tyaa022

[41] LAMBRECHT, Anja, TUCKER, Catherine. When does retargeting work? Information specificity in online advertising. *Journal of Marketing research* [online]. 2013, roč. 50, č. 5 [cit. 2. 2. 2023], s. 561–576. Dostupné z SagePub: https://journals.sagepub.com/doi/pdf/10.1509/jmr.11.0503

[42] LASSEY, Brad. Combating Fingerprinting with a Privacy Budget. In*: github.* [online]. 25. 2. 2022 [cit. 6. 3. 2022]. Dostupné z: https://github.com/bslassey/privacy-budget

[43] LAURISTIN, Marju. REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), A8-0324/2017.In: *European Parliament.* [online] 20. 10. 2017 [cit. 11. 1. 2023]. Dostupné z: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html

[44] LAZUIK, Estelle. iOS 14 Opt-in Rate - Weekly Updates Since Launch. In: *Flurry.* [online]. 25. 5. 2021. [cit. 2. 2. 2023]. Dostupné z: https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/

[45] LEE, Timothy B. Google defends tracking cookies—some experts aren't buying it. In: *Ars Technica* [online] 26. 8.2019. [cit. 26. 2. 2022]. Dostupné z: https://arstechnica.com/tech-policy/2019/08/why-some-experts-are-skeptical-of-googles-new-web-privacy-strategy/

[46] LEENES, Ronald E. Do They Know Me? Decomposing Identifiability *University of Ottawa Law and Technology Journal* [online]. 2007, roč. 4, č. 1-2 [cit. 6. 1. 2023], s. 135-161. Dostupné z: https://research.tilburguniversity.edu/files/1310856/Leenes_Do_they_know_me_110216_publishers_immediately.pdf

[47] MAYER, Jonathan R., MITCHELL, John C. Third-party web tracking: Policy and technology. In: 2012 *IEEE symposium on security and privacy* [online]. IEEE, 2012 [cit. 27. 5. 2023]. s. 413-427. Dostupné z: https://ieeexplore.ieee.org/abstract/document/6234427

[48] VON LEWINSKI, Kai. Geschichte des Datenschutzrechts von 1600 bis 1977. In: *Freiheit-Sicherheit-Öffentlichkeit*. Heidelberg: Nomos Verlagsgesellschaft mbH & Co. KG, 2009, s. 196–220.

[49] LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*. Boca Raton: CRC Press, 2020.

[50] MCDONALD, Aleecia M., CRANOR, Lorrie Faith. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* [online]. 2008, roč. 4, č. 3 [cit. 6. 3. 2022], s. 543. Dostupné z HeinOnline: https://heinonline.org/HOL/Page?handle=hein.journals/isjlpsoc4&div=27&g_sent=1&casa_token=

[51] MCNAIR, Brian. Journalism and Democracy. In: *Journalism and Democracy* [online]. New York: Routledge, 2009, s. 257–269 [cit. 20. 1. 2023]. ISBN 978-0-203-87768-5. Dostupné z: doi:10.4324/9780203877685-27

[52] MERCADO KIERKEGAARD, Sylvia. How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law & Security Review* [online]. 2005, roč. 21, č. 4 [cit. 2. 2. 2023], s. 310–322. ISSN 0267-3649. Dostupné z: doi:10.1016/j.clsr.2005.06.002

[53] MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie* [online]. 2014, roč. 5, č. 9 [cit. 23. 1. 2023], s. 3–74. Dostupné z: https://journals.muni.cz/revue/article/view/5017

[54] MOORE, Adam D. *Privacy rights: Moral and legal foundations*. Pennsylvania: Penn State Press, 2010.

[55] NOUWENS, Midas et al. 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]. New York, NY, USA: Association for Computing Machinery, 2020, s. 1–13 [cit. 2. 2. 2023]. ISBN 978-1-4503-6708-0. Dostupné z: https://doi.org/10.1145/3313831.3376321

[56] PAPAKONSTANTINOU, Vagelis, DE HERT, Paul. The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights. *John Marshall Journal of Computer and Information Law* [online]. 2011, roč. 29, č. 1 [cit. 2. 2. 2023], s. 29–75. ISSN 1078-4128. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jmjcila29&section=5

[57] PURTOVA, Nadezhda. From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law* [online]. 2022, roč. 12, č. 3 [cit. 2. 2. 2023], s. 163–183. ISSN 2044-3994. [cit. 2. 2. 2023]. Dostupné z: doi:10.1093/idpl/ipac013

[58] REN, Tongwei et al. An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections. In: *Workshop on Measurements, Attacks, and Defenses for the Web*: *Proceedings 2021 Workshop on Measurements, Attacks, and Defenses for the Web* [online]. Virtual: Internet Society, 2021 [cit. 4. 1. 2023]. ISBN 978-1-891562-67-9. Dostupné z: doi:10.14722/madweb.2021.23018

[59] RICHARDS, Neil. *Intellectual privacy: rethinking civil liberties in the digital age*. Oxford, UK: Oxford University Press, 2015, 220 s. ISBN 978-0-19-994614-3.

[60] RICHARDS, Neil M., HARTZOG, Woodrow. Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review* [online]. 2016, roč. 19, č. 3, [cit. 30. 1. 2021], s. 431-472. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/stantlr19&section=19

[61] ROBERTSON, Adi. Google antitrust suit takes aim at Chrome's Privacy Sandbox. In: *The Verge.* [online] 16. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy

[62] RUSSINOVICH, Mark. Sony, Rootkits and Digital Rights Management Gone Too Far. In: *Mark's Blog* [online] 31. 10. 2015 [cit. 11. 1. 2023]. Dostupné z: https://web.archive.org/web/20150317040653/http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx

[63] RYAN, Johnny. Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR. In: brave [online] 12. 9. 2018 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/adtech-data-breach-complaint/

[64] RYAN, Johnny. Update on GDPR complaint (RTB ad auctions). In: *brave* [online] 28. 1. 2019 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/update-rtb-ad-auction-gdpr/

[65] RYAN, Johnny. ICCL sues DPC over failure to act on massive Google data breach. In: *Irish Council for Civil Liberties.* [online] 15. 3. 2022 [cit. 23. 1. 2023]. Dostupné z: https://www.iccl.ie/news/iccl-sues-dpc-over-failure-to-act-on-massive-google-data-breach/

[66] SCHUH, Justin. Building a more private web: A path towards making third party cookies obsolete. In: *Chromium Blog*[online]. 14. 1. 2020 [cit. 7. 8. 2021]. Dostupné z: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

[67] SCHUH, Justin. Building a more private web. In: *Google* [online] 22. 8. 2019 [cit. 26. 2 2022]. Dostupné z: https://blog.google/products/chrome/building-a-more-private-web/

[68] SMIT, Edith G., VAN NOORT, Guda, VOORVELD, Hilde A. M. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior* [online]. 2014, roč. 32, s. 15–22. ISSN 0747-5632. [cit. 2. 2. 2023]. Dostupné z: doi:10.1016/j.chb.2013.11.008

[69] SPEICHER, Till et al. Potential for Discrimination in Online Targeted Advertising. In: *Conference on Fairness, Accountability and Transparency*: *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* [online]. PMLR, 2018 [cit. 6. 3. 2022], s. 5–19. Dostupné z: https://proceedings.mlr.press/v81/speicher18a.html

[70] THOMSON, Martin. A *Privacy Analysis of Google's Topics Proposal*. In: github [online]. 6. 1. 2023 [cit. 28. 5. 2023]. Dostupné z: https://mozilla.github.io/ppa-docs/topics.pdf s. 12.

[71] TOMÍŠEK, Jan. Cookies a GDPR. *Právní rozhledy* [online]. 2018, roč. 26, č. 20 [cit. 6. 2. 2023], s. 687–696. Dostupné z beck-online: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxa4s7giyf6427gy4do

[72] TOMÍŠEK, Jan. Souhlasy s cookies a přístupy k ochraně osobních údajů [online]. *Právník*. 2022, roč. 161, č. 6 [cit. 6. 2. 2023], s. 561–577. Dostupné z: https://www.ilaw.cas.cz/casopisy-a-knihy/casopisy/casopis-pravnik/archiv/2022/2022-06.html?a=3686

[73] TUROW, J. et al. Americans Reject Tailored Advertising and Three Activities that Enable It. In: *SSRN* [online]. 29. 9. 2009 [cit. 2. 2. 2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[74] UTZ, Christine et al. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [online]. New York, NY, USA: Association for Computing Machinery, 2019, s. 973–990 [cit. 2. 1. 2022]. CCS '19. ISBN 978-1-4503-6747-9. Dostupné z: doi:10.1145/3319535.3354212

[75] VEALE, Michael, BORGESIUS, Frederik J. Zuiderveen. Adtech and real-time bidding under European data protection law. *German Law Journal* [online]. 2022, roč. 23, č. 2 [cit. 6. 2. 2023], s. 226–256. Dostupné z: https://www.cambridge.org/core/journals/german-law-journal/article/adtech-and-realtime-bidding-under-european-data-protection-law/017F027B4E78EBCAE1DCBC1E12B93B9D

[76] WARREN, Samuel D., BRANDEIS, Louis D. Right to privacy. *Harvard Law Review* [online]. 1890, roč. 4, č. 5 [cit. 6. 2. 2023], s. 193–220. Dostupné z JSTOR: https://www.jstor.org/stable/1321160

[77] WHITE, Alexandra. Privacy Budget. In: *Chrome Developers* [online] 4. 3. 2022. [cit. 28. 10. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/privacy-budget/

[78] WILANDER, John. Intelligent Tracking Prevention. In: *WebKit* [online]. 5. 6. 2017 [cit. 26. únor 2022]. Dostupné z: https://webkit.org/blog/7675/intelligent-tracking-prevention/

[79] WILANDER, John. Full Third-Party Cookie Blocking and More. In: *WebKit* [online]. 2020. [cit. 26. 2. 2022]. Dostupné z: https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

[80] YUAN, Shuai et al. Internet Advertising: An Interplay among Advertisers, Online Publishers, Ad Exchanges and Web Users. In: *arXiv* [online]. 2. 7. 2012 [cit. 18. 11. 2022]. Dostupné z: http://arxiv.org/abs/1206.1754

[81] YUAN, Shuai, WANG, Jun; ZHAO, Xiaoxue. Real-time bidding for online advertising: measurement and analysis. In: *Proceedings of the Seventh International Workshop on Data Mining for Online Advertising* [online]. 2013 [cit. 18. 11. 2022], s. 1–8. Dostupné z ACM Digital Library: https://dl.acm.org/doi/abs/10.1145/2501040.2501980

[82] ZHANG, Kaifu, KATONA, Zsolt. Contextual advertising. *Marketing Science* [online]. 2012, roč. 31, č. 6 [cit. 6. 2. 2023], s. 980–994. Dostupné z: https://pubsonline.informs.org/doi/abs/10.1287/mksc.1120.0740

[83] ZHENG, Guangzhi, PELTSVERGER, Svetlana. Web analytics overview. In: *Encyclopedia of Information Science and Technology, Third Edition* [online]. IGI Global, 2015 [cit. 6. 2. 2023], s. 7674–7683. Dostupné z: https://www.igi-global.com/chapter/web-analytics-overview/112470

[84] ZITTRAIN, Jonathan. How to Exercise the Power You Didn't Ask For. *Harvard Business Review* [online]. 19. 9. 2018 [cit. 30. 10. 2022]. ISSN 0017-8012. Dostupné z: https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for

[85] Autorité de protection des données. The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR In: *Autorité de protection des données* [online] 2. 2. 2022 [cit. 23. 1. 2023]. Dostupné z: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

[86] Competition and Markets Authority. Online platforms and digital advertising. In *Competition and Markets Authority*. [online]. 1. 7. 2020. Dostupné z: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

[87] Competition and Markets Authority. CMA to keep 'close eye' on Google as it secures final Privacy Sandbox commitments. In: *GOV.UK*. [online] 11. 2. 2022 [cit. 26. 2. 2022]. Dostupné z: https://www.gov.uk/government/news/cma-to-keep-close-eye-on-google-as-it-secures-final-privacy-sandbox-commitments

[88] Early design review for the Topics API #726. 25. 3. 2023 [cit. 28. 5. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459

[89] Electronic Frontier Foundation. SunnComm MediaMax Security Vulnerability FAQ. In: *Electronic Frontier Foundation* [online]. 19. 7. 2007 [cit. 11. 1. 2023]. Dostupné z: https://www.eff.org/pages/sunncomm-mediamax-security-vulnerability-faq

[90] Evropská komise. Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. In: *Evropská komise*. [online]. Červen 2011 [cit. 2. 2. 2023]. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Part%20I%20of%20Special%20Eurobarometer%20359%20-%20Attitudes%20on%20Data%20Protection%20and%20Electronic%20Identity%20in%20the%20European%20Union.pdf

[91] Evropská komise. Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. In: *Evropská komise* [online]. 30. 1. 203 [cit. 2. 2. 2023]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en

[92] Evropský sbor pro ochranu osobních údajů. Prohlášení Evropského sboru pro ochranu osobních údajů o revizi nařízení o soukromí a elektronických komunikacích a jejím dopadu na ochranu fyzických osob v souvislosti se soukromím a důvěrným charakterem jejich komunikace. In: *European Data Protection Board*. [online]. 5. 5. 2018 [cit. 16. 7. 2018]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_cs_0.pdf

[93] Evropský sbor pro ochranu osobních údajů. Pokyny 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů Verze 2.0 Přijato dne 20. října 2020. In: *European Data Protection Board.* [online]. 20. 10. 2020. [cit. 31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2021-04/
edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_cs.pdf

[94] Evropský sbor pro ochranu osobních údajů. Stanovisko č. 5/2019 ke vzájemnému působení mezi směrnicí o soukromí a elektronických komunikacích a obecným nařízením o ochraně osobních údajů (GDPR), zejména pokud jde o příslušnost, úkoly a pravomoci úřadů pro ochranu údajů. In: *European Data Protection Board* [online]. 12. 3. 2019. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_cs.pdf

[95] Evropský sbor pro ochranu osobních údajů. Pokyny č. 8/2020 k cílení na uživatele sociálních médií ze dne 13. dubna 2021. In: *European Data Protection Board* [online]. 13. 4. 2021. [cit. 1. 2. 2023] Dostupné z: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_c_cs_0.pdf

[96] Evropský sbor pro ochranu osobních údajů. Závazné rozhodnutí 1/2021 ve věci sporu ohledně návrhu rozhodnutí irského dozorového úřadu týkajícího se společnosti WhatsApp Ireland podle čl. 65 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů. In: *European Data Protection Board* [online]. 28. 7. 2021 [31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2022-03/
edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_cs.pdf bod 191.

[97] Evropský sbor pro ochranu osobních údajů. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them Version 1.0 Adopted on 14 March 2022. In: European Data Protection Board [online]. 14. 3. 2022 [cit. 1. 2. 2023] Dostupné z: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

[98] Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022 In: *European Data Protection Board.* [online]. 5. 12. 2022 [cit. 31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf

[99] Evropský sbor pro ochranu osobních údajů. Report of the work undertaken by the Cookie Banner Taskforce, Adopted on 17 January 2023. In: *European Data Protection Board* [online]. 17. 1. 2023. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

[100] GlobalStats. Browser Market Share Worldwide. In: *StatCounter Global Stats* [online] nedatováno [cit. 31. 1. 2023]. Dostupné z: https://gs.statcounter.com/browser-market-share

[101] Google. How We're Protecting Your Online Privacy.In: *The Privacy Sandbox*. [online] nedatováno [cit. 18. 1. 2023]. Dostupné z: https://privacysandbox.com/open-web/

[102] Google. IP masking in Universal Analytics. In: Analytics Hepl [online]. Nedatováno [cit. 12.2. 2023]. Dostupné z: https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631

[103] hotjar. What Are Session Recordings (Session Replays) + How to Use Them. In: *hotjar*. [online] 31. 1. 2023 [cit. 23. 1. 2023]. Dostupné z: https://www.hotjar.com/session-recordings/

[104] Information Commissioner's Office. How do we comply with the cookie rules? In: *Information Commissioner's Office* [online]. [cit. 1. 2. 2023]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/

[105] Information Commissioner's Office. ICO calls on Google and other companies to eliminate existing privacy risks posed by adtech industry. In: *Information Commissioner's Office*. [online] 25. 11. 2021 [cit. 23. 1. 2023]. Dostupné z: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-calls-on-google-and-other-companies-to-eliminate-existing-privacy-risks-posed-by-adtech-industry/

[106] Information Commissioner's Office. Data protection and privacy expectations for online advertising proposals. In: *Information Commissioner's Office.* [online]. 25. 11. 2021 [cit. 2. 2. 2023]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf

[107] Interactive Advertising Bureau. ePrivacy Regulation. In: *Interactive Advertising Bureau* online]. Nedatováno. [cit. 20. 1 2023]. Získáno z: https://iabeurope.eu/proposed-eprivacy-regulation/

[108] Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era. In: *Interactive Advertising Bureau* [online]. Březen 2022 [cit. 31. 1. 2023]. Dostupné z: https://iabeurope.eu/wp-content/uploads/2022/03/IAB-Europe-Guide-to-a-Post-Third-Party-Cookie-Era-March-2022.pptx.pdf

[109] Interactive Advertising Bureau. IAB Europe Transparency & Consent Framework Policies. In: *Interactive Advertising Bureau*. [online]. 21. 6. 2022 [cit. 22. 1. 2023]. Dostupné z: https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[110] Internet Engineering Task Force. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content [online]. Červen 2014. [cit. 1. 2. 2023]. In: *Data Tracker*. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7231#section-5

[111] noyb. noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints In: *nyob* [online] 31. 5. 202 [cit. 24. 1. 2023]. Dostupné z: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints

[112] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2007 k pojmu osobní údaje In: *Evropská komise* [online]. 20. 6. 2007 [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf

[113] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies. In: *Evropská komise* [online]. 7. 6. 2012 [cit. 23. 1. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf

[114] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES In: *Evropská komise* [online]. 9. 4. 2014 [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

[115] Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29. Stanovisko č. 9/2014 k uplatňování směrnice 2002/58/ES na otisky zařízení. In: *Evropská komise* [online]. 25. 11. 2014 [cit. 1. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

[116] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Presidency note. 2017/0003 (COD), 10866/17. In: *EUR-Lex* [online]. 3. 7. 2017 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10866_2017_INIT

[117] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003 (COD), 11995/17. In: *EUR-Lex* [online]. 8. 9. 2017 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11995_2017_INIT

[118] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency. 2017/0003 (COD), 15333/17. In: *EUR-Lex* [online]. 5. 12. 2017 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15333_2017_INIT

[119] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper 2017/0003(COD), 5165/18. In: *EUR-Lex* [online]. 11. 1. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5165_2018_INIT

[120] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion. 2017/0003(COD), 7207/18. In: *EUR-Lex* [online]. 22. 3. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7207_2018_INIT

[121] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 017/0003(COD), 10975/18. In: *EUR-Lex* [online]. 10. 6. 2018, [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT

[122] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 10975/18. In: *EUR-Lex* [online]. 10. 7. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT

[123] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 13256/18. In: *EUR-Lex* [online]. 19. 10. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT

[124] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions 2017/0003(COD), 5934/19. In: *EUR-Lex* [online]. 4. 2. 2019 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5934_2019_INIT

[125] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 11291/19. In: *EUR-Lex* [online]. 26. 7. 2019 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11291_2019_INIT

[126] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003(COD), 5979/20. In: *EUR-Lex* [online]. 21. 2. 2020 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT

[127] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Progress report. 2017/0003(COD), 13106/20. In: *EUR-Lex* [online]. 23. 11. 2020 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-13106-2020-INIT/en/pdf

[128] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications) – Presidency discussion paper 2017/0003(COD), 9243/20. In: *EUR-Lex* [online]. 6. 6. 2020 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT

[129] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications). 2017/0003(COD), 9931/20. In: *EUR-Lex* [online]. 4. 11. 2020 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT

[130] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 5008/2. In: *EUR-Lex* [online]. 5. 1. 2021 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf

[131] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP. 2017/0003(COD), 6087/21. In: *EUR-Lex* [online]. 10. 2. 2021 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT

[132] Request for Position: Topics API #622. In: github [online]. 17. 3. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/mozilla/standards-positions/issues/622

[133] Spolek pro ochranu osobních údajů. Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022. In: *Spolek pro ochranu osobních údajů* [online]. 15. 12. 2021 [cit. 1. 2. 2023]. Dostupné z: https://www.ochranaudaju.cz/wp-content/uploads/2021/12/Stanovisko_cookies_2021_final.pdf

[134] The Topics API #111. In: github [online]. 20. 12. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/WebKit/standards-positions/issues/111

[135] Úřad pro ochranu osobních údajů. Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018. In: *Úřad pro ochranu osobních údajů* [online]. 25. 6. 2020 [cit. 6. 7. 2018]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=42915

[136] Úřad pro publikace Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 52017PC0010. In: *EUR-Lex* [online]. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010

[137] w3schools. HTML Web Storage API. In: *w3schools.* [online] nedatováno [cit. 18. 1. 2023]. Dostupné z: https://www.w3schools.com/html/html5_webstorage.asp

---
