Souhlasy s cookies a přístupy k ochraně osobních údajů

Jan Tomíšek*

Abstrakt: **Předmětem článku je diskuse aktuálních přístupů k ochraně osobních údajů ve světle novelizované právní úpravy ukládání a čtení údajů z koncových zařízení uživatelů služeb elektronických komunikací, která mj. rozšiřuje požadavky na sběr souhlasů s použitím tzv. cookies. Článek proto představuje přístup k ochraně osobních údajů založený na kontrole ze strany osoby, které se údaje týkají, a přístup založený na ochraně důvěry vložené v ty, kteří osobní údaje zpracovávají. Následně je diskutována vhodnost obou přístupů pro zajištění ochrany osobních údajů v současné společnosti charakterizované velkým rozsahem zpracování osobních údajů. Autor dospívá k závěru, že přístup založený na kontrole by neměl být dominantním přístupem k ochraně osobních údajů, protože kontrola takového rozsahu zpracování ze strany dotčených osob není možná s ohledem na omezené časové zdroje a limity racionálního rozhodování. Proto navrhuje klást v ochraně osobních údajů důraz na přístup založený na důvěře. Ten je již široce promítnut do obecné právní úpravy ochrany osobních údajů, nikoli však do oblasti ochrany soukromí a osobních údajů v elektronických komunikacích. Autor proto navrhuje opustit požadavek na souhlas s ukládáním a čtením údajů z koncových zařízení uživatelů služeb elektronických komunikací a nahradit jej vazbou na obecná pravidla ochrany osobních údajů, doplněná výkladem Evropského sboru pro ochranu osobních údajů rozpracovávajícím zásady přístupu založeného na důvěře.**

Klíčová slova: **ochrana osobních údajů, osobní údaje, cookies, kontrola, důvěra**

Úvod

K datu 1. ledna 2022 vstoupila v účinnost novela zákona č. 127/2005 Sb. o elektronických komunikacích, ve znění pozdějších předpisů (dále jen „z. el. kom.“), která mění znění § 89 odst. 3 z. el. kom.[1] Do tohoto ustanovení byl nově vložen požadavek na získání souhlasu s ukládáním a čtením údajů z koncových zařízení služeb elektronických komunikací.[2] Praktickým důsledkem této novely je řada nových dialogů žádajících o udělení souhlasu s ukládáním a čtením tzv. cookies,[3] které zaplavují uživatele českého internetu při vstupu na různé webové stránky.

Obsah novely § 89 odst. 3 citovaného zákona přitom není v podstatném rozsahu vlastní tvorbou českého zákonodárce, ale pouze nápravou dřívější chybné transpozice směrnice

* Mgr. et Mgr. Ing. Jan Tomíšek. Ústav práva a technologií Právnické fakulty Masarykovy univerzity a advokátní kancelář ROWAN LEGAL. E-mail: jantomisek@gmail.com. ORCID: https://orcid.org/0000-0003-1442-4982.

1 Srov. zákon č. 374/2021 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.

2 Konkrétně novelizované znění § 89 odst. 3 citovaného zákona ukládá tomu, kdo *„hodlá používat nebo používá sítě elektronických komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních účastníků nebo uživatelů“*, povinnost získat *„od těchto účastníků nebo uživatelů předem prokazatelný souhlas s rozsahem a účelem jejich zpracování“* přičemž 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“*.

3 Cookies jsou krátké textové soubory, které se ukládají do internetového prohlížeče a lze do nich mimo jiné zapsat údaje, kterým lze konkrétní internetový prohlížeč na konkrétním zařízení jednoznačně identifikovat při opakované návštěvě webové stránky. Při určitém způsobu implementace lze cookies využít ke sledování chování uživatelů internetu napříč webovými stránkami.

Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) (dále jen „směrnice 2002/58/ES“).[4] Záplava žádostí o souhlas s ukládáním a čtením cookies tak není českým specifikem, ale pouze přiblížením se standardu západní Evropy.

Cílem směrnice 2002/58/ES je v kontextu elektronických komunikací zajistit ochranu základních práv, zejména práva na soukromí a ochranu osobních údajů.[5] Ve vztahu k ukládání a čtení cookies jde přitom především o zajištění ochrany osobních údajů, protože teprve zpracováním osobních údajů získaných pomocí cookies typicky dochází k případnému zásahu do soukromí.[6]

Požadavek na získání souhlasu s ukládáním a čtením cookies, vyjádřený v čl. 5 odst. 3 směrnice 2002/58/ES a transponovaný do § 89 odst. 3 z. el. kom., je projevem přístupu k ochraně osobních údajů založeného na kontrole. Jeho podstatou je předpoklad, že ochrana osobních údajů bude nejlépe zajištěna, pokud jednotlivec bude mít možnost rozhodovat o nakládání s údaji, které se ho týkají.

Cílem tohoto článku je ukázat, že přístup založený na kontrole není jediným možným přístupem k ochraně osobních údajů a ačkoli v ní má své místo, neměl by být přístupem dominantním. Dále je cílem tohoto článku poukázat na alternativní přístup založený na ochraně důvěry dotčených jednotlivců v ty, kteří s chráněnými údaji nakládají, a na základě diskuse těchto dvou přístupů předložit návrhy *de lege ferenda*, jak lépe přistoupit k právní úpravě ukládání a čtení cookies. Tento článek je proto strukturován následovně. První část článku vymezuje pojem ochrany osobních údajů. Druhá část článku pak popisuje základní koncepce ochrany soukromí a diskutuje jejich relevanci v kontextu rozsahu zpracování osobních údajů v současné společnosti. Třetí část článku představuje návrhy *de lege ferenda* a čtvrtá část shrnuje jeho závěry.

1. Pojem ochrany osobních údajů

Jak je v právu obvyklé, odpověď na jednoduchou otázku, co to je ochrana osobních údajů, není zdaleka jednoduchá. Historickou perspektivu tohoto pojmu nabízí von Lewinski, který ochranu osobních údajů považuje za regulaci informační asymetrie – jejím cílem je zmírnit nerovnost subjektů práva v případech, kdy jeden z nich disponuje „datovou mocí“ (*Datenmacht*), tedy se dostává do postavení silnější strany vztahu vlivem osobních údajů, kterými disponuje.[7] Za právní předpis upravující ochranu osobních údajů tak považuje jakýkoli předpis, který omezuje možné dopady datové moci na jednotlivce, přičemž takové právní předpisy je dle von Lewinského možné vysledovat od doby vzniku moderního státu v 19. století.[8] Obdobně podle Gellerta lze říct, že *„předmětem ochrany*

4 K dřívější chybné transpozici srov. např. MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*. 2014, roč. 5, č. 9. TOMÍŠEK, Jan. Cookies a GDPR. *Právní rozhledy*. 2018, roč. 26, č. 20.

5 Srov. bod 2 odůvodnění směrnice 2002/58/ES.

6 Ochrana osobních údajů je zde primárním právním nástrojem k prevenci zásahů do hodnot, které sekundárně chrání právo na soukromí.

7 Srov. VON LEWINSKI, K. Geschichte des Datenschutzrechts von 1600 bis 1977. In: *Freiheit-Sicherheit-Öffentlichkeit*. Nomos, 2009, s. 200.

8 Srov. ibidem, s. 204.

osobních údajů je jednoduše veškerá společenská újma, která může vzniknout ze zpracování osobních údajů".[9]

Toto vymezení je však příliš obecné pro diskusi právní úpravy, protože je obtížné pod něj podřazovat jednotlivé skutkové stavy. Praktičtější vymezení nabízí Kasl, dle kterého je ochrana osobních údajů *„preventivním právním rámcem veřejnoprávní povahy"*[10], jehož účelem je *„preventivní omezení rizika vzniku situací, při kterých dojde k vážnému zásahu do práv a svobod subjektu údajů, jelikož technologický pokrok činí tyto zásahy potenciálně příliš závažné a plošné na to, aby postačovaly nástroje ochrany osobnosti"*.[11] Obdobně přistupuje k vymezení ochrany osobních údajů Míšek, dle kterého právo na ochranu osobních údajů *„připomíná deštník, který překrývá další základní práva"*,[12] protože působí jako prevence před zásahem do těchto dalších základních práv.[13]

Odvozené právo na ochranu osobních údajů je proto právem „instrumentálním"[14] – podobně jako právo na spravedlivý proces nevytváří samo o sobě chráněnou hodnotu, ale zajišťuje ochranu jiným právům, respektive hodnotám chráněným základními právy. Tuto ochranu zajišťuje stanovením záruk, které působí preventivně proti zásahům do základních práv, respektive jimi chráněných hodnot prostřednictvím zpracování osobních údajů.

Toto vymezení je však samo o sobě stále málo obsažné, dokud nejsou vymezeny pojmy osobní údaj a zpracování. Ty je v evropském kontextu možné vykládat ve světle platné právní úpravy v podobě nařízení Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR"). Podle čl. 4 bod 1) GDPR jsou osobními údaji veškeré informace o fyzické osobě, kterou lze přímo či nepřímo identifikovat. Zpracováním je pak podle bodu 2) téhož článku jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů. V souladu s čl. 4 GDPR pak pro přehlednost v dalším výkladu označuji fyzickou osobu, které se osobní údaje týkají, jako subjekt údajů, a osobu, která údaje zpracovává, jako správce.[15]

Ochranu osobních údajů tedy lze vnímat jako soubor opatření směřujících k prevenci zásahů do základních práv, respektive jimi chráněných hodnot prostřednictvím operací s údaji, které se týkají fyzických osob, jež lze přímo či nepřímo identifikovat. Právo na ochranu osobních údajů je pak na jednu stranu pozitivním právem subjektu údajů na zavedení a dodržování těchto opatření. Toto právo přitom působí jak vertikálně vůči státu, kterému zakládá povinnost přijmout konkrétní legislativu k zavedení těchto opatření, tak horizontálně vůči subjektům zpracovávajícím osobní údaje, kterým z něj plyne povinnost zákonem stanovená opatření dodržovat – tato povinnost pak samozřejmě stíhá

9 Srov. GELLERT, R. *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press, 2020, s. 18. Obdobně srov. MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita, 2020, s. 48.

10 Srov. KASL, F. Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, R. (ed.). *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 401.

11 Srov. ibidem.

12 Srov. MÍŠEK, J. *Moderní regulatorní metody ochrany osobních údajů*, s. 51.

13 Srov. ibidem.

14 Srov. GELLERT, R. *The Risk-Based Approach to Data Protection*, s. 18. s odkazem na BENNETT, C. J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992, s. 33.

15 Osobní údaje může samozřejmě zpracovávat i zpracovatel ve smyslu čl. 4 bod 8 GDRP. Pro účely tohoto článku je však toto zjednodušení možné bez újmy na obecnosti.

i složky státu. Na druhou stranu jej lze vnímat jako právo negativní, jež může jednotlivec uplatňovat proti těm, kteří příslušná opatření nezavedou či porušují.[16]

2. Přístupy k ochraně osobních údajů

Opatření směřující k prevenci zásahů do základních práv prostřednictvím zpracování osobních údajů lze realizovat různými způsoby. Podle jejich volby se liší různé koncepční přístupy k ochraně osobních údajů. Cílem této části článku je popsat dva možné přístupy – přístup založený na kontrole a přístup založený na důvěře – včetně jejich projevů v platné právní úpravě a diskutovat jejich vhodnost pro naplnění účelu ochrany osobních údajů v současné společnosti.

2.1 Přístup založený na kontrole

Jakkoli je ochrana osobních údajů samostatnou právní úpravou a právo na ochranu osobních údajů je samostatným základním právem odděleným od jiných základních práv, včetně práva na soukromí,[17] historické sepětí práva na ochranu soukromí a práva na ochranu osobních údajů je neoddiskutovatelné.

Jak uvádí Solove, ve Spojených státech amerických v 60. letech 20. století vedly rozšiřující se využití počítačů a množící se rejstříky a databáze federálních úřadů k rostoucím veřejným obavám o ochranu soukromí.[18] Reakcí na tyto obavy byla mimo jiné zpráva amerického Ministerstva zdravotnictví, školství a sociálního zabezpečení (*Department of Health, Education and Welfare*) z roku 1973, nazvaná Záznamy, počítače a občanská práva (*Records, Computers, and the Rights of Citizens*). Zpráva poukázala na to, že jednotlivec musí poskytovat informace o sobě relativně neuchopitelným institucím, přičemž často ani neví, jaká organizace o něm zpracovává informace, a nemůže ověřovat jejich přesnost, kontrolovat jejich šíření či zpochybňovat způsob jejich použití.

V této zprávě se také poprvé objevuje výčet následující zásad nazývaných Zásady férového nakládání s informacemi (*Fair Information Practices* nebo též *FIPs*, překlad autora):

- *Nesmí existovat žádné rejstříky s osobními údaji, jejichž samotná existence je tajná.*
- *Jednotlivec musí mít možnost zjistit, jaké informace jsou o něm vedeny a jak jsou používány.*
- *Jednotlivec musí mít možnost zabránit tomu, aby informace shromážděné o něm za jedním účelem byly použity nebo poskytnuty za jiným účelem bez jeho souhlasu.*
- *Jednotlivec musí mít možnost opravy záznamů o jeho osobě.*
- *Jakákoli organizace, která vytváří, udržuje, užívá nebo šíří záznamy obsahující údaje o identifikovatelných osobách, musí zajistit jejich spolehlivost pro zamýšlený účel a přijmout rozumná opatření k zabránění jejich zneužití.*[19]

---

16 Uplatnění připadá v úvahu přímo formou výkonu práv subjektu údajů podle čl. 15 až 22 GDPR, případně skrze stížnost k příslušnému dozorovému úřadu podle čl. 77 GDPR nebo soukromoprávní cestou na základě čl. 79 GDPR.

17 Srov. MÍŠEK, J. *Moderní regulatorní metody ochrany osobních údajů*, s. 55.

18 Srov. SOLOVE, D. J. A Brief History of Information Privacy Law. In: *SSRN Scholarly Paper* [online].ID 914271. Rochester, NY: Social Science Research Network, 2006, s. 24 [cit. 2022-01-04]. Dostupné z: <https://papers.ssrn.com/abstract= 914271>.

19 Srov. *Records, Computers, and the Rights of Citizens [online]*. Departnemt of Health, Education and Welfare. 1973 [cit. 2021-08-08], s. xx. Dostupné z: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.

Z jednotlivých zásad je patrný důraz na kontrolu jednotlivce[20] – zejména v požadavku na transparentnost (která je předpokladem kontroly – nemohu kontrolovat něco, o čem nevím) a v požadavku na souhlas jednotlivce v případě poskytnutí či použití informací za účelem jiným, než za kterým byly původně shromážděny.

Tento důraz na kontrolu má svůj původ právě v ochraně soukromí. Pravděpodobně nejstarší výslovně formulovanou koncepci práva na soukromí obsahuje hojně citovaný článek Samuela D. Warrena a Louise D. Brandeise nazvaný *Právo na soukromí* (*The Right to Privacy*), publikovaný v roce 1890. Autoři v tomto článku postulovali, že jednotlivci by na základě *common law* mělo být přiznáno právo na soukromí – slovy soudce Cooleyho právo „být ponechán sám sobě" (*„right to be let alone"*).[21] Jeho obsah pak konkrétně spatřují v *„právu jednotlivce rozhodovat o tom, v jakém rozsahu budou jeho myšlenky a pocity komunikovány jiným"*.[22]

Tento přístup k ochraně soukromí přitom neztratil svůj význam ani v moderní době. Obdobně hojně citovaná práce Alana Westina *Soukromí a svoboda* (*Privacy and Freedom*) vymezuje soukromí jako *„nárok jednotlivců, skupin nebo institucí na to, aby si sami určili, kdy, jak a v jakém rozsahu budou informace o nich sdělovány jiným"*.[23] Na Warrena a Brandeise myšlenkově navazuje také Adam D. Moore, který soukromí vymezuje prostřednictvím obsahu práva na soukromí, a to popisuje jako právo kontrolovat přístup k vlastní osobě a informacím o vlastní osobě.[24] Obdobně Roger Clark vymezuje soukromí jako *„zájem jednotlivců na zachování ‚osobního prostoru' bez zásahů ze strany jiných osob a organizací"*.[25] Clarkova definice vychází z Morisona, který soukromí popisuje jako stav jednotlivce, kdy není předmětem zásahů do jeho hluboce osobních zájmů (*intimate personal interests*).[26]

Historické sepětí ochrany osobních údajů s ochranou soukromí tak vedlo k promítnutí koncepčních prvků ochrany soukromí do základních principů ochrany osobních údajů. Jsou to totiž právě Zásady férového nakládání s informacemi, které významně ovlivnily řadu pozdějších právních úprav ochrany osobních údajů, vč. úpravy aktuálně platné na území Evropské unie v podobě GDPR.

Ze Zásad férového nakládání s informacemi například do značné míry vychází Směrnice OECD pro ochranu soukromí a přeshraniční toky osobních údajů (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, dále jen „Směrnice OECD") připravená na půdě Organizace pro ekonomickou spolupráci a rozvoj (OECD) v roce 1980, která formuluje osm principů ochrany soukromí. Přístup založený na kontrole se ve Směrnici OECD promítá šířeji než v původních Zásadách férového nakládání

---

20 Daniel Solove v této souvislosti pracuje s pojmem *privacy self-management*. Srov. SOLOVE, D. J. Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*. 2012, Vol. 126, s. 1880.

21 Srov. WARREN, S. D. – BRANDEIS, L. D. Right to privacy. *Harvard Law Review*. 1890, Vol. 4, č. 5, s. 195. Warren a Brandeis v tomto směru odkazují na dnes běžně nedostupnou publikaci *Cooley on Torts*. 2. vydání, s. 29. Polčák ke spojení *„right to be let alone"* nabízí přiléhavější překlad *„právo na to, aby nás ostatní nechali na pokoji"*. Srov. POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 328, poznámka po čarou č. 764.

22 Srov. WARREN, S. D. – BRANDEIS, L. D. *Right to privacy*, s. 198.

23 Srov. WESTIN, A. *Privacy and Freedom*. New York: Ig Publishing, 2018, s. 24.

24 Srov. MOORE, A. D. *Privacy rights: Moral and legal foundations*. Pennsylvania: Penn State Press, 2010, s. 16.

25 Srov. CLARKE, R. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* [online]. July 2016 [cit. 2021-08-03]. Dostupné z: <http://www.rogerclarke.com/DV/Intro.html#Priv>.

26 Srov. MORISON, W. L. *Report on the law of privacy*. Canberra: Government Printer, 1974, s. 1. Parliamentary paper, no. 85 of 1973.

s informacemi, současně Směrnice OECD lépe reflektuje některé nuance kontroly. Například hned první zásada omezení shromažďování požaduje, aby údaje byly získávány „s vědomím nebo souhlasem subjektu údajů“ pouze „ve vhodných případech“, tj. požadavek na kontrolu není paušální.

Směrnice OECD (a tedy zprostředkovaně i Zásady férového nakládání s informacemi) pak podstatně ovlivnily první komunitární úpravu ochrany osobních údajů v podobě směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice 95/46/ES“). Koncepce kontroly, mající původ v ochraně soukromí, tak byla dominantní koncepcí i v rámci této směrnice. Promítala se nejvýrazněji v jejím čl. 7 upravujícím právní základy pro zpracování osobních údajů. Dle tohoto článku směrnice měly členské státy Evropské unie zajistit, že zpracování osobních údajů bude provedeno pouze v případě, že je naplněn jeden z právních základů uvedených v tomto článku, přičemž na prvním místě je jako právní základ jmenován souhlas subjektu údajů. Jakkoli tedy souhlas nebyl jediným možným právním základem, byl na něj kladen značný důraz. Promítnutím koncepce kontroly byly v rámci směrnice dále například požadavek na zavedení povinnosti informovat subjekt údajů o zpracování osobních údajů dle čl. 10 nebo individuální práva subjektu údajů čl. 12 až 15, zejména právo na námitku proti zpracování osobních údajů.

Směrnici posléze nahradilo GDPR, které dále zvětšuje důraz na kontrolu ze strany jednotlivce. Tento záměr je explicitně deklarován v bodě 7 odůvodnění GDPR, který uvádí, že *„[f]yzické osoby by měly mít možnost kontrolovat své vlastní osobní údaje“*. Vedle převzetí veškerých výše jmenovaných prvků kontroly ze směrnice 95/46/ES doplňuje GDPR prvky další. V prvé řadě jsou to požadavky na kvalitu souhlasu subjektu údajů. Ty se promítají nejprve do definice souhlasu v čl. 4 bodě 11, který oproti směrnici 95/46/ES navíc požaduje, aby souhlas byl *„jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*. Dále je požadavkům na souhlas věnován celý nový čl. 7, který vyžaduje doložitelnost souhlasu a rozpracovává požadavky na jeho svobodnost a odvolatelnost.

Ještě markantnější je pak koncepce kontroly v již citovaném čl. 5 odst. 3 směrnice 2002/58/ES a jeho transpozici v § 89 odst. 3 z. el. kom. Ty povolují ukládání a čtení údajů z koncového zařízení uživatele služby elektronických komunikací pouze s jeho souhlasem, pokud tento úkon není technicky nezbytný[27] – žádný jiný způsob legitimizace není přípustný. Souhlas přitom nelze udělit např. prostřednictvím předem zaškrtnutého políčka[28] a musí být získán provozovatelem webové stránky před uložením či čtením údajů z koncového zařízení uživatele služby elektronických komunikací.[29]

---

27 Tj. nezbytný pro *„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“*.

28 Srov. rozsudek Soudního dvora Evropské unie ze dne 1. října 2019 ve věci C-673/17, *Planet49*, body 52 a 55.

29 Srov. rozsudek Soudního dvora Evropské unie ze dne 29. července 2019 ve věci C-40/17, *FashionID*, bod 102. Soud se zde sice specificky vyjadřuje k souhlasu podle směrnice 95/46/ES, nicméně čl. 2 písm. f) směrnice 2002/58/ES stanoví, že souhlas pro účely této směrnice odpovídá souhlasu subjektu údajů podle směrnice 95/46/ES. Závěry soudu jsou tedy plně aplikovatelné i na souhlas s uložením či čtením údajů z koncového zařízení uživatele služby elektronických komunikací podle směrnice 2002/58/ES.

2.2 Vhodnost přístupu založeného na kontrole

Při úvaze, zda je koncepce kontroly vhodná pro naplnění účelu ochrany osobních údajů, tedy ochrany základních práv před zásahy způsobenými zpracováním osobních údajů, je třeba si uvědomit, že Warren a Brandeis položili základ této koncepci v roce 1890. V této době bylo potenciálně možné uvažovat o tom, že bude jednotlivec rozhodovat o tom, v jakém rozsahu budou jeho myšlenky, pocity, respektive obecně osobní údaje týkající se jeho osoby komunikovány jiným.

Taková představa je však nereálná v 21. století, kdy počet i komplexnost informačních procesů, které by bylo třeba takto kontrolovat, narostl oproti konci 19. století exponenciálně. Naše schopnost činit rozhodnutí ohledně našich osobních údajů však exponenciálně nenarostla.[30] Slovy Woodrowa Hartzoga, kontrola není *„bezedná studna"*.[31]

Ačkoli je tedy možné vykonat kontrolu ve vztahu k jednotlivé webové stránce – prostudovat si poskytnuté informace o zpracování osobních údajů a následně učinit informované rozhodnutí ohledně udělení či neudělení souhlasu s použitím cookies a zpracováním osobních údajů pro určité účely – není to možné ve vztahu k desítkám webových stránek, které průměrný uživatel internetu během jednoho dne navštíví.

Například podle výzkumu z roku 2008 by průměrný Američan musel strávit v průměru 201 hodin tím, aby si rychle prošel všechny zásady ochrany soukromí, se kterými se za rok setká.[32] Je přitom velmi pravděpodobné, že dnes by toto číslo bylo výrazně větší s ohledem na empiricky pozorovatelné zvětšení rozsahu zásad ochrany soukromí, kterou přineslo mimo jiné přijetí GDPR, i větší množství a komplexnost služeb a webových stránek, se kterými se jednotlivec setkává. Nároky na čas a související kognitivní zátěž, kterou by měl člověk věnovat výkonu kontroly nad svými osobními údaji, jsou tedy obrovské. Rostoucí kognitivní zátěž přitom prokazatelně vede k rozhodnutím, jež mají horší dopady na ochranu osobních údajů.[33]

Vedle nároků na čas a kognitivní zátěže čelí subjekt údajů také informační asymetrii. Disponuje totiž zpravidla pouze omezenými informacemi o tom, jak budou jeho osobní údaje zpracovány. Podrobnosti o informačním sytému použitému k tomuto zpracování mu však zpravidla zůstávají z logických důvodů skryty, protože jsou pro správce často konkurenčně významné, popřípadě by zpřístupnění těchto informací mohlo vytvářet riziko pro bezpečnost osobních údajů v daném systému.

Dále je kontrola prostřednictvím nástrojů, jako jsou souhlasy s použitím cookies, založena na předpokladu, že lidé budou o předložené volbě rozhodovat racionálně. Tento předpoklad však neodpovídá skutečnosti. Pokud se člověk rozhoduje o možnostech, které jsou v čase velmi nejisté (jako právě například dlouhodobé důsledky jednotlivého zpřístupnění osobních údajů), má nedostatek informací a obecně nedostatek mentálních zdrojů, a jeho rozhodování pak není plně racionální.

---

30 Srov. SOLOVE, D. J. The myth of the privacy paradox. *George Washington Law Review*. 2021, Vol. 89, s. 37.

31 Srov. HARTZOG, W. *Privacy's blueprint*. Cambridge, Massachusetts: Harvard University Press, 2018, s. 63.

32 Srov. MCDONALD, A. M. – CRANOR, L. F. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*. 2008, Vol. 4, s. 565.

33 Srov. HARRISON, P. *Exacerbating the privacy paradox: Investigating cognitive load's impact on disclosure* [online]. Victoria University of Wellington, 2020, s. 79 [cit. 2022-01-03]. Dostupné z: <http://researcharchive.vuw.ac.nz/handle/10063/9166>.

Na místo toho využívají lidé tzv. heuristiky neboli zkratky v rozhodování. Za heuristiku lze například považovat přeceňování pravděpodobnosti jevů, které člověk pozoruje ve svém okolí (oproti těm, se kterými se nesetkal). To může vést k podcenění negativních dopadů na ochranu osobních údajů, protože tyto negativní dopady nejsou v populaci časté a jsou obtížně pozorovatelné. Způsob rozhodování s využitím heuristik se označuje pojmem *„omezená racionalita"*.[34]

Vedle heuristik pak jednotlivce v racionálním rozhodování omezují kognitivní a behaviorální zkreslení. Tato zkreslení se jako systematické chyby v úsudku či jednání uplatňují na veškerá rozhodnutí bez ohledu na jejich komplexnost, a to na rozdíl od heuristik.[35] Příkladem chyby úsudku je hyperbolické diskontování, kdy jednotlivec například podceňuje dlouhodobé negativní důsledky určitého jednání ve světle jeho okamžitých přínosů.[36]

Vedle omezené racionality a zkreslení je rozhodování v rámci výkonu kontroly ovlivněno uživatelským rozhraním, ve kterém jednotlivec kontrolu vykonává. Toto ovlivnění se zpravidla označuje jako postrkování (*„nudging"*).[37] K postrkování uživatelů určitého rozhraní může ze strany jeho tvůrce docházet vědomě i nevědomky. Postrkování může být použito jako manipulativní technika k ovlivnění uživatele směrem k rozhodnutí s negativním dopadem na ochranu jeho osobních údajů,[38] ale také jako nástroj ke zmírnění výše popsaných problémů výkonu kontroly.[39]

Negativní důsledky chybných rozhodnutí ohledně ochrany osobních údajů (ať už vlivem kognitivních a behaviorálních zkreslení nebo ovlivňování) přitom nelze podceňovat. Chybné rozhodnutí ohledně ukládání a čtení cookies (tedy takovém rozhodnutí, které je svými důsledky v rozporu se skutečnými preferencemi jednotlivce ohledně nakládání s jeho osobními údaji) může vést k předání osobních údajů jednotlivce například společnosti, která pomocí nich vytvoří či doplní již existující profil jednotlivce a použije jej pro zobrazení cílené manipulativní reklamy (např. s politickým obsahem) tomuto jednotlivci.[40] Takové negativní důsledky nemusí být pro jednotlivce vůbec patrné, protože jednotlivec nemusí zaznamenat, že zobrazená reklama je manipulativní, a má minimální šanci zjistit, jak byly získány údaje použité pro manipulaci.

Pokud by přesto jednotlivec své chybné rozhodnutí odhalil, možnost odstranění jeho důsledků (byť pouze *pro futuro*, nikoli zpětně), je minimální – je sice možné smazat příslušnou cookie z internetového prohlížeče, vysledovat tok údajů získaných pomocí takové cookie skrze ekosystém internetové reklamy a zamezit jejich dalšímu zpracování je v podstatě nemožné. Ekosystém internetové reklamy je v současnosti natolik komplexní a současně málo transparentní, že sledování toku údajů „z vnějšku" není možné, přičemž „uvnitř" tohoto ekosystému zatím nejsou nastaveny příslušné korekční mechanismy.[41]

---

34 Srov. ACQUISTI, A. et al. Nudges for Privacy and Security: Understanding and Assisting Users Choices Online. *ACM Computing Surveys* [online]. 2017, Vol., No. 3, s. 5. Dostupné z: <https://doi.org/10.1145/3054926>.

35 Srov. ibidem, s. 6.

36 Srov. ibidem, s. 8.

37 Srov. ibidem, s. 10.

38 Srov. ibidem, s. 25.

39 Srov. ibidem, s. 10.

40 Takový postup byl cílem aktérů ve známém případu Cambridge Analytica. Srov. *Letter from the Information Commissioner to Julian Knight MP*. Information Commissioner's Office [online]. 2. října 2020 [cit. 2021-08-08]. Dostupné z: <https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf>.

Výše popsané problémy komplexnosti rozhodnutí, omezené racionality a ovlivňování vedou k tomu, že lidé málokdy vykonávají kontrolu nad svými osobními údaji v případě, že je jim možnost jejího výkonu nabídnuta, a pokud ji vykonají, jejich jednání často neodpovídá obecně projevovaným preferencím ohledně ochrany osobních údajů (respektive specificky ochrany soukromí). Tento fenomén se označuje jako paradox ochrany soukromí (*privacy paradox*).[42]

Problém ilustrují aktuální data Českého statistického úřadu za rok 2021. Podle respondentů průzkumu o využívání informačních a komunikačních technologií *„[z]aznamenávání, co lidé vyhledávají a dělají na internetu, znepokojuje alespoň mírně 72 % jeho uživatelů, 23 % uživatelů dokonce uvedlo, že je to znepokojuje velmi“*. Současně však *„[k] omezení množství nebo změně nastavení cookies přistoupilo ve sledovaném roce 27 % uživatelů internetu“*.[43]

Jak však uvádí Solove, tento rozdíl hodnot není nutné vnímat jako paradox či rozpor mezi vyjádřenou preferencí a skutečným chováním. Jeho příčinou s největší pravděpodobností do značné míry jsou popsané kognitivní a behaviorální problémy spojené s realizací kontroly, které vedou k frustraci uživatelů a následné rezignaci či cynickému přístupu.[44] Tento rozdíl je tak spíše argumentem podporujícím závěr, že přístup založený na kontrole by neměl být dominantním přístupem k ochraně osobních údajů.

Výše popsané argumenty však nesměřují k závěru, že koncepce kontroly nemá v ochraně osobních údajů své místo. Uplatnit se může a má tam, kde je kontrolující osoba schopna obsáhnout potřebné informace a učinit na základě nich smysluplné rozhodnutí. Příkladem správně aplikovaného principu kontroly (v jiné oblasti, než je právní úprava cookies) je dle mého názoru čl. 13 odst. 2 směrnice 2002/58/ES, který je v našem právním řádu transponován do § 7 odst. 3 zákona č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů (dále jen „z. sl. inf. spol.“).

Čl. 13 odst. 1 směrnice 2002/58/ES a § 7 odst. 2 z. sl. inf. spol. stanoví, že obchodní sdělení lze na elektronický kontakt určité osoby (typicky e-mailovou adresu či telefonní číslo) zasílat pouze s jejím souhlasem. Čl. 13 odst. 2 směrnice 2002/58/ES a § 7 odst. 3 z. sl. inf. spol. však stanoví z tohoto pravidla výjimku pro případ, kdy je kontakt oprávněně získán v souvislosti s prodejem výrobku nebo služby. V takovém případě stačí dané osobě nabídnout jednoduchou možnost zasílání obchodních sdělení odmítnout v okamžiku sběru

---

41 Srov. např. *Update report into adtech and real time bidding*. Information Commissioner's Office [online]. 20. června 2019 [cit. 2022-02-05]. Dostupné z: <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>.

42 Pojem byl poprvé použit v roce 2007 (srov. NORBERG, P. A. – HORNE, D. R. – HORNE, D. A. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*. 2007, Vol. 41, No. 1, s. 100), samotný problém však byl pozorován již o několik let dříve. Srov. SOLOVE, D. J. The myth of the privacy paradox. *George Washington Law Review*. 2021, Vol. 89, s. 5. V českém prostředí na tento problém v obecné rovině poukazuje např. Radim Polčák. Srov. POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 333.

43 Srov. *Využívání informačních a komunikačních technologií v domácnostech a mezi osobami za období 2021* [online]. Praha.: Český statistický úřad. Listopad 2021, s. 118. Dostupné z: <https://www.czso.cz/documents/10180/142872020/06200421.pdf/c4028fae-5d47-4b27-999e-14dc55064d9c?version=1.3>.

44 SOLOVE, D. J. *The Myth of the Privacy Paradox*, s. 37. Někteří autoři dokonce hovoří o cynismu ochrany soukromí jako pojmu. Srov. HOFFMANN, C. P. – LUTZ, Ch. – RANZINI, G. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*. 2016, Vol. 10, No. 4. Obdobně srov. RICHARDS, N. M. – HARTZOG, W. Taking Trust Seriously in Privacy Law. *SSRN Electronic Journal* [online]. 2016, s. 446 [cit. 2021-01-30]. Dostupné z: <http://www.ssrn.com/abstract=2655719>.

údajů. Pokud této možnosti nevyužije, je možné na získané kontakty zasílat obchodní sdělení týkající se vlastních obdobných výrobků nebo služeb toho, kdo kontakt tímto způsobem získal. Jednoduchá možnost odmítnout další sdělení pak musí být rovněž poskytnuta v každém zaslaném sdělení.

Prakticky se toto pravidlo projevuje například při nákupu v internetovém obchodě, kdy uživateli obchodník v průběhu objednávkového procesu může zobrazit předvyplněné pole s textací například „Chci dostávat informace o slevách a akcích na e-mail a telefon". Vyplnění (zaškrtnutí) tohoto pole má uživatel možnost zrušit. Pokud tak uživatel neučiní, obchodník mu může zasílat e-mailem či pomocí SMS nabídky svého souvisejícího zboží a služeb.

Takový typ volby je smysluplný, protože část nakupujících může skutečně mít zájem o nabídky od daného obchodníka a část nikoli. Současně bude taková volba zpravidla v mezích mentální kapacity uživatele, protože nevyžaduje složité uvážení relativně abstraktních a dlouhodobých důsledků sdílení osobních údajů s relativně neurčitými či uživateli zcela neznámými subjekty, ani studium rozsáhlých a podrobných informací, jaké zpravidla uvnitř sebe skrývají nástroje pro sběr souhlasu s cookies. Uživatel musí pouze zvážit, zda si přeje dostávat nabídky příslušného obchodníka do své e-mailové schránky či jiným obdobným kanálem, přičemž totožnost obchodníka (respektive alespoň jeho obchodní označení) a charakter nabídek bývají v této souvislosti obvykle zřejmé.

Současně když uživatel vlivem omezené racionality, ovlivňování nebo z jiného důvodu přesto dospěje k chybnému rozhodnutí (neodmítne zasílání obchodních sdělení, která nakonec shledá jako nežádoucí), může svou chybu snadno napravit bez trvalé újmy – požadavkem čl. 13 odst. 2 a 4 směrnice 2002/58/ES a § 7 odst. 3 a 4 ZSIS je možnost odmítnutí dalšího zasílání obchodních sdělení v každé zaslané zprávě. Negativní důsledky chybného rozhodnutí jsou tak výrazně mírnější než ve výše popsaném případě chybného rozhodnutí ohledně souhlasu s ukládáním a čtením cookies.

Výše předloženou diskusi lze tedy shrnout tak, že princip kontroly by neměl být dominantním principem právní úpravy ochrany osobních údajů (zejména by se neměl uplatňovat v oblasti ukládání a čtení údajů z koncového zařízení uživatele služby elektronických komunikací), má v ní však své místo v jiných oblastech a nebylo by vhodné jej zcela opustit.

2.3 Přístup založený na důvěře

Daniel Solove v rámci své kritiky ochrany soukromí, respektive osobních údajů založené na kontrole předkládá návrh, aby se tato ochrana namísto kontroly zaměřila na *„architekturu ekonomiky osobních údajů – shromažďování, používání, uchovávání a předávání údajů"*.[45] Pro tento přístup nepředkládá žádný konkrétní název ani bližší vymezení, pouze vyjmenovává příklady nástrojů ochrany. Jsou jimi smluvní ochrana v rámci předávání údajů, omezení či úplný zákaz některých typů předávání, řízení ochrany soukromí, respektive osobních údajů v organizaci (včetně role pověřence pro ochranu osobních údajů) a zahrnutí ochrany soukromí, respektive osobních údajů do procesů návrhu produktů a služeb.

45 Srov. SOLOVE, D. J. *The myth of the privacy paradox*, s. 40.

Tyto myšlenky přitom nejsou svou podstatou nové či průlomové. Podobný přístup k ochraně osobních údajů je ve svém zárodku patrný již ze Zásad férového zpracování informací, které mj. stanoví povinnost zajistit spolehlivost údajů pro zamýšlený účel a přijmout rozumná opatření k zabránění jejich zneužití. Tyto povinnosti přijmout preventivní opatření zohledňují skutečnost, že správce získává vůči subjektu údajů do určité míry dominantní postavení – vzniká asymetrie, na kterou upozorňuje již zmíněný von Lewinski.[46]

Regulace silnější strany právního vztahu obecně pak není pro právo žádnou novinkou. V českém, respektive evropském právu se dominantně projevuje např. v právu spotřebitelském. V systému *common law* se pak projevuje např. v úpravě tzv. fiduciárních vztahů (*law of fiduciaries*), jejímž cílem je ochrana před zneužitím zranitelnosti vzniklé důvěrou v jiného. V systému *common law* se tento institut aplikuje např. na vztah lékaře a pacienta či advokáta a jeho klienta.[47] Obdobu této regulace fiduciárních vztahů přinesl do českého práva zákon č. 89/2012 Sb., občanský zákoník, zavedením institutu svěřenského správce, respektive správce cizího majetku obecně.[48]

Ve fiduciárních vztazích hledají pro oblast ochrany osobních údajů inspiraci Neil Richards a Woodrow Hartzog. Obdobně jako Solove formulují své návrhy pro oblast ochrany soukromí. Tato skutečnost je však dána tím, že je formulují především v kontextu právního řádu Spojených států amerických, který komplexní právní úpravu ochrany osobních údajů neobsahuje a ochrana základních práv před zásahy skrze zpracování osobních údajů je realizována především aplikací práva na soukromí. Jak je však z jejich textu patrno, třída řešených problémů by (s ohledem na svou šíři) v evropském právu spadala do působnosti právní regulace ochrany osobních údajů. Jejich přístup proto lze aplikovat i na ochranu osobních údajů. Tento závěr podporuje i to, že je jejich koncepce vystavěna na pozměněné podobě Zásad férového zpracování informací, které rovněž řeší problémy z třídy ochrany osobních údajů, nikoli pouze ochrany soukromí.[49]

Fiduciář, jakožto povinná osoba z fiduciárního vztahu, má v systému *common law* dvě základní povinnosti, a to povinnost péče a povinnost loajality. Povinnost péče zahrnuje především řádný výkon činnosti, kterou je konkrétně vůči oprávněnému z daného vztahu povinován (tedy např. v případě lékaře poskytnutí zdravotní služby postupem *de lege artis*). Pokud oprávněný v souvislosti s realizací dané činnosti svěřuje fiduciáři důvěrné informace, plyne z povinnosti péče též povinnost mlčenlivosti. Druhá povinnost, povinnost loajality pak znamená, že fiduciář nesmí zneužít svého dominantního postavení vůči oprávněnému k tomu, aby jednal na jeho úkor (třeba aby se na jeho úkor obohatil nebo ho jinak poškodil). Tím přitom není vyloučeno, aby činnost fiduciáře byla odměňována. Celkově je cílem těchto povinností zabránit tomu, aby fiduciář zradil důvěru, kterou do něj vkládá oprávněný.[50] Z důvodu ochrany důvěry nazývám tento přístup k ochraně osobních údajů v dalším výkladu jako přístup založený na důvěře.

---

46 Srov. VON LEWINSKI, K. *Geschichte des Datenschutzrechts von 1600 bis 1977*, s. 200.

47 Srov. RICHARDS, N. M. – HARTZOG, W. *Taking Trust Seriously in Privacy Law*, s. 457.

48 Srov. část třetí, hlava II, díl 6 citovaného zákona.

49 Srov. RICHARDS, N. M. – HARTZOG, W. *Taking Trust Seriously in Privacy Law*, s. 458 an. Samotná myšlenka přenesení poznatků z oblasti fiduciárních vztahů do oblasti ochrany soukromí byla poprvé formulována Jackem Balkinem. Srov. BALKIN, J. M. Information fiduciaries and the first amendment. *UC Davis Law Review*. 2015, Vol. 49, No. 4; *Balkinization* [online]. [cit. 2022-01-03]. Získáno z: <https://balkin.blogspot.com/search?updated-max=2021-12-11T15:13:00-05:00>.

50 Srov. BALKIN, J. M. *Information fiduciaries and the first amendment*, s. 1207.

Na základě inspirace z těchto povinností Richards a Hartzog navrhují přeformulovat Zásady férového nakládání s informacemi tak, že namísto zásad důvěrnosti, transparentnosti a bezpečnosti by upravovaly diskrétnost, upřímnost, ochranu a loajalitu (jako novou zásadu). Diskrétnost vymezují jako širší koncept než důvěrnost, spočívající v chování či komunikaci takovým způsobem, že nedojde k odhalení soukromých informací. Nejstriktnější forma diskrétnosti je důvěrnost, kdy informace nejsou vůbec sdíleny. Diskrétnost však umožňuje odlišit jemnější nuance, kdy ten, kdo určitou informaci sdílí, předpokládá, že bude šířena, avšak v rámci určitého okruhu osob, například blízkých přátel. Prakticky tak diskrétnost spočívá v omezení, jaké informace budou sdíleny, s kým a jak, a chrání před škodlivým či nežádoucím sdílením informací. Oproti plné důvěrnosti poskytuje větší flexibilitu při zachování důvěry ze strany osoby, jíž se informace týkají.[51]

Upřímnost je pak v pojetí Richardse a Hartzoga nástavbou transparentnosti. Princip transparentnosti obsažený v Zásadách férového nakládání s informacemi a jeho promítnutí v konkrétních povinnostech pouze vyžaduje, aby ten, kdo zpracovává osobní údaje, zpřístupnil informace o svých postupech. Nehraje přitom roli, jestli si je ten, jehož údajů se mají postupy týkat, skutečně přečte a jestli skutečně chápe podstatné aspekty těchto postupů. Upřímnost by měla tento nedostatek překonávat aktivní povinností vyjasňovat možné omyly a mylné dojmy a zdůraznit podstatné informace, které mohou být zdrojem rizika pro toho, jehož se příslušné postupy týkají. Cílem upřímnosti by tedy nemělo být větší množství poskytovaných informací, ale jejich větší kvalita.[52]

Ochrana pak má být rozšířením bezpečnosti. Zahrnovat by měla postupy jako pravidelné audity úložišť osobních údajů a kontinuální posuzování rizik na základě aktualizovaných modelů hrozeb, minimalizace rozsahu zpracovávaných údajů a doby jejich uložení nebo příprava plánů pro případ bezpečnostního incidentu. Ochrana má překryv s diskrétností v oblasti sdílení anonymizovaných dat – právě důsledná anonymizace je jedním z prvků ochrany, nikoli však jediným. V kontextu rostoucích rizik zpětné identifikace díky sofistikovanějším algoritmickým metodám i neustále se zvětšujícímu dostupnému výpočetnímu výkonu by v rámci ochrany měla být zvažována také další opatření, jako např. smluvní závazky zakazující provedení zpětné identifikace.[53]

Zcela novou zásadou by pak měla být loajalita, která nejvíce vychází z práva fiduciárních vztahů. Loajalita by v kontextu práva na soukromí a osobních údajů měla znamenat povinnost toho, komu byly svěřeny osobní údaje, nepoužívat je ve svůj prospěch na úkor osoby, které se osobní údaje týkají. Tím není myšleno, že by ten, komu byly informace svěřeny, je nemohl ve svůj prospěch využívat vůbec. Například vytěžování údajů pro zlepšení služby, poskytování anonymizovaných dat pro výzkum, sdílení dat s těmi, kteří jsou připraveni respektovat stejné zásady jejich ochrany, nebo jejich použití pro cílení reklamy nemusí být porušením loajality. Tyto aktivity jsou však v mezích loajality pouze do jisté míry, protože použití informací k újmě toho, koho se týkají, je snadné. Například použití dat pro manipulaci cen v rámci zobrazovaných nabídek nebo zobrazování obsahu, který cíleně manipuluje s pocity či postoji uživatele, by již představovalo porušení loajality.[54]

---

51 Srov. RICHARDS, N. M. – HARTZOG, W. *Taking Trust Seriously in Privacy Law*, s. 458 an.

52 Srov. ibidem, s. 462 an.

53 Srov. ibidem, s. 467.

54 Srov. ibidem, s. 468.

Je přitom třeba vnímat, že v právním prostředí Spojených států amerických má přístup k ochraně soukromí, respektive ochrany osobních údajů na základě fiduciárních povinností specifický význam, protože otevírá cestu zákonodárci, respektive soudům vytvořit rámec pro obecnou ochranu osobních údajů v případě splnění znaků fiduciárního vztahu. Toto řešení by ve Spojených státech mohlo pomoci překonat dosud roztříštěnou ochranu tvořenou mozaikou sektorových zákonů, zákonů jednotlivých států a obecné ochrany pomocí definovaných civilních deliktů v oblasti ochrany soukromí (*privacy torts*). V Evropské unii však nedostatkem fundamentálního zakotvení práva na ochranu osobních údajů netrpíme, koncepce je pro nás proto zajímavá primárně po výše popsané obsahové stránce.

S ohledem na systematickou úpravu ochrany osobních údajů pro nás také jednotlivé povinnosti inspirované fiduciárními vztahy nejsou neznámé. Pokud budeme sledovat strukturu povinností fiduciáře, jak ji předkládají Richardse a Hartzog, projev diskrétnosti můžeme spatřovat v bodu 26 odůvodnění GDPR, dle kterého by se (v kontextu anonymizace) při určování, zda je fyzická osoba identifikovatelná, *„mělo přihlédnout ke všem prostředkům, jako je například výběr vyčleněním, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby“*. Prakticky toto ustanovení ukládá tomu, kdo chce určité údaje šířit mimo režim GDPR jako anonymní (tedy nikoli jako osobní údaje), aby zvážil, zda je schopen dostatečně zdůvodnit, že určitá osoba, jíž se původně údaje týkaly, není identifikovatelná. V takovém případě přitom musí být zváženy i případné nástroje a postupy zpětné identifikace, bude-li v daném případně možné jejich použití rozumně předpokládat.

Projev principu upřímnosti lze najít v čl. 12 GDPR, dle kterého mají být informace o zpracování osobních údajů poskytovány *„srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků“*. Akcentováno je tedy nejen prosté poskytnutí informací, ale také kvalita informování, a to tak, aby byl naplněn cíl skutečného zvýšení informovanosti jednotlivce, jehož údaje jsou zpracovávány.

Princip ochrany se v GDPR projevuje v obecné rovině v zásadě odpovědnosti správce dle čl. 5 odst. 1. Podle této zásady správce osobních údajů odpovídá za dodržení ostatních zásad dle čl. 45 odst. 1 GDPR a musí být schopen jejich dodržování doložit. Dále se projevuje zejména v čl. 24 a 25. Podle čl. 25 by správce osobních údajů měl zavést *„vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením“*, přičemž *„[t]ato opatření musí být podle potřeby revidována a aktualizována“*. Pokud je to vhodné, měl by opatření zavést pomocí politik ochrany osobních údajů. Čl. 26 pak požaduje *„vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět účinným způsobem zásady ochrany údajů, jako je minimalizace údajů, a začlenit do zpracování nezbytné záruky“*, přičemž tato opatření mají být zavedena již v době určení prostředků pro zpracování (záměrná ochrana osobních údajů – *data protection by design*). Rovněž požaduje *„vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné“*, a to z hlediska *„množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti“*.

Projevem principu loajality je zásada omezení účelem dle čl. 5 odst. 1 písm. b) GDPR, dle které nelze osobní údaje bez dalšího použít pro jiný účel, než pro který byly původně shromážděny, přičemž veškeré účely zpracování musí být výslovně určené a legitimní. Tato zásada otevírá prostor pro aplikaci na případy, kdy by zpracování osobních údajů

bylo v rozporu s povinností loajality, jak ji formulují Richards a Hartzog. V takových případech by bylo možné dovozovat, že zpracování osobních údajů není legitimní, přestože lze pro něj najít právní titul ve smyslu čl. 6 GDPR (například přesto, že k němu dotčený jednotlivec udělil souhlas). Nedostatek legitimity by mohl spočívat právě ve skutečnosti, že zpracování se děje na úkor dotčeného jednotlivce (např. z důvodu jeho diskriminace, manipulace, zásahu do soukromí či jiného základního práva).

Konkrétní odraz zásady loajality pak lze nalézt v právní úpravě oprávněného zájmu jako právního základu pro zpracování osobních údajů dle čl. 6 odst. 1 písm. f). Dle tohoto ustanovení je zpracování osobních údajů přípustné, pokud *„je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů“*. Správce osobních údajů tedy musí v každém případě zvažovat, zda konkrétní zpracování v jeho prospěch nepůsobí nepřiměřenou újmu subjektu údajů.

Nakonec je třeba konstatovat, že prvky přístupu založeného na důvěře naopak nelze identifikovat v právní úpravě ukládání a přístupu k údajům v koncových zařízeních uživatelů služeb elektronických komunikací. Jak čl. 5 odst. 3 směrnice 2002/58/ES, tak § 89 odst. 3 z. el. kom. uplatňují v této oblasti ochrany osobních údajů pouze přístup založený na kontrole.

2.4 Vhodnost přístupu založeného na důvěře

Vhodnost přístupu chránícího důvěru subjektu údajů ve správce jako přístupu k zajištění ochrany osobních údajů je dána tím, že překonává řadu nedostatků přístupu založeného na kontrole, jež jsem výše vytknul. Především se přístup založený na důvěře žádným způsobem neopírá o znalosti či schopnosti subjektu údajů. Tím překonává problém omezených časových a mentálních zdrojů při výkonu kontroly. Zatímco subjekt údajů může efektivně kontrolovat pouze omezený okruh webových stránek, aplikací a správců, počet těch, kterým může důvěřovat a které mohou jeho důvěru zachovat, je neomezený. Současně zachování důvěry ze strany správce není limitováno případnými kognitivními omezeními na straně dotčeného jednotlivce, protože jeho kognice není předpokladem či prvkem ochrany.

Za nedostatek přístupu založeného na důvěře lze zdánlivě považovat menší odolnost vůči nekalému jednání správců – jestliže subjekt údajů nemůže zpracování kontrolovat, musí se spoléhat, že správce nezradí jeho důvěru. Domnívám se však, že tento nedostatek není větší než v případě přístupu založeného na kontrole. Ani v případě aplikace přístupu založeného na kontrole nemá jednotlivec přímý vliv na probíhající zpracování (neovlivňuje např. technicky, jaké cookies webová stránka do jeho prohlížeče uloží), ale pouze spoléhá na to, že jeho projevené preference budou respektovány. Tento předpoklad však nemusí být naplněn a toto riziko je přinejmenším stejně velké jako riziko, že stejný subjekt poruší důvěru v něj vloženou jednotlivcem v případě, kdy žádná kontrola nebyla vykonána.

Dále je třeba připustit, že přístup založený na důvěře je ve vztahu k subjektu údajů do jisté míry paternalistický. Zpracování, při kterém by byly naplněny povinnosti spojené s postavením fiduciáře, by podle tohoto přístupu bylo právně přípustné i přes případnou nelibost dotčených jednotlivců. Bylo by tedy přípustné i v případech, kdy by jednotlivec jinak byl takové zpracování odmítl, pokud by měl možnost nad ním vykonat kontrolu.

Tento nedostatek přístupu založeného na důvěře je možné kompenzovat vhodnou kombinací s přístupem založeným na kontrole. Jak jsem již uvedl v části 2.2, přístup založený na kontrole má podle mě v ochraně osobních údajů stále své místo, byť by neměl být přístupem dominantním. Uplatnit se může tam, kde je možné o osobních údajích skutečně a smysluplně rozhodovat, a obecně v podobě práv subjektu údajů podle kapitoly III GDPR.

Přístup založený na důvěře je tak dle mého názoru způsobilý být dominantní koncepcí ochrany osobních údajů, neměl by však být přístupem jediným a je třeba jej doplnit zejména o prvky kontroly jednotlivce.

3. Návrhy de lege ferenda

Na základě výše předložené diskuse se domnívám, že probíhající reforma právní úpravy ochrany soukromí v elektronických komunikacích by se v rovině ukládání a čtení údajů ze zařízení koncových uživatelů měla zaměřit právě na upozadění přístupu založeného na kontrole a upřednostnění přístupu založeného na důvěře. To by v praxi znamenalo především ústup od obecného požadavku na získání souhlasu s ukládáním a čtením údajů ze zařízení koncového uživatele dle čl. 5 odst. 3 směrnice 2002/58/ES a § 89 odst. 3 z. el. kom.

Takový návrh logicky vyvolává otázku, čím zaplnit právní vakuum vzniklé případným vypuštěním požadavku na souhlas. Domnívám se, že řešením může být silnější vazba na stávající obecnou právní úpravu ochrany osobních údajů, která již implementuje ve velké míře přístup založený na důvěře. Pomocí stávající úpravy ochrany osobních údajů lze tuto ochranu zajistit v případech, kdy kontrola není možná. Pokud by tedy přístup ke koncovým zařízením a údajům v nich uloženým podléhal obecným povinnostem podle GDPR, zejména povinnosti dodržovat základní zásady dle čl. 5, mít pro danou činnost legitimizaci v podobě právního titulu podle čl. 6, zajištění odpovědnosti podle čl. 5 odst. 2 a čl. 25 a bezpečnosti podle čl. 32, pak by bylo možné kontrolu nahradit mechanismy chránícími důvěru koncových uživatelů.[55]

Ve zbývajícím rozsahu je podle mého názoru možné zásady diskrétnosti, ochrany, upřímnosti a loajality prosazovat vhodnou interpretací právě obecné právní úpravy ochrany osobních údajů v podobě GDPR. Kontrolu je možné dále upozadit vhodným výkladem čl. 6 odst. 1 písm. f) GDPR, který by rozšířil okruh případů, na které by (konkrétně např. v oblasti sběru údajů pomocí cookies) bylo možné aplikovat právní titul oprávněného zájmu. Tento výklad by však měl jít v ruku v ruce s vymezením podmínek a omezení, za kterých se tímto způsobem lze na oprávněný zájem spolehnout.

Zásadu transparentnosti je možné promítnout do výkladu čl. 13 a 14 GDPR, který by akcentoval zejména poskytování smysluplných informací o rizicích spojených s příslušným nakládáním s osobními údaji, které vznikají pro jednotlivce. Zásady diskrétnosti, ochrany a loajality by pak bylo možné prosadit zejména uplatněním požadavku na legitimitu účelu dle čl. 5 odst. 1 písm. b) GDPR a odpovědnost podle čl. 5 odst. 2, ze kterých

[55] Tento návrh samozřejmě vyvolává otázku, jak si poradit se skutečností, že ne každé čtení a ukládání údajů do zařízení koncového uživatele je spojeno se zpracováním osobních údajů, a tedy působnost směrnice 2002/58/ES je v tomto ohledu širší než působnost GDPR. Diskuse aplikace směrnice 2002/58/ES na jiné oblasti, než je nakládání s osobními údaji, však přesahuje záběr tohoto článku.

lze podle mě dovozovat požadavky na okruh subjektů, kterým lze údaje získané pomocí cookies předávat – například, že tyto údaje mohou být předávány jen prověřeným partnerům, na základě jasných smluvních závazků jejich ochrany a pouze v podobě, která dostatečně brání zneužití údajů k újmě konkrétního jednotlivce (díky nastavení rozsahu údajů a jejich pseudonymizaci). Tato sada odvozených požadavků by měla bránit tomu, že předané údaje budou jednoduše zneužitelné k újmě jednotlivce např. v důsledku předání citlivých informací širokému okruhu třetích stran, jejich použití diskriminujícími postupy nebo použití pro zobrazení manipulativní reklamy.

Cestou k tomuto výkladu mohou podle mého názoru být pokyny Evropského sboru pro ochranu osobních údajů jakožto orgánu sdružujícího všechny dozorové úřady pro ochranu osobních údajů v Evropské unii.[56] Ačkoli GDPR obsahuje nástroje jako kodexy chování a certifikace,[57] bylo by podle mě příliš optimistické očekávat, že subjekty na trhu v této oblasti samy zásadně změní svůj dosavadní přístup k nakládání s osobními údaji získanými z cookies a vypracují např. kodexy chování, které budou reflektovat přístup založený na důvěře.

Proto se domnívám, že prvotní impulz v této oblasti bude muset vyjít právě od dozorových úřadů. Pokyny Evropského sboru pro ochranu osobních údajů se pak jeví být pro tento účel vhodným nástrojem s ohledem na to, že nejsou bezprostředně právně závazné a díky tomu je možné je flexibilně přijímat, doplňovat a měnit. Kodexy chování a certifikace pak mohou následně základní požadavky vyjádřené v pokynech Evropského sboru pro ochranu osobních údajů dále rozpracovávat do konkrétních praktických postupů včetně technických protokolů.

Závěr

Ochranu osobních údajů lze vnímat jako soubor opatření směřujících k prevenci zásahů do základních práv, respektive jimi chráněných hodnot prostřednictvím operací s údaji, které se týkají fyzických osob, jež lze přímo či nepřímo identifikovat.

V předchozím výkladu jsem představil základní koncepční přístupy k ochraně osobních údajů – přístup založený na kontrole a přístup založený na důvěře. Ukázal jsem, že přístup založený na kontrole se silně projevuje v platné právní úpravě ochraně osobních údajů, a to z důvodu jejího historického sepětí s právní ochranou soukromí. V oblasti ochrany soukromí a osobních údajů v elektronických komunikacích pak tento přístup zcela dominuje a jeho důsledkem jsou souhlasy s ukládáním a čtením cookies, se kterými se nyní na internetu často setkáváme.

Diskusí těchto dvou přístupů jsem dospěl k závěru, že přístup založený na kontrole není vhodný jako dominantní přístup pro zajištění ochrany osobních údajů v současné společnosti, a to s ohledem na rozsah a mnohost informačních procesů, které by měly být předmětem takové kontroly. Jednotlivec čelí informační asymetrii a disponuje omezenými časovými a mentálními zdroji. Tváří v tvář velkému počtu složitých rozhodnutí o svých osobních údajích uplatňuje mentální zkratky, projevují se obecná mentální zkreslení a je snadným terčem manipulace v podobě postrkování k určitému rozhodnutí.

56 Srov. kapitolu VII, oddíl 3 GDPR.
57 Srov. kapitolu IV, oddíl 5 GDPR.

Důsledkem je tzv. paradox ochrany soukromí, kdy lidé v obecné rovině deklarují, že ochrana osobních údajů je pro ně důležitá a mají obavy ze zneužití svých údajů, tyto obavy však nepromítají do konkrétního chování například při používání internetu. Důvodem však není to, že by skutečná hodnota ochrany osobních údajů byla pro ně nižší, než deklarují, ale to, že v kontextu omezených zdrojů a informační asymetrie nejsou schopni udělat rozhodnutí, která by odpovídala jejich preferencím, nebo mají pocit, že své preference nejsou schopni prakticky prosadit a na tuto snahu rezignují.

Dle mého názoru je proto třeba hledat jiný přístup k zajištění ochrany osobních údajů, který nespočívá na aktivitě jednotlivce. Tento přístup nazývám přístupem založeným na důvěře v souladu s návrhem Richardse a Hartzoga. Richards a Hartzog hledají pro svůj přístup k ochraně osobních údajů inspiraci v úpravě fiduciárních vztahů, kde se typicky projevují povinnost péče a povinnost loajality. Do prostředí ochrany osobních údajů tyto povinnosti přenáší v podobě zásad diskrétnosti, ochrany, upřímnosti a loajality.

Platná právní úprava ochrany osobních údajů přístup založený na důvěře v mnoha ohledech odráží a v evropském kontextu nejde o žádné novum. Naopak tento přístup je součástí ochrany osobních údajů v Evropské unii od jejího počátku a jeho význam v čase roste. Není však promítnut do právní úpravy ochrany soukromí a osobních údajů v elektronických komunikacích v rovině ukládání a čtení údajů ze zařízení koncových uživatelů, tj. zejména do zmiňované problematiky právní úpravy ukládání a čtení cookies.

Domnívám se, že vhodným řešením tohoto problému by bylo opuštění obecného požadavku na souhlas s ukládáním a čtením údajů z koncového zařízení uživatele a jeho nahrazení vazbou na obecnou právní úpravu GDPR. Tuto úpravu je pak možné vyložit tak, aby byly prosazeny zásady přístupu založeného na důvěře, tedy diskrétnost, transparentnost, ochrana a loajalita. Cesta k tomuto výkladu podle mého názoru vede skrze pokyny Evropského sboru pro ochranu osobních údajů, které mohou být následně rozpracovány do konkrétních praktických postupů a technických protokolů skrze kodexy chování a mechanismy certifikace.

Cookie Consents and Approaches to Data Protection

Jan Tomíšek (https://orcid.org/0000-0003-1442-4982)

Abstract: This article discusses the current approaches to the protection of personal data in the light of the amended legal regulation on the storage and reading of data from end devices of electronic communications services users, which, among other things, extends the requirements for the collection of consent to the use of so-called cookies. The article therefore presents an approach to data protection based on control by the data subject and an approach based on protecting the trust placed in those who process personal data. Subsequently, the suitability of both approaches for establishing data protection in today's society characterized by large-scale processing of personal data is discussed. The author concludes that the control-based approach should not be the dominant approach to the protection of personal data, as control of such a scale of processing by those concerned is not possible given the limited time and the limits of rational decision-making. Therefore, he proposes to emphasise the trust-based approach in the protection of personal data. This is already widely reflected in general data protection legislation, but not in the area of privacy and personal data protection in electronic communications. The author therefore proposes to abandon the requirement for consent to store and read data from electronic communications services users' devices and to replace it with a link to the general rules on data protection, complemented by an interpretation of the European Data Protection Board elaborating on the principles of the trust-based approach.

Keywords: data protection, personal data, cookies, control, trust