550—560

Lloyd vs. Google aneb spočívá v prostém zásahu do informačního soukromí člověka škodlivý následek a musí být takový zásah vždy škodlivý?

Jakub Vostoupal*

Abstrakt: **Článek rozebírá aktuální rozhodnutí anglických soudů ve věci Lloyd vs. Google. Úvodní část je věnována krátkému představení problematiky soukromí a souvisejících pojmů, včetně stručného rozebrání potenciálních následků zásahu do soukromí. Po položení alespoň základního teoretického rámce jsou v článku kriticky rozebrána všechna rozhodnutí se zaměřením na zodpovězení otázky „zda v prostém zásahu do informačního soukromí člověka spočívá škodlivý následek". V závěru se pak autor zaměřuje na argument kontextu, kterého se dovolával prvoinstanční soud, a představí dva scénáře, které mají potenciál tento argument podpořit.**

Klíčová slova: **soukromí, ochrana osobních údajů, zásah do soukromí, kybernetická bezpečnost**

Úvod

Ve dnech 21. až 23. května roku 2018 rozhodoval londýnský Court of Justice poněkud kuriózní případ, který si, zvláště s ohledem na rozhodnutí soudu v druhé instanci, získal celosvětovou pozornost. Jednalo se o případ č. HQ17M01913, známý spíše jako *Lloyd vs. Google*. Soudce stál před nelehkým úkolem – Richard Lloyd zažaloval Google za porušení povinnosti, kterou mu ukládal § 4 odst. 4 britského *Data Protection Act* z roku 1998 (dále jen jako „DPA"), tedy tehdejší transpozice směrnice 95/46/ES (předchůdce obecného nařízení o ochraně osobních údajů[1]),[2] přičemž spor stál primárně na jediné otázce: *„Může v prostém zásahu do informačního soukromí člověka spočívat škodlivý následek?"*

1. Co je soukromí?

Pro lepší uchopení toho, jak k této otázce přistoupily anglické soudy, je nutné alespoň stručně představit základní teoretický rámec toho, co vlastně *„soukromí"* a další relevantní pojmy znamenají.

Otázka „co je soukromí?" bohužel nemá jednoduchou odpověď, a jak Míšek na několika příkladech demonstruje, *„dodnes jde o velice těžko uchopitelný pojem, který není možné*

* Mgr. Jakub Vostoupal je doktorandem na Ústavu práva a technologií Právnické fakulty a studentem bakalářské psychologie na Fakultě sociálních studií Masarykovy univerzity v Brně. Vedle toho působí v rámci projektů např. Centra excelence pro kyberkriminalitu, kyberbezpečnosti a ochranu kritických informačních infrastruktur. E-mail: jakub.vostoupal@law.muni.cz. ORCID: https://orcid.org/0000-0002-1669-9931. Vznik tohoto příspěvku byl podpořen projektem MUNI/A/1484/2021 (*Právo a technologie X*). Autor též děkuje anonymním recenzentům za cenné připomínky.

1 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.

2 Viz bod 2 daného rozhodnutí.

svázat do jedné pevné a trvalé definice".[3] I navzdory neurčitosti pojmu soukromí, se našlo hned několik autorů, kteří se pokusili právo na soukromí definovat a popsat jeho jednotlivé vrstvy uspokojivým způsobem. Pravděpodobně jednou z nejoblíbenějších variant je *„právo být ponechán sám sobě"*.[4, 5]

Tento pojem poprvé užívá soudce T. M. Cooley v práci *A Treatise on the Law of Torts* při popisu základních práv, konkrétně práva jedince k sobě samému.[6] Až o dva roky později tento termín využívají i Warren s Brandeisem, kterým je v tomto ohledu prvenství nesprávně přisuzováno (přestože se na Cooleyho ve svém díle odkazují).[7] Jejich práce pak odstartovala evoluci významu práva na soukromí.[8] Mezi navazující modely hodné zmínky patří bezpochyby již citovaný model Daniela Solovea, ve kterém kromě práva být ponechán sám sobě autor navrhuje ještě dalších 5 kategorií, které dohromady mají vystihovat právo na soukromí jako celek – umožnění omezení přístupu k vlastní osobě, možnost utajení či zachování tajemství, kontrola nad osobními informacemi, ochrana osobnosti (tedy individuality, důstojnosti a autonomie člověka), a intimita.[9, 10]

S pokračujícím rozvojem technologií, které umožňují masivní narušování soukromí, je možné vysledovat v těchto teoretických modelech určitou reakci – mj. vzestup důležitosti tzv. informačního soukromí. Dobře patrná je tato skutečnost na modelu týmu B. J. Koopse, který kromě osmi oddělených (standardních) kategorií obsahuje i speciální, všeprostupující kategorii devátou.[11] Tato kategorie je právě informační, ne fyzické soukromí. V této myšlence se výzkumný tým odkazuje na Blokea, který uvádí, že i fyzické kategorie soukromí mají aspekt informačního soukromí, tedy že soukromí je nejen právo na to, že se nikdo nebude dívat oknem do naší kuchyně, ale také právo na *„ochranu před šířením informací"*,[12] tedy že nikdo nebude šířit, co v té kuchyni viděl.

Jako vysoce relevantní model, zvláště pro případ *Lloyd vs. Google*, zde uvádím ještě model Helen Nissenbaum, který je založen na kontextové integritě.[13] Nissenbaum zdůrazňuje, že *„problém často nespočívá v tom, že někdo pracuje s informacemi soukromého charakteru vztahující se k člověku, ale jakým způsobem s nimi pracuje"*.[14] Pokud jsou informace využívány v souladu s očekáváními, která odpovídají danému kontextu, nepůsobí to mezi stranami problémy.

---

3 Viz MÍŠEK, J. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita, 2020, s. 29–30.

4 V originále *„right to be alone"*, viz SOLOVE, D. J. Conceptualizing Privacy. *California Law Review*. 2002, Vol. 90, Iss. 4, s. 1099–1102.

5 Český překlad *„být ponechán o samotě"*, který stvořil Ústavní soud, je bohužel poněkud nešťastný, a proto používám raději tuto formu.

6 Viz COOLEY, T. M. *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*. Chicago: Callaghan and Company, 1879, s. 29.

7 Viz WARREN, S. D. – BRANDEIS, L. D. Right to Privacy. *Harvard Law Review*. 1890, Vol. 4, No. 5.

8 Více viz MÍŠEK, J. *Moderní regulatorní metody ochrany osobních údajů*, s. 30–32.

9 Viz SOLOVE, D. J. *Conceptualizing Privacy*, s. 1102–1125.

10 Solove na toto navazuje v článku *A Taxonomy of Privacy*, ve kterém pojednává o zásazích do informačního soukromí, více viz SOLOVE, D. J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*. 2006, Vol. 154, No. 3.

11 Viz KOOPS, B.-J. et al. A Typology of Privacy. *University of Pennsylvania Journal of International Law*. 2017, Vol. 38, No. 2.

12 Ibidem, s. 554–555.

13 Viz NISSENBAUM, H. F. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, California: Stanford University Press, 2010.

14 Helen Nissenbaum (2010), cit. dle MÍŠEK, J. *Moderní regulatorní metody ochrany osobních údajů*, s. 36–37.

2. Sociální a psychologický aspekt zásahu do soukromí

Nebylo by vhodné opomenout, že sdělování informací soukromého charakteru je jeden z esenciálních projevů prosociálního chování, který intenzivně posiluje schopnost jedince navazovat a utužovat vztahy.[15] Míra intenzity a kvantity tohoto projevu se zásadně liší v závislosti na prostředí, ve kterém ke sdělování dochází (např. fyzické/kyberprostor[16] nebo domácí/pracovní).[17] Kromě toho ovšem záleží i na bezpečí daného prostředí. Pokud tedy člověk ztrácí kvůli zásahům do soukromí pocit kontroly a bezpečí ve svém prostředí, dochází k normalizaci jeho chování, k omezování svěřování a k tzv. *„chilling efektu"*.[18] Omezené svěřování či míra zatajování soukromých a intimních informací (tzv. *self-concealment*) s sebou přináší plejádu negativních projevů jak fyzické povahy (zvýšená únava, menší fyzická výdrž),[19] tak i psychické a sociální.[20, 21]

Zásahy do soukromí narušují i základní sociální procesy. V případě, že se někomu člověk rozhodne vyjevit určitou intimní informaci, má kontrolu nad tím, jak a komu danou informaci sděluje, případně může určité aspekty zamlčet. Zásah tuto kontrolu obchází. Příkladem budiž vyjevení historie vyhledávání v internetovém prohlížeči – člověku nehrozí poškození toliko jeho reputace a sociálního kreditu, ale také nejrůznějších sociálních vazeb, jeho ochoty se svěřovat, sebedůvěry a mnohého dalšího. Zásah do soukromí tak může fakticky narušit jeden z nejzákladnějších aspektů člověka – společenskost.

3. Osobní údaje, informační soukromí a právo na informační sebeurčení

Vymezit pojem osobních údajů je oproti pojmu soukromí podstatně jednodušší, neboť existuje relativně jasná zákonná definice – jedná se o jakýkoliv údaj, o jakákoliv data, která mohou přímo nebo nepřímo vést k identifikaci fyzické osoby.[22] Osobním údajem může být např. IP adresa, cookies soubory, ale v určitých situacích také historie procházení, u které může dojít k identifikaci osoby přímo (navštívením např. osobní stránky na FB), či nepřímo (kumulativně s dalšími údaji uživatele).[23] Ochrana osobních údajů je oproti ochraně soukromí postavena jako ochrana *ex post*, chrání tedy subjekt údajů před neoprávněným zpracováním osobních údajů, nebrání *ex ante* zásahu. I ochrana osobních údajů

15 Viz např. SLEPIAN, M. L. – MOULTON-TETLOCK, E. Confiding Secrets and Well-Being. *Social Psychological and Personality Science*. 2019, Vol. 10, Iss. 4.

16 Viz TRUB, L. A portrait of the self in the digital age: Attachment, splitting, and self-concealment in online and offline self-presentation. *Psychoanalytic Psychology*. 2017, Vol. 34, No. 1.

17 Viz např. BATHJE, G. J. et al. Attitudes toward Face-to-Face and Online Counseling: Roles of Self-Concealment, Openness to Experience, Loss of Face, Stigma, and Disclosure Expectations among Korean College Students. *International Journal for the Advancement of Counselling*. 2014, Vol. 36, Iss. 4.

18 Více viz STOYCHEFF, E. et al. Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*. 2019, Vol. 21, Iss. 3; HERMSTRÜWER, Y. – DICKERT, S. Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge. *International Review of Law and Economics*. 2017, Vol 51, Iss. C.

19 Viz např. LARSON, D. G. et al. Self-Concealment: Integrative Review and Working Model. *Journal of Social and Clinical Psychology*. 2015, Vol. 34, No. 8.

20 Viz např. UYSAL, A. – LEE LIN, H. – RAYMOND KNEE, C. The Role of Need Satisfaction in Self-Concealment and Well-Being. *Personality and Social Psychology Bulletin*. 2010, Vol. 36, Iss. 2.

21 Dále viz SLEPIAN, M. L. – MOULTON-TETLOCK, E. *Confiding Secrets and Well-Being*; SLEPIAN, M. L. – KIRBY, J. N. – KALOKERINOS, E. K. Shame, guilt, and secrets on the mind. *Emotion*. 2020, Vol. 20, No. 2.

22 Viz článek 4, odst. 1 obecného nařízení o ochraně osobních údajů.

23 Ibidem.

ovšem přispívá k ochraně soukromí, jak je mimo jiné patrné z § 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

S právem na informační soukromí pak úzce souvisí právo na informační sebeurčení, které má své kořeny v judikatuře německého Spolkového ústavního soudu a je dle ELSP součástí práva na soukromý a rodinný život.[24] Právo na informační sebeurčení bylo vzápětí přejato i naším Ústavním soudem, který jej vymezil jako možnost kontroly nad informacemi o sobě samém (zjednodušeně řečeno).[25, 26]

Právo na informační sebeurčení nalezneme zakotvené i v článku 10 Listiny základních práv a svobod, kde doplňuje právo na ochranu soukromého a rodinného života a lidské důstojnosti. Vzhledem k jejímu postavení v Listině i způsobu, jakým ji vymezil Ústavní soud, stojí dle mého názoru právo na informační sebeurčení na obdobné pozici jako informační soukromí v modelu Koopse a ostatních, tedy přesahujíc a prostupujíc všechny kategorie.

Dalo by se tak konstatovat, že všechna výše zmíněná práva spadají pod jednu meta-kategorii „ochrany soukromí“,[27] leč např. Polčák uvádí, že: *„V současné době je možno […] označit za integrální součást práva na informační sebeurčení následující instituty: svoboda projevu, ochrana soukromí, právo na vzdělání, ochrana osobních údajů a právo na informace veřejného sektoru.“*[28] Je tedy možná jednodušší stavit se k jednotlivým institutům jako k článkům jednoho řetězu, než vymezovat nadřazené a podřazené pojmy.

S tímto základním teoretickým rámcem přišel čas vrátit se na začátek, k soudnímu sporu a otázce, zda v prostém zásahu do informačního soukromí může spočívat škodlivý následek.

4. Lloyd vs. Google I

Richard Lloyd podal na Google žalobu jménem 4,4 milionu uživatelů telefonů značky iPhone[29] kvůli tomu, že Google mezi červnem 2011 a únorem 2012 zpracovával data[30] generovaná prohlížečem prostřednictvím souborů cookies[31] ukládaných uživatelům do zařízení za účelem zvyšování efektivity cílené reklamy.[32] Cookies jsou obecně využívány k monitorování chování uživatelů na webu (tzv. *tracking cookies*), ke statistikám, k personalizaci prohlížení, ale také např. k autentizaci, a představují jeden ze základních kamenů internetu již od devadesátých let.[33] Zpracovávání dat v tomto konkrétním případě

24 Viz rozsudek ESLP ve věci *Atakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku*, cit. dle MÍŠEK, J. *Moderní regulatorní metody ochrany osobních údajů*, s. 40.

25 Tedy srovnatelné s jedním z aspektů modelu Daniela Solovea, srov. SOLOVE, D. J. *Conceptualizing Privacy*, s. 1106.

26 Viz nález Ústavního soudu ze dne 22. 3. 2013, PL. ÚS 24/10: *„Vedle tradičního vymezení soukromí v jeho prostorové dimenzi (ochrana obydlí v širším slova smyslu) a v souvislosti s autonomní existencí a veřejnou mocí nerušenou tvorbou sociálních vztahů (v manželství, v rodině, ve společnosti) právo na respekt k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům.“*

27 Srov. SOLOVE, D. J. *Conceptualizing Privacy*, s. 1106.

28 Viz POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 327.

29 Viz body 3 a 4 rozhodnutí *Lloyd vs. Google I*.

30 Např. IP adresu zařízení či URL navštívené stránky.

31 Konkrétně se jednalo o *DoubleClickAd*, což jsou tzv. cookies třetí strany.

32 Viz body 6–10 daného rozhodnutí.

umožňovalo detailně sledovat aktivitu uživatelů, jakmile „zabrouzdali“ na jakýkoliv web, na kterém byla reklama spadající pod Google (což je skutečně rozsáhlá síť), a v některých případech také skrze IP adresu vysledovat geografickou polohu uživatele.[34]

Prohlížeč Safari (od Apple) v roce 2011 obsahoval jako jeden z mála možnost blokovat cookies třetích stran, která byla defaultně povolena.[35] Až do února roku 2012 ovšem obsahoval řadu výjimek, které Googlu umožnily své cookies ukládat do těchto zařízení bez ohledu na vůli, vědomí či souhlas uživatelů.[36] Zpracované informace navíc umožnily Googlu roztřídit uživatele podle vzorců chování (např. na milovníky fotbalu či lezení po skalách), což posléze využíval při jednání s inzerenty, kteří si mohli zvolit konkrétní skupiny, na které svou reklamu zacílí.[37]

Richard Lloyd se na základě tohoto počínání domáhal kompenzace nikoliv za nějakou finanční škodu, ale za porušení práv vyplývajících z DPA a ztrátu kontroly nad osobními údaji.[38] Alternativně se pak pan Lloyd domáhal odškodnění ve výši zisku, který Google díky těmto údajům získal.[39]

Prvoinstanční soud se s argumentací žalobce neztotožnil. Naopak konstatoval, že nárok na odškodnění vzniká v případě, kdy porušením práv zakotvených v DPA dojde ke škodě, což jsou dle názoru soudce *„dvě samostatné události, které jsou kauzálně spojeny“*, nikoliv jedna a tatáž.[40] Na základě textu zákona i směrnice tak dle něj prostý zásah není způsobilý vyvolat újmu jednotlivci. Zvláště, když jedinec tento zásah do soukromí nepocítil. Soudce vyslovil nesouhlas s tím, že by pouhý zásah (ať už způsobený porušením práv nebo narušením kontroly, kterou nad osobními údaji daná osoba má) měl automaticky způsobit subjektu údajů škodu nebo psychickou újmu s nárokem na odškodnění.[41] Takový přístup by dle něj znamenal nepřiměřenou a nespravedlivou zátěž pro správce údajů.[42] Soudce dále argumentoval tím, že zásah může být i přínosný, což dokládal na několika situacích z běžného života (např. oblíbeností překvapivých oslav apod., více viz bod 74 daného rozhodnutí).

V tomto bodě s argumentací nesouhlasím, neboť soud dle mého názoru mísí „jablka s hruškami“. Porovnává zásah na úrovni osobní (tedy vlastně obdoba *data sharing*[43]) se zásahem na úrovni komerční, dlouhodobé a automatizované (tedy obdoba *data disclosure*[44]), což je ostatně něco, co rozlišuje i GDPR v článku 2 [odstavec 1 a 2 písmeno c)]. Užité argumenty tak považuji za liché, přestože se zdůrazněním důležitosti kontextu v zásadě souhlasím.[45]

---

33 Více viz What are Cookies? [online]. *Kaspersky*. 13. 1. 2021 [cit. 2021-08-02]. Dostupné z: <https://www.kaspersky.com/resource-center/definitions/cookies>.

34 Viz bod 11 daného rozhodnutí.

35 Viz bod 10 daného rozhodnutí.

36 Ibidem.

37 Viz bod 12 daného rozhodnutí.

38 Viz body 3 a 4 daného rozhodnutí.

39 Viz body 3, 58 a 59 daného rozhodnutí.

40 Viz body 55 a 56 daného rozhodnutí.

41 Viz body 55, 56 a 74 daného rozhodnutí.

42 Ibidem.

43 Viz CUSTERS, B. – URŠIČ, H. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. 2016, Vol. 6, Iss. 1, s. 10.

44 Ibidem.

45 Srov. NISSENBAUM, H. F. *Privacy in context: technology, policy, and the integrity of social life*.

5. Lloyd vs. Google II

Prvoinstančním rozhodnutím zajímavost sporu *Lloyd proti Googlu* nekončí. Odvolací soud se k předmětné otázce postavil jinak[46] a upozornil, že transponovaná směrnice, a tedy i DPA v relevantní části slouží jako prostředek ochrany práva zakotveného v článku 8 Charty základních práv EU, sklon k restriktivnímu výkladu tak není na místě.[47] Soud se neztotožnil s konstatováním, že by ztráta kontroly nebyla sama o sobě škodlivá, naopak konstatoval, že samotná kontrola je aktivem, které má ekonomickou hodnotu a je možné ji směnit mj. za služby na internetu (aneb *nic na internetu není zadarmo*).[48] Ztrátou této kontroly je jedinec o toto aktivum chudší a nemůže je využít.[49] V tomto si dovoluji upozornit, že toto platí pouze *inter partes*, nikoliv *erga omnes*. Žalobce, který byl ze strany Googlu připraven o tuto kontrolu, přijde o ekonomickou hodnotu těchto dat pouze ve spojitosti s Googlem (protože ten k nim již přístup má). Tato data však nezaniknou a poškozený je může u dalších zainteresovaných stran dále směňovat.

Soud na závěr upozornil, že Google údaje sbíral úmyslně, cíleně a protiprávně, nejedná se tak o žádné *„automatické připisování schopnosti působit újmu každému zásahu“* a ignorování této ztráty by bylo nejen nespravedlivé, ale zároveň ignorovalo základní principy obecné evropské ochrany soukromí.[50]

Dle druhé instance tedy spočívá škodlivý následek prostého zásahu ve ztrátě kontroly. Takový zásah nemusí znamenat žádné zneužití či propad v reputaci, přesto se však jedná o odepření svobody rozhodnout se, komu danou informaci sdělím. Připravuje nás o ekonomickou hodnotu tohoto aktiva. Vystavuje nás i určité nejistotě, protože stejně jako v normální lidské interakci, informace raději předáváme důvěryhodnému zdroji. Toto počínání by bylo možné s určitou mírou nadsázky přirovnat ke zneužití séra pravdy, kdy informace vyjevíme, ale nemáme kontrolu nad tím, jaké a komu, nemáme svobodu vůle. Můžeme je tedy vyjevit někomu nedůvěryhodnému či někomu, s jehož názory či obchodním modelem nesouhlasíme (to bývalo relativně časté např. v případě obchodního modelu Facebooku a související oblíbeností aplikace Signal[51]).

Celý příběh se ale relativně nedávno dočkal překvapivého „rozuzlení“ v podobě rozhodnutí Nejvyššího soudu ve věci *Lloyd vs. Google III*.

6. Lloyd vs. Google III

Soud se nejdříve zaobíral povahou samotného řízení, respektive reprezentujícím postavením pana Lloyda, a představil vskutku zajímavou exkurzi do historie tohoto institutu, která je naneštěstí mimo záběr tohoto článku.[52] Soudce v kontextu specifického postavení žalobce konstatuje, že se jedná o relativně flexibilní nástroj, který je rozšířený i v jiných zemích, mj. Austrálii, Kanadě či Novém Zélandu, a jehož užitečnost s nástupem digitali-

46 Viz bod 70 daného rozhodnutí.
47 Tedy práva na ochranu osobních údajů a jejich korektní zpracování. Viz body 40–42 daného rozhodnutí.
48 Viz body 45 až 47 daného rozhodnutí.
49 Viz body 45 až 57 daného rozhodnutí.
50 Viz body 55–57 daného rozhodnutí.
51 Nyní jsou již rozdíly mezi těmito službami částečně setřeny, neb Facebook/Meta se na trhu adaptovaly.
52 Viz body 33–68 rozhodnutí *Lloyd vs. Google III*.

zace (a související možností poškodit masy osob najednou) jenom roste.[53] S ohledem na tuto skutečnost argumentuje, že výklad pojmu „shodný zájem" reprezentovaných osob musí být pragmatický a racionální, nikoliv doslovný, neb nemá být využíván a zneužíván k tomu, aby se poškozené masy nedovolaly spravedlnosti z finančních důvodů.[54] Naopak i ze strany výpočtu náhrady škod stačí, aby bylo možné použít shodný systém výpočtu, není ovšem nutné, aby byla samotná výše náhrad shodná.[55]

Pan Lloyd, jak již bylo uvedeno výše, se v tomto případě domáhal paušální náhrady škody, a to nikoliv na základě prokázání škody či mentální újmy způsobené zpracováním, ale zmíněnou ztrátou kontroly. S tím se soud neztotožnil hned ze dvou důvodů. První se týkal výkladu pojmu „škody" ve smyslu článku 13 DPA, u nějž soud zdůraznil, že se pojí buď k materiálnímu aspektu ve smyslu např. finanční ztráty,[56] nebo mentální újmě způsobené zpracováním, přičemž obojí musí být v řízení prokázáno.[57] Obojí je však způsobeno nelegálním zpracováním, nejedná se o nárok založený nelegálním zpracováním samotným.[58]

Jako druhý důvod zamítnutí soud uvedl, že domáhat se náhrady škody bez prokazování povahy a existence nelegálních zásahů v jednotlivých případech, společně s neprokazováním, že jednotlivci skrze tento zásah utrpěli materiální či mentální újmu, je jednoduše neúnosné.[59] Zamítl tím tak konstrukt kontroly nad osobními daty prezentovaný Lloydem a druhoinstančním soudem.

Přestože tento krok v zásadě chápu, vnímám jej spíše jako opatrný, zčásti i formalistický. Jsem toho názoru, že zvláště v informační společnosti s posilující datovou ekonomikou a s přihlédnutím k obecnému fungování internetu a obchodním modelům společností jako jsou Google nebo Facebook by bylo vhodné uznat důležitost ekonomické hodnoty kontroly nad daty.[60] Stejně tak, jako že kontrola nad určitými daty osobního charakteru je součástí práva na soukromí, jak ostatně uvádí i výše zmíněný Daniel Solove, a jako taková je hodna právní ochrany. Takové pojetí totiž nabízí ochranu jedince i před takovým predátorským zpracováním, kterého se v tomto případě dopustil Google. Navzdory tomu, že případ *Lloyd vs. Google* nakonec odmítá škodlivost prostého zásahu do informačního soukromí člověka, já se daleko snadněji ztotožňuji s argumentací a myšlenkami druhoinstančního soudu, neboť je považuji do budoucna za udržitelnější a efektivnější metodu ochrany.

7. Důležitost kontextu

Ani ochrana kontroly před prostým zásahem ve smyslu rozhodnutí *Lloyd vs. Google II* by samozřejmě nemohla být bezbřehá. V této souvislosti narazil na důležitost kontextu i prvoinstanční soud,[61] a přestože s použitými argumenty plně nesouhlasím, s myšlen-

53 Viz body 38–41 rozhodnutí *Lloyd vs. Google III*.
54 Viz body 69–75 a 80-83 rozhodnutí *Lloyd vs. Google III*.
55 Viz body 80–83 rozhodnutí *Lloyd vs. Google III*.
56 Viz body 93–96 rozhodnutí *Lloyd vs. Google III*.
57 Viz body 97–104 rozhodnutí *Lloyd vs. Google III*.
58 Viz body 93–108 rozhodnutí *Lloyd vs. Google III*.
59 Viz body 144–157 rozhodnutí *Lloyd vs. Google III*.
60 Navíc je patrné, že se nejedná o naprosto výjimečnou myšlenku, podobný názor zazněl i v případě United States v. Rockyou, Inc., Case No. 3:12-cv-01487-SI (N.D. Cal. Mar. 27, 2012). Tento případ byl bohužel nakonec ukončen smírem.
61 Viz bod 74 rozhodnutí *Lloyd vs. Google I*.

kou, která stojí za nimi a vlastně navazuje na kontextuální model Helen Nissenbaum, se plně ztotožňuji. V případě, že se k druhoinstančnímu konstruktu stavím jako k možnému budoucímu vývoji na tomto poli, je tak dle mého názoru vhodné se alespoň stručně zabývat otázkou, jak by mohlo vypadat narušení kontroly, které by nepředstavovalo škodlivý zásah do práva na informační soukromí z důvodu vyvážení kontextem takového narušení.

Pro zodpovězení jsem si vybral dva případy s kyberbezpečnostní tématikou, které by potenciálně mohly přesně takové narušení reprezentovat. Prvním případem je postup amerického Ministerstva spravedlnosti při boji proti zneužívání zranitelností Microsoft Exchange Serveru z dubna roku 2021.[62] Na tuto zranitelnost se zejména v lednu a únoru 2021 zaměřily hackerské skupiny, což jim umožnilo nabourat se do soukromých emailových schránek a skrze škodlivý kód si v nich otevřít zadní vrátka, která jim umožňovala se do schránek libovolně vracet.[63] Vzhledem k závažnosti této zranitelnosti přistoupila US administrativa k poněkud radikálnímu kroku. Svolila, aby FBI vymazala (s přivolením soudu) škodlivý kód z jednotlivých infikovaných počítačů, u kterých se odstranění soukromému sektoru do té doby nedařilo.[64] Jednalo se samozřejmě o zásah mimo kontrolu majitelů těchto strojů, o automatizovaný, úmyslný a cílený zásah, který byl zároveň (vzhledem k probíhajícímu vyšetřování a kopírování škodlivého kódu) i aktivním zásahem do soukromí, přestože kvantitativně (snad) o poznání nižší intenzity než v případě *Lloyd vs. Google*.[65] Navíc je nutné zdůraznit, že se jednalo o zásah aktivní, tedy umožňující jednání v rámci určité soukromé domény, bylo by tak možné jej považovat i za potenciálně závažnější než v případě *Lloyd vs. Google*. V tomto případě byl ovšem zásah legitimizován povahou zasahujícího orgánu, právními limity, kontrolou nad procesem, časovou omezeností zásahu i důvodem k akci (boj proti kyberkriminalitě a ochrana majetku, osob i soukromí).

Takový případ je sice choulostivý, představuje ale dle mého relativně jasný limit pro ochranu kontroly nad daty. Proto jsem si jako druhý případ zvolil situaci komplexnější a méně jednoznačnou. Jedná se o incident z roku 2012, jednu z kyberbezpečnostních „legend".

8. Botnet Carna

Tento příběh začíná u neznámého jedince či skupiny jedinců, pravděpodobně bezpečnostních výzkumníků, kteří se jali zkoumat zabezpečení počítačů připojených v té době k internetu. Konkrétně se zaměřili na zařízení stále využívající službu Telnet[66] s továrně

62 Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities [online]. *United States Department of Justice*. 13. 4. 2021 [cit. 2021-10-11]. Dostupné z: <https://www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft>.

63 Microsoft Exchange Server Vulnerabilities Mitigations [online]. *Microsoft Security Response Center*. 15. 3. 2021 [cit. 2021-10-11]. Dostupné z: <https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/>.

64 *Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities*, 2021.

65 Ibidem.

66 Jedná se o pozůstatek 90. let, který umožňuje po autentizaci vzdáleně ovládat počítač, jedná se tudíž o silnou službu, bohužel s nedokonalým zabezpečením (přihlašovací jméno a heslo se posílá ve formě prostého textu či SSH).

přednastaveným heslem.[67, 68] Existence takového hesla, takové zranitelnosti samozřejmě představuje obrovské bezpečnostní riziko, které bylo tou dobou již téměř 3 roky známé, a výrobci tak měli více než dost času na sjednání nápravy.[69] Pro relativně malou známost kyberbezpečnostních témat ve společnosti však trh tyto výrobce dostatečně „netlačil" ke sjednání nápravy a nebylo tak jasné, o jak široký problém se i po 3 letech jedná.[70] Výzkumník/výzkumníci tedy začali skenovat IP adresy a zkoušet jednu ze čtyř defaultních možností přihlašovacích údajů, přičemž nezabezpečené systémy na sebe nenechaly dlouho čekat. Co výzkum limitovalo, byla výpočetní kapacita a rychlost procesu skenování – proskenovat 100 000 IP adres zabralo 16 hodin. Internet obsahoval tou dobou téměř 4 miliardy IP adres.

Výzkumníci tudíž přišli s řešením – napsali program, který uměl skenovat a nacházet nezabezpečené systémy a v případě pozitivního nálezu nahrát sám sebe na zranitelné zařízení a zapojit i tento (nově infikovaný) systém do skenovacího procesu.[71] Stvořili tím botnet, který dostal jméno Carna. Tento postup je samozřejmě z pohledu trestního práva nelegální sám o sobě.[72]

Výzkumníci během několika málo hodin infikovali více než 30 000 zařízení, mimo jiné televize, systémy SCADA či kamery.[73] Poté, co botnet dokončil sken, výzkumníci věděli o 1,2 milionu zařízení, která byla stižena touto zranitelností, přičemž 420 000 z nich bylo součástí botnetu.[74] Tuto výpočetní sílu posléze využili k něčemu, co do té doby nebylo nikdy učiněno – internetový census.[75] Při opakovaných skenech ovšem náhodou objevili další botnet, který byl založen na stejné zranitelnosti jako Carna, ale byl využíván ke kyberkriminálním účelům. Tento botnet se jmenoval Aidra a jeho tvůrci jím způsobovali nemalé škody.[76] Výzkumníci využili svého unikátního postavení a skrze vlastní botnet zablokovali IP adresy, které Aidra používala ke komunikaci, a následně předali data zachycující infikovanou infrastrukturu (přes 30 000 zařízení) OČTŘ, což vedlo k vyřazení většiny sítě z provozu a ochromení botnetu Aidra.[77]

V rámci internetového censu došlo samozřejmě k masivnímu zásahu do soukromí, který je možná i závažnější než v případě *Lloyd vs. Google*, a to vzhledem ke zveřejnění

---

67 Při výzkumu využili následující kombinace: admin/admin, admin bez hesla, root/root a root bez hesla.

68 Viz Internet Census 2012. In: *Census 2012* [online]. 2013 [cit. 2021-08-03]. Dostupné z: <http://census2012.sourceforge.net/paper.html>.

69 Viz Default Telnet password: admin password „password". In: *Rapid7* [online]. [cit. 2021-08-03]. Dostupné z: <https://www.rapid7.com/db/vulnerabilities/telnet-default-account-admin-password-password/>.

70 Viz ibidem.

71 Viz *Internet Census 2012*.

72 Viz § 230 zákona č. 40/2009 Sb., trestní zákoník.

73 Viz *Internet Census 2012*; Carna Botnet Scans. In: *CAIDA* [online]. 30. 7. 2020 [cit. 2021-08-03]. Dostupné z: <https://www.caida.org/archive/carna/>; INTERNET CENSUS 2012 GROUP. Full Disclosure: Port scanning /0 using insecure embedded devices. In: *SecLists* [online]. 17. 3. 2013 [cit. 2021-08-03]. Dostupné z: <https://seclists.org/fulldisclosure/2013/Mar/166>.

74 Viz *Internet Census 2012*; *Carna Botnet Scans*; INTERNET CENSUS 2012 GROUP. *Full Disclosure: Port scanning /0 using insecure embedded devices*.

75 Viz *Internet Census 2012*.

76 Více viz NJCCIC Threat Profile: Aidra Botnet. In: *NJCCIC* [online]. 2016 [cit. 2021-08-03]. Dostupné z: <https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/aidra-botnet>; HIGGINS, K. J. What The Carna Botnet Also Found. In: *Dark Reading* [online]. 14. 11. 2013 [cit. 3. 8. 2021]. Dostupné z: <https://www.darkreading.com/vulnerabilities-threats/what-the-carna-botnet-also-found>.

77 HIGGINS, K. J. *What The Carna Botnet Also Found*.

celého datasetu sesbíraných IP adres včetně geografické identifikace a mapy, která mimo jiné zachycuje, kdy jsou jaké IP adresy aktivní.[78, 79] I v tomto případě bych ovšem namítl, že navzdory jisté morální ambivalenci, společenská škodlivost tohoto zásahu byla minimální. Oproti minulému příkladu a analogicky k *Lloyd vs. Google* byly v případě botnetu Carna pachateli zásahu soukromé osoby. Zásah tak nebyl posvěcen státní mocí, nebyl ani povolen soudem, ani nectil žádné právní mantinely. Oproti případu *Lloyd vs. Google* však zásah skrze botnet Carna své tvůrce nijak neobohatil (ani finančně, ani reputačně, neboť skupina, která provedla první kompletní internetový census, zůstává dodnes v anonymitě). Místo prospěchu jednoho konkrétního subjektu vedl k prospěchu široké veřejnosti, neboť díky němu bylo možné zmapovat značně rozšířenou a jednoduše zneužitelnou kyberzranitelnost. Zveřejnění těchto informací sice představovalo pro postižené subjekty krátkodobé ohrožení,[80] ale zároveň konečně vedlo k odstranění této zranitelnosti ze strany některých výrobců.[81] Je také krajně nepravděpodobné, že by bez zásahu tohoto botnetu došlo k tak výraznému ochromení kyberkriminálních aktivit vyvíjených prostřednictvím botnetu Aidra, což předešlo značným škodám. Činnost botnetu Carna byla posléze dobrovolně ukončena.

Zveřejnění datasetu by pak pro některé mohlo představovat onu hranici, která je i z pohledu jinak přínosného zásahu nepřekročitelná. V tomto musím upozornit na obsah poznámky pod čarou č. 79, tedy že analyzovat dataset a následně jej zneužít si vyžadovalo až mimořádnou výpočetní kapacitu, zdaleka převyšující tehdejší možnosti řadových kyberkriminálních skupin.[82] Zveřejnění tak bylo přínosné spíše pro akademické instituce.

Po zhodnocení celého případu docházím k názoru, že obdobně jako v případech materie *bug bounty* či *responsible vulnerability disclosure*, ani botnet Carna nakonec nenaplňuje potřebnou společenskou škodlivost, a přestože se jednalo o zásah do kontroly značného množství uživatelů, byl veřejnosti (i konkrétním zasaženým uživatelům) v mnoha ohledech naopak velice přínosný.[83]

---

78 Slovo „možná" zde používám z důvodu, že musíme vzít v potaz výpočetní možnosti té doby – dataset měl v době zveřejnění několik TB, tudíž taková analýza, která by umožňovala data zneužít, nebyla v možnostech normálního člověka ani většiny hackerských skupin té doby.

79 Dark Reading Staff. Carna Compromise Delivers Data, But Casts Suspicions. In: *Dark Reading* [online]. 4. 4. 2013 [cit. 2021-10-11]. Dostupné z: <https://www.darkreading.com/vulnerabilities-threats/carna-compromise-delivers-data-but-casts-suspicions>.

80 Což je srovnatelné s hlášením zranitelností ze strany tzv. *grey-hat* hackerů. V případě, že jedinec nalezne v službě, aplikaci či např. stránce zranitelnost a rozhodne se ji nahlásit odpovědnému subjektu za účelem jejího odstranění, občas se stává, že odpovědný subjekt na dané hlášení nereaguje, či se dokonce snaží oznamovatele umlčet. Jedním z mála způsobů, jak přinutit odpovědný subjekt k odstranění zranitelnosti, je pak její zveřejnění.

81 Viz *Internet Census 2012*.

82 V celém tomto pojednání se vyhýbám obecně trestněprávním aspektům. Už jenom samotné proniknutí do systému by v takovémto případě bylo ilegální a případné prokazování, že akt nebyl společensky škodlivý ve smyslu trestního práva, by sice mohlo mít určitou naději na úspěch, ale jedná se bohužel o nedostatečně projudikovanou otázku, přičemž tato materie je příliš komplexní pro rozebrání v tomto článku. Mimo jiné se jedná o situaci analogickou s nevyžádaným *pen-testingem/vulnerability disclosure* procesem, což je právě důvod, proč zastávám názor, že by mohlo být možné prokázání *„společenské neškodlivosti"*.

83 Dle mého názoru je ale zároveň nutné dodat, že podobné případy nesmí překročit hranici vigilantismu, kdy by soukromé subjekty braly právo do vlastních rukou. Postavení tvůrců botnetu Carna bylo v tomto relativně specifické – využili vlastních kapacit, kterými OČTŘ ani zdaleka nevládlo, k ochromení části botnetu Aidra (blokace IP adres, tedy naprosto minimální zásah), a ve zbytku pouze předaly nasbírané informace odpovědným orgánům. Nejednalo se o boj proti zločinu jako takový.

Závěr

Koncept kontroly nad osobními informacemi jakožto součást informačního soukromí není ničím novým, co by se vyskytovalo teprve v rozhodnutí *Lloyd vs. Google*. Zvláště s rozvíjející se důležitostí datové ekonomiky a možnostmi zpracovávat obrovská množství dat (*big data*) však získává tento fenomén na důležitosti. Ve spojení s obchodními modely společností jako Google nebo Facebook pak nepřekvapivě roste touha informovanějších uživatelů kontrolovat, komu poskytují svá data, což reprezentuje např. koncept *„data minimalism"*. Anglické soudy měly v případě *Lloyd vs. Google* možnost tento vývoj uznat a zareagovat na něj, bohužel se nakonec rozhodly jinak. Dle mého názoru odpovídá směru aktuálního technologického i společenského vývoje daleko vhodněji rozhodnutí *Lloyd vs. Google II*, které uznává ekonomickou hodnotu kontroly jako aktiva a poskytuje jí právní ochranu. Nečiní tak bezbřeze, ale za konkrétních podmínek. Účelem přitom není paralyzovat datovou ekonomiku, ale spíše adaptovat ochranu soukromí a osobních údajů. I tím je pro mne přístup druhoinstančního soudu funkčnější a *pro futuro* udržitelnější.

Jednou z podmínek, které samozřejmě musí limitovat dosah takové ochrany, je kontext zásahu, na což narážel soud již v rozhodnutí *Lloyd vs. Google I*. V často opomíjené oblasti kybernetické bezpečnosti jsem tak představil dva případy, ve kterých kontext dle mého soudu hraje hlavní roli. Oblast kybernetické (i obecně vzaté) bezpečnosti je pro ilustraci tohoto fenoménu zvláště vhodná, neboť zde dochází ke kolizi práva na soukromí a ochranu osobních údajů s bezpečností jakožto veřejným statkem, což může ve specifických případech připravit půdu pro legitimizaci zásahů do informačního soukromí. U obou případů tak nakonec docházím k závěru, že tyto zásahy nenaplňují požadavek společenské škodlivosti, jejich pozitivní účinek pro distributivní i nedistributivní práva převažuje nad negativy a potvrzují tím sílu kontextu jako limitace výše zmíněného práva.

Lloyd vs Google or does a Plain Breach of a Person's Informational Privacy have Harmful Consequences, and must such a Breach always be Harmful?

Jakub Vostoupal (https://orcid.org/0000-0002-1669-9931)

Abstract: The article discusses the latest decisions of the English courts in the case of Lloyd v. Google. The first section is devoted to a brief introduction to the issue of privacy and related concepts, including a brief discussion of the potential consequences of a breach of privacy. After laying at least a basic theoretical framework, the article critically analyses all of the courts' decisions, focusing on answering the question "does a plain breach of a person's informational privacy have harmful consequences". The author concludes by focusing on the "context" argument as presented by the first-instance court and presents two scenarios that have the potential to support this argument.

Keywords: Carna Botnet Privacy, data protection, invasion of privacy, cybersecurity, Carna Botnet