Transformace pojmu soukromí na počátku třetího milénia*

Zdeněk Kühn**

Transformation of the concept of privacy at the outset of the third millennium

Summary: *The Internet has substantially changed the way we conceive human conduct; it has fundamentally altered our chance to control the spreading of information and the impact of human behaviour in the course of time. The paper analyzes the transforming modes of privacy invasion over centuries. It explains the transformation of invasion of privacy in the Internet era and the transformation of the concept of privacy itself. Next, it attempts to show that the protection of privacy by public law against giant providers of telecommunication and data services and corporations, such as Google and Facebook, is relevant. Efficient regulation should be exercised by the law of the European Union because autonomous domestic regulations would endanger the free movement of services across the EU; moreover, separate national regulation in fighting global giants like Google could hardly be successful. On the other hand, not much sense can be seen in public law or even European regulation of activities that are local by nature, such as CCTV systems in private buildings, which are to serve for the protection of property by the CCTV system operators. The author explains that regulation under public law becomes toothless in such cases, sanctioning becomes selective and essentially random. In addition, such regulation has a potential to further alienate the law from its ordinary recipients.*

Keywords: *Internet, privacy, Google, CCTV systems*

Smyslem tohoto článku je poukázat na některé teoretické i praktické dopady masového průniku nových technologií ve spojení s internetem do našeho života. Těmito novými technologiemi jsou všudypřítomné chytré telefony a kamery, ať již pevně umístěné na domech nebo v automobilech, natáčející průběh jízdy, či nejnověji kamery umístěné v dronech či podobných zařízeních nebo zatím spíše výjimečný Google Glass (kamerka instalovaná přímo v brýlích).[1] U řady těchto zařízení je uživatel schopen dát natočený obsah v řádu sekund na internet. Záznamy jsou nezřídka pořizovány právě za účelem toho, aby byly následně přeneseny na nejrůznější webové služby. I u těch kamer, kde to primárně neplatí (typicky bezpečnostní kamery chránící dům, byt či jiný majetek proti vandalismu, vloupání nebo krádeži), budou okamžiky páchání trestné činnosti umisťovány na internet, typicky na sociální sítě, v zájmu vypátrání pachatele.[2]

Podobné obrazové či audiovizuální záznamy samotné jsou však jen malým střípkem v mozaice naprosto zásadní proměny pojmu soukromí na počátku třetího tisíciletí. Samy o sobě, ponechány někde na izolovaných nosičích dat, nebo sice umístěné na web, ovšem v podstatě nedohledatelné, by tyto záznamy zásadním způsobem ochranu soukromí neproměnily. Mým základním argumentem je, že ve vztahu k ochraně soukromí představuje internet – a zejména vyhledávače typu Google a služby typu Facebook či Twitter – nejen kvalitativní nárůst veřejně dostupných informací zasahujících do soukromí

* Tento článek byl zpracován v rámci projektu Grantové agentury ČR reg. č. 16-22016S „Právní jednání a odpovědnost právnických osob".

** Autor je docentem na Právnické fakultě Univerzity Karlovy a soudcem Nejvyššího správního soudu (NSS). Byl soudcem zpravodajem kauzy *Ryneš* na NSS, v tomto textu mnohokráte zmiňované. Veškeré zde vyslovené názory jsou názory autora tohoto článku, nikoliv institucí, na kterých působí. Autor děkuje účastníkům konference v Dubrovniku roku 2016 za jejich cenné připomínky, jmenovitě zejména Tamaře Čapetě a Dericku Wyattovi. Za další podněty a nápady pak děkuje Karlu Beranovi a Václavu Janečkovi. Veškeré omyly a nepřesnosti tohoto článku jdou samozřejmě na vrub jeho autora. E-mail: kuhnz@prf.cuni.cz.

1 Google, tvůrce Google Glass, se snaží připodobnit tento produkt mobilním chytrým telefonům – srov. https://plus.google.com/+GoogleGlass/posts/axcPPGjVFrb (navštíveno 21. 7. 2016). V každém případě se doposud jedná jen o prototyp a lze čekat na jeho další vývoj.

2 Viz typicky věc řešená NSS v rozsudku ze dne 8. 6. 2016, čj. 3 As 118/2015 – 34, kauza *e-kolo.cz*. Zde majitel prodejny elektrických kol umístil na Facebook fotografii zloděje, jehož se mu díky tomu podařilo následně vypátrat.

dotčených osob, ale zejména proměnu paradigmatu vnímání soukromí a jeho ochrany.

Samotný význam právního pojmu ochrany soukromí zůstává předmětem mnoha definic a chápání. Pro účely tohoto článku je relevantní především jeden aspekt ochrany soukromí, možnost jednotlivce rozhodovat o tom, které informace z jeho života se stanou veřejnými, respektive budou dále šířeny již bez toho, aby měl jednotlivec možnost toto šíření nějak ovlivnit. Jak v průkopnickém článku k tomuto tématu lapidárně shrnul Frederick Schauer, ochrana soukromí předpokládá rovněž „právo kontrolovat fakta o svém vlastním životě".[3] Podobně to chápe R. Posner ve své ekonomické analýze práva. Zdůrazňuje totiž aspekty práva na soukromí týkající se kontroly jednotlivců nad šířením informací o sobě samých.[4]

Je nesporné, že internet zcela změnil podobu lidského jednání a zcela změnil možnost kontroly nad šířením informací a dopady lidského jednání v průběhu času. Zaměstnavatel dnes kupříkladu zjistí jednoduchým dotazem do internetového vyhledávacího systému o zájemci o zaměstnání tolik informací, které by ještě na sklonku 90. let minulého století musel vyhledávat za velké prostředky detektivní agenturou. Jde sice často o informace, které byly vždy součástí veřejné sféry, dramaticky se ale mění jejich dostupnost, a to s ohledem na nové médium, které tyto informace obsahuje. Na konci 90. let minulého století sice již existoval internet, neobsahoval však zdaleka tolik informací, jako je tomu dnes. Především však neexistoval sofistikovaný vyhledávací systém typu Google. Google a podobné vyhledávače během několika sekund na základě vhodně položeného dotazu zjistí údaje (texty, obrázky, videa atp.), které bychom v minulém století zjišťovali soustavným sledováním dotčené osoby, vyslýcháním známých atd.[5] Snadnost, s jakou lze pořídit informace určitého druhu, byť zdaleka ne vždy pravdivé, nemá v lidské historii paralelu.

Nejde však jen o „nesnesitelnou lehkost zjišťování informací". Sbírání dat totiž bylo vždy omezeno přirozenou lidskou vlastností – zapomínáním. Internet nezapomíná. Skutečnost, že někdo podepsal nějakou petici, natočil pornofilm či zbil svého spolužáka, v něm zůstává navěky. Navěky v něm ostatně zůstává i onen pornofilm, pokud jej již někdo na internet umístil.

V tomto článku se pokusím vysvětlit proměnu zásahů do soukromí v době internetové a proměnu pojmu soukromí. Budu argumentovat, že veřejnoprávní ochrana soukromí ze strany práva Evropské unie vůči velkým poskytovatelům telekomunikačních a datových služeb či korporacím typu Google a Facebook je namístě. Odlišné národní regulace by ohrožovaly volný pohyb služeb napříč Evropskou unií, navíc samotná regulace jednotlivých národních států ve vztahu k aktivitám gigantů typu Google bývá jen málokdy dostatečně účinná. Naproti tomu ale budu argumentovat ve prospěch teze, že veřejnoprávní a tím méně evropská (veřejnoprávní) regulace svou povahou lokálních aktivit typu monitorovacích kamer na soukromých domech, sloužících k ochraně majetku provozovatelů těchto kamerových systémů, smysl nedává. Veřejnoprávní regulace těchto aktivit je totiž jednak bezzubá, jednak je jejich postih s ohledem na nespočet zpracovatelů dat z povahy věci selektivní a ve své podstatě náhodný. Regulace má tak potenciál ještě více odcizit právo jeho běžným adresátům.

Diametrálně odlišná kvalita zásahů do soukromí v době před internetem a v době internetové

Právo na soukromí prodělává v posledních dvou dekádách zásadní proměnu. Tu je možno popsat jako kvantitativní, ale též kvalitativní. Současně je patrné, že samotný pojem soukromí prodělává zásadní transformaci.[6]

Internet přináší nepochybně kvalitativní proměnu sdělování a sdílení informací. Není to samozřejmě proměna historicky první. První zásadní změnou byl knihtisk a snadnost šíření do té doby luxusní komodity – rukopisů. Snadnost sdílení psaného slova, ale i nejrůznějších karikatur v knihách či pamfletech zásadním způsobem ovlivnila lidskou historii (jejich produktem byla i Velká francouzská revoluce v roce 1789). Druhou zásadní proměnu přinesly vynálezy devatenáctého a dvacátého století – fotografie a posléze elektronická masmédia (rozhlas, televize). Internet tak přináší třetí a podle mne zatím největší proměnu soukromí.

Již na prvý pohled jsou patrné kvalitativní rozdíly mezi typickým narušováním

[3] Schauer, F. Internet Privacy and the Public-Private Distinction, 38 Jurimetrics 555 (1998), s. 556.
[4] Posner, R. Privacy, In: Newman, P. (ed.) The New Palgrave Dictionary of Economics and the Law 3, Palgrave Macmillan 2004, s. 103 a 104.
[5] K systému Google srov. vynikající článek Tene, O. What Google Knows: Privacy and Internet Search Engines, *Utah Law Review,* 2008, s. 1433 (dále jen „Tene, What Google Knows").
[6] Srov. např. Schauer, *op. cit.,* s. 557 a násl.

soukromí v době internetové a v době před internetem.[7] Zásahy do soukromí v době před internetem a Googlem byly obvykle fyzické: domovní prohlídka, narušování listovního tajemství, sledování osoby, odposlouchávání, atd. Jejich aktérem byla obvykle vláda, policie či jiní státní aktéři nebo klasická média tištěná či elektronická (rozhlas, televize). Takovéto zásahy byly zpravidla výjimečné, každý zásah sám o sobě byl však pro dotčeného velmi citelný. Obvykle byly také relativně snadno zjistitelné.

V době internetové je tomu naopak: postižený o těchto zásazích nezřídka vůbec neví, jsou velmi časté, každý jednotlivý zásah sám o sobě je však obvykle jen málo intenzivní. Intenzivní zásah vzniká zpravidla kombinací dat. Nejtypičtěji jsou to stopy, které my sami nebo někdo třetí o nás zanechává na internetu (naše vlastní projevy na sociálních sítích a diskusních webech nebo výroky někoho, kdo se za nás vydává, zprávy o nás, a to z jakýchkoliv seriózních či neseriózních zdrojů, fotografie a videa, které my sami nebo kdokoliv třetí na web umisťuje, slovní ataky a výmysly o určité osobě na diskusních serverech atd.). Méně známým zásahem jsou údaje ve vyhledávači Google, který shromažďuje na léta zpět jednotlivá vyhledávaná hesla z jedné IP adresy. Z doby před internetem k tomu snad lze přirovnat pokradmé pomlouvání osoby, ovšem okruh potenciálních adresátů byl drasticky odlišný.

Aktérem typického zásahu doby internetové je zřídkakdy státní moc či klasická média. Pokud tu již nějak stát figuruje, tak proto, že se úspěšně či neúspěšně domáháme jeho ochrany proti takovýmto zásahům do soukromí. V drtivé většině případů však takovéto zásahy do našeho soukromí jednoduše ignorujeme, nebo o nich dokonce vůbec nevíme.

Naše stopy na internetu

Podívejme se nejprve na naše stopy, které zanecháváme během používání internetu. Jednotliví provozovatelé komerčních internetových stránek tak např. využitím tzv. *cookies* shromažďují informace o počítači, z něhož je na danou stránku přistupováno.[8] Toho si běžný uživatel internetu všimne již jen proto, že např. největší internetový prodejce knih Amazon nám při jakékoliv další návštěvě nabízí právě ty produkty, které jsme při předchozích návštěvách zkoumali, případně jsou nám nabízeny reklamy, které nějak souvisí se stránkami, které jsme si předtím prohlíželi (pokud jsem například hledal zájezd do Tuniska, v následujících týdnech se mi budou zobrazovat reklamy nabízející pobyt v Tunisku).

Počítač, ze kterého se na internetovou stránku přistupuje, tak přestává být pro tuto stránku anonymní. Naopak, internetová stránka mu nabídne např. horory, DVD s dětskými pohádkami, ženské romány nebo třebas právněfilozofickou četbu právě proto, že při předchozím přístupu se na tyto produkty uživatel daného počítače díval (nebo je dokonce koupil). Protože cookies umožňují kombinací dat identifikovat počítač, ze kterého se na určitou stránku přistupuje, lze mít za to, že jsou v zásadě chráněným osobním údajem.[9]

Ostatně na cookies výslovně pamatuje i obecné nařízení o ochraně osobních údajů z roku 2016,[10] podle jehož preambule, bodu 30 „[f]yzickým osobám mohou být přiřazeny síťové identifikátory, které využívají jejich zařízení, aplikace, nástroje a protokoly, jako například adresy internetového protokolu či identifikátory cookies, nebo jiné identifikátory, jako jsou štítky pro identifikaci na základě rádiové frekvence. Tímto způsobem mohou být zanechány stopy, které mohou být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použity k profilování fyzických osob a k jejich identifikaci."

Obdobně fenomén prvých dvou dekád 21. století Google zcela změnil naši práci s internetem. Před nástupem inteligentního vyhledávače představoval internet džungli informací, v níž se ta relevantní dala vyhledat jen s velkými problémy. Skutečnost, že se určitá informace objevila na internetu, sama

7 Srov. k dalšímu např. Cate, F. H. Principles of Internet Privacy, 32 Connecticut Law Review 877 (1999–2000), s. 877–878.

8 Takto funkci cookies vysvětluje Google: „*Soubor cookie je malý soubor obsahující řetězec znaků, který je při návštěvě webové stránky odeslán do vašeho počítače. Při další návštěvě soubor cookie webové stránce umožní rozpoznat váš prohlížeč. Pomocí souborů cookie lze uložit uživatelská nastavení a další údaje. Svůj prohlížeč můžete nastavit tak, aby všechny soubory cookie odmítal nebo aby hlásil, když se vám soubor cookie někdo pokusí zaslat. Některé funkce nebo služby na webových stránkách však bez souborů cookie nemusí fungovat správně. Na ostatních platformách, kde soubory cookie nejsou dostupné nebo je nelze použít, například v Inzertním ID dostupném v mobilních zařízeních Android, jsou k obdobným účelům používány jiné technologie.*" Viz Google Ochrana soukromí a smluvní podmínky, http://www.google.com/intl/cs/policies/privacy/key-terms/#toc-terms-cookie (navštíveno 29. 6. 2016).

9 Pro názor, že cookies jsou osobním údajem, srov. již Tene, What Google Knows (cit. v pozn. č. 5), s. 1448. V češtině např. Mišek, J. Souhlas se zpracováním osobních údajů za časů internetu, *Revue pro právo a technologie*, č. 9/2014, s. 3 a násl., ke cookies zejména s. 55–66 (s jednoznačným závěrem, že cookies v zásadě představují chráněné osobní údaje).

10 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 (obecné nařízení o ochraně osobních údajů) Úř. Věst. L 119, 4. 5. 2016, s. 1–88.

o sobě mnoho neznamenala, neboť danou informaci bylo téměř nemožné dohledat. Po nástupu Google může informace na internetu vyhledávat kdokoliv, i naprostý počítačový ignorant. Při zadání jména určité osoby nám vyjedou nejen relevantní textové záznamy, ale rovněž fotografie a videa (byť se ne vždy budou k hledané osobě opravdu vztahovat).

Google a jiné inteligentní vyhledávače ovšem rovněž pečlivě shromažďují naše stopy, které zanecháváme ve vyhledávacím poli. Na prvý pohled může být tato skutečnost snadno podceněna, protože z toho, že jsme dnes večer vyhledávali např. levný hotel ve Vídni, nelze mnoho dovodit. Citlivým problémem ale samozřejmě není jedna prostá informace z dnešního večera, ale spíše kombinace desetitisíců informací k jednomu počítači, které vyhledávač shromáždí za delší dobu jeho užívání. Z hlediska práva může být podstatná již jen otázka, za jak dlouhou dobu mohou být tato data uložena, jak mají být chráněna před zneužitím, na základě jakých procedur mají být vydána státním orgánům atd.

V právě uvedeném příkladu samozřejmě platí, že systém identifikuje nikoliv individuálního člověka, ale IP adresu počítače, z něhož je na danou stránku přistupováno.[11] IP adresa „je numerickým či alfanumerickým řetězcem, ze kterého lze identifikovat konkrétní počítač".[12] Identitu uživatele počítače lze zjistit především dožádáním u jeho poskytovatele internetu. Prakticky všechny světové vyhledávače však již dnes disponují snadnou možností, jak uživatele IP adresy identifikovat, aniž by musel být poskytovatel internetu vůbec kontaktován. V prvé řadě je to prostřednictvím e-mailových schránek poskytovaných společností, která provozuje daný vyhledávač, případně jiných jimi nabízených služeb, které individualizují osobu uživatele. Google nabízí svůj Gmail, resp. bloggerské konto blogspot.com, Seznam stejnojmennou e-mailovou schránku atd. Kombinací údajů o uživateli dané služby s IP adresou, ze které na internet přistupuje, tak lze snadno zjistit identitu uživatele IP adresy (byť věc samozřejmě komplikuje to, že z jedné IP adresy na internet často, třebas v rodinách, přistupuje vícero uživatelů).

Soudní dvůr EU již v roce 2011 učinil závěr, že IP adresy internetových uživatelů jsou chráněnými osobními údaji, neboť umožňují přesně určit totožnost těchto uživatelů, a to v situaci, kdy shromažďování a identifikování IP adres internetových uživatelů bylo prováděno poskytovateli služby připojení k internetu.[13] O pět let později Soudní dvůr svůj závěr dále rozvedl a upozornil, že „dynamická IP adresa, kterou poskytovatel online mediálních služeb uchovává v souvislosti s přístupem osoby na internetovou stránku, kterou tento poskytovatel zpřístupnil veřejnosti, pro uvedeného poskytovatele představuje osobní údaj ve smyslu [čl. 2 písm. a) směrnice 95/46],[14] pokud má k dispozici právní prostředky, které mu umožňují nechat identifikovat subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu."[15]

Co je pro právě uváděné příklady typické, je informační asymetrie mezi běžným uživatelem internetu a provozovatelem internetové adresy ohledně využití informací o návštěvě těchto stránek určitým počítačem *(cookies)*, resp. skutečnosti, že provozovatelé služeb Google nebo Seznam shromažďují a ukládají vyhledávané údaje směřované z určité IP adresy. O zásazích do práva na soukromí tak daná osoba zpravidla vůbec neví.[16] I když snad o nich tuší, nemá naprosto žádnou, a to ani přibližnou představu, jaké povahy určitý zásah může být, ostatně již jen s ohledem na obtížnost porozumění komplikovaným technickým jevům souvisejícím s fungováním internetu.[17]

V této souvislosti je třeba si uvědomit, že ten, kdo informace vyhledává, zpracovává a archivuje, je sice z technického hlediska „vyhledávač" jako jakási umělá inteligence, ta však ve skutečnosti žádným opravdovým subjektem není. Oním subjektem je typicky právnická osoba – obchodní korporace,[18] která tento „vyhledávač" používá jako svůj „výrobní nástroj". Asymetrie, která existuje

11 Omer Tene IP adresu přirovnává k adrese bytu. Tene, *op. cit.*, s. 1445. Poněkud komplikovanější je tato identifikace tam, kde se nejedná o IP adresu statickou, ale dynamickou, tedy v průběhu doby se proměňující. I tam ovšem identifikace počítače možná je, jakkoliv je komplikovanější. Jak říká Tene, dynamická IP adresa je srovnatelná s měnícími se hotelovými adresami jednoho obchodníka na cestách. Srov. tamtéž, s. 1446.

12 Otevřel, P. Je IP adresa osobním údajem?, Právo IT, 26. 2. 2008, http://www.pravoit.cz/article/je-ip-adresa-osobnim-udajem (navštíveno 28. 6. 2016). V češtině srov. též Mišek, J. – Harašta, J. IP adresy v kybernetické bezpečnosti, *Revue pro právo a technologie*, č. 12/2015, s. 21 a násl.

13 Rozsudek ze dne 24. listopadu 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, bod 51.

14 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. 1995, L 281, s. 31; Zvl. vyd. 13/15, s. 355).

15 Rozsudek ze dne 19. října 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, bod 49.

16 Informační asymetrii mezi společností Google a uživatelem prokazuje skutečnost, že např. 90 % uživatelů Google.com v USA vůbec netuší, že se o nich shromažďují data. Viz Tene, *op. cit.*, s. 1455. Pochybuji, že pro informovanost českých uživatelů vyhledávače Google.cz nebo Seznam.cz by byl případný průzkum lichotivější.

17 Schwartz, P. M. Internet Privacy and the State, 32 Connecticut Law Review 815 (1999–2000), s. 822.

18 Srov. k tomu obecně Beran, K. *Pojem osoby v právu: (osoba, morální osoba, právnická osoba)*, 1. vyd. Praha: Leges, 2012.

mezi těmito korporacemi a osobami, o nichž jsou informace shromažďovány, není jen informační. Faktická moc těchto korporací je v této oblasti nesrovnatelně větší než u klasických veřejnoprávních korporací,[19] jejichž prostředky se možnostem těchto korporací mohou jen stěží rovnat. Státní orgány, které v minulosti představovaly z hlediska soukromí největší hrozbu, představují nyní zřejmě jedinou instituci, která může ochranu soukromí před těmito korporacemi alespoň zčásti garantovat.

Kvantitativní a kvalitativní proměna práva na soukromí

Jak jsem již uvedl shora, změnou kvantitativní je především skutečnost, že počet zásahů do soukromí v době internetové dramaticky stoupá. Jde často o různé invektivy a smyšlenky o určité osobě v internetových diskusích, přičemž s ohledem na početnost těchto invektiv, nepravd i naprostých nesmyslů se ztrácí možnost jednotlivce efektivně se proti takovýmto zásahům bránit soukromoprávní cestou. Je nicméně pravdou, že pomluva např. v diskusi na obskurním blogu má nepoměrně menší dosah než pomluva osoby v hlavním vysílacím čase ve zpravodajství v celoplošné televizi. Problémem se internetové pomluvy a nactiutrhání mohou stát teprve v okamžiku, kdy jich bude příliš mnoho a kdy je běžnému uživateli internetu nabídne například vyhledávač na jedné z prvních stránek jako informaci o dané osobě.

S tím souvisí problém tzv. „našeptavače", což je dnes velmi populární nástroj vyhledávacích systémů. Jak vysvětluje P. Mališ, systém Google suggest „nabízí uživatelům po zadání úvodních několika písmen vyhledávaného pojmu nebo slovního spojení v reálném čase pod polem pro zadání hledaného výrazu seznam deseti nejčastěji vyhledávaným výrazů, odpovídajících uživatelem zadaným písmenům."[20] Může se tak např. stát, že u určité vyhledávané osoby Google či jiný vyhledávač „našeptává" určitou informaci, která nemusí být pro vyhledávanou osobu vůbec lichotivá.[21]

Celá věc se ještě komplikuje tím, že význam tradičních elektronických médií v tomto století evidentně dramaticky klesá a naopak význam internetových informací dramaticky stoupá, což samozřejmě nemusí být vždy ku prospěchu věci.

Změna kvalitativní je ještě významnější. Díky novým technologiím se dnes totiž mohou dít zásahy do soukromí, které by ještě před deseti lety nebyly myslitelné. Díky internetovým vyhledávačům jsou dnes zdi našich domů doslova „průhledné". Jak jsem ukázal výše, databáze internetových vyhledávačů nabízejí neuvěřitelné množství komerčně velmi lákavých dat.

V neposlední řadě bychom neměli přehlédnout též změnu samotného chápání soukromí. Ochrana soukromí je a vždy byla pojmem kontextuálním. Proměňuje se s proměňujícím se chápáním společenských hodnot. Podejme si několik příkladů.

Elektronická pošta např. v podstatě vykrádá soukromí člověka. Dnes je již standardem na e-maily reagovat bezodkladně, odpověď v řádu dnů se považuje přinejmenším za nezvyklou. Rovněž mobilní telekomunikace radikálně změnila naše chápání toho, kdy je určitá osoba dosažitelná.[22] Asi největší změny se pak dějí s nejmladší „facebookovou" generací, což u nás víceméně odpovídá lidem narozeným po roce 1989. Množství informací, které jsou uživatelé společenských sítí ochotni o sobě veřejně uvést, a zpřístupnit je tak třetím osobám, je pozoruhodně velké. Takovéto informace zpětně z internetu lze odstranit jen s potížemi.[23] Vyhledávače uchovávají též předchozí verze internetových stránek (třebaže tyto byly později změněny).[24] Obsah jednotlivých internetových stránek je navíc často kopírován a přebírán na internetové stránky jiné, nad kterými ovšem již uživatel stránky původní nemá naprosto žádnou kontrolu. Pokud někdo v době svých studií

19 K tomu srov. Beran, K. *Právnické osoby veřejného práva: Veřejnoprávní subjektivita.* 1. vyd. Praha: Linde, 2006.

20 Obecně více Mališ, P. Soudní spory z našeptávače Google suggest, IT právo, 1. 3. 2010, http://www.pravoit.cz/article/soudni-spory-z-naseptavace-google-suggest (navštíveno 30. 5. 2016). Z evropských soudů se k tomuto tématu doposud vyjádřil např. německý Spolkový soudní dvůr, a to v rozhodnutí ze dne 25. 6. 2013, sp. zn. VI ZR 269/12 (tzv. kauza *Scientologie,* v níž si žalobce stěžoval, že Google vyhledávač u jeho jména automaticky nabízí též slova „podvod" a „scientologie"). Spolkový soudní dvůr dovodil, že podobným způsobem poškození lidé mohou provozovatele vyhledávače zavázat k odstranění nabídky sporné kombinace. V češtině srov. Myška, M. – Harašta, J. Odpovědnost Google za dokončování vyhledávacích dotazů, *Revue pro právo a technologie,* č. 7, 2013, s. 33.

21 Pokud se například podíváme na naše dva poslední prezidenty, uvidíme, že našeptavač u toho předposledního napovídá, že „krade" (čímž navádí ke slavnému videozáznamu „krádeže" chilského pera), zatímco u stávajícího prezidenta našeptává výrazy spojené s požíváním alkoholu (a navede nás k neméně slavnému videu spojenému s kauzou „viróza").

22 Může pak být ovšem písemné podání vskutku automaticky srovnáváno s podáním elektronickým? Pokud ano, mělo by to důsledky např. též pro otázku, kdy je určité podání doručeno správnímu úřadu. Pro skeptičtější pohled na toto zdánlivě mechanické srovnání viz rozsudek NSS ze dne 16. prosince 2010, čj. 1 Ans 5/2010-171, jehož soudcem-zpravodajem byl autor tohoto článku.

23 Na mysl se nám může vkrást případ bývalé ministryně spravedlnosti D. Kovářové, která na svém blogu ještě ve své předchozí funkci hodnotila sama sebe sexuálně explicitními výrazy. V situaci, kdy se pro ni staly nevhodnými z důvodu nové „seriózní" funkce ministryně spravedlnosti, však již tyto informace nebyly z internetu odstranitelné, třebaže ministryně sama své webové stránky upravila.

24 Nutno nicméně podotknout, že Facebook neumožňuje svému internetovému rivalovi Google hledat uvnitř jeho stránek.

na internet umístí lechtivé informace o svém životě, nemá v podstatě možnost vzít je zpět, třebaže uběhne dlouhá doba a z původního extravagantního mladíka se stává seriózní úředník.

Výhody regulace aktivit přeshraničního významu právními předpisy Evropské unie

Všechny tyto jevy probíhaly po značnou část své existence bez jakékoliv veřejnoprávní ingerence. Dochází k nim nezávisle na státu a jeho orgánech, motorem těchto jevů jsou komerční zájmy jednotlivých provozovatelů internetových portálů. Stát tu původně bezradně stál jen jako nečinný přihlížející. Podnět k veřejnoprávní regulaci dala na prvním místě skutečnost, že nijak neregulované zpracovávání informací velkými korporacemi typu Google či Facebook může dramaticky zasáhnout do práv lidí. Současně ovšem data generovaná způsobem shora naznačeným jsou velmi lákavým zdrojem informací pro jeho policejní a jiné orgány. V zájmu veřejné moci proto není generování těchto dat a metadat znemožnit, ale spíše jim dát pevná pravidla. V posledních letech na tyto jevy veřejná moc reaguje. Snaží se stanovit určitá pravidla a omezení, za kterých mohou být data týkající se přístupu na internet uložena v databázích.

S ohledem na to, že internet nezná hranice, a velké korporace jako Google či Facebook operují globálně, se v Evropě z povahy věci nabízí na prvém místě regulace právem Evropské unie.

Listina základních práv EU z roku 2000, byť pouze o dekádu mladší než česká Listina základních práv a svobod, již na tyto otázky pamatuje a upravuje v ústavněprávní rovině otázky zde naznačené celkem detailně. Podle čl. 8 Listiny EU má každý právo na ochranu osobních údajů, které se ho týkají (odst. 1). „Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu" (odst. 2).

Na poli evropského práva je pro realizaci tohoto práva důležité zejména obecné nařízení o ochraně osobních údajů z roku 2016,[25] které od roku 2018 nahradí současnou směrnici 95/46. Nařízení je obecně založeno na předpokladu, že shromažďování údajů zásadně předpokládá souhlas dotčených uživatelů[26] (samozřejmě vedle řady výjimek). Tento souhlas uživatelé tradičně dávali zaškrtnutím políčka, podle něhož souhlasí s všeobecnými obchodními podmínkami provozovatele daného portálu, aniž by ovšem tyto obchodní podmínky drtivá většina z nich četla.[27] Takovýto souhlas je tedy naprosto fiktivní, což nevyřeší ani novější praxe tím, že na uživatele bude vyskakovat celá plejáda různých upozornění a varování. Ovšem i těch několik málo uživatelů, kteří další informace čtou, záhy zjistí, že nemají alternativu, neboť podmínky jiných stránek jsou naprosto srovnatelné, ne-li dokonce horší.

Veřejnoprávní regulaci shromažďování informací poskytovateli veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí právními předpisy Evropské unie je nutno považovat za rozumnou. Poskytovatelé internetu, telekomunikačních služeb, nejrůznější vyhledávače atd. operují napříč jednotlivými národními státy. Rozdílná veřejnoprávní regulace by tedy vskutku představovala překážku volnému pohybu poskytování těchto služeb napříč Unií. Například rozdílná regulace „práva být zapomenut" v internetových vyhledávačích napříč Evropou by skutečně omezovala svobodu pohybu služeb a současně stavěla občany států EU do nerovného postavení.[28] Navíc je

[25] Cit. v poznámce č. 10 shora. Vedle toho lze zmínit ještě Směrnici o soukromí a elektronických komunikacích z roku 2002 (Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací) a do roku 2014 též Směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí. Směrnici 2006/24 ovšem zrušil Soudní dvůr EU pro porušení zásady proporcionality ve vztahu k ochraně osobních údajů rozsudkem ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12 *Digital Rights Ireland a Seitlinger a další* (ECLI:EU:C:2014:238).

[26] K tomu tématu v češtině obecně srov. zejména Míšek, J. Souhlas se zpracováním osobních údajů za časů internetu, *Revue pro právo a technologie*, č. 9, 2014, s. 3 a násl.

[27] Srov. k tomu též bod 32 preambule nařízení: „*Souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení. Mohlo by se například jednat o zaškrtnutí políčka při návštěvě internetové stránky, volbu technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání, které v této souvislosti jasně signalizuje souhlas subjektu údajů s navrhovaným zpracováním jeho osobních údajů. Mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za souhlas. Souhlas by se měl vztahovat na veškeré činnosti zpracování prováděné pro stejný účel nebo stejné účely. Jestliže má zpracování několik účelů, měl by být souhlas udělen pro všechny. Má-li subjekt údajů vyjádřit souhlas na základě žádosti podané elektronickými prostředky, musí být žádost jasná a stručná a nesmí zbytečně narušit využívání služby, pro kterou je souhlas dáván.*"

[28] Srov. rozsudek Soudního dvora *Google Spain*, C-131/12, ECLI:EU:C:2014:317. V něm Soudní dvůr poprvé (kontroverzně) zformuloval evropský princip „práva být zapomenut". Ve vztahu ke směrnici 95/46/ES, předchůdkyni obecného nařízení o ochraně osobních údajů, uvedl, že činnost vyhledávače spočívající ve vyhledávání informací

třeba si uvědomit, že ve vztahu ke gigantům typu Vodafone, Telefónica, T-Mobile, Orange, Facebook nebo Google má smysl především společná regulace evropská, nikoliv regulace malého státu typu České republiky.

Regulace ochrany soukromí jako další byrokratická zátěž pro občany?

Co však podle mého názoru smysl moc nedává, je celoevropská regulace i takových aktivit a zveřejňování osobních údajů, které globální či celoevropský dopad nemají. Provozování statické bezpečnostní kamery pod střechou rodinného domu a ukládání takto pořízených záběrů na pevný disk je aktivita bytostně lokální. Ani skutečnost, že provozovatel kamerového systému záběry eventuálně zveřejní na internetu (typicky proto, aby se dopátral identity pachatele trestné činnosti), bez dalšího neznamená, že by mělo jít o aktivitu hodnou pozornosti práva Evropské unie. Lze si jen obtížně představit, že by, slovy obecného nařízení o ochraně osobních údajů z roku 2016, právě rozdíly v úrovni ochrany osobních údajů při těchto aktivitách mohly bránit volnému pohybu osobních údajů v rámci Unie.[29]

Jedna věc je pochopitelně ochrana osobních údajů při zpracovávání informací internetovým vyhledávačem, jejíž rozdílná regulace napříč Unií by skutečně mohla negativně ovlivnit volný pohyb služeb, případně shromažďování dat poskytovateli komunikačních služeb (poskytovatelé internetu, telefonní operátoři atp.). Věc zcela jiná je provozování domácího kamerového systému[30] či zveřejnění fotografie z takovéhoto systému na Facebooku.[31]

Regulace všech těchto aktivit právem EU znamená povinnost členských států do všech těchto oblastí zapojit veřejné právo, dohledovou činnost úřadů na ochranu osobních údajů s veřejnoprávními sankcemi za porušení práva.[32] Členské státy tak nemají možnost dospět k řešení, že alespoň některé z těchto čistě *lokálních* jevů si s ohledem na lokální specifika buď vůbec veřejnoprávní regulaci nezaslouží (a postačí tedy ochrana prostředky práva soukromého), anebo i když by snad byla i na některá takováto jednání veřejnoprávní regulace užitečná, nastavit alespoň svá pravidla, odlišná od požadavků práva EU.

V rozhodnutí *Ryneš* měl Soudní dvůr Evropské unie šanci deklarovat, že část těchto problémů vskutku nepodléhá právu EU. Mohl je totiž podřadit pod poměrně neurčitě formulovanou výjimku z působnosti tehdejší směrnice 95/46 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. K tomu byl Soudní dvůr dokonce předkládajícím Nejvyšším správním soudem přímo vyzván.[33]

Soudní dvůr nicméně tuto šanci nevyužil. Namísto toho postupoval poměrně formalisticky, totiž kvazideduktivním postupem stylu: smyslem směrnice 95/46 je zajištění vysoké úrovně ochrany základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů, proto => výjimky z ochrany osobních údajů musí být interpretovány restriktivně, proto => výjimka zpracování údajů „pro výkon výlučně osobních či domácích činností" ve smyslu čl. 3 odst. 2 druhé odrážky uvedené směrnice není aplikovatelná na soukromé kamerové systémy zabírající část veřejného prostranství.[34]

Protože Soudní dvůr Evropské unie postupoval formalisticky, tedy zůstal jen u zdánlivě jazykového rozboru textu směrnice, opepřeného obdobně formálním lidskoprávním

zveřejněných nebo umístěných na internetu třetími osobami, v jejich automatickém indexování, v jejich dočasném ukládání a konečně v jejich poskytování uživatelům internetu v určitém preferenčním pořadí musí být kvalifikována jako „zpracování osobních údajů" ve smyslu uvedeného čl. 2 písm. b), pokud uvedené informace obsahují osobní údaje. Provozovatel uvedeného vyhledávače musí být považován za „správce" odpovědného za dané zpracování ve smyslu uvedeného čl. 2 písm. d). Provozovatel vyhledávače má za určitých podmínek povinnost vymazat ze zobrazeného seznamu výsledků vyhledávání provedeného na základě jména osoby odkazy na webové stránky zveřejněné třetími osobami a obsahující informace týkající se této osoby rovněž v případě, že toto jméno nebo tyto informace nebyly předtím nebo současně vymazány z uvedených webových stránek, a to případně i tehdy, jestliže je jejich zveřejnění na uvedených stránkách samo o sobě v souladu se zákonem. Další konkretizace podmínek rozsudkem je však velmi kostrbatá a v praxi do značné míry obtížně aplikovatelná. Největší poskytovatelé vyhledávacích služeb se nicméně snaží rozsudkem *Google Spain* řídit. Kauza samotná vyvolala mimořádnou pozornost právní vědy. Čtenáře odkazuji např. na článek Dana Jerkera B. Svantessona The Google Spain case: Part of a harmful trend of jurisdictional overreach, EUI Working Papers, RSCAS 2015/45, který se snaží ukázat na jeden z mnoha deficitů rozsudku, totiž nedomyšlenou otázku působnosti práva EU na tyto svou povahou globální věci.

29 Bod 9 preambule obecného nařízení o ochraně osobních údajů z roku 2016.

30 Rozsudek Soudního dvora ve věci *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, resp. na něj navazující rozsudek NSS ze dne ze dne 25. února 2015, čj. 1 As 113/2012-133, č. 3222/2015 Sb. NSS.

31 Věc řešená NSS v kauze *e-kolo.cz*, cit. v pozn. č. 2 shora.

32 Interakce veřejnoprávního dohledu a soukromoprávních nároků ve vztahu k ochraně osobních údajů ovšem není vůbec jednoduchá, a je proto často předmětem pozornosti soudů, které upřesňují rozhraničení působnosti ÚOOÚ, civilních a správních soudů. Srov. usnesení rozšířeného senátu NSS ze dne 4. září 2012, čj. 1 As 93/2009-273, č. 2732/2013 Sb. NSS, body 40–59 (včetně tam dále cit. judikatury zvláštního senátu). Tato otázka však již významně přesahuje rámec tohoto článku a proto ji dále nerozebírám.

33 Přesně k tomu směřovala i předběžná otázka položená NSS – viz usnesení NSS ze dne 20. března 2013, čj. 1 As 113/2012-59, bod 15, kde se NSS přiklonil k výluce z aplikovatelnosti evropské ochrany osobních údajů na domácí kamerové systémy, „*s tím, že by bylo na každém členském státě, zda takovéto situace podřadí či nepodřadí pod právní úpravu ochrany osobních údajů.*"

34 Rozsudek Soudního dvora *Ryneš*, body 27–33.

žargonem typu „čím více regulace, tím více lidských práv“[35], nemusel se ani zabývat skutečnými dopady jeho rozhodnutí na realitu společenských vztahů. Na to upozorňovala zejména vláda Spojeného království ve svém vyjádření k řízení, podle níž nebudou-li domácí kamerové systémy podřazeny pod výjimku z evropské regulace, vyvolá to naprosto zbytečnou byrokratickou zátěž pro běžné občany. Navíc se chce říci, že právě tyto svou povahou zcela lokální projevy zásahů do soukromí Evropanů by měly být regulovány domácí legislativou. Domácí zákonodárce zná dobře kriminalitu ve svém státě a efektivitu policie v boji s ní. Proto domácí zákonodárce také nejlépe ví, zda je třeba soukromé kamerové systémy řešit veřejnoprávní legislativou či zda postačí úprava soukromoprávní.

Rozsudek Soudního dvora otevírá mnoho dalších otázek, především jak daleko vlastně sahá dopad směrnice 95/46, resp. dnes obecného nařízení o ochraně osobních údajů. Generální advokát ve svém stanovisku ke kauze *Ryneš* sice uvádí, že kamerové sledování snímající veřejné prostranství se vyznačuje trvalostí a systematičností bez ohledu na dobu případného uchovávání záznamů, naproti tomu „právní otázky související se záznamy prováděnými pomocí mobilních telefonů, videokamer nebo digitálních fotografických přístrojů jsou jiné povahy“.[36] To však nemusí platit bezvýjimečně. Bude-li například student smartphonem každý den v průběhu jednoho týdne v době mezi 11. a 12. hodinou nahrávat odchod svých spolužáků z univerzity (to se mu zpravidla automaticky uloží na cloudové uložiště), event. bude po dobu několika týdnů točit telefonem či videokamerou časosběrné video postupné proměny ovocného stromu, bude však přitom zabírat i kolemjdoucí, i takovéto otázky by se v logice analyzovaného rozhodnutí Soudního dvora měly dostat pod regulaci evropských předpisů na ochranu osobních údajů.

Neurčitost dopadů směrnice 95/46, resp. obecného nařízení o ochraně osobních údajů, lze hezky ilustrovat i na otázce, kterou sice Soudní dvůr výslovně neřešil, zmiňuje ji však generální advokát. Na jednání Soudního dvora byla řešena ještě další otázka, a sice jak je třeba posuzovat kamery instalované ve vozech. Generálnímu advokátovi přitom s ohledem na jeho výklad, který převzal i Soudní dvůr, připadalo zřejmé, „že se na tyto přístroje pro sledování veřejných komunikací včetně osob, které na nich projíždějí, nemůže uvedená výjimka vztahovat, a že tedy jejich používání plně podléhá podmínkám stanoveným směrnicí 95/46“.[37] V domácí aplikační praxi napříč EU se posuzování obdobných kamer dramaticky liší, někde jsou zakázané, někde jsou naopak legální. Příkladem posledně uvedené země je i Česká republika, jejíž Úřad pro ochranu osobních údajů má za to, v rozporu s právě cit. stanoviskem generálního advokáta, že takovéto kamery nejsou srovnatelné s kamerami instalovanými na domech.[38]

S expanzí nových technologií se můžeme ptát, jak vůbec nastavit veřejnoprávní regulaci, aby účinně fungovala. Pokud se určitý produkt paušálně nezakáže nebo nereguluje již při prodeji (např. kamerové systémy nebo Google Glass), nebude mít veřejná moc účinné prostředky k regulaci zásahů do soukromí. Podívejme se na praktické příklady. Předmětem veřejnoprávní regulace jistě nejsou atrapy kamerových systémů, ale ani kamerové systémy, které jejich provozovatel sice na nemovitost nebo do auta umístil, ale nezapnul je a fakticky je tak nepoužívá.

Skutečnost, že na domě nebo v autě vidíme kamerové zařízení, tedy bez dalšího neznamená, že veřejnoprávní regulaci podléhá. Může to být atrapa, může to být zařízení, které není zapnuté. Protože kontrolní orgány (u nás Úřad pro ochranu osobních údajů) nemají za platné právní úpravy právo přístupu do nemovitostí nebo do osobních či nákladních automobilů, reálně vůbec nemají šanci porušování zákona zjistit. Pokud již k nějakým postihům dochází, děje se to až *ex post*, v okamžiku, kdy je záznam využit proti pachateli protiprávního činu, a ukáže se tak, že k pořizování záznamu vskutku dochází či docházelo.

Nové obecné nařízení o ochraně osobních údajů na některé tyto problémy pamatuje, a v čl. 58 dokonce dává dozorovému úřadu (u nás Úřadu pro ochranu osobních údajů) v rámci vyšetřovacích pravomocí mj. pravomoc získat přístup do všech prostor, v nichž

---

35 Srov. body 28 a 29 tamtéž.

36 Stanovisko generálního advokáta Niila Jääskinena přednesené dne 10. 7. 2014, ECLI:EU:C:2014:2072, bod 30.

37 Tamtéž, text v poznámce pod čarou č. 43.

38 Viz Stanovisko ÚOOÚ č. 1/2015 z března 2015, „Provozování kamery v motorovém vozidle se záběrem mimo toto vozidlo“, s. 3, bod 6: „*Vzhledem k tomu, že takové zpracování je z hlediska zásahu do práva na ochranu soukromí a osobních údajů subjektů údajů z pohledu Úřadu považováno za nerizikové (oproti stacionárním kamerovým systémům například není způsobilé zajistit provozovateli pravidelný přehled o výskytu a chování lidí v konkrétním prostoru, nezasahuje do práva na obydlí ani neznamená sledování zaměstnanců na pracovišti, které je zakázáno § 316 odst. 2, zákona č. 262/2006 Sb., zákoník práce) a současně se nepředpokládá využití záznamu z kamerového systému v motorovém vozidle za jiným účelem (např. zveřejnění), nemusí být předmětem předběžného šetření dozorového orgánu, a tudíž se na takové zpracování oznamovací povinnost dle § 16 zákona č. 101/2000 Sb. vztahovat nebude*.“

správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů. Do května 2018, kdy toto ustanovení vstoupí v účinnost, tak bude muset český zákonodárce vytvořit procesní normy, které tuto pravomoc dále specifikují. Ale ani tato nová pravomoc problémy shora nastíněné neřeší, ale naopak je jen dále umocní. Pokud se snad český Úřad pro ochranu osobních údajů nemá stát orwellovským úřadem vybaveným mnoha tisíci kontrolorů, pravidelně procházejících statisíci prostor, kde se v Česku osobní údaje zpracovávají, zůstane i tato nová pravomoc v podstatě nevyužita, resp. bude náhodně využita jen v návaznosti na různá udání a sousedské spory.

Takováto „regulace" chytrých technologií tedy podle mne je a i po roce 2018 bude povýtce formálního charakteru. Celkově snižuje respekt k právnímu řádu, který většina občanů jednoduše nerespektuje. Sankce za jeho porušení mohou z povahy věci přijít jen výjimečně, naopak čas a energie investované do oznamovacího řízení před orgánem chránícím osobní údaje[39] jsou takové, že se bohužel mnoha lidem vyplácí riskovat a zákon nedodržet.

Procedura spojená s oznamovací povinností kamerového systému se snadno stává zbytečným byrokratickým rituálem. Úřad v rámci svých vrchnostenských pravomocí totiž může v praxi jen těžko rozumně přezkoumávat např. přiměřenost rozhodnutí vlastníků bytového domu, kteří se v reakci na vandalismus či krádeže v domě rozhodnou do domu umístit kamerový systém. Lze jen obtížně akceptovat, aby úřad nahradil úsudek vlastníků bytových jednotek o potřebnosti kamerového systému úsudkem svým, kterým rozhodnutí vlastníků chránících si svůj majetek nahradí vlastním vrchnostenským rozhodnutím, že s ohledem na okolnosti si vlastníci svůj majetek mohou a mají chránit jinak. Úřad si přitom činí ambice přezkoumávat i takové technické detaily, jako je úhel, kterým kamery snímají společné prostory, nebo umístění jednotlivých kamer v domě.[40]

Dalším problémem je, že výklad práva ze strany Úřadu pro ochranu osobních údajů se někdy dostává do naprostého rozporu s přirozeným lidským cítěním, co je spravedlivé a namístě při ochraně majetku a jiných práv – viz např. ochrana „soukromí zlodějů" (sankce za to, že majitel odcizené věci, který se snaží získat věc zpátky, umístí fotografii pachatele na Facebook za účelem zjištění identity pachatele).[41] V neposlední řadě i orgán chránící osobní údaje v průběhu času proměňuje svá stanoviska a interpretace předpisů na ochranu osobních údajů, což dále oslabuje právní jistotu a předvídatelnost práva.[42]

Všechny tyto problémy mne vedou k závěru, že by se veřejnoprávní regulace neměla vyčerpávat v boji s větrnými mlýny – tedy neměla by se snažit chránit soukromí tam, kde ho nové technologie ze své povahy narušují v běžných mezilidských vztazích. Právě v těchto oblastech se totiž pojem soukromí v posledních dvou dekádách radikálně změnil. Při volbě veřejnoprávní regulace si normotvůrce musí být vědom povahy regulovaného vztahu. Smysl má veřejnoprávní regulace tam, kde s ohledem na zjevný nepoměr vyjednávacích možností mezi klientem a poskytovatelem služby a s ohledem na omezenou možnost běžného člověka pochopit všechna specifika internetových služeb nelze hovořit o informovaném souhlasu se všemi aspekty poskytování služeb typu Google, Seznam, Twitter, MyHeritage[43] nebo Facebook, eventuálně služeb telekomunikačních. Spor mezi obyvatelem domu, který se cítí omezen umístěním kamery na domu souseda, však řešit veřejná moc nemusí a podle mého názoru ze shora uvedených důvodů ani nemá. Soukromé právo vždy poskytovalo dostatek možností, jak se proti excesům a zneužití takové kamery bránit. Současně soukromé právo může mnohem pružněji reagovat na proměňující se koncepci soukromí v době internetu, všudypřítomných chytrých telefonů atp.[44]

---

39 Například pokyny na webové stránce českého Úřadu pro ochranu osobních údajů jsou všechno, jen ne uživatelsky přívětivé. Přinejmenším některé formuláře tam obsažené jsou tak komplikované, že vyplnit je dokáže jen zvláštní osoba mixující v sobě IT specialistu a právníka – specialistu na ochranu osobních údajů.

40 Stanovisko ÚOOÚ č. 1/2016 z ledna 2016, „Umístění kamerových systémů v bytových domech".

41 Což je příběh řešený rozsudkem NSS v kauze *e-kolo.cz*. Zdravému selskému rozumu se bohužel vzdálil v rozsudku i NSS, který potvrdil postih toho, kdo chránil svá vlastnická práva v rámci svépomoci umístěním fotografie na Facebook. Podle NSS (aniž by však vysvětlil, jak k tomuto závěru dospěl) „účelem provozování kamerových systémů při ochraně majetku není (ve zkratce řečeno) pořizování záznamů pro jejich budoucí zveřejnění, ale pouze pro eventuální předání k tomu určeným orgánům k dalším úkonům. Vyšetřování a postihování trestné činnosti (do něhož lze zahrnout i páchání přestupků) je přitom plně v kompetenci orgánů státu." Pokud tedy osoba umístila fotografii zloděje na Facebook, nebylo to prý nezbytné pro ochranu jejích práv nebo právem chráněných zájmů.

42 Viz např. rozsudek NSS v kauze *Ryneš*, část V.D.

43 MyHeritage je globální on-line službou, v základní verzi neplacenou, která poskytuje lidem možnost vypracovat si vlastní rodokmen. S daty, které tam klienti vkládají, pak MyHeritage obchoduje, neboť dostat se k datům třetích osob může jen platící klient služby. V prvé půlce roku 2016 začala nabízet novou službu, která spočívá ve shromažďování DNA od svých zákazníků.

44 Srov. rozsudek Krajského soudu v Brně ze dne 6. listopadu 2009, sp. zn. 24 C 45/2007, a jeho interpretaci Nejvyšším správním soudem v rozsudku *Ryneš*, body 96 a 97.