

UNIVERZITA KARLOVA V PRAZE

FAKULTA HUMANITNÍCH STUDIÍ

KATEDRA ELEKTRONICKÉ KULTURY A SÉMIOTIKY



DOHLED, MÉDIA, INTERAKTIVITA:

**PROBLEMATIKA DOHLEDU V KONTEXTU MODERNÍHO
MEDIÁLNÍHO PROSTORU**

Diplomová práce

Bc. Michal Šafránek

Vedoucí práce: Mgr. Daniel Slaviček, Ph.D.

Praha 2015

Čestné prohlášení

Prohlašuji, že jsem práci vypracoval samostatně. Všechny použité prameny a literatura byly řádně citovány. Práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 25. června 2015 _____

Poděkování

Děkuji Mgr. Danielu Slavičkovi, Ph.D. za vedení mé diplomové práce, přínosné konzultace a diskuze. Rovněž bych rád poděkoval mým rodičům a nejbližšímu okolí za neutuchající podporu.

Abstrakt

Práce se bude zabývat klíčovými aspekty problematiky dohledu v rámci současné sociálně-mediální reality. Popíše základní přístupy k tématu dohledu (se zaměřením na tzv. moderní elektronická média) z pozice interdisciplinárního oboru surveillance studies, děl M. Foucaulta, G. Deleuze aj., přičemž se nadále bude věnovat především teoretickým i praktickým aspektům dohledu a monitorování moderního mediálního prostoru. Práce si rovněž klade za cíl přinést vyvážený, místy kritický pohled na současné prostředky online komunikace a způsoby, či možnosti, kterými jsou uživatelé webu sledováni, aniž by o tom často měli ponětí.

Klíčová slova

Surveillance studies, dohled, média, online interakce, interaktivita, sociální sítě, marketing

Abstract

The purpose of this thesis is to describe the key aspects of the surveillance in the contemporary social media reality. It aims to take note of the basic approaches and theories in the field of surveillance and tries to fully describe and understand the impact of the – so called social media in the (post) modern situation, using the position of the interdisciplinary field of Surveillance studies, and also the works of M. Foucault, G. Deleuze etc., with the emphasis put on the theoretical and practical aspects of surveillance and monitoring of the modern media reality. The work also aims to bring balanced, sometimes critical view on the contemporary means of online communication and the tools, or means, that can be used to monitor the users of the internet - with, or without their consent or notion.

Key words

Surveillance studies, surveillance, media, online interactions, interactivity, social media, marketing

Ještě, než přistoupím k výkladu samotné diplomové práce, bych rád případným čtenářům přednesl na zřetel pár nezbytných poznámek, které se k této práci nevyhnutelně váží. Ačkoliv se jedná o text, který lze pochopitelně číst zcela odděleně, přeci jen si neodpustím drobný odkaz na mou bakalářskou práci, nazvanou *Sociální aspekty virálního marketingu*. V jejím rámci jsem se totiž pokusil vysvětlit, jakými změnami prošel moderní marketing - od klasických offline marketingových kampaní s jasnou cílovou skupinou a jednotlivými, zřetelně po sobě následujícími fázemi, po současnou postmoderní realitu, v níž se v rámci marketingové komunikace a jejích strategií nevyhnutelně mísí prostor offline s tím internetovým, tedy online. Nechtěl bych tedy znovu v rámci mé diplomové práce opakovat teze a definice, jež jsou obsaženy v mé práci bakalářské, ale zároveň na některé z, v tamějším textu uvedených myšlenek budu chtít nechtě nucen navazovat, jelikož za těch několik málo let od sepsání bakalářské práce dle mého názoru nedošlo, alespoň v některých důležitých aspektech této problematiky, k výraznější revizi.

Přesto je tuto práci samozřejmě možné číst jako zcela samostatný celek, v němž jsem se snažil snad pochopitelným a logickými argumenty podpořeným způsobem vylíčit současné teorie dohledu a především vysvětlit, jakým způsobem se odehrávají, pokud se tedy odehrávají, mocenské boje mezi výrobcí reklamních sdělení, provozovateli služeb a jejich příjemci. V rámci práce se již nebudu příliš zabývat například základními teoriemi online publik po vzoru dvou význačných autorů online (kyber) komunit Pierre Lévyho a Howarda Rheingolda, či rozdílem mezi offline a online médii jako takovým – důraz bude kladen především na jednotlivé aspekty, týkající se ultra moderních marketingových strategií, které si z určitých důvodů vzaly do hlavy, že nic jako lidské soukromí by nemělo existovat a jakékoliv osobní informace a data jsou dále bezostyšně perfektně zpeněžitelná komodita.

„Ti, co nemají co skrývat, se nemají čeho bát.“

Mark Zuckerberg – CEO, Facebook¹

¹Larry Page „dreams of a place with no privacy laws“, Axel Springer CEO claims in open letter to Google. *TheDrum.com*, dostupné z: <http://www.thedrum.com/news/2014/04/19/larry-page-dreams-place-no-privacy-laws-axel-springer-ceo-claims-open-letter-google>

OBSAH

ÚVOD	9
1. HISTORICKÉ PŘÍSTUPY K DOHLEDU A HLAVNÍ TEZE SURVEILLANCE STUDIES V RÁMCI ELEKTRONICKÝCH MÉDIÍ – OD PANOPTIKONU A KARTOTÉK K SYNOPTIKONU A BIG DATA	12
1.1 Počátky studia dohledu v díle Michela Foucaulta.....	12
1.2. Dohled z pohledu Gillese Deleuze – Přechod od disciplinárních společností ke společnostem kontroly a parcializace dohledu.....	17
1.3. Tekuté časy a tekutý dohled v pojetí Zygmunta Baumana	20
1.4. Teorie dohledu v díle současných teoretiků a autorů Surveillance studies	24
1.4.1. Tři fáze vývoje dohledu dle Davida Lyona.....	24
1.4.2. Teorie dohledu v rámci elektronických médií – důsledky modernity a digitální uzavření	28
1.4.3. Digitální uzavření Marka Andrejevice	30
1.4.4. Synoptikon – pokračovatel Panoptikonu v současném rozpojeném prostředí	32
1.4.5. Roger Clarke a dataveillance	34
1.4.6. Big data	35
1.4.7. Koncept producers jako způsob uživatelského vytváření obsahu.....	36
2. PROBLEMATIKA DOHLEDU V KONTEXTU MODERNÍHO MEDIÁLNÍHO PROSTORU	39
2.1.1. Nástup Webu 2.0 a zrození nové interaktivity	39
2.1.2. Dohled před nástupem sociálních médií – microsites, webové stránky a internetová fóra – personalizace obsahu	41
2.1.3. Dohled v rámci sociálních sítí	50
2.1.4. Problematika podmínek užití – Podmínky a zásady služby Facebook a EULA.....	61
3. PRAKTICKÉ PŘÍPADY UŽITÍ ELEKTRONICKÉHO DOHLEDU – KONTROVERZE A ODMÍTNUTÉ PROJEKTY	68
3.1. Případy kontroverzí v důsledku úniku uživatelských dat a odmítnutí dohledu v zahraničí.....	69
3.1.1. Případ Sony PlayStation Network.....	69
3.1.2. Microsoft Xbox Kinect – odmítnutí projektu dohledu ze strany uživatelů.....	71
3.2. Případy úniku uživatelských dat v České republice a prostředí tuzemského internetu.....	74
3.2.1. Únik citlivých dat z Komerční banky.....	76
3.2.2. Únik citlivých dat z České spořitelny.....	77
ZÁVĚR	79
SEZNAM POUŽITÉ LITERATURY A OSTATNÍCH ZDROJŮ	83

ÚVOD

Když jsme před pár měsíci v rámci jednoho z povinných předmětů na naší fakultě narazili na problematiku dohledu – tedy sledování, kontroly, sběru informací a moderních dohledových strategií, pokládal vyučující, pan profesor Miroslav Marcelli do pléna otázku, jaký postoj, coby mladá generace, zaujímáme k různým praktikám sledování ze strany státu a velkých soukromých firem. Jestli nás stále se rozmáhající dohled ze všech možných stran a úhlů ještě děsí, jsme vůči němu lhostejní, či k jeho postupům dokonce cítíme určité sympatie. Reakce má a mých ročníkových kolegů jej, řekl bych, mírně překvapila. Kupodivu se nekonaly žádné hlasité protesty, žádný rychlý odsudek dohledu, coby špiclování ze strany státu a dalších soukromých organizací za neurčitými a minimálně podezřelými účely.

Zdá se, že postupem času si uživatelé, žijící v současné mediální realitě, na dohled pomalu začínají zvykat. Jedná se však skutečně o Stockholmský syndrom, v rámci kterého má deprimovaná oběť sklon soucítit se svým trýznitelem? Právě tyto otázky jsem si pokládal, když jsem se rozhodoval, jakému tématu se chci v rámci obsahu této práce věnovat. Nechtěl jsem pouze opětovně vykládat a tlumočit myšlenky zakladatelů a nejvýznamnějších autorů ještě stále relativně mladého multidisciplinárního oboru *Surveillance studies*, které jsou, byť často objevené a dobře artikulované, dosud v našem prostředí takřka neznámé – především proto, že se prozatím nenašel nikdo, kdo by je přeložil a následně vydal v českém jazyce.

Chtěl jsem však těchto myšlenek využít pro demonstraci zcela jiného problému, se kterým se současná, nejen online realita potýká. Co když je současný dohled výměnným obchodem, ke kterému uživatelé přistupují nakonec zcela dobrovolně? Jak je možné, že jedním pohybem prstu uživatel bez jakýchkoliv okolků povolí elektronické

aplikaci přístup k úplnému obsahu svého telefonního adresáře, jenž ještě donedávna měl být ukryt před zraky všech nám neznámých lidí? Na internetu jako by soukromí nechtělo, ba ani nemělo existovat. Vše má být transparentní, iluminované. Je však současná mediální realita skutečně taková? A co na to uživatelé? Právě tyto otázky mi proudily hlavou a právě na tyto jsem chtěl znát – když ne rovnou odpověď, tak alespoň nějakými reálnými případy podpořenou domněnku. Tím se dostávám k poslednímu bodu tohoto úvodu, který má čtenáře alespoň stručně uvést do problematiky, o níž bude pojednáváno na následujících stranách.

Tato práce si tedy bere za cíl nejen vycházet z teoretických děl uznávaných autorů a odborníků z řad *Surveillance studies* a dalších teoretiků dohledu, ale především se soustředit na praktické příklady moderního dohledu z hlediska dichotomie autor/příjemce/, či zákazník/konzument, která v internetové realitě dostává zcela nové a dosud neviděné obrysy. Jednoduše – práce si bere za cíl popsat, jakým způsobem probíhá sběr uživatelských dat v prostředí online a proč současní uživatelé internetu a interaktivní komunikace jako takové berou dohled jako zcela hotovou věc, s níž není třeba bojovat, ale naopak ji neřešit, nevzpouzet se, zcela se jí poddat.

Text je posléze pro větší přehlednost rozdělen do tří částí. Ta první se zabývá historií dohledu, ovšem jen do takové míry, která ukazuje vývoj od prvních, do kronik zanášených osobních informací a údajů, až po současný sběr a třídění ryze elektronických tzv. velkých dat². Jak se totiž domnívám, klasická období dohledu se od současné reality a praxe dohledu liší do takové míry, že delší prodlévání v historickém diskurzu naše bádání příliš neusnadní. Jistě nám ovšem pomůže pochopit jednotlivé zlomy, které

² Z anglického slova „*Big data*“, které označuje shluk velkých balíků elektronických informací, dostupných na vzdálených serverech. Bude o nich pojednáno dále.

v rámci problematiky nastaly - a že ne všechny historické procesy se nevyhnutelně mění – alespoň co do jejich jádra a účelu.

Druhá část se bude zabývat současnými přístupy ke sběru osobních dat a následným dalším užitím. Vzhledem k tomu, že práce navazuje na sociologicko-marketingově orientovaný text, rovněž nás budou zajímat především formy, jež se uplatňují na poli současné marketingové komunikace. Nebude tedy brán přílišný zřetel na globální politickou situaci, banoptikon letiště a problematiku hranic jednotlivých suverénních politických celků a států, stejně, jako na problematiku institucí, s jasnou výjimkou těch mediálních. V případě zájmu o tato, v rámci Surveillance studies rozsáhle popsaná pole bádání doporučím relevantní kapitoly diplomové práce kolegyně Andrey Špačkové³, či některé ze souborných textů, v nichž je tato problematika podrobněji zpracovávána.

Třetí část se posléze bude věnovat především praktickým příkladům. V tomto oddílu se práce bude snažit co nejpodrobněji popsat, jakým způsobem se popsané teoretické přístupy prakticky uplatnily v minulosti i přítomnosti. Zvláštní pozornost bude věnována především případům, kdy uživatelé nezůstali pouhými pasivními příjemci, a tedy vykonavatel dohledu získal snadným způsobem nadvládu nad všemi osobními informacemi, které se mu jen zlíbily, ale svou aktivitou společně dospěli k určité změně. Troufám si totiž tvrdit, že právě tato interaktivní stránka internetu, totiž schopnost vyjádřit svůj názor vzhledem k autorovi sdělení, či služeb, je tím, co je často skloňováno jako největší přínos tohoto elektronického média a je otázka, do jaké míry se skutečně tato demokratizace v současné mediální realitě vyskytuje a funguje.

³ ŠPAČKOVÁ, Andrea - Elektronický dohled v oblasti spotřeby a médií, Diplomová práce, 2014, vedoucí práce Mgr. Daniel Slaviček, PhD.

1. HISTORICKÉ PŘÍSTUPY K DOHLEDU A HLAVNÍ TEZE SURVEILLANCE STUDIES V RÁMCI ELEKTRONICKÝCH MÉDIÍ – OD PANOPTIKONU A KARTOTÉK K SYNOPTIKONU A BIG DATA

1.1 Počátky studia dohledu v díle Michela Foucaulta

Ačkoliv slavného francouzského filozofa a všestranného vědce Michela Foucaulta jistě nelze považovat za teoretika dohledu, či snad rovnou zástupce multidisciplinárního oboru *Surveillance studies*, jenž se naplno rodí až někdy v polovině 90. let 20. století, přesto se dá říci, že svým dílem, které přesahuje rámec jednotlivých vědních disciplín, alespoň částečně zažehl snahy o studium dohledu v univerzitním prostředí i mimo něj. Je samozřejmé, že ještě před vytvořením skutečné vědecké školy se našla řada teoretiků, kteří o dohledu psali, ale ti byli okolím relativně často označováni za paranoiky a šířitele zbytečných poplašných zpráv - a jejich předpovědím nebyla věnována žádná zvláštní pozornost.

Foucault, jakkoliv se ve svém díle věnoval především teoriím moci, přesto odborné veřejnosti představil možné, jím samým nezamýšlené základy studia dohledu a především nastínil přechod od klasických společností po společnosti postmoderní, včetně změny dohledových strategií a jimi využívaných prostředků.

Za nutnou zmínku považuji jeho rozdělení historie dohledu, které načrtl ve svém obsáhlém, ovšem velice čtivě zpracovaném díle *Dohlížet a trestat*. Důležité přitom je, že Foucault se neobrací pouze k sobě samému a svým předchozím teoriím, ale vypůjčuje si například i ze sociologického přístupu Maxe Webera, jenž v rámci svého díla rozdělil společenské epochy na předmoderní a moderní, přičemž ta moderní se dle Webera vyznačuje především racionalizací a neustále narůstající byrokracií, která postupem času

dostala do vínku od státu pravomoc třídít obyvatele pomocí rutinního sběru a organizace osobních údajů. Je přitom důležité, že právě spojení stále rostoucího kapitalistického trhu, společně s neustále narůstající populací a rozvojem měst, jež se vznikem větších aglomerací vymanila z módu, který lze s trochou nadsázky popsat jako *větší vesnice*, v nichž se každý s každým osobně poznával, a nebylo tedy nutné pro tamější samosprávu nutné sahat k vytváření rozsáhlých evidencí obyvatel, jelikož umírající i právě narození vždy prošli nějakým přijetím ze stran měšťanů a jejich komunity. To samozřejmě neznamená, že by v předmoderní situaci nic jako census obyvatelstva neexistovalo. Pouze nešlo o tak rozsáhlý projekt, jelikož migrace obyvatelstva nebyla tak značná a územní legitimizace byla dána smlouvou s panovníkem, či určitým zmocněncem.

Michel Foucault si velice dobře všímá, že právě tato transformace společnosti – od společnosti, žijící v pospolitosti, ke společnosti do jisté míry vzájemně odcizené vlivem narůstající individualizace (kterou můžeme ve zřetelných obrysech vidět v procesu, nastalém po vypuknutí Velké francouzské revoluce začátkem „dlouhého“ 19. století) vedla i k proměně způsobu trestání. Svým barvitým popisem hrůzného trestání těla připravuje čtenáře na plné uvědomění si změny, která od krvavého fyzického trestu tělesného masa přichází k vytváření poslušných těl prostřednictvím racionálních a především institucionálních změn. Moderní společnost ohlašuje příchod institucí – všezahrnujících legitimizačních patentů, ustanovitelů diskurzu a jeho shluků.

Nikoho již nejspíše nepřekvapí, že západní společnosti a především moderní západní civilizace postupem času přešly od krveprolití k odnímání svobody v domnění, že každý člověk, byť i vrah, či násilník, si zaslouží druhou šanci. Současná společnost snad jakoby vyměňovala ekonomické náklady, které je nutné vynaložit na obživu svobody (nikoliv však života) zbavených vězňů, za společenský klid a mír. Každý pokus

o odplatu přímo na viníkovi je institucionálními aparáty státu potrestán, a osoba, která by odplatu provedla, si ponese dle systému moderního práva jasně stanovené následky.

Moderní stát tímto sankčním jednáním přitom pouze posiluje to, co vedlo k jeho samotné historické formaci – na jeho suverénním území se občané a rezidenti musejí chovat dle jeho zákonů a pokud je nerespektují, mají pouze dvě možnosti – buď odejít, či si nést následky. Tato dichotomie je pro další výklad této práce velice důležitá a postupem času znovu vyvstane, jelikož se částečně jedná o analogii v rámci ryze současné mediální sféry.

Prapočátky moderního dohledu Foucault nachází v morem zasaženém pozdně středověkém městě⁴. To musí být uzavřeno vzhledem k vnějšímu světu, vidíme zde tedy opětovnou myšlenku vytvoření karantény, operativního uzavření, což v historickém diskurzu pochopitelně není nic nového a oddělení nemocných od zdravých obyvatel bylo relativně časté již ve starověku, byť Louis Pasteur a jeho objevy v oblasti mikrobiologie a imunologie neměly přijít ještě dalších 2000 a více let.

Zajímavostí posléze je, že tato karanténa je vynucována za každou cenu – kdo by se snad pokusil z karantény odejít, bude zastaven všemi možnými prostředky. Město je rozděleno na samosprávné celky (distrikty), které mají vždy určenou osobu, jež za dodržování všech předpisů plně zodpovídá. Foucault tímto popisem trefně naznačuje další skutečnost - a to parcializaci a racionalizaci dohledu – udržet pořádek v rozkouskovanějších celcích je jednodušší, než se snažit o dokonalé ovládnutí velké spojené masy.

Zde samozřejmě můžeme vidět odkaz na základy moderního managementu, kdy velké nadnárodní korporace rovněž mají své, regionálním vedením spravované pobočky

⁴ FOUCAULT, M.: Dohlížet a trestat: kniha o zrodu vězení, Dauphin, 2000, str. 287

a místní kanceláře, či buňky, jelikož organizovat nadnárodní korporace jiným způsobem není výhodné a často ani možné.

Středověké, morem nakažené město tedy skutečně nese znaky jakéhosi předvoje moderního dohledu. Každý nakažený je zanesen v pečlivě vedené evidenci, každý má své úkoly a jasně vymezený prostor, v němž je možné a také nutné se pohybovat. Při neuposlechnutí rozkazu následují sankce, často tvrdé.

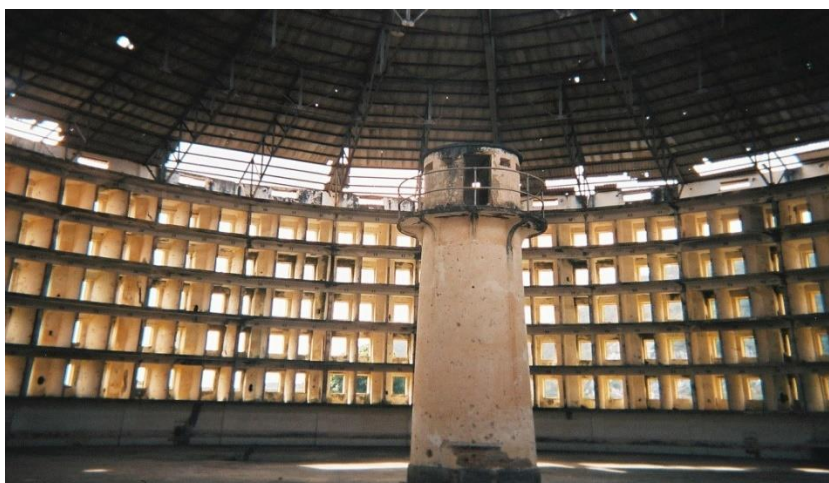
Na těchto pevně daných základech posléze přichází koncem 18. století stavět osvícenský filosof a právní teoretik Jeremy Bentham, kterému se daří rozpracovat projekt, jenž je až do dnešních dnů často uváděn, jakožto příklad moderního dohledu par excellence.

Michel Foucault si tohoto úctyhodného myšlenkového projektu, zvaného Panoptikon⁵, ihned všimá a dokonalým rozborem pokládá základy studia moderního dohledu. Jedná se o dokonale jednoduchý koncept, který ovšem vyjadřuje právě onen přechod od způsobu trestání těl klasické doby. Zatímco dřívější vězení a šatlavy (eventuálně věže, či sklepení) fungovaly na principu uzavření vězně, oddělení od zbytku obyvatelstva, zbavení světla⁶, Panoptikon naopak chce nechat světlo prosvítit vše.

Jedná se o stavbu kruhového půdorysu, přičemž po obvodu stavby jsou umístěny například skleněné kóje, či místnosti, které poskytují dokonalou viditelnost ze všech možných směrů. Uprostřed stavby se posléze nachází kontrolní věž, ze které je vidět do všech stran, ovšem věžeň naopak nevidí to, co se děje uvnitř ní. Tento koncept *asymetrické viditelnosti* je posléze klíčový. Nejen, že věžeň nevidí, jestli je někdo ve věži zrovna přítomen, on ani neví, jestli tam někdy někdo vůbec přítomen je, či kdy byl.

⁶ tamtéž s. 281

Kromě této autoregulace chování, založené na nedostatku informací, je posléze dle Foucaulta důležitá i přítomnost ostatních vězňů, kteří své chování regulují navzájem. Tento laterální dohled, jakožto Benthamem zamýšlený vedlejší produkt, je velice podobný tomu, co můžeme vidět a posléze i uvidíme například v rámci sociálních sítí. Ačkoliv se dá říci, že historický projekt Panoptikonu, jakožto racionalizovaného, na správu relativně výhodného způsobu dohledu nad vězni, či chovanci⁷, se v rámci moderního vězeňství nakonec spíše neprosadil (jelikož důraz na právo na soukromí vězňů, kteří jsou i přes své skutky stále plnohodnotnými lidskými bytostmi, převážil nad ekonomicky lákavými výhodami tohoto projektu), přesto lze říci, že minimálně ovlivnil metodiku vězeňství minimálně z hlediska racionalizace organizace prostoru (vzpomeňme na dlouhé rovné chodby se zamřížovanými celami, za kterými jsou vězni relativně dobře viditelní a často kontrolování, tedy je možné snížit personál ke kontrole potřebný). Panoptikon, jak uvidíme, se rovněž jako bumerang vrací i v rámci současných elektronických médií, byť s drobnou revizí, o které bude o ještě v tomto historickém exkurzu pojednáno.



Obrázek č. 1 – Příklad zrealizovaného konceptu Panoptikonu

⁷ Původně byl tento koncept zamýšlen i pro různé nápravné instituce, například ústavy pro duševně choré.

1.2. Dohled z pohledu Gillesse Deleuze – Přechod od disciplinárních společností ke společnostem kontroly a parcializace dohledu

Foucaultem rozpracovaným tématem se rovněž zabývá další velikán současné filosofie a kulturních teorií, který je často řazen do myšlenkového směru poststrukturalismu a postmodernismu jako takového - totiž Foucaultův krajan Gilles Deleuze.

V krátké, ale myšlenkově velice přínosné stati *Postskriptum ke společnosti kontroly* se částečně odkazuje právě na Foucaulta a připomíná již naznačený přechod od společností disciplinárních, k těm kontrolním.

Disciplinární společnosti lze řadit do 18. a 19. století, přičemž vrcholu dosáhly počátkem století 20. Dle Deleuze se jedná o vytváření uzavřených prostředí, z nichž každé si vytváří svou vlastní instituci – institucí je stejně rodina, jako například škola, vojenská kasárna, nemocnice, zaměstnání (v úvahách teoretiků je často kladen důraz na prostředí moderní, racionalizované továrny) a stejně tak další, v moderním prostředí vytvářené uzavřené celky.

Deleuze si rovněž všímá opětovného problému *parcializace*, v níž každá instituce má vlastní soubor pravidel a nařízení, což pozornému čtenáři jistě připomene dalšího velkého autora – Niklase Luhmanna a jeho systémové teorie, které právě s diferenciací a konceptem parcializace jednotlivých sociálních subsystémů operují.

Co se týče současnosti, zde Deleuze vidí jasnou krizi jednotlivých institucí s tím, že disciplinární společnosti jsou již v současném sociálním vývoji masově opouštěny.

Přímo píše: „*Každý však ví, že tyto instituce pouze oddalují svůj zánik*“⁸. Dle jeho názoru tedy dochází k proměně – od disciplinárních společností ke společnostem kontroly.

Předpovídá, že moderní kapitalistická společnost brzy opustí klubko stabilních institucí a roli některých z nich (například roli školy, coby odděleně institucionalizovaného vzdělávacího systému) převezmou pracovní podniky. Při pohledu na současný trend školení a dalšího sebevzdělávání, či zvyšování kvalifikace placené zaměstnavateli, to vypadá, že Deleuze skutečně narazil na jeden z dalších současných trendů.

Pro tuto práci ovšem je stěžejní především autorova představa toho, že ke každé společnosti, ať už jakkoliv organizované, či nacházející se v jakémkoliv stádiu vývoje, lze přiřadit určitý typ stroje⁹. Od panovnických společností, disponujících jednoduchými pákami, hodinami a kladkami, přes energetické stroje, náchylné k sabotážím (vzpomeňme na události konce 18. století a účelné rozbíjení strojů dělníky, kteří se báli, často i právem, že jejich existence je postupnou tovární mechanizací a automatizací ohrožena) až k současným společnostem kontroly, které ke svým účelům používají, slovy autora „*stroje třetího druhu*“ - počítače¹⁰, jejichž slabinou je dle Deleuze počítačové pirátství a šíření virusů. Ohledně prvně zmíněného palčivého problému však v rámci této práce bude alespoň ve stručnosti pojednáno později. Jistě se sluší dodat, že kromě předcházející bystré úvahy změny v pokrok zajišťujících prostředcích, přenesených na počítačovou techniku, si autor neméně trefně všimá i orientace moderní formy kapitalismu, která se od výroby přenesla k samotným výrobkům¹¹.

⁸ DELEUZE, G.: Rokovania 1972-1990, Archa, Bratislava, 1998, str. 196

⁹ DELEUZE, G.: Rokovania 1972-1990, Archa, Bratislava, 1998, str. 199

¹⁰ tamtéž str. 199

¹¹ tamtéž str. 200

V současné, globalizací stíženě společnosti, je možno tuto myšlenku ještě drobně aktualizovat – slovo výrobek by snad šlo zaměnit za slovo *produkt*, které vyjadřuje fakt, že kromě samotných výrobků jsou v současnosti prodávány a tržně směřovány i služby, čehož si ve svém díle koneckonců všímá i sám Deleuze - a jak postupem času dochází k přechodu od fyzických paměťových nosičů koncových zákazníků (hard disků) k online síťovým úložištím a celkově ke *cloud computingu*¹², dá se předjímat, že se s tímto slovem budeme setkávat stále častěji.

Důležitá v kontextu této práce každopádně je jeho poznámka, že postupem času se z individuí vytvořila *dividua*¹³, přičemž masy jsou užitečné především díky tomu, že z nich lze extrahovat cenná data. Právě tyto poznámky jsou tváří v tvář současné společnosti a elektronickému dohledu velice trefné, jelikož právě data, zdá se, jsou tím nejcennějším, co může většinová společnost současným nadnárodním korporacím, soukromým firmám, i státnímu aparátu nabídnout.

Tím by alespoň pro tento okamžik byly vyčerpány filozofické perspektivy a pro účely práce je stěžejní se alespoň ve stručnosti věnovat jednomu z nejuznávanějších současných sociologů, v sousedním Polsku narozenému Zygmuntu Baumanovi, jenž svým dílem často postihuje především aspekty současného konzumerismu, které pro další vývoj v oblasti současného marketingu a dohledových strategií mají zásadní význam.

¹² *Cloud computing* je na internetu založený model vývoje a používání počítačových technologií. Jedná se například o poskytování služeb či programů, k jejichž obsahu se uživatel dostane prostřednictvím rozhraní webového prohlížeče.

¹³ Digitální datový obraz našich osobností.

1.3. Tekuté časy a tekutý dohled v pojetí Zygmunta Baumana

Zygmunta Baumana můžeme díky jeho kritickým a často podnětným názorům řadit mezi teoretiky a zástupce postmodernismu, jelikož ve svých dílech často naráží na rozpad v historickém vývoji jasně daných struktur. Pro vysvětlení tohoto fenoménu si vypůjčuje Deleuze a Guattariho rhizomatický model¹⁴, který klade důraz na náhodnost, nahodilost, decentralizaci a proměnlivost. Bauman s tímto konceptem pracuje tak, že představuje obraz jakési tekuté současnosti, v níž současné společnosti ztrácejí povahu (a)historických struktur a mohou být čím dál častěji vnímány jako sítě bez nějakého reálného mocenského centra. Jak autor píše ve své knize *Tekuté časy: Život ve věku nejistoty* - jedná se o matrix¹⁵ náhodných spojení a rozpojení, kde množství permutací je nekonečné.¹⁶

Právě různá provázání státních i soukromých institucí, individualit, spojení účelného *goodwillu* velkých korporací s jejich důsledným brand marketingem a nenápadným dohledem, se dle něj odehrává jaksi nahodile a jednotlivé části skládky do sebe zapadají vždy sledem více méně nahodilých okolností.

Bauman zde znovu naráží na trend individualizace společnosti, v jehož rámci sociální i komunitní pohyb není nikdy dokončen. Díky globálním trhům, které nějakým způsobem vždy musejí interagovat mezi sebou, pak již nelze říci, že by existovalo něco, co se nás materiálně netýká. Dopad událostí americké hypoteční krize z roku 2007, která

¹⁴ DELEUZE, G.; GUATTARI, F.: Tisíc plošin, Herman & synové, 2010, str. 13

¹⁵ Lze přeložit jako matice, ale zároveň se jedná o virtuální prostor, známý ze stejnojmenného filmu

¹⁶ BAUMAN, Z.: – Tekuté časy: život ve věku nejistoty, Academia, 2008, str. 10

postupem času přerostla ve finanční krizi světového formátu, je jasně znatelný do dnešních dnů a Baumanovy teorie relativně úspěšně ilustruje.

Globalizace společnosti je dle něj kromě vzrůstající individualizace částečně dána i jasným postojem velkých nadnárodních korporací, jejichž hlavním zájmem je prodávat své produkty do celého světa a díky značnému finančnímu kapitálu toho často mohou docílit.

Je pak docela dobře možné, že současný konzument si již nespojí značku Coca-Cola, či Marlboro s nějakým symbolem americkosti (jako tomu bylo v dobách, kdy se na toto téma prováděl jeden marketingový výzkum za druhým), ale rozhodně si je spojí se silným nadnárodním brandem, u nějž má jistotu, že jeho pozice nebude nikterak otřesena.

Ačkoliv dle článku vlivného časopisu Time, musel nejznámější řetězec restaurací s rychlým občerstvením, symbol globálního úspěchu McDonald's, vlivem narůstajících ekonomických ztrát uzavřít počátkem roku 2015 již 350 restaurací¹⁷, přesto to globální pozici „*Golden Arches*“ nikterak neotřásl. A rozhodně to neznamená, že by jedno z nejznámějších log světa někdo snad měl přestat poznávat.

Zajímavostí je především Baumanův náhled na problematiku osobního bezpečí. V tomto věku nejistoty, kdy je naše víra v cokoli již notně otřesena (zde naráží na převrácení dříve uznávaných hodnot, jakými jsou například náboženství, osobní čest, rodina a další) je osobní bezpečí hlavním arktiklem všemožných marketingových strategií. Kromě volebních hesel a různých manifestů, jejichž vlna se mohutně zvedla především po velké krizi bezpečnosti, odstartované teroristickým útokem na USA 11. září 2001, jde především o samotnou funkci pořádkových aparátů – tedy kupříkladu policii,

¹⁷ „Mc Donald's Is Closing Hundreds of Stores This Year.“ *Time.com*, dostupné z: <http://time.com/3832101/mcdonalds-closing-stores-2015/>

jejíž účel musí být občanům náležitým způsobem osvětlen a dále legitimizován. Odkazuje se přitom na autora Raye Suretta, který ve své knize *Media, Crime and Criminal Justice* napsal: “Svět na obrazovkách televizí se sestává z občanů-ovcí, chráněných před zločinci-vlky a to policií – ovčáckými psy.”¹⁸

Proč je právě osobní bezpečí v současné společnosti tolik protěžovaným a žádaným artiklem si vysvětluje její, v historii dosud nevídanou, atomizací – každý se v ní stará jen sám o sebe a ostatní jsou mu často lhostejní, pokud pro něj nepředstavují možnost vytěžení, tedy využití k jakémusi osobnímu prospěchu. Bauman, ačkoliv není považován za teoretika dohledu (a ani se jím primárně nezabývá, ačkoliv, jakožto autor, jenž se věnuje modernitě, se těmito tématům ve své tvorbě nikdy nemohl zcela vyhnout), se posléze do ryze současných teorií dohledu naplno ponořil především v rámci své knihy *Tekutý dohled*, což je v podstatě vydaný záznam e-mailové komunikace, kterou si Bauman vyměňoval s jednou z největších osobností z řad teoretiků dohledu a Surveillance studies, Davidem Lyonem. V rámci této knihy tak konečně dostal příležitost rozpracovat svůj teoretický příspěvek k dohledu v rámci ryze současných elektronických médií a postmoderní společnosti.

Bauman píše, že internet přináší *smrt anonymity*¹⁹. Ztráta soukromí je snad uživateli chápána jako přijatelná cena za zábavu, kterou získáváme na oplátku. Internet na své uživatele, jak tvrdí, vytváří tlak, kterému je schopno odolat jen málo lidí. Ostatní se drží stádní mentality, která internetový dohled buď neřeší, či tomuto tlaku důsledkem okolností podléhá.

¹⁸ SURETTE, R.: *Media, Crime and Criminal Justice*, Brooks/Cole, 1992, str. 43

¹⁹ BAUMAN, Z.; LYON, D.: *Tekutý dohled*, Broken Books, 2013, str. 32

Bauman zdůrazňuje, že dnes již není problém kohokoliv na internetu bez potíží dohledat. Uvádí příklad fotografa Richarda Lama, kterému trvalo pouhý jeden den, aby zjistil, koho že to zachytil na svých fotografiích při vášnivých polibcích – osoby, které posléze kontaktoval, nejen, že nebyly dotčeny zásahem do svých osobnostních práv, ale dokonce byly vděčné a dožadovaly se zarámovaných kopií pořízených snímků.

Jak Bauman uvádí, vše soukromé, co se dnes děje na veřejnosti, se může s pomocí internetu stát předmětem *veřejné spotřeby* a vydrží v podstatě navěky, jelikož internet dokáže přehlédnout celé město jedním pohybem (zde nejspíše Bauman naráží na aplikace typu Google Maps²⁰, v jejichž rámci jsou skutečně všechna města fotograficky zpracována, přičemž nechybí ani interaktivní pohled na jednotlivé ulice, se kterým je možno volně otáčet. Abychom ovšem firmě Google nekřivdili, v tomto případě jsou na veřejně dostupných mapách všechny potenciálně citlivé informace rozmazány – ať už SPZ značky automobilů a dalších vozidel, či tváře náhodných kolemjdoucích. To ovšem neznamená, že Google k necenzurovaným mapám nemá přístup a už vůbec to neznamená, že nemá přístup k, v reálném čase generovaným satelitním snímkům. Přesto, jelikož Google při získávání dat pro technologii *Street View*, díky které si můžeme ulice prohlížet kdekoliv na světě prostřednictvím webového prohlížeče, využívá především 360 stupňovou 3D kamerou vybavená vozidla, dá se říci, že zpracování celé Zeměkoule pouze za pomoci satelitu v současnosti ještě není právě optimální.

Na druhé straně, pokroky v komplementárních technologiích, především stále se zlepšující rozlišení vizualizace celé naší planety Google Earth²¹, jež Street View pochopitelně obsahuje rovněž, nastiňuje možný budoucí vývoj, jenž se bude odehrávat v podobném duchu, jako v současnosti – v duchu postupné *automatizace*. Stejně tak je

²⁰ Mapy Google. *Google.cz*, dostupné z: <https://www.google.cz/maps>

²¹ Google Earth. *Google.cz*, dostupné z: <http://www.google.cz/intl/cs/earth/>

nutno pozornost věnovat i různým dronům a dalším bezpilotním strojům²², které již brzy budou díky Facebooku²³ brázdřit nebesa i několik měsíců vkuse díky přítomnosti solárních panelů, určených pro sběr energie – a jen budoucnost ukáže, zda kromě internetového připojení do různých koutů světa přinesou i další mechanismy kontroly.

Bauman zdůrazňuje, že dnešního člověka ani tak netrápí, že zde existuje jasná a častá možnost narušení, či obnažení soukromí – problematickým se jeví především opačný vývoj - tedy uzavření východů. Člověk bez východů je izolován, chybí mu publikum, které by dychtilo po poznání jeho tajemství. Jinými slovy – Bauman popisuje to, co již tolik teoretiků před ním od prvního objevení televizních reality show – současná společnost je společnost nezřízeného voyerství a ochoty prozradit na sebe cokoliv, ve snaze oslnit své okolí.

Možná se jedná o poněkud paradoxní situaci, ale právě tato proměna od společnosti, úzkostlivě si střežící svá osobní data, po společnost, která žádá taková data mít nechce, je, zdá se, jedním z největších zlomů ve vývoji současné v duální realitě se vyskytující společnosti. Oním duálním výskytem je pochopitelně myšleno prolínání dvou realit – té fyzické offline a té - spíše afyzické, či, trochu smířlivě nazvané - smíšené – online.

1.4. Teorie dohledu v díle současných teoretiků a autorů *Surveillance studies*

1.4.1. Tři fáze vývoje dohledu dle Davida Lyona

Dohled je pochopitelně odvětví, které se, podobně, jako jakákoliv jiná činnost, během jednotlivých historických období měnilo. Na druhé straně se ovšem nedá říci, že by někdy došlo k situaci, kdy přestal být jeden typ dohledu uplatňován a na jeho místo

²² BAUMAN, Z.; LYON, D. – Tekutý dohled, Broken Books, 2013, str. 30

²³ Facebook wants solar drone to bring internet far and wide. *Cnet.com*, dostupné z:

<http://www.cnet.com/news/facebook-solar-powered-drones-to-take-flight-this-summer/>

nastoupil typ jiný. Spíše neustále dochází k jejich vzájemnému prolínání, zastupování a doplňování, což přetrvává až do současnosti. Přední teoretik oblasti dohledu, kanadský profesor sociologie, působící na Queenském centru Surveillance studies, David Lyon, pak rozlišuje následující fáze:

1. fáze – předmoderní – dohled tváří v tvář (face-to-face)

2. fáze – moderní – dohled v rámci vytváření archivů a kartoték (file-based)

3. fáze – postmoderní – dohled založený na užití rozhraní (interface)²⁴

Zajímavostí je samozřejmě určitý vývoj – zatímco v rámci dohledu tváří v tvář se jednalo o dohled spíše nesystematický, u kartoték a dalšího rutinního sběru informací se jedná o systematický dohled.

U dohledu tváří v tvář je posléze stěžejní, že se jedná o asymetrický i symetrický model zároveň. Tedy – osoba, na kterou je dohlíženo, vidí, že je na ní dohlíženo. Přesto existují i situace, kdy o takovém dohledu nemůže vědět, například, nevidí-li do místa, odkud je na ni dohlíženo.

Pokud nevidění nasloucháme něčí konverzaci, či jsme schováni například za závěsem, jedná se určitě o asymetrickou situaci dohledu. Rovněž, pokud uvedeme za příklad ředitele (či manažera) továrny, který má z okna své, na vyvýšeném prostoru se nacházející kanceláři přehled nad celým podnikem, může snadno kontrolovat, kdo pracuje s jakým nasazením, aniž by byl sám viděn, tak v takovém případě se jedná rovněž i případ veskrze asymetrické formy dohledu. Mezi fáze se spíše asymetrickými formami

²⁴ LYON, D.: Surveillance Studies: An Overview, Polity, 2007, str. 71-93

dohledu posléze již řadíme druhou a třetí, ovšem i zde lze najít případy symetrického dohledu (například, pokud si oba subjekty navzájem vymění sebrané informace jeden o druhém). Příklad sociálních médií, jak uvidíme, je v tomto velice specifický.

Druhý typ dohledu, jenž je založen na archivech, rejstřících a různých kartotékách, pak můžeme pozorovat v podstatě každý den. Jakožto plnoletí obyvatelé nějakého státu disponujeme občanským průkazem, cestovním pasem, zdravotní kartičkou, legitimací do knihovny, do prostředků městské hromadné dopravy a podobně. Přitom legitimace je pouze konečným, hmatatelným produktem rozsáhlé sítě systematických úkonů, které musí jednotlivá oddělení jednotlivých úřadů provést – a pochopitelně zanést do svých databázových a informačních systémů. Před příchodem počítačů a ukládání informací na serverech se tyto informace shromažďovaly právě v kartotékách, které měly a stále, oproti dohledu tváří v tvář, mají nesmazatelnou výhodu – v jejich rámci lze hledat informace, které se vztahují i k minulosti a dále a jsou rovněž vysoce systematické.

Vezměme za příklad zdravotní kartu u lékaře. Personál rychlým pohledem do naší karty zjistí, jaké nemoci jsme prodělali a zdali je v rámci našeho zdravotního stavu, vzhledem k riziku možných komplikací, možné předepsat určitý lék. Rovněž není problém pro policistu nahlédnout do našeho trestního rejstříku, pro potenciálního obchodního partnera do registru dlužníků a podobně.

Právě s tím, jak se tyto registry a další služby postupem času přesouvají na internet, souvisí třetí, poslední rozlišovací fáze, která je založena na užití *interface*.

K interface se váže především problém přístupu k těmto databázím – zatímco dříve měla přístup k osobním informacím, v těchto registrech zanesených, povětšinou státem, případně soukromými subjekty jasně pověřená osoba (jejíž pochybení tedy bylo

snadněji odhalitelné a eventuálně postižitelné), v případě interface se k informacím často může dostat kdokoliv, kdo zná i tak základní údaje, jakými jsou jméno a příjmení. Jelikož se ovšem personálie v současnosti za citlivé osobní informace již spíše nepovažují, postižení takového jednání se stává čím dál neřešitelnějším problémem.

Další pro tuto práci důležitou okolností je Lyonovo rozlišení *účelu* sledovacích technologií. Obhájci sledovacích metod často a rádi poukazují na fakt, že je lze využít nejen k získávání osobních informací a omezování soukromí, ale například i k účelům sledovaným osobám a vlastně všem zainteresovaným osobám prospěšným.

Kromě pouličních CCTV kamer, které například sledují dopravní situaci a trvale dohlíží na dodržování zákonů (a tím přispívají k bezpečnosti a plynulosti dopravy), se jedná i o sledovací zařízení, které může zachraňovat životy – například náramek, který sleduje zdravotní stav seniorů a odesílá jej lékařům, či přítomnost aplikací v mobilních telefonech a počítačích, které v případě nouze mohou rychle přivolat záchrannou službu.

Zvláštností v současnosti není ani přítomnost GPS čipu, který v případě potřeby může mobilní telefon a možná i jeho majitele lokalizovat s odchylkou přesnosti maximálně několika metrů. Existují dokonce takzvané mobily pro seniory, které disponují speciálním hardwarovým tlačítkem, jež geografickou polohu telefonu okamžitě odešle na zadané telefonní číslo a příbuzní, či opatrovatelé tak mohou ihned začít kontaktovat pověřené úřady.

David Lyon tuto dvojznačnost dohledu nazývá **Care/Control**²⁵, tedy je možné, aby tato zařízení a teoreticky každé sledovací zařízení pomáhalo a zároveň dohlíželo nad svěřeným objektem, či subjektem. Soukromí při užití těchto dohledových prostředků bude omezeno vždy, otázkou tedy zůstávají především okolnosti užití a převážení

²⁵ LYON, D.: Surveillance Studies: An Overview, Polity, 2007, str. 3

pozitivních účinků nad negativními, což je problematika, se kterou se setkáváme i právě při užití sledovacích metod na internetu.

1.4.2. Teorie dohledu v rámci elektronických médií – důsledky modernity a digitální uzavření

Od poloviny 90. let se rozliční autoři, hnaní vpřed Anthony Giddensem a jeho koncepty vývoje moderních společností, jež vyjádřil například v knize *Důsledky modernity*, tedy nástupem postmodernity, postkapitalismu, nastolením informační společnosti a především zvýšení nejistoty a z toho vyplývajících důsledků nedostatku pocitu bezpečí, důvěry a vzrůstajícího rizika (zde je v souladu s výše uvedenými tvrzení Zygmunta Baumana) snaží nějakým způsobem osvětlit vyvstání nových sociálních formací a vyrovnat se s jejich novými krizemi a výzvami.

Giddens například usiluje o přednesení myšlenky ontologického bezpečí²⁶, s jehož pomocí se jednotlivé instituce, jež autor často označuje jakožto *expertní systémy*, snaží s touto situací vyrovnat. Uvádí příklad letiště, které se v rámci svého účelně organizovaného prostředí, profesionálně odměřeným chováním zaměstnanců a vůbec celkovou fasádou snaží vzbudit v cestujících důvěru, jelikož se právě nacházejí v systému, jenž je dokonale vymyšlen a efektivně spravován.

²⁶ GIDDENS, A.: *Důsledky modernity*, Sociologické nakladatelství, 2010, str.85

Rovněž si všímá i dalšího jevu, který označuje jakožto vyprázdnění času a prostoru, mluví o takzvaném *časoprostorovém rozpojení*²⁷. Jedná se o postřeh, že televize a nová média překonávají časovou a prostorovou bariéru, jelikož v přímém přenosu lze v podstatě vidět události z celého světa. Zatímco dříve se zprávy šířily jen pomalu a různé události mohli bez časového posunu sledovat jen obyvatelé v dané oblasti žijící, televize a další nová média nás mohou v řádu několika sekund přenést na druhý konec planety. Čas a prostor je tedy zrušen a vládu nad ním přebírají média. Elektronická média pochopitelně tyto události dovádějí do extrému a jedinec, mající k těmto technologiím přístup a vlastní potřebné povědomí o nich, je tak schopen takřka okamžitého a téměř bezlatenčního²⁸ spojení s kýmkoliv, ať už se ten nachází v podstatě kdekoliv na světě, za podmínky, že disponuje internetovým připojením.

Právě nutnost vlastnit internetového připojení je často v rámci internetu uváděna *coby technologický determinant*, jenž určité osoby vykazuje za hranice současného mediálního prostoru. V současné situaci, kdy je například jen v České republice k internetu připojeno více jak 8 milionů lidí, což činí 77,48% české populace²⁹, přičemž penetrace světové populace internetem činí 40,4%, se ovšem tato bariéra začíná pomalu rozpadat a dá se říci, že rozvinuté západní společnosti se skutečně postupem času začínají houfně přesouvat do virtuálního prostoru.

Giddens rovněž mimoděk mluví i o vzrůstajícím vlivu dohledu a jeho postupné automatizaci, ať už v armádním, či civilním prostředí, ovšem nějakou rozsáhlejší teorii

²⁷ tamtéž, str.26

²⁸ *Latence* je anglický výraz pro zpoždění, který je způsoben zpracováním informace zpracovávané serverem na trase klient-server (klient)

²⁹ Internet users by country (2014). *Internetlivestats.com*, dostupné z: <http://www.internetlivestats.com/internet-users-by-country/>

v tomto ohledu nerozvíjí, jelikož mu nejde primárně o soukromí a problematiku současného dohledu, ale o bezpečí.

V rámci této práce je tedy nutné věnovat se především vysvětlení některých teorií dohledu, které jsou pro námi zkoumané prostředí současných elektronických médií klíčové - a dá se říci, že mezi odborníky z rychle se rozvíjejícího oboru Surveillance studies v podstatě zlidověly. Jedná se především o díla autorů Marka Andrejevice, Marka Postera, Rogera Clarkea - a z ryze současných badatelů například Daniela Trottiera, jenž některé své publikace přímo věnuje výzkumu sociálních sítí a současných elektronických médií se zvýšenou mírou interakce – a těm bude dále věnována přednostní pozornost.

1.4.3. Digitální uzavření Marka Andrejevice

Jeden z nejvlivnějších autorů ryze současného studia dohledu, Mark Andrejevic, přichází s teorií vzniku tzv. *digitálního uzavření* (digital enclosure)³⁰, což je situace, v níž každá aktivita vytváří digitálně zpracované informace o sobě samé. Například každý telefonní hovor, návštěva internetových stránek, platba přes nejrůznější internetové brány – to vše vytváří informace, které jsou posléze zaneseny do různých elektronických databází. Tyto databáze, které postupem času, s nárůstem uživatelů daných služeb nabývají na objemu, samozřejmě mají potenciálně obrovskou komerční cenu. Jak uvidíme v případě nejznámější a nejužívanější sociální sítě (alespoň tedy západního)

³⁰ ANDREJEVIC, M.: iSpy: Surveillance and Power in the Interactive Era, Univ Pr of Kansas, 2007, str. 2

světa - Facebooku, právě uživatelská data nakonec byla tím, co z nápadu tehdejšího studenta Harvardu Marka Zuckerberga vytvořilo miliardový byznys.

Jednoduše – v okamžiku, kdy se stále více našich každodenních interakcí odehrává na internetu – nejen výměny názorů a další sociální interakce, ale především naše nákupy a další spotřební chování, tím více se budou určité společnosti snažit se k těmto citlivým informacím dostat, jelikož v nich dřímá velký potenciál další monetizace a vytěžení informací pro marketingové a další strategické, ryze ekonomické účely – Vincent Mosco dodává, že tyto digitalizované informace se stávají kybernetickou komoditou. Philip Agre mluví o digitálním stínu – *digital shadow*³¹.

Jiní autoři, například Haggerty a Ericson přicházejí s konceptem *data doubles*³² – datových dvojníků, kteří jsou našimi druhými já - jakýmsi digitálním otiskem, trvalou manifestací našeho chování v kybernetickém prostředí. Tento dvojník však nemizí, podobně, jako mizíme my z reálného prostředí, pokud nás tedy v objektu nezachytilo oko bezpečnostní kamery, či jiné záznamové zařízení. Jeho digitální stopa zůstává trvale udržena v serverových a databázových systémech, dokud není vlastníky této informace smazána, či zcela vytěžena. Nejsme pak již sledováni pouze státním aparátem, soukromými společnostmi, ale sledujeme se i sami navzájem – digitální uzavření nás jednoduše udržuje ve stavu neustálé viditelnosti pro kohokoliv, kdo se zrovna dívat chce.

Digitální uzavření má pro Marka Andrejevice i další důsledky. Jedná se o situaci, kdy jednotliví jeho obyvatelé o sobě mají sklon říci i věci, které by se jinak při přímé interakci říci styděli. Tyto informace jsou ovšem často klíčové pro různá odvětví byznysu,

³¹ AGRE P. E.: The Market Logic of Information, 2000. Dostupný z: <http://polaris.gseis.ucla.edu/pagre/hamburg.html>

³² HAGGERTY et al. 2000

přičemž náš digitální dvojník je o nás ochoten poskytovat skrze iluzi internetové anonymity více informací, než kdy dříve.

Andrejevic uvádí příklad této rozšířené interaktivity digitálních dvojníků na příkladu marketingové kampaně firmy Nike s názvem iD, která byla spuštěna v roce 2005. Jejím prostřednictvím si uživatelé mohli sami navrhnout své vysněné boty – a kampaň sloganem vybízela k tomu, aby se sami uživatelé stali designéry.

Co mohlo být považováno za neškodnou a hravou kampaň, byla ve skutečnosti od marketingového týmu společnosti Nike promyšlená hra, jelikož pro nejlepší návrh posléze mohli všichni uživatelé hlasovat. Zaměstnanci firmy Nike tedy nejen, že získali informace o tom, jaký návrh se zákazníkům líbí nejvíce a tedy je největší pravděpodobnost, že výroba těchto bot přinese největší zájem a zisky, ale zároveň přenesli část své práce (návrhu bot, o kterém jsou přesvědčeni, že se bude prodávat), na uživatele samotné. Nutno dodat, že právě tento koncept přenesení práce, za kterou by za normálních podmínek někdo měl být placen, na komunitu uživatelů, kteří chtějí (v rámci soutěže) pomoci své oblíbené firmě, patří do problematiky *producers*, což je další termín, jenž s postupujícím přesunem marketingových snah na web nabírá na vážnosti.

1.4.4. Synoptikon – pokračovatel Panoptikonu v současném rozpojeném prostředí

Výše rozebraný Foucaultův náhled na Benthamovský projekt Panoptikonu, coby racionalizovaného prostoru totálního dohledu, již tváří v tvář současnému vývoji dohledu i současných médií není trvale udržitelný. Hned několik autorů si všímá, že situace současného internetu je o poznání složitější. Není jen jeden sledující, který by mohl, podobně jako v Orwellově románu postava Velkého bratra, sledovat miliony lidí a sám

přítom v podstatě nebýt viděn, chtěl-li by zůstat v anonymitě. Norský sociolog Thomas Mathiesen v rámci této revize přichází s pojmem *Synoptikon*, jímž jako by se chtěl vyrovnat se symetrickou strukturou internetu, kdy není pár sledujících, kteří pozorují mnoho (*few watches many*), ale často mnoho, kteří pozorují pár, či jednoho (*many watches few*). Oba tyto koncepty se posléze v realitě překrývají, navíc nesmíme zapomenout ani na samotného sledujícího, jenž je rovněž ostatními uživateli sledován.

Každý je tak neustále viditelný a jeho činy a kroky jsou posléze posuzovány. Není pak možné říci, kdo je vlastně největším špiónem internetu, ačkoliv o těch, kteří jsou považováni za jedny z největších, bude pojednáno v některé z pozdějších kapitol. Je každopádně důležité zdůraznit, že ačkoliv koncept Panoptikonu byl jedním z hlavních impulzů pro zahájení bádání v oblasti dohledu, v současnosti je již poněkud vyčerpán a nahrazen právě konceptem Synoptikonu, jenž je dle slov Zygmunda Baumana zástupcem DIY³³ dohledu – dohledu, který nad sebou uživatelé vykonávají sami, bez nutnosti konceptu jakýchkoliv dozorců³⁴.

Kromě Synoptikonu pak v rozličné literatuře můžeme najít i další termíny, které označují změnu, jíž koncept Panoptikonu prošel v současném postmoderním prostředí – Didier Bigo například mluví o konceptu *Banoptikonu*³⁵, jenž značí, že někteří lidé mají v určitých uzavřených a pod dohledem se nacházejících systémech větší svobodu, než jiní.

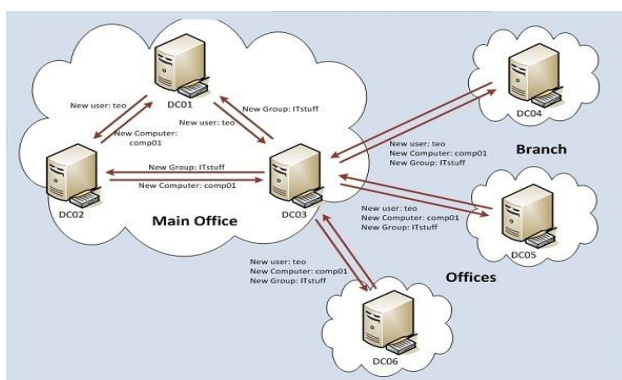
Například arabsky vypadající osoby budou po útocích z 11. září častěji podrobovány letištní kontrole, nežli ty, které tyto personální znaky nesdílejí. Dohled se tak v podstatě stává novou formou sociální stratifikace a sociálního škatulkování (*social*

³³ Z anglického termínu *Do It Yourself*, jenž označuje činnost, vykonávanou svépomocí.

³⁴ BAUMAN, Z.; LYON, D.: Tekutý dohled, Arch-polygrafické práce, Brno, 2013, str. 73

³⁵ BIGO, D., 2005

sorting)³⁶, a jelikož se k těmto úkonům v posledních letech začíná přidávat i pozvolně se rozvíjející metoda predikce (tedy snaha odhadnout, kdo by mohl být potenciálně nebezpečný sobě, či svému okolí na základě určitých vzorců jeho chování), zjišťujeme, že digitální uzavření, v němž se nacházíme, skutečně přechází do fáze, v níž začíná fungovat jako nástroj, určený k opětovné snaze o ustanovení bezpečí, které tak zoufale postrádají postmoderní sociologové – například výše jmenovaní Anthony Giddens a Zygmunt Bauman.



Obrázek 2 – Schéma zapojení počítačů v síti, umožňující snadný synchronní dohled

1.4.5. Roger Clarke a dataveillance

Stěžejní teorii současného dohledu v době elektronických médií posléze rovněž přináší australský vědec Roger Clarke, když tyto dohledové vztahy označuje termínem *dataveillance* (*data dohled*), který charakterizuje jako: „*systematické užívání systémů, zpracovávajících osobní data při zkoumání a monitorování jednání nebo komunikací jedné nebo více osob*“³⁷ Výhodou takového řešení je pochopitelně ekonomická efektivita

³⁶ ANDREJEVIC, M.: *iSpy: Surveillance and Power in the Interactive Era*, Univ Pr of Kansas 2007, str. 94

³⁷ CLARKE, R.: *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. *rogerclarke.com*, dostupné z: <http://www.rogerclarke.com/DV/Intro.html#DV>

– po vytvoření programu, schopného automatického sběru dat, již není nutné dalších radikálních zásahů, či aktivity sledující osoby a všechny údaje jsou generovány, tříděny a indexovány automaticky.

Clarke rozlišuje dva druhy tohoto dohledu – osobní a masový. Osobním je označováno systematické monitorování komunikace a interakcí jedné identifikované osoby, či subjektu. Masový dohled je posléze zaměřen na větší skupiny osob – a může sloužit jak k jejich identifikaci, tak například zastrašování pomocí získaných dat a informací.

Dataveillance je pochopitelně v prostředí elektronických médií již převládající technika a jedinec se tak v podstatě mění na shluk dat (která jsou získávána z jeho digitálního dvojníka, datového stínu). Zde lze najít parafrázi se systémem kartoték a systematizací dat ve druhé fázi vývoje dohledu, ovšem užitými technikami jednoznačně spadá do fáze třetí – interface.

Clarke je každopádně relevantní především díky rozlišení tohoto vývoji v rámci dohledu – od zkoumání samotné osoby ke zkoumání dat, jež osobu zastupují (či ji nějakým způsobem charakterizují).

1.4.6. Big data

S neustálým rozšiřováním objemů vytvářených dat a datových toků je rovněž potřeba úměrně zvýšit kapacitu nástrojů, nutných k jejich zaznamenávání. Kvůli neskutečným objemům institucemi sbíraných osobních dat, jež si lze jen těžko představit (například v roce 2013 se již vyjadřovala v řádech desítek terabytů, či petabytů), je potřeba tyto balíky informací, které jsou přijímány z různých odvětví elektronické komunikace, například při používání platebních karet a bran, RFID čipů, chytrých

telefonů, sociálních médií, webových vyhledávačů a podobně skladovat v obrovských datových skladech, někdy rovněž nazývaných *datová centra*. Toto skladování informací je doménou především soukromých firem, ale zabývají se jím i státy a některé další veřejné instituce. Všechna data se posléze analyzují a využívají pro další účely. Největším zájemcem o tyto informace je pochopitelně především komerční sféra a marketing, ovšem jsou známy i případy, kdy velkými data centry disponují i tajné vládní organizace, například FBI, či NSA³⁸ a tamější analýzy se zaměřují především na predikci a vyhledávání potenciálních teroristických skupin a dalších narušitelů vnitrostátního i vnějšího pořádku. V tomto odvětví se pochopitelně předpovídá pouze růst a otázkou zůstává, zdali někdy situace dospěje do stádia, že objem dat nebude možné ukládat již vůbec.

Se stále rostoucím segmentem chytrých mobilních telefonů, GPS navigací, sociálních služeb všeho druhu a nově i chytrých domácností, operačním systémem vybavených televizorů, lednic a praček³⁹, se zdá, že se situace, kdy obrovská datová centra přestanou stačit, dočkáme možná i relativně brzy.

1.4.7. Koncept produsers jako způsob uživatelského vytváření obsahu

Producersage je termín, jehož autorství je často připisováno americkému profesoru Axelu Brunsovi a poprvé jej formuloval ve svém díle *Blogs, Wikipedia, Second Life and Beyond: From Production to Producersage*⁴⁰. Jedná se o popsání změny v procesu samotné tvorby (nejen) reklamních sdělení a vytváření internetového obsahu. Zatímco dříve byly vztahy výrobce – příjemce sdělení jasně diferencovány, v prostředí elektronických

³⁸ National Security Agency, v překladu Národní bezpečnostní agentura.

³⁹ Tato vybavenost zařízení je IT odborníky i obchodníky často nazývána *Internet věcí* – anglicky Internet of Things a zdá se být moderním trendem, jenž brzdí pouze různé technické komunikační standardy napříč zařízeními jednotlivých výrobců.

⁴⁰ BRUNS, A.: *Blogs, Wikipedia, Second Life, and Beyond: From Production to Producersage*, Peter Lang Publishing, 2008

interaktivních médií je toto pouto často bořeno právě ve prospěch využívání vztahu *producers*. Samotné slovo vzniklo spojením dvou anglických slov *user* a *producer* a vyjadřuje právě tuto změnu – od pasivního příjemce sdělení a konzumenta k příjemci sdělení a zároveň jeho tvůrci.

Původně bylo sousloví spojeno s principem současné demokratizované síťové komunikace a koncepty uživateli vytvářeného obsahu – za příklad může sloužit otevřená encyklopedie Wikipedia⁴¹ (počátek fungování roku 2001), jejíž jednotlivá hesla mohou být volně editována – a to téměř kýmkoliv.

Ovšem v osidlech současné komunikace se pojí spíše s opačnými účinky - marketingové a různé reklamně - produkční firmy si totiž postupem času uvědomily, že pracovat s komunitou lidí, kteří mohou být v podstatě považováni za *cílovou skupinu* jejich produktu, je jednodušší a také podstatně levnější, než najímat nové pracovníky, kteří tato sdělení za úplatu vytvářejí. Od těchto fanouškovských „komunitních manažerů“ (tedy dobrovolníků, kteří například firmě mohou spravovat fórum, za příslib napsání dobré reference do životopisu, či s výhledem na pozdější možnou nabídku zaměstnání), či kampaní, které jsou založeny přímo na interakci s komunitou a jejími příslušníky – často je komunitní management dělán v podstatě zdarma a s nadšením.

V kapitole, věnované konceptům Marka Andrejevice uvedený příklad kampaně firmy Nike iD je posléze pouze špičkou ledovce. Firmy často prostřednictvím svých PR, či marketingových oddělení a jejich zaměstnanců vyzývají své fanoušky, aby jim posílali různé vyplněné dotazníky, či zpětnou vazbu, své fotografie a další materiály, které je posléze jednoduché přetavit do marketingové kampaně. Čím oblíbenější pak firma a její produkty jsou, tím větší šance, že obdrží zpětnou vazbu v podstatě zdarma, zatímco

⁴¹ *Cs.wikipedia.org*, dostupné z: <https://cs.wikipedia.org>

některé menší firmy, které by pro další úspěšný růst a rozjezd právě tyto informace nejvíce potřebovaly, mají s jejich sběrem veliké potíže.

Koncept *producers* tedy můžeme vnímat, jako, dá se říci, výhodný spíše pro jednu ze dvou zúčastněných stran. Firma, či korporace, nejen, že snadno zjistí preference svých zákazníků, ale přenese na ně část nákladů, které by jinak musela při tvorbě komerčního sdělení vynaložit s často stejným výsledkem. Je sice pravdou, že oproti klasickému vztahu *výrobce-příjemce* nemá nad příspěvky, které ze samotné povahy vztahu zpracovávají fanoušci, tedy externí osoby, takovou kontrolu (pokud tyto nejsou důsledně vnitrofiremně spravovány), ovšem je velice složité odmítnout práci, která je nabízena zdarma - a navíc – v případě problému je mnohem snazší se od nevhodného sdělení distancovat a přenést odpovědnost na samotného jeho tvůrce.

Mezi další specifika konceptu *producers* rovněž patří i přeposílání sdělení dalším uživatelům, ať už v rámci systému tzv. *referral*⁴², či jako protislužba za určité výhody, které z toho takovému přeposílateli plynou. Produšeři tedy nejen, že často nezištně vytvářejí a spravují firemní internetové stránky, fóra, či *microsite*, v ideálním případě jsou navíc schopni na ně pouhou interakcí s komunitou přivést i další uživatele, tedy potenciální zákazníky. Je snad již nad slunce jasné, že tento koncept má neskutečný potenciál, kterého jsou si určité firmy moc dobře vědomy a hodlají je v prostředí internetu patřičně využít a již jen samotný uživatelský příspěvek na fóru má pro firmu velikou cenu, jelikož kolem firmy a jejích produktů vytváří bzukot, aktivitu.

⁴² Dle publikace JURÁŠKOVÁ, O.; HORŇÁK, P. et al.: *Velký slovník marketingových komunikací* se jedná o formu *word of mouth marketingu*, díky kterému mohou uživatelé doporučovat určitý produkt, či službu ostatním uživatelům. V reálném užití se často jedná o doprovodný jev například různých firem na bázi pyramidového systému, či v rámci určitých volně hratelných počítačových her, které jsou postaveny na užití mikrotransakcí uvnitř samotné aplikace.

2. PROBLEMATIKA DOHLEDU V KONTEXTU MODERNÍHO MEDIÁLNÍHO PROSTORU

2.1.1. Nástup Webu 2.0 a zrození nové interaktivity

Nejspíše většina čtenářů tohoto textu již někdy slyšela o konceptu Webu 2.0, což je termín, který byl poprvé použit v roce 1999 autorkou Darcy DiNucci v jejím článku „Fragmented Future“⁴³. DiNucci tímto termínem chtěla postihnout změnu, která se v rámci vývoje World Wide Webu odehrála od jeho vzniku po tehdejší současnost, jež nejpozději počátkem 21. století začínala být nakloněna vyšší míře interaktivity díky neutuchajícím investicím do vývoje tohoto nového elektronického média. Klasický programovací jazyk HTML (*Hyper Text Markup Language*), jenž nadále zůstal hlavní pohonnou jednotkou webu, byl postupem času plynule doplňován prvky, které zajišťovaly objektové programování. Tak hojně vznikaly různé extenze a přídatky, se kterými se můžeme setkávat i dnes – například Java (vyvinuta společností Sun

⁴³ DINUCCI, D.: Fragmented Future, Print Magazine 1999, str. 32, dostupné z: http://darcy.com/fragmented_future.pdf

Microsystems v roce 1995), či Adobe Flash, poháněný programovacím jazykem ActionScript.

Právě Flash i v současné době těží ze stále pevné tržní pozice, z velké části i díky faktu, že právě Flash Player je používán k přehrávání videí na největší video službě světa – Youtube, jež je vlastněna a spravována společností Google.

Web 2.0 tedy do statických stránek, zřetězených pomocí hypertextových odkazů, přinesl něco, co jeho dřívější mutace tak zoufale postrádaly – totiž zvýšenou míru interaktivity a rychlý nárůst objemu audiovizuální informace. Nyní bylo možné kromě statických stránek přidávat i velké množství animovaných obrázků (například ve formátu GIF), oblíbenými se brzy staly i všemožné webové animace a flashové bannery, které se, zvláště v začátcích, ukázaly být relativně efektivním způsobem internetové reklamy, jež pestrými animacemi hojně poutala uživatelskou pozornost. V současnosti se již, nutno podotknout, od všemožných animovaných bannerů pomalu začíná upouštět, jelikož bývaly častým zdrojem virových nákaz počítačů, do kterých se dostávaly přes bezpečnostní díry právě Adobe Flash.⁴⁴ Přesto však právě tato změna, jež se odehrála koncem 90. let a přinášela pohled do budoucnosti, která měla patřit a také patří ultra interaktivnímu virtuálnímu prostoru, měla být vyjádřena označením, jež povyšovalo tehdejší World Wide Web na novou verzi, úroveň.

Pochopitelně netrvalo dlouho a firmy si všimly obřího reklamního potenciálu, jenž se ve zrození interaktivního prostoru nachází. Pokud v roce 1995 bylo na internet připojeno pouhé asi 1% celkové populace a míra zasažení populace internetem tvořila asi 1,3 %, v roce 1999 to bylo už 4,6%. Ve statistikách pro rok 2014 se hovoří o 40,4%, což

⁴⁴ Když dírou do systému, tak přes Adobe Reader, Flash, nebo Javu. *Viry.cz*, dostupné z: <http://www.viry.cz/kdyz-dirou-systemu-tak-pres-adobe-reader-flash-nebo-javu/>

činí více než 2,9 miliardy internetových uživatelů, či osob, které mají připojení k dispozici - a prognózy pro rok 2015 jsou pochopitelně podobně optimistické, jako pro každý rok předešlý. Podíl internetových uživatelů jednoduše každým rokem vytrvale roste a s ním roste i míra možností, jakými řídit svůj internetový byznys.

Pokud se Pierre Lévy koncem 90. let rozplýval nad zvýšenou mírou interaktivity a dosud nevídané demokratizace⁴⁵, kterou koncept rhizomaticky zesíťovaného mediálního prostoru přinášel, musel by se nad současnou situací minimálně podívat. Zdá se, že individualizace a demokratizace, která měla každému internetovému uživateli přinést možnost svobodně se vyjádřit, vyměňovat si zkušenosti i informace s dalšími uživateli, dostává tvář v tvář současné situaci nový rozměr.

Není cílem práce čtenáře příliš zatěžovat obsáhlou historií vývoje internetu, kterým se dospělo až do fáze, jakou známe dnes – k nadvládě elektronických sociálních médií a sítí. Přesto však nelze pominout alespoň drobný exkurz do toho, co jim předcházelo a jakým způsobem sběr zákaznických uživatelských dat v rámci elektronických médií probíhal právě před jejich masivním nástupem.

2.1.2. Dohled před nástupem sociálních médií – microsites, webové stránky a internetová fóra – personalizace obsahu

Potřeba sběru specifických uživatelských dat⁴⁶ se pochopitelně objevovala ještě před započítáním jejich dobrovolného odevzdávání v současné společnosti, kterou někteří odborníci, jako například Bauman, či Trottier, nazývají společností „internetového voyerismu“. Klasické „offlinové“ firmy, i mladí, draví podnikatelé, kteří v průběhu 90. let pomalu objevovali další prodejní kanál, jímž by se velmi dobře mohlo tak pokrokové

⁴⁵ LÉVY, P.: Kyberkultura, Karolinum, 2001, str. 115

⁴⁶ A specifická, je, zdá se, naprostá většina z nich.

médium, jakým již tehdy byl internet, stát, pomalu přicházeli s možnostmi, jak svůj internetový byznys rozšiřovat. Již v 90. letech bylo mnohým internetovým podnikatelům známo, že výpovědní hodnota uživatelských dat, jejich preferencí, historie nákupů a dalších, především s nákupem spojených úkonů, je značná a že bez sběru těchto dat nemají šanci zoptimalizovat a dále vylepšovat svůj byznys.

Marketingové výzkumy nebyly v té době již nic nového a offline komerce jimi byla přesycena. Tudíž zbývalo přenést již publikované poznatky a aplikovat je na novou situaci, která se s nástupem komerčního využití internetu vytvořila.

Když Jeff Bezos v roce 1994 zakládal dnes největší internetový obchod Amazon, byl si této situace až příliš dobře vědom a po několika měsíční epoše, během níž se jeho internetový obchod zaměřoval pouze na knihy, přistoupil i k dalším výzkumům, o jaké zboží by zákazníci měli zájem. A jelikož zájem byl o rozličné věci, tak je Jeff se svou firmou brzy začal nabízet. A o tom, že se jednalo o úspěch, svědčí současné tržby Amazonu, jež se za rok 2013 se odhadují na 25,59 miliard dolarů, což oproti roku 2012 představuje zvýšení o pětinu⁴⁷. Amazon se spoléhal a nadále spoléhá především na široký sortiment (jejich mottem bylo a je, že je možné sehnat a následně zákazníkem přes internet objednat téměř vše), ale zároveň velkou mírou *personalizace*, což je termín, u kterého bychom se měli zastavit, jelikož nás bude provázet v podstatě neustále.

Personalizace je v samé podstatě přizpůsobení služeb na míru. Je jasné, že každý zákazník má rozličné požadavky, má rád rozličné, pro něj na míru přizpůsobené zboží a právě u něj je statisticky největší šance mu je prodat. Uvedme si příklad s oblíbenou značkou parfémů, oblečení, spotřební elektroniky, oblíbeného autora knih, filmový žánr a

⁴⁷ Amazon zvýšil zisk i tržby. Investory ale zklamal, čekali ještě lepší čísla. *Byznys.ihned.cz*, dostupné z: <http://byznys.ihned.cz/c1-61639880-amazon-zvysil-zisk-i-trzby-investory-ale-zklamal-cekali-jeste-lepsi-cisla>

podobně. Kdokoliv s pomocí prohlížeče vstupuje do internetového obchodu, povětšinou tak činí s intencí si něco koupit, či se jen na své vysněné zboží podívat, nebo porovnat parametry a posléze se pro určité zboží rozhodnout.

Tohoto módu spotřebního chování si velice rychle všimli nejen provozovatelé e-shopů a zaměstnanci jejich marketingových oddělení, ale především samotné *internetové vyhledávače*, které jsou často pomyslnou vstupní branou do prostoru internetu a e-komerce. Personalizace, tedy přizpůsobení obsahu na míru pro konkrétního zákazníka/uživatele již nevyhnutelně musí začínat zde.

Internetový vyhledávač tedy s pomocí tzv. cookies, jež se automaticky ukládají do prohlížeče, zjistí, o jaké zboží se dotyčný zajímá a dle toho mu nabídne obsah, určený přesně na míru pro něj. Brouzdá-li tedy určitý uživatel například stránkami, které jsou zaměřeny na fotbalové zpravodajství, vyhledávač automaticky vyhodnotí, že dotyčný je fotbalový fanoušek a nejspíše mu při dalším vyhledávání nabídne reklamu, která opět bude zaměřena sportovním směrem. Tento přístup k reklamě se nazývá kontextová reklama a jedná se o jeden z nejklassičtějších způsobů, jakým v rámci webových stránek cílit reklamu na konkrétního uživatele.

S tím souvisí i další, modernější marketingový postup - a to takzvaný remarketing. Ten využívá PPC systému Google AdWords a obecně se mezi marketéry soudí, že jde o systém, jenž je ve srovnání s ostatními marketingovými nástroji několikrát účinnější.

Remarketing je postaven na podobné bázi, jako výše zmíněná kontextová reklama. Pomocí informací, obsažených v cookies, a na základě unikátní IP adresy návštěvníka systém AdWords vyhodnotí, jestli uživatel na stránky přichází opakovaně a dle historie vyhledávání mu další obsah přizpůsobí na míru – každý specifický uživatel tak například

uvidí jiný reklamní banner, jenž bude personalizován přesně podle jeho minulých hledání na dotyčných stránkách.

Z českých řešení, určených pro remarketingové aktivity, lze jednoznačně uvést český Sklik⁴⁸, který spadá pod oblíbený český portál Seznam.cz a jedná se v podstatě o domácí ekvivalent globálního Google AdWords. Jelikož se mezi tuzemskými firmami v diskuzích často vedou spory o výhodnosti jednoho, či druhého řešení⁴⁹ (příčemž princip obou je podobný), jejich podrobnější srovnání je lepší ponechat mimo rámec této práce.

Tyto systémy jsou povětšinou založeny na jedné premise – že uživatel, kterému systém nabídne personalizovaný obsah, bude mít větší nutkání si jej zakoupit, než za stavu, když by se k produktu musel dostat prostřednictvím hned několika hypertextových odkazů. Marketéři se tak snaží využít informací, které je schopen automaticky a zcela logicky obstarat samotný prohlížeč, aniž by museli vynaložit jakékoliv další úsilí k jejich získávání.

Jak vidíme, Google, jakožto firma, která se již od dob Gmailu⁵⁰ snaží razit filosofii poskytování veškerých svých služeb zdarma s cílením na co největší počet uživatelů, spoléhá právě na pozici poskytovatele reklamních řešení, která je schopna dodat díky agregovaným datům z vyhledávačů (a rovněž se nebojí jít ani tak daleko kvůli další porci dat číst i uživatelské e-maily, jak v roce 2014 informoval například magazín *The Inquirer*⁵¹.

⁴⁸ Sklik.cz, dostupné z: <https://www.sklik.cz/>

⁴⁹ V našich podmínkách, nasazení Skliku v globálním kontextu nedává smysl.

⁵⁰ Gmail je e-mailový poštovní klient společnosti Google, jenž byl založen roku 2004. K datu 28.5.2015 má kolem 900 milionů uživatelů – viz. *By the Numbers: 12 Amazing Gmail Statistics*. *ExpandedRamblings.com*, dostupné z: <http://expandedramblings.com/index.php/gmail-statistics>

⁵¹ Google admits its reading your emails. *theinquirer.net*, dostupné z: <http://www.theinquirer.net/inquirer/news/2340003/google-admits-its-reading-your-emails-because-advertising>

Toho si všímá Mark Andrejevic, když píše: „*Pokud v dávných dobách služby jako Google, či Facebook mohly být považovány za nezpлатněné služby, které byly poskytovány komerčními firmami s nejasnými motivy, stále více se přibližujeme k méně romantické představě výměny, která se za tím vším skrývá – za tyto služby neplatíme jen naší pozorností, kterou jim věnujeme, ale platíme našimi daty.*“⁵² Andrejevic zde rovněž rozvíjí koncept jakéhosi dluhu – podvědomě uživatel cítí, že za službu by měl nějakým způsobem zaplatit a autor se domnívá, že právě poskytnutím jeho dat je tento dluh formálně splacen.

Thomas Allmer, Christian Fuchs, Verena Kreilinger a Sebastian Seignani, kteří v jedné kapitole knihy *Media, Surveillance and Identity* zveřejnili výsledky výzkumu, jenž byl proveden na vzorku 3,558 rakouských studentů, ovšem dodávají: „*Když jsme se zeptali našich respondentů, jestli skutečně chtějí, aby webové stránky přizpůsobovaly reklamu jejich osobním zálibám, neotřesitelná většina 82,1% byla proti těmto praktikám.*“⁵³ Zdá se tedy, že uživatelé tento koncept personalizace reklamního obsahu příliš v oblibě nemají a nedůvěřují mu.

K problematice poskytování uživatelských dat se ještě vrátíme později, tento rozbor byl pouhou snahou nastínit, jakým způsobem se již samotným procesem zadání vyhledávací fráze do vyhledávače formujeme jakožto potenciální zákazník.

Za pro zmínění důležitou lze posléze uvažovat i problematiku *microsites*, tedy jakýchsi přidružených stránek, které jsou jejich autory vytvářeny s několika úmysly:

⁵² ANDREJEVIC, M. in JANNON A.; CHRISTENSEN, M.: *Media, Surveillance and Identity: Social Perspectives (Digital Formations)*, Peter Lang Publishing, 2013, str. 97

⁵³ tamtéž str. 59

- 1) buď jsou vytvořeny jakožto podpora prodeje samostatného produktu v rámci určité řady (parfémy Old Spice pro muže a pro ženy mohou mít například oddělené marketingové stránky), s odkazem na domovskou stránku firmy Old Spice, či
- 2) mohou sloužit coby alternativní prostor, v jehož rámci se lze vyjádřit k domovské značce, či si vyměnit názory a informace se zaměstnanci značky – za příklad můžeme uvést microsite *Na Rovinu!*⁵⁴, která se do určité míry dá brát jako CRM⁵⁵ stránka firmy McDonald's, jejímž prostřednictvím se uživatelé mohou anonymně ptát na věci kolem pokrmů i firmy samotné, nebo například microsite hudební skupiny Aquababes⁵⁶, která je ovšem očividně propojena s marketingovými aktivitami značky Aquila a tedy firmy Karlovarské Minerální Vody a.s.
- 3) slouží jakožto alternativní firemní prostor, jakýsi blog, na který zaměstnanci (či prodávající) přidávají postřehy a komentáře. Tuto určitou neformálnost a hravost, se kterou microsite může být psána, lze nadále využít k vylepšení image společností a značek jako takových.

Microsites bývaly, zvláště v dřívějších dobách, častým a poměrně účinným prostředkem, jak přilákat publikum (tedy vytvořit návštěvnost, tzv. traffic) na domovské stránky společnosti. Kvůli problematice ohledně kódování a psaní microsites, což je proces, jenž se příliš neliší od vytváření klasických webových stránek, ovšem jejich četnost začíná rapidně klesat ve prospěch firemních profilů na sociálních sítích, které poskytují již hotovou platformu, a vyžadují jen obsah. Nutno však dodat, že, například v případě zmíněného užití firmou McDonald's v projektu *Na Rovinu* microsites stále fungují jako relativně dobrý indikátor toho, co zákazníci od produktů firmy očekávají,

⁵⁴ <http://www.narovinu.mcdonalds.cz/>

⁵⁵ Customer relationship management – vytvoření partnerského vztahu mezi zákazníkem a společností.

⁵⁶ <http://aquababes.cz/>

jsou cenným zdrojem připomínek a rad, jak dále optimalizovat a rozšiřovat nabídku zboží a služeb.

Opět se tedy jedná o již viděný jev – společnost získá (pozitivní) reklamu a zároveň, coby vedlejší produkt, spoustu rad od samotných zákazníků a uživatelů. Ceněné jsou samozřejmě i negativní reakce, které opět mohou být dále zapracovány do různých reportů a vést ke zkvalitnění, či optimalizaci portfolia nabízených služeb a zrušení těch, které se netěší přílišné zákaznické oblibě. Pro firmu se tedy jedná o situaci, během níž je relativně složitě ztrácet, ale jednoduché získat.

S dohledem se pochopitelně můžeme setkat i v případě různých internetových fór, jež byla ještě donedávna jedněmi z největších internetových sociálních médií vůbec. Vyvinula se koncem 70. let 20. století z různých bulletin boards, což byly stránky, na kterých si uživatelé mohli nechávat různé vzkazy a diskutovat na různá témata.

Internetová fóra byla a stále jsou prospěšná především uzavřenějším komunitám se specifickými zájmy – oblíbená jsou například v oblasti zábavy (existují např. rozličná filmová, videoherní, hudební fóra), či životního stylu (mateřství, poradny různého typu a jiné). Výhodou internetových fór z hlediska dohledu a sondování osobních údajů oproti sociálním médiím současného typu je, že jsou jednodušeji sledovatelná.

Informace, které se na internetových fórech nacházejí, jsou relativně stabilní, neproměnné a nepodléhají tolik mnohanásobným editacím a rychlé možnosti přepsání, či smazání. Díky struktuře fóra, kdy odpovědi jsou lineárně přiřazeny každému vláknu zvlášť, jdou veškeré informace relativně dobře srovnat a roztřídit.

Osoby, které se posléze internetovým dohledem zabývají (ti nebývají pro samotné uživatele viditelné, často se jedná o subjekty různých tajných služeb, zaměstnanců oddělení pro boj s kybernetickým zločinem, ale i například nebezpečné *stalkery*) a jsou

jeho vykonavateli, tak mohou jednoduše postupovat podle vláken a snadno tak organizovat získané informace. Nevýhodou internetových fór pro účely současných firem, které chtějí získávat data a pracovat s uživatelskou komunitou, je posléze jejich relativně obtížná dostupnost pro samotného uživatele – zatímco na sociálních sítích je možné se z jednoho uživatelského profilu přihlásit do, v podstatě jakékoliv skupiny a všechny příspěvky tak mít ihned dostupné a zobrazitelné, internetové fórum často vyžaduje registraci, což je první překážka k přilákání čtenářů a diskutérů.

Dá se říci, že každé specifické fórum vyžaduje od uživatele alespoň minimální míru aktivity, zatímco sociální síť je jedním globálním řešením – s jedním přihlášením se uživatel dostane do všech jejích koutů, pokud jsou mu dostupné (tedy dostupnost určitých skupin není specificky určena jen jejím vybraným uživatelům) a ihned může začít interagovat. Fórum pak zůstává funkce specializovaného prostoru, v němž lze vyhledat specifické informace a názory uživatelů, které spojuje stejný zájem do takové míry, že jsou ochotni podobnou registrační proceduru podstoupit.

Sběr dat u těchto média typů lze tedy charakterizovat přibližně takto – jedná se o asymetrický vztah, vysoce automatizovaný, kdy uživatel již tím, že vstupuje na nějaké internetové stránky přes webový prohlížeč, zanechává svou digitální stopu prostřednictvím dat, přidaných do cookies prohlížeče, ze kterých jsou posléze vybrány informace, jež slouží k nějakým dalším účelům (k identifikaci návštěvníka, k analýze jeho nákupního chování a podobně).

Samozřejmostí je v rámci internetových fór i dohled ze strany státních, soukromých, polovládních/agenturních a dalších institucí, které především dohlížejí na online bezpečnost a pořádek – ovšem to je pochopitelně skutečnost, o které se na veřejnosti nemluví a pro zainteresované osoby je žádoucí, aby se nemluvílo – a tedy

internet nadále alespoň formálně zůstává nikým nevlastněným a hlavně nekontrolovaným médiem (na skutečnost, že internet a další elektronická média jsou sledována, poukázal v roce 2013 i Edward Snowden, do té doby zaměstnanec CIA, který informace, jež tato sledování prokázala⁵⁷ předal novináři Glenovi Greenwaldovi a tím si vysloužil hrozbu exemplárního potrestání ze strany vládní garnitury USA, čímž je mu efektivně znemožněn návrat na území Spojených států).

K nejvýznamnější práci těchto složek patří potírání kybernetické kriminality, mezi níž se často řadí pirátství autorským zákonem chráněných audiovizuálních děl, po 11. září sledování teroristických hrozeb a dále je důraz kladen především na boj proti šíření dětské pornografie, která se v 90. letech distribuovala právě prostřednictvím internetových fór, později přes torrentové klienty⁵⁸ a konečně, díky intranetu, či různým, relativně neprostopupným, na soukromém, pozvánkovém systému založeným „*oblastem internetu*“, zvaných dark web⁵⁹. Právě sem se často stahují uživatelé, kteří mají nějaký důvod chránit se před dohledem výše zmíněných institucí, k jehož setřesení nestačí anonymizér, či VPN tunel.

Za příklad dark webu lze uvést hned jeho nejznámějšího zástupce – internetový černý trh Silk Road, na němž neměl uživatel problém sehnat různé lehké i těžké drogy, zaplatit likvidaci nepohodlné osoby nájemnými vrahy, obstarat padělané doklady a podobně, přičemž platba probíhala pomocí nevystopovatelné kryptoměny Bitcoin⁶⁰.

⁵⁷ Jednalo se o projekty PRISM a Tempora, které umožňují vládním složkám přístup k všemožným osobním informacím a datům – dále viz. CDR SecUpdate 23 – Důkazy o špehování uživatelů: Google, Facebook, Apple, Yahoo, Skype. *Cdr.cz*, dostupné z: <http://cdr.cz/clanek/cdr-security-update-projekt-prism-umoznuje-vladam-spehovat-komunikaci-obcanu>

⁵⁸ Torrent, či někdy označovaný BitTorrent, je nástroj pro P2P distribuci souborů s rozkladem přenosových dat mezi klienty. V podstatě se jedná o situaci, kdy jeden uživatel poskytuje určitý úsek dat ke stažení jinému uživateli, čímž odpadá nutnost vlastnit fyzický server. Ten je použit pouze pro indexování, vyhledávání souborů, které se nacházejí ve specifikovaných složkách na klientském počítači. Takovému serveru se říká tracker

⁵⁹ Most of the Web is Invisible to Google. Here's what it contains. *Popsoci.com*, dostupné z: <http://www.popsoci.com/dark-web-revealed>

⁶⁰ Což byl mimochodem jeden z důvodů, jenž během roku 2014 vedl k raketovému nárůstu jeho ceny.

Zrovna Silk Road však nedávno přestal operovat, když soud jeho autora Rosse Ulbrichta poslal na doživotí do vězení⁶¹.

Přesto – samotná existence jevů, jako jsou intranet, či dark web, poukazují na skutečnost, že i v rámci zdánlivě perfektně viditelného prostředí internetu existuje množství odlišných prostředí a situací, což jen podporuje teorie některých badatelů, kteří tomuto elektronickému médiu v odkazu na Felixe Guattariho a Gillesse Deleuze přisuzují rhizomatickou strukturu, kdy z každého oddenku může vyrůst jiný v absolutní nenávaznosti na jakýkoliv další a vytváření dalších formací nelze nikdy dopředu předvídat.

2.1.3. Dohled v rámci sociálních sítí

Koncept sociální sítě je v podstatě pokračovatelem internetových fór, ovšem oproti nim přináší větší porci interaktivity, díky které se sociální sítě v souladu s filosofií Webu 2.0 brzy staly celosvětovým fenoménem. Uživatelé mohou psát, publikovat a zobrazovat rozličné příspěvky a sdílet je se svými přáteli, či uživateli po celém světě. Kromě toho ovšem vybrané sociální sítě rovněž disponují možností chatu v reálném čase (tedy funkcí, jež je odvozena z dřívější existence a oblíbenosti programů typu IRC⁶², jakými jsou například ICQ, či mobilní Viber). Jedná se o tzv. řešení vše v jednom – kromě osobního prostoru pro tvorbu a publikování tzv. statusů má uživatel k dispozici i rychlý synchronní chat, pomocí kterého se lze snadno spojit s kterýmkoliv uživatelem, ať už se ten nachází v listu takzvaných Přátel (Friends), či nikoliv.

⁶¹ Silk Road Creator Ross Ulbricht Sentenced to Life In Prison. *Wired.com*, dostupné z: <http://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/>

⁶²IRC je zkratka pro Internet Relay Chat, jedná se o jedno z prvních řešení internetové komunikace v reálném čase – v podstatě jde o programy, potřebné pro synchronní online chatování

V současnosti je pochopitelně nejčastěji autory z oboru Surveillance studies uváděna a analyzována sociální síť Facebook, jelikož má na vývoj internetu a vůbec celého odvětví našeho soukromí největší vliv. S více jak 1,4 miliardou uživatelů⁶³ daleko vede i před dlouho připravovanou sítí Google+, která, i přes svou komplementaritu s největší video službou internetu Youtube zdaleka nedosahuje takové oblíbenosti a počtu aktivních uživatelů, kterých je v rámci Google+ řádově méně – odhady hovoří o údajích 300 milionů, přičemž mezi internetovými uživateli kolují vtipy, že jde pouze o zaměstnance společnosti Google a jejich rodiny.

Úspěšnější jsou v tomto porovnání například sociální síť WhatsApp, primárně určena pro mobilní telefony se 700 miliony, či čínská QQ s 800 miliony uživatelů. LinkedIn se může pochlubit 347 miliony, Skype podobným číslem jako Google+, tedy 300 miliony⁶⁴.

Jelikož je Skype od roku 2011 vlastněn společností Microsoft, vidíme, že tento IT moloch se snaží alespoň částečně držet krok se společností Google, podobně, jako v segmentu chytrých telefonů, kde nabízí konkurenční operační systém i vlastní mobilní řešení. To pochopitelně není náhodou, jelikož ve vytrvale rostoucím segmentu právě těchto chytrých mobilních zařízení (viz. Obrázek č. 3) se, zdá se, ukrývá neskutečný a dosud plně nevytěžený potenciál, uvážíme-li, že dle vlastních slov společnosti Google se v roce 2015 již v 10 zemích více vyhledává s pomocí mobilního telefonu, než klasického počítače – desktopu⁶⁵.

⁶³ Leading social networks worldwide as of March 2015, ranked by number of active users (in millions). *Statista.com*, dostupné z: <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>

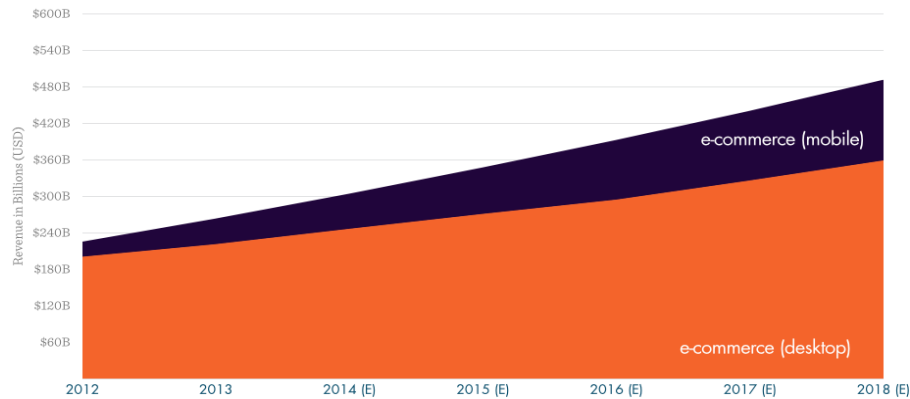
⁶⁴ tamtéž.

⁶⁵ Building for the next moment. *Adwords.blogspot.co.uk*, dostupné z: <http://adwords.blogspot.co.uk/2015/05/building-for-next-moment.html>

E-Commerce Growth Will Be Driven by Mobile



US desktop e-commerce and mobile e-commerce sales 2012 - 2018 (estimated)



eMarketer April 2014 [E] designates estimates

Obrázek č. 3 – Predikce rostoucí mobilní komerce ve Spojených státech v letech 2012-2018

Zajímavostí a posledním médiem, jež je záhodno na tomto místě představit, je Twitter, který je s 288 miliony povážlivě pozadu, vzhledem ke svému renomé (zvláště) v našich podmínkách, kde patří mezi tzv. „velkou mediálně marketingovou trojku“ současných českých startupů (Facebook, Twitter, Instagram). Nutno dodat, že Twitter je specifickou sociální sítí, kdy jeden „tweet“ je omezen na 140 znaků, což mnoho firem vnímá jako limitující. Skutečnost, že lze poslat 1000 přímých zpráv a 2400 tweetů denně již posléze není zase až tak důležitá, jelikož firmy, zdá se, sázejí spíše na menší množství reklamních sdělení, aby se uživatel necítil obtěžován nadměrným množstvím informací a nabídek, jež se mohou ve vnímání uživatele snadno změnit ve spam, neboli nevyžádaná sdělení⁶⁶.

⁶⁶ (tuto skutečnost mám prakticky ověřenu i z mého pracovního úsilí, kdy se podílím na internetové komunikaci největšího e-shopu v ČR)

Facebook je jednoduše globálně úspěšný nikoliv pouze proto, že byl spuštěn již v únoru 2004 – tehdy se na trhu vyskytovaly i další sociální sítě a jim podobné služby, například Friendster (založen roku 2002), či Myspace (2003), ale proto, že se z uzavřeného univerzitního prostředí amerického Harvardu, v němž umožňoval studentům na kolejích rychlé spojení s přáteli a známými z domovského města, či s rodinou, rychle přesunul mezi ostatní uživatele, které lákal koncept Facebooku jakožto něčeho exkluzivního – původně byl totiž Facebook dostupný, podobně, jako některé další sítě, včetně Orkutu (založen Orkutem Büyükköktenem měsíc před Facebookem) pouze na pozvánku jiným uživatelem. Právě tato uzavřenost, všestrannost užití a punc exkluzivity – to vše bylo tím, co tuto mladou sociální síť rychle rozšířilo mezi tisíce, miliony a nakonec více jak 1,5 miliardy uživatelů.

Facebook je místem, kde je vše pohromadě – lze se na něm vzdělávat prostřednictvím uzavřených skupin jako v případě diskuzních fór, lze se na něm bavit díky možnosti rychle sdílet například videa z Youtube, Vimea a dalších služeb. Jeho prostřednictvím lze sdílet dokumenty, soubory (jakéhokoliv charakteru) a fotografie z dovolených. Facebook se jednoduše stává digitálním otiskem jedince par excellence – je skladištěm vzpomínek, myšlenek, osobních údajů, informací, místem zábavy s tisíci různými hrami a nekonečnou zásobou uživateli sdíleného audiovizuálního obsahu - jednoduše platformou, která je pro uživatele velice zábavná – a zároveň skýtá mnoho nebezpečí, jichž si nemusí být na první pohled vědom.

Facebook a vůbec sociální sítě jako takové totiž představují skutečnou hrozbu především z toho důvodu, že informace na nich uvedené lze velice těžko spravovat a kontrolovat. Fenomémem této nově se objevivší formy komunikace, která dle některých predikcí internetových uživatelů hrozí zcela vytlačit klasickou komunikaci tváří v tvář, se podrobně zabývá Daniel Trottier, který Facebook označuje za novou formou

„příbytku“, „domova“ (dwelling)⁶⁷. V jeho pojetí se jedná o novou formu sociálního života, nový způsob, jakým se lidé mohou prezentovat ostatním lidem a vytvářet si vlastní identitu.

Všimá si ambivalence – zatímco dříve byl internet brán coby místo, kde každý mohl být tím, kým být chtěl (z této situace pochází například vtip o tom, že na internetu se nikdy žádné ženy nevyskytovaly, jenž byl adresován na tehdejší boom různých internetových seznamek bez užití webkamer), sociální sítě tento prostor zdánlivé anonymity⁶⁸ boří. Na sociální síti každý chce být pod svým jménem, jelikož na zed' píše své názory, za které chce slyšet sova uznání od svých kolegů, známých a dalších sledujících osob. Všimá si především socializace, kterou uživatelé podstupují, když veřejně dávají svým kolegům informace o konání párty, demonstrace a podobně. Rovněž klade důraz i na schopnost sociálních sítí vyburcovat uživatele k boji za společnou věc, tedy podněcování sociálních akcí. Účastník se stává členem – je začleňován do skupiny, či hnutí, což pochopitelně může mít určité sociální projevy.

Ovšem primární důsledek těchto sítí je jiný – Trottier mluví o tom, o čem jsme se v rámci tohoto textu již zmínili – o tzv. *vystavení (exposure)*. Uživatel sociální sítě chce být viděn a zároveň vidí. Dohledová situace se tak v rámci sociálních sítí komplikuje – uživatel vidí ostatní uživatele a ti vidí jej. K tomu ovšem nevidí jiné uživatele, kteří jej rovněž sledují a sami zůstávají skrytí, přičemž on sám je takovým uživatelem, jenž sleduje jiné a sám zůstává skryt. Vztahy dohledu v rámci sociálních sítí tedy připomínají spíše pavučinu, kdy každé vlákno vede ke každému dalšímu vláknu, na rozdíl od „relativně“ (zde bych si dovolil klást důraz) lineárního dohledu v rámci statických diskuzních fór (v

⁶⁷ TROTTIER, D.: *Social Media As Surveillance: Rethinking Visibility in a Converging World*, Ashgate Publishing, 2012, str. 1

⁶⁸ KENNEDY, T.: „Gender and the Household Internet” in *Gender and Information Technology Encyclopedia*, (ed) Eileen M. Trauth, Information Science Publishing, 2006, str. 859

jejichž rámci informace není dalšími uživateli ihned viditelná a dobře sdílitelná a může být snadněji editována, než způsobí větší rozruch).

Uživatel sociální sítě jednoduše, jak si správně všímá nejen Trottier, nemůže ovlivnit počínání ostatních uživatelů, kteří mohou trvale učinit viditelným něco, co on sám nechce. Za příklad lze uvést události roku 2014, kdy nahé fotky celebrit, stažené bez jejich vědomí ze soukromých profilů na sociálních sítích opětovně vyvolaly plamenné diskuze ohledně bezpečnosti dat a informací na síti.

Komunikace na sociálních sítích je totiž vysoce kontextualizovaná, tedy lze, podobně, jako v případě kteréhokoliv jiného média, vyjmout určitý výrok, či informaci z kontextu a na jeho základě dotyčnou osobu zdiskreditovat. U internetové komunikace však tento problém nabírá na intenzitě, jelikož veškerý obsah internetových stránek si lze poměrně pohodlně stáhnout do počítače, či pořídit tzv. print screen. Nahé fotky celebrit mohou být odstraněny z jejich profilů, profilů jejich přeposílatelů a šířitelů, ovšem elektronická stopa, jejich digitální otisk, se již posléze nadále šíří internetem a i v okamžiku psaní tohoto textu jsou inkriminované fotografie bez problému dostupné komukoliv, kdo by o jejich zobrazení měl zájem. Není pak důležité, zda byly pořízeny jako ryze soukromá vzpomínka na líbánky, pro partnera, či za nějakým jiným účelem – rozhodná je pouze jejich elektronická existence.

Trottier si tohoto aspektu ztráty soukromí a z toho vyplývajících důsledku všímá i ve své další studii, kterou nazval *Identity Problems In The Facebook Era*. Obracejí se na klasiku přístupu *dramaturgické perspektivy*, amerického sociologa kanadského původu Ervinga Goffmana a především jeho dílu *Stigma*, vydanému v roce 1963. Model vzniku stigmatu, jakožto problému, vyplývajícího z narušení soukromí, posléze aktualizuje na současnou situaci. V jeho pojetí sociální média jako Twitter, či Facebook umožňují nový

typ sociálního problému – **digitální stigma**⁶⁹. Sem spadá i výše uvedený případ – pokud jsou osobní digitální data užita takovým způsobem, jímž dojde k trvalému poškození reputace, či diskriminaci, jedná se o vznik digitálního stigmatu. Takové trvalé narušení identity lze posléze označit termínem **spoiled identity**⁷⁰.

Trottier sám uvádí příklad dvou vysokoškolských studentů – Tylera Clementiho a Dharuna Raviho, přičemž jeden z nich natočil toho druhého při intimním styku s jiným mužem ve společně sdíleném pokoji vysokoškolské koleje. Ravi posléze prostřednictvím sítě Twitter pozval uživatele, aby video zhlédli. Toto „*vystavení na odiv*“ nakonec vedlo až k sebevraždě Clementiho, jenž se s nastalou situací – a možná i nechtěným coming outem - nedokázal vyrovnat⁷¹.

Schopnost sociálních médií prostřednictvím veřejné viditelnosti jedince ovládat jeho společenské renomé, vnitřní identitu, a další, pro plnohodnotný život nezbytné atributy, se ovšem nezastavuje pouze u případů tohoto jednorázového narušení identity (které prostřednictvím opakovaného přeposílání sdělení může trvat v podstatě neomezeně dlouhou dobu), důležitým a stále nepříliš často řešeným problémem je i vznik a existence fenoménu *kyberšikany (cyberbullying)*.

Jako mnoho dalších odvětví lidské činnosti, se i šikana s tím, jak se na internet postupně přesouvá valná část společnosti 21. století s přívěskem informační, stala bohužel pevnou součástí internetové kultury. Není jisté, na kolik lze věřit validitě/reliabilitě výzkumu, jenž byl proveden fondem Anti-Bullying Alliance (jelikož na věci mají svůj osobní a nejspíše i hmotný zájem), každopádně dle zjištěných údajů se již v roce 2010 ze vzorku 1452 mladých lidí (v rovnocenném poměru pohlaví 50%)

⁶⁹ TROTTIER, D.: Identity Problems in the Facebook Era (Framing 21st Century Social Issues), Routledge, 2013, str. 1

⁷⁰ tamtéž, str. 7

⁷¹ tamtéž str. 1

s kyberšikanou v nějaké formě setkala více než 31% dětí ve věku 10-11 let, 46% ve věku 12-13 let a 20% ve věku 14-15 let, přičemž 48 chlapců (7% ze zkoumaného vzorku) a 46 děvčat (6%) připustilo, že již někdy v minulosti jiné osoby prostřednictvím elektronických médií šikanovalo⁷².

K problematičnosti kyberšikany - kromě její perzistentní, často skryté povahy, přispívá i zvýšená míra anonymity, možnost například vydávat se za někoho jiného a lákat ze zneužívané osoby (aniž by ona měla o možnosti probíhající šikany nějaké povědomí) citlivé informace, které lze posléze zneužít k její diskriminaci, vytvoření stigma, či, v tom ještě horším případě, dalšímu vydírání za účelem například pohlavního, či emocionálního zneužití – jak tomu často bývá v případě na internetu se vyskytujících *lovců* – pedofilů. Procento kyberšikany, přicházející právě ze stran sociálních sítí, je posléze nebezpečně vysoké – některé zdroje uvádějí až 39%⁷³. Často se pochopitelně pojí i s klasickou šikanou – za příklad lze uvést nahrání šikanované osoby na mobilní telefon a následnou distribuci nahrávky právě prostřednictvím sociálních sítí, společně s například zesměšňujícím komentářem.

Sociální sítě jsou, jak vidíme, dějištěm nejen mnoha přínosných konverzací, místem uskutečňování interakcí a navazování užitečných sociálních vztahů, ale i prostorem, jehož samotná povaha, přinášející dosud nemyslitelnou viditelnost jednotlivých osob, může skrývat nikým neuvažované, pro osobní integritu jedince i závažné důsledky.

Tímto jsme ovšem probrali pouze povahu vztahu uživatele k dalším uživatelům, nedotkli jsme se například případů, kdy jsou posty, či tweety na soukromých profilech

⁷² The Essex Cybersurvey. *Essexprimaryheads.co.uk*, dostupné z: <http://www.essexprimaryheads.co.uk/sites/essexprimaryheads.co.uk/files/Essex%20Cybersurvey%20Spring%202011%20Executive%20summary.pdf>

⁷³ Co je kyberšikana. *E-bezpeci.cz*, dostupné z: <http://cms.e-bezpeci.cz/content/view/14/39/lang.czech/>

zaměstnanců sledovány jejich zaměstnavateli, uchazeči o zaměstnání jsou lustrováni například přes největší pracovní sociální síť LinkedIn a podobně. Možností zneužití osobních informací, uvedeným na sociálních sítích je jednoduše celá řada a jen dále poukazují na vysokou problematičnost tohoto fenoménu.

Na tomto místě je záhodno se ještě zastavit u srovnání komerční stránky a potenciálu sociálních sítí, jmenovitě Facebooku, jehož neoddiskutovatelně největším trumfem je obří uživatelská základna – a jejich osobní data.

Dá se říci, že sociální sítě se, co se týče vydělávání peněz, zase tolik neliší od například internetových vyhledávačů. Dieter Bohn, redaktor internetového magazínu The Verge, v únoru 2012 publikoval zajímavé statistiky, které uváděly, že celkový podíl, jenž v tržbách Facebooku zaujímá zobrazování reklamního obsahu uživateli, je 85%. Zbýlých 12% podílu tehdy tvořily příjmy aktivit americké společnosti Zynga, což je firma, která se specializuje na vývoj počítačových her na tuto platformu. Co tvoří zbylá 3%, zůstává nevyjasněno. Jisté však je, že akumulované tržby z této sítě každoročně rostou, jak narůstá i počet jejích uživatelů.

Pokud v roce 2007 Facebook vydělal 138 milionů dolarů, v roce 2011 to již bylo kolem 1 miliardy. O tři roky později již 2,93 miliardy. Zobrazování, dle zvláštního algoritmu personalizovaných reklam uživateli, zdá se, tvoří, společně s mikro platbami, uskutečněnými skrz některou z tisíců přítomných aplikací, drtivou většinu příjmů tohoto globálně vysoce úspěšného média, ovšem, má to háček.

Ačkoliv tržby Facebooku stále rostou, postupem času, jak informoval například magazín PageFair, rovněž přibývá lidí, kteří používají zásuvný modul Adblock, jenž

umožní reklamy v prohlížeči - a tedy i na sociálních sítích efektivně blokovat⁷⁴. Celkově se procento uživatelů, kteří začínají být odrazováni přemírou reklamy, celosvětově zvedá. V roce 2014 modul Adblock užívalo již 144 milionů internetových uživatelů, přičemž jejich počet se od června 2013 do stejného měsíce roku 2014 zvedl o téměř 70%.

Studie dále uvedla ještě jeden zajímavý demografický údaj. Tvrdí, že 41% z těchto uživatelů jsou právě nejdůležitější cílová skupina Facebooku – lidé od 18 do 29 let. Jakým způsobem si, jak Facebook, tak Google s touto odezvou na zvyšující se reklamní zatížení svých uživatelů poradí, prozatím není známo.

V okamžiku psaní tohoto textu jsem se odhodlal pustit jedno z milionů videí na službě Youtube, abych jej mohl použít jako referenci pro tuto práci. V následujících vteřinách se již začala před samotným spuštěním videa přehrávat reklama serveru Mall.cz, přičemž jsem měl možnost sledovat, kolik vteřin reklamy ještě zbývá, a dokonce se i pomocí přiloženého odkazu mohl zajít podívat na domovské stránky tohoto internetového obchodu. Reklama, která trvá 20 vteřin, jde sice po 5 vteřinách kliknutím přeskočit, přesto se přehrání tohoto úseku považuje za její zhlédnutí a majitel Youtube kanálu, na jehož video jsem se chtěl podívat, dostane 55%, Google pak 45% výtěžku ze systému AdSense, jehož prostřednictvím zadavatelé reklam svůj obsah na Youtube přidávají. Právě tento koncept reklam ve videích, či před nimi, je tím, co pomáhá udržet největší video službu světa v chodu, ačkoliv dle hlášení ze samotné společnosti Google, se stále nejedná o výnosný podnik⁷⁵. Facebook pochopitelně se systémem AdSense pracuje rovněž a na příjmech z něj je více méně závislý, tedy i jemu dělá rostoucí obliba

⁷⁴ 2014 Report – Adblocking Goes Mainstream. *Blog.pagefair.com*, dostupné z: <http://blog.pagefair.com/2014/adblocking-report/>

⁷⁵ Youtube reportedly not profitable. *Siliconbeat.com*, dostupné z: <http://www.siliconbeat.com/2015/02/26/youtube/>

Adblocku vrásky natolik, že se začíná pomalu spekulovat nad tím, jakým způsobem tyto „ztráty“ bude chtít kompenzovat.

Někteří uživatelé uvažují to, nad čím se tiše spekuluje už dávno – tedy, že prodejem uživatelských dat třetím subjektům, povětšinou firmám, které se spravováním a analyzováním těchto velkých balíků dat⁷⁶ profesionálně zabývají. Mezi nimi lze najít i skutečně známé, globální značky – například IBM, Hewlett-Packard, Dell, SAP, Oracle a další⁷⁷. Právě trh s big/massive data skýtá další miliardové výdělky a vzhledem k množství osobních údajů a dalších dat, jež Facebook vlastní, se jedná o obchodní příležitost, kterou lze jen těžko nechat ležet ladem.

Z této analýzy nejen fungování, ale především finančního potenciálu Facebooku je, doufejme, viditelné, že sociální síť není jen o navazování kontaktů, sdílení informací a publikování různorodých myšlenek (statusů) – tedy místem *nové demokracie*, ale především se jedná o velice efektivní stroj na vydělávání peněz – ze studentského nápadu se stal jeden z nejvýnosnějších byznysů světa.

Otázka, jež byla kladena na samém počátku této práce, však zůstává – jsou uživatelé smíření s tím, že za návštěvu tohoto média je nutné zaplatit svými osobními údaji? A jaký je vůbec vztah mezi uživatelem a tímto elektronickým médiem? Jednoduše řečeno – co se vlastně nachází v oněch podmínkách služby, které musí každý uživatel přijmout během registrace a určuje další vztahy mezi ním a provozovateli těchto rozličných online služeb?

⁷⁶ Pro něž se vžil název „big data“, v současné situaci již „massive data“.

⁷⁷ Top 10 Big Data Companies (By Revenues). *Information-management.com*, dostupné z: <http://www.information-management.com/gallery/top-10-big-data-companies-revenues-10026248-1.html>

2.1.4. Problematika podmínek užití – Podmínky a zásady služby Facebook a EULA

2.1.4.1. Podmínky a zásady služby Facebook

Jelikož Facebook na svých stránkách poskytuje relativně přehledné, byť poněkud právníckou formou psané podmínky a prohlášení, není pro uživatele ani tak složité zanalyzovat, co vlastně obsahují.

Přesto z příkladu sama sebe, jenž by rozhodně neměl být, v rámci zachování kritického odstupu, nikterak zobecňován na další internetové uživatele (a najít relevantní výzkumy na dané téma je poměrně obtížné), totiž vím, že v drtivé většině případů je nečtu příliš pozorně, či, spíše vůbec. I z těchto vnitřních pohnutek vzniklo puzení přistoupit k hlubší analýze toho, s čím vlastně souhlasilo těch více, jak 1,4 miliardy uživatelů.

Předně, Facebook označuje rozhodnutí uživatelů službu používat (a tedy s podmínkami souhlasit) za tzv. informované rozhodnutí. Počítá tedy s tím, že před odsouhlasením podmínky služby přečetli a bere to jako hotovou věc. Zajímavá je přitom již zmínka, týkající se duševního vlastnictví obsahu, jenž uživatel na sociální síť zveřejní. V české mutaci podmínek se píše následující: *„Pro obsah chráněný právy k duševnímu vlastnictví, jako jsou fotografie a videa (obsah podléhající duševnímu vlastnictví, DV), nám výslovně udělujete následující oprávnění, v souladu s vaším nastavením soukromí a nastavením aplikací: udělujete nám nevýhradní, přenosnou, převoditelnou, celosvětovou bezúplatnou (royalty-free) licenci na použití veškerého obsahu podléhajícího DV, který zveřejníte na Facebooku nebo v návaznosti na něj (Licence k DV). Tato licence k DV*

končí, jakmile svůj obsah podléhající DV odstraníte ze svého účtu, s výjimkou případů, kdy jste tento obsah sdíleli s ostatními (pokud jej také oni neodstranili).“⁷⁸

Právě tento bod patřil v rámci nových podmínek k uživatelsky často rozporovanému, ale vede k jednomu zjištění – pokud uživatel nechce, aby Facebook vlastnil jakoukoliv licenci k užití jeho díla, ať už z toho plynou jakékoliv reálné důsledky, nemá takový obsah na sociální síti v první řadě vůbec sdílet.

Další důležitou klauzulí je obsah bodu číslo 9, tedy právo Facebooku užít jméno uživatele k následujícímu: *„Povolujete nám použít vaše jméno, profilovou fotku, obsah a informace ve spojení s komerčním, sponzorovaným nebo souvisejícím obsahem (například značku, která se vám líbí), který poskytujeme nebo zprostředkováváme. To kupříkladu znamená, že nás tímto opravňujete, abychom mohli za poplatek firmám nebo jiným subjektům zobrazovat vaše jméno nebo profilový obrázek s vaším obsahem nebo informacemi, aniž bychom vás museli jakkoli finančně kompenzovat. Pokud jste pro svůj obsah nebo informace vybrali konkrétní skupinu příjemců, budeme při použití vaši volbu respektovat.“⁷⁹*

Právě těchto pár nenápadných vět mimo jiné odkazuje na další zdroj příjmů Facebooku, kdy na svých stránkách může ostatním uživatelům ve vašem okruhu zobrazovat doporučení na základě vámi vybraných oblíbených komerčních značek, aniž by vám, coby doporučitelům, musel vyplatit jakýkoliv finanční obnos. Znovu opakujeme – jedná se o Andrejevicem teoreticky zmíněnou platbu za využívání služby, kterou nelze ani zaplatit jiným způsobem, jelikož je poskytována „*zdarma*“, uvedenou do praxe.

⁷⁸ Prohlášení o právech a povinnostech. *Facebook.com*, dostupné z: <https://cs-cz.facebook.com/legal/terms>

⁷⁹ tamtéž.

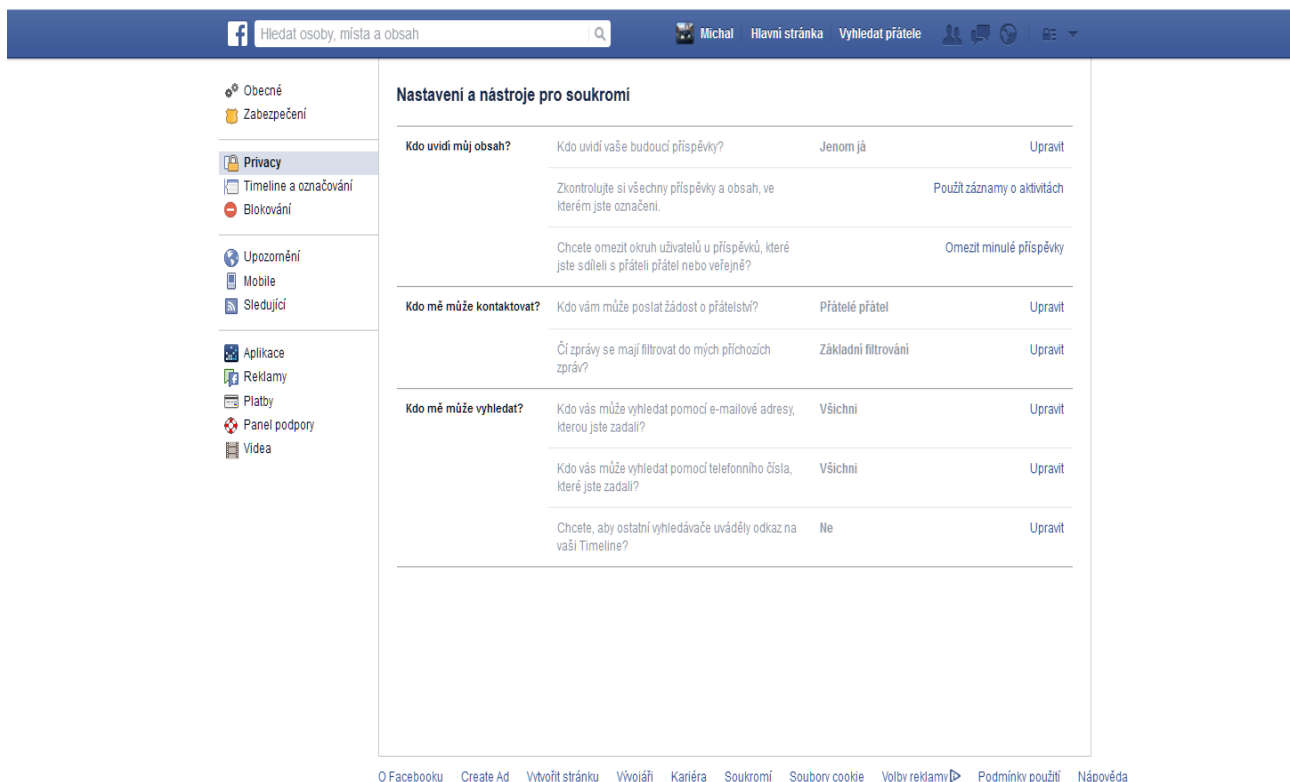
Obsahem dokumentu je i hned několik zmínek ohledně zaznamenávání geografické polohy, jež je službou automaticky aktualizována a je zaznamenávána i v rámci dalších akcí - například, když z nějakého místa uživatel nahraje na službu fotografie, navštíví určité místo, či instituci. Zde se pochopitelně nabízí polemika se sociálními sítěmi typu Yelp⁸⁰, či Foursquare⁸¹, které se primárně specializují právě na sdílení hodnocení návštěv různých zábavních podniků a restaurací, ale opět – Facebook v sobě tyto funkce integruje rovněž.

Za problematické posléze lze vnímat to, že ačkoliv Facebook skutečně nabízí určitou možnost nastavení toho, co bude sdíleno a s kým (viz. Obrázek 4), či kdo může uživatele požádat o přátelství, právě možnost vypnutí zaznamenávání geografické polohy zůstává uživateli víceméně skryta. Faktem ovšem zůstává, že v době chytrých telefonů, GPS navigací, webových kamer, chatovacích systémů, mobilních aplikací, dalších sociálních služeb a různorodého softwaru, je skrýt svou momentální geografickou polohu na síti již skutečně velice obtížné, či dokonce nemožné.

Přesto je nutné mít neustále na paměti, že kliknutím na tlačítko *Souhlasím* při vytváření profilu na těchto službách, uživatel skutečně vstupuje do smluvního vztahu, v němž jsou jasně dané podmínky plnění pro obě strany. Pokud s jednou z podmínek nesouhlasí, **nesmí** službu vůbec využívat. Informovaný souhlas tak v podstatě lze uvažovat jakožto jednu ze dvou možností, jakým způsobem situace může dopadnout – buď uživatel podmínky přijme (a tedy bude poskytovat službě svá osobní data a informace ke komerčním i jiným účelům), nebo nepřijme a za takových okolností je mu přístup trvale uzavřen, dokud svůj postoj nepřehodnotí.

⁸⁰ Yelp.cz. Dostupné z: <http://www.yelp.cz/>

⁸¹ Foursquare.com. Dostupné z: <https://foursquare.com/>



Obrázek č. 4 – Příklad nastavení soukromí na sociální síti Facebook

2.1.4.2. Problematika EULA

S výše uvedeným se pojí i situace ohledně tzv. EULA, což je anglická zkratka, kterou lze přeložit jako: *licence pro koncového uživatele (End-User-License-Agreement)*. Ta se uzavírá především při užívání software, a obsahuje rovněž několik zajímavých klauzulí, které lze užít k demonstraci toho, jaké jsou vlastně vztahy mezi výrobcem (poskytovatelem) a uživatelem elektronického zboží, či služeb. V podstatě se jedná o situaci, kdy jakýkoliv software není uživateli skutečně prodáván (tedy nestává se jeho právoplatným vlastníkem), je pouze vlastníkem licence, jež jej opravňuje k užití díla.

Stejně, jako v případě podmínek pro užívání služby, již samotnou instalací se má za to, že uživatel je se zněním EULA seznámen. Smlouva tuto licenci poskytuje určitému jedinci, je zcela nepřenositelná a v okamžiku, kdy by se například chtěl zbavit ochrany proti kopírování, je jednou ze stran smlouva porušena a zaniká. Uživatel má posléze povinnost všechny kopie softwaru zničit a dalším užíváním porušuje zákon a vzniká škoda, jež může být právně vymáhána.

Zajímavá je i část, věnovaná duševnímu vlastnictví uživatelů. Na příkladu znění EULA firmy Rovio, která na trhu uspěla s celosvětovým fenoménem Angry Birds, můžeme vidět, že veškerý uživatelský obsah, jenž uživatel v rámci hry vytvoří, nadále zůstává majetkem firmy Rovio.⁸² Ze znění podmínek: *„Služby Rovio vám mohou umožnit vytvářet obsah, zahrnující, ale nikoliv omezující se na nové herní mapy, herní obrázky, či videa z vašeho hraní. Výměnou za užití služeb Rovio a v rozsahu vašeho užití služeb Rovio, které mohou vést k vytvoření designu, duševního, či dalšího vlastnictví, na který se vztahuje zákon o duševním vlastnictví, tímto poskytujete společnosti Rovio exkluzivní, bezplatné, nezrušitelné, zcela přenositelné a licencovatelné celosvětové právo na licencování pro jakýkoliv účel zahrnující, ale nikoliv omezující se na reprodukci, kopírování, přizpůsobení, modifikovatelnost, vystavení, vydání, přenesení, či jiné ukázání veřejnosti bez dalšího upozornění, či jakékoliv kompenzace vůči vám po dobu trvání ochrany, která se vztahuje na duševní vlastnictví dané zákony a mezinárodními úmluvami.“*

Uživatel, jenž tedy například vytvoří úspěšné rozšíření, postavené na enginu původní hry, nemá právo v podstatě vůbec na nic, pouze podstoupit svá práva společnosti

⁸² EULA. *Rovio.com*, dostupné z: <http://www.rovio.com/eula>

Rovio právě na základě těchto podmínek, které jsou v okamžiku započetí užívání služby považované za automaticky odsouhlasené.

Za, pro tuto práci stěžejní, pak lze považovat nenápadnou zmínku v závěru dokumentu: „ *Instalací, přístupem, či užíváním služeb Rovio souhlasíte se sběrem informací a přenášením dat do zemí mimo Evropskou unii, či Spojené státy americké.* “

Samotný sběr osobních dat firmou Rovio je posléze ještě rozebírán v samostatném dokumentu, nazvaném *Privacy Policy*, který se klasicky zabývá možností využití cookies pro personalizaci zobrazovaných reklam, sběrem geografických dat a možností jejich další analýzy. S tímto vším uživatel souhlasí již samotnou instalací a používáním služeb. Pokud nesouhlasí, měl by disk se softwarem zničit, či jej vrátit tam, odkud jej zakoupil a produkt či službu nepoužívat, ani jejich užívání nezačínat.

Jak tedy vidíme – podmínky užití služeb i smlouvy EULA, které jsou dostupné u drtivé většiny komerčního softwaru, opravňují provozovatele k leccemu a skutečně bedlivě si chránit svá osobní data znamená vzdát se užívání v podstatě valné většiny internetových služeb. Samozřejmě stále existují služby, které jsou skutečně poskytovány zdarma, a nejde jim primárně o vytěžení uživatelských dat, coby *platby za službu*, problémem však zůstává, jak je rozpoznat.

Internetový dohled a komerční sběr osobních dat mají to specifikum, že, pokud uživatel neumí jeden z řady programovacích jazyků, je pro něj relativně složité dopátrat se k tomu, na jaké servery a ke komu vlastně jeho data proudí. Je to provozovatel sociální sítě, online hry, vydavatel, či rovnou nějaká třetí strana, již ke sběru inkriminovaných dat opravňuje právoplatně uzavřená elektronická smlouva? Něco takového jednoduše průměrný uživatel-laik nemůže tušit a otázka je, do jaké míry se jej tato problematika vůbec dotýká.

Jak jsme se totiž ptali na samém začátku této práce – jsou uživatelé online služeb (například sociálních sítí) smířeni se sběrem osobních dat a internetovým dohledem? A po tomto odstavci si již společně můžeme, snad trochu cynicky, odpovědět – ano, jsou. Pokud by nebyli, uživateli daných služeb by vůbec neměli být – a tedy nejsou uživateli.

Zajímavý je především tento přerod, jenž se s příchodem sociálních sítí, zdá se, ustanovil – zatímco dříve uživatelé dbali na to, aby jejich osobní informace zůstaly co možná nejvíce utajeny před zraky veřejnosti a institucím, vykonávajícím dohled – k čemuž sloužily i různé anonymizéry, TOR systémy, VPN brány a další nástroje, sociální sítě přinesly koncept, v němž uživatelé své osobní údaje poskytují dobrovolně, zdarma a ještě rádi, jelikož se jejich prostřednictvím chtějí zviditelnit před svými známými (které možné ani v životě naživo neviděli) – předvést, v čem jsou dobří a co se jim v jejich životě daří.

Sociální sítě tímto konceptem generalizované *viditelnosti (exposure)* rovněž umožňují, aby se každý uživatel stal celebritou. Youtube komentátoři, hvězdy Twitteru, uznávaní a dobře vydělávající bloggeři (za příklad lze uvést například Pereze Hiltona⁸³, jenž se specializuje na psaní o celebritách, jehož měsíční příjem z tohoto blogu se v roce 2011 odhadoval na 450 000 dolarů, či například Mashable.com s odhadovaným měsíčním příjmem ve stejném období 600 000 dolarů⁸⁴) – ti všichni a další různé osobnosti internetu našli na síti nejen prostředek zábavy, ale i velice kvalitní obživu. Právě s tímto záměrem se někteří podnikaví uživatelé pouštějí do propagování sebe sama jako osobní značky, přičemž právě osobnostní marketing je odvětvím, jež se s internetovým marketingem, startupy a vůbec celým IT odvětvím rozvíjí v současné situaci velice živelně.

⁸³ Perez Hilton.com. Dostupné z: <http://perezhilton.com/>

⁸⁴ Top Earning Blogs – Make Money Online Blogging. *Incomediary.com*, dostupné z: <http://www.incomediary.com/top-earning-blogs>

Jednoduše – viditelnost je, zdá se, novou modlou současné společnosti, jelikož s viditelností často přicházejí lákavé finanční příležitosti (například u veřejně známých a uznávaných internetových osobností možnost nabídek účinkování v reklamách, či další marketingová a reklamní spolupráce), či nějaké zajímavé obchodní nabídky (odprodej a inzerce na sledovaném blogu, či zapojení do systémů typu referral – nenápadného doporučování zboží a služeb uživatelům, maskované za upřímně myšlené rady - a podobně). Nejsem si jist, jestli skutečně dochází k Baumanově již uvedené teorii – tedy ke smrti anonymity, ale je jisté, že anonymita na internetu z finanční stránky mnoho nepřináší – její absence často přesně naopak.

3. PRAKTICKÉ PŘÍPADY UŽITÍ ELEKTRONICKÉHO DOHLEDU – KONTROVERZE A ODMÍTNUTÉ PROJEKTY

Podrobně bylo popsáno, jakým způsobem sběr osobních dat v rámci elektronických médií a komunikace probíhá, jaké jsou vlastně smluvní vztahy mezi provozovateli služeb a uživateli. Tedy nezbyvá, než se obrátit k praktickým případům užití elektronického dohledu, či z něj vyplývajících důsledků, které z nějakého důvodu rozpoutaly v rámci současného mediálního prostoru značné kontroverze. Pověštinou se jedná o příklady z velkých IT firem, či nadnárodních korporací, jelikož právě zde je potenciální únik uživatelských informací nejpálčivějším problémem, kvůli jejich často značnému rozsahu a dopadům na velkou základu uživatelů.

3.1. Případy kontroverzí v důsledku úniku uživatelských dat a odmítnutí dohledu v zahraničí

3.1.1. Případ Sony PlayStation Network

V roce 2011 se japonské nadnárodní korporaci Sony přihodila skutečně neblahá událost, která strhla vlnu nevole převážně díky svému skutečně velkému rozsahu. Mezi 17. a 19. dubnem roku 2011 proběhl hackerský útok na servery PlayStation Network (dále jen PSN) a služby Qriocity, jehož následky byly drtivé.

Nejen, že Sony byla kvůli přetrvávajícím útokům nucena službu PSN pozastavit (čímž pochopitelně v daném období přicházela o příjmy z ní plynoucí), ale 4. května poslal tehdejší náměstek ředitele Sony Kazuo Hirai americké sněmovně reprezentantů (dolní komoře Kongresu Spojených států amerických) obsáhlou zprávu⁸⁵, jež šokovala nejen uživatele služby Sony PlayStation Network, ale i značnou část zainteresované internetové komunity.

Hackerům se podařilo dostat se k informacím, uloženým na serverech Sony, obsahujících přes 77 milionů registrovaných uživatelských účtů, čímž se jednalo o jeden z největších masových úniků dat v dějinách, jenž byl dokonce ještě rozsáhlejší, než únik informací americké společnosti TJX Companies (jehož důsledkem došlo k expozici více jak 45,7 milionů uživatelských dat v průběhu 18 měsíců, aniž by si tohoto úniku někdo ze zaměstnanců firmy všiml)⁸⁶. V případě Sony pochopitelně nepomohl ani fakt, že Sony

⁸⁵ Kazuo Hirai's Letter to the U.S. House of Representatives. *flickr.com*, dostupné z: <https://www.flickr.com/photos/playstationblog/sets/72157626521862165/>

⁸⁶ TJX hack the biggest in history. *Computerweekly.com*, dostupné z: <http://www.computerweekly.com/news/2240080607/TJX-hack-the-biggest-in-history>

své uživatele o skutečné povaze a dopadech útoku informovala až s týdenním zpožděním, během něhož mohlo být těchto dat bez potíží masově zneužito.

Přitom se nejednalo o nic tak neškodného, jako pouze přihlašovací údaje k jednotlivým uživatelským účtům. Ukradena z databáze byla skutečná uživatelská jména, osobní adresy a dokonce platební údaje kreditních karet, včetně data ukončení jejich platnosti. O problémech zabezpečení se údajně vědělo dlouho, ovšem postupem času začala najevo vyplývat ještě děsivější skutečnost. Osobní údaje se v databázích Sony zcela nepochopitelně vyskytovaly v nezašifrované podobě, tedy útočníci (ale nejen útočníci, například i samotní zaměstnanci firmy Sony) si je mohli okamžitě přecíst bez nutnosti použití jakéhokoliv dalšího dešifrovacího nástroje. Šifrované naštěstí zůstaly údaje o platebních kartách⁸⁷, ovšem i tak se jednalo o bezprecedentní porušení firemní kultury ohledně zpracovávání citlivých údajů.

Snadno si lze představit, jaké byly odezvy na tyto kardinální nedostatky v zabezpečení a Sony, ve snaze zachránit si svou pověst a jméno společnosti, se rozhodla ke kroku, jenž firmu stál další výdaje – uživatele služby odškodnila hrami zdarma hned ve dvou vlnách, přičemž ta druhá byla v celkovém úhrnu 15 milionů dolarů, a uživatelé, kterým by se podařilo prokázat zneužití jejich osobních údajů, si mohli přijít v rámci odškodnění až na 2500 dolarů (v přepočtu 51 tisíc Kč)⁸⁸. Sony rovněž od britských úřadů obdržela pokutu 250 tisíc dolarů (8,7 milionů korun)⁸⁹. Jak vidno, tak masivní únik dat přináší zdrcující následky a znovu se rozhořely bouřlivé debaty nad tím, zda jsou shromažďovaná osobní data skutečně řádně chráněna a v rukou povolanych osob.

⁸⁷ How the Playstation Network was Hacked. *Extremetech.com*, dostupné z:

<http://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked>

⁸⁸ Sony odškodní uživatele PlayStation Network hrami za 15 milionů dolarů. *Lupa.cz*, dostupné z:

<http://www.lupa.cz/clanky/sony-odskodni-dalsi-uzivatele-playstation-network-hrami-za-15-milionu-dolaru/>

⁸⁹ Sony fined over 'preventable' PlayStation data hack. *Bbc.com*, dostupné z:

<http://www.bbc.com/news/technology-21160818>

Problémy firmy Sony pochopitelně nebyly pouze vnitrofiremním problémem, který mohl přinést újmu na dobrém jménu společnosti, ale nahrávaly i dalším firmám, jimž tato situace mohla přinést zisky - lze uvažovat především rozličné firmy, zabývající se bezpečnostní stránkou ať už serverů, či samotných klientských stanic (například poskytovatele antivirových programů a dalších preventivních řešení, určených do korporátní, i soukromé sféry), ale především přímé konkurenty firmy Sony – Nintendo a Microsoft. Právě druhá uvedená společnost se skandálu ohledně dohledu a možného zneužití osobních informací rovněž vyhnout nedokázala.

3.1.2. Microsoft Xbox Kinect – odmítnutí projektu dohledu ze strany uživatelů

Souboje na poli tržního segmentu konzolí, používaných ke hraní her, se v posledních letech uskutečňují především mezi třemi největšími hráči – výše zmíněnou firmou Sony, japonskou stálicí Nintendo a firmou Microsoft, která se svou první verzí herní konzole přišla již v roce 2001. Posléze světlo světa spatřila další verze, v roce 2005 uvedený Xbox 360, jehož součástí bylo i zařízení Kinect, díky němuž je možno ovládat uživatelské rozhraní konzole, či herní prostředí vybraných her například za pomoci hlasu a různých tělesných gest.

K tomu je pochopitelně potřeba k zařízení připojit speciální kameru, určenou právě k těmto účelům. V rámci konzole Xbox 360 ještě toto zařízení nebudilo žádné zvláštní kontroverze, byť některé hlasy se obávaly možného zneužití – nikoliv snad přímo společností Microsoft, ale právě hackery a dalšími třetími stranami, například vládními agenturami. V roce 2013, s příchodem nové generace konzole Xbox, pojmenované

jednoduše Xbox One, se však ihned po odhalení strhla vlna nevole ze strany uživatelů, která měla pro Microsoft relativně závažné důsledky. Microsoft totiž kromě nekompromisně restriktivního systému protipirátské ochrany, kdy bylo nutné konzoli jednou za 24 hodin připojit k internetu, jinak odmítala pracovat, připravil i nový systém Kinect, s jehož pomocí mělo být možné ovládat vše – od spuštění filmu až po hraní nejnovějších her. Mělo to ovšem jeden háček – kamera systému Kinect měla být zapnuta neustále, i v případě, že uživatel konzoli vypne⁹⁰. Microsoft se tento fakt snažil vykomunikovat tak, že v rámci co nejrychlejší odezvy ze strany systému na hlasové pokyny uživatele (hlasem se zařízení pochopitelně mělo i zapínat) je nutné nechat kameru snímat pokoj, v němž se nachází, neustále. To pochopitelně nemohlo být internetovou komunitou přijato, zvláště po propuknutí kontroverze ohledně tajného vládního projektu PRISM⁹¹ agentury NSA, jež se opakovaně připojovala na servery společností Apple, Google, Yahoo a právě Microsoftu, odkud bez jakéhokoliv souhlasu uživatelů systematicky získávala různé audio a video nahrávky, obsah e-mailů a další dokumenty⁹².

Prezident Barack Obama posléze uvedl, že v rámci sběru těchto dat nešlo o americké občany, ale osoby cizího původu, přesto šlo o jasné poselství těm, kteří stále věřili v internetovou neutralitu a svobodu. Microsoft k odhalení projektu PRISM dodal následující: *„Uživatelská data poskytujeme pouze, pokud obdržíme soudní příkaz k jejich vydání, ale nikdy dobrovolně. K podobným krokům navíc přistupujeme pouze v případě jednotlivých požadavků, týkajících se jednotlivých účtů, či identifikátorů. Pokud existuje vládní program, jenž se zaměřuje na rozsáhlejší sběr uživatelských dat, tak se do něj*

⁹⁰ The Xbox One will always be listening to you, in your own home (update). *The Verge.com*, dostupné z: <http://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening>

⁹¹ Vznikl v roce 2007 za prezidenta George W. Bushe a obnoven byl Barackem Obamou v prosinci 2012.

⁹² Dissecting Big Tech's Denial of Involvement in NSA's PRISM Spying Program. *Abcnews.go.com*, dostupné z: <http://abcnews.go.com/Technology/nsa-prism-dissecting-technology-companies-adamant-denial-involvement/story?id=19350095#.UcNRdTvVBNs>

*vědomě nezapojujeme.*⁹³ Znovu se tedy dostáváme k již několikrát zmiňované problematice důvěry, jelikož právě důvěra je často tím, co uživateli, jenž není technicky vzdělán, a tedy není schopen vlastními silami rozebrat kód stránky, či určité služby, aby zjistil, kam vlastně jeho uživatelská data plynou, zbývá.

Microsoft byl každopádně nakonec vlivem uživatelské nevole, která hrozila přihrát důležitý podíl zákazníků nové generace konzolí na stranu firmy Sony, jež v to samé období pilně pracovala na propagaci své konzole PlayStation 4, nucen ze svých požadavků ustoupit – nejen, že konzole Xbox One nemusí být každých 24 hodin připojována na internet, ale senzor Xbox Kinect lze trvale vypnout a není vyžadován ani pro samotné spuštění a obsluhu konzole. Nejen nevole uživatelů, ale paradoxně hrozící vznik potenciálně drtivé konkurenční výhody tedy vedly k tomu, že společnost byla okolnostmi nucena ustoupit z požadavků, jež ještě před několika měsíci považovala a směrem k veřejnosti komunikovala jako zcela revoluční a pro vývoj herního odvětví nezbytné⁹⁴.

Podobných případů se posléze najde celá řada, téměř každý rok se objeví bezpočet dalších kontroverzí, týkajících se úniku, či podivného nakládání s uživatelskými daty.

V roce 2014 například rychle rostoucí výrobce mobilních telefonů Xiaomi čelil nařčení z odesílání uživatelských dat na čínský server⁹⁵. Opět se jednalo o fotografie a textové zprávy, jejichž obsah byl přeposílán na server, umístěný v Pekingu. Firma Xiaomi se bránila proti tomu, že by kamkoliv odesílala uživatelská data, či spolupracovala

⁹³ tamtéž.

⁹⁴ Xbox One dumps Kinect requirement, no sensor required to play. *Nbcnews.com*, dostupné z: <http://www.nbcnews.com/technology/xbox-one-dumps-kinect-requirement-no-sensor-required-play-6C10904079>

⁹⁵ Xiaomi allegedly sending your info to Chinese servers [UPDATED]. *Blog.gsmarena.com*, dostupné z: <http://blog.gsmarena.com/xiaomi-secretly-sending-info-chinese-servers/>

s čínskou vládou na jejich akumulaci, ale důkazů ohledně jejich sběru a odesílání, ať už za jakýmkoliv účelem, je přesto dostatek. (viz. Obrázek č. 5)

Current IP Range:	42.62.48.0 - 42.62.48.255
IP Range Location:	China, Beijing, Beijing
IP Owner:	Forest Eternal Communication Tech. Co.ltd
Owner Full IP Range:	42.62.0.0 – 42.62.127.255
Owner Address:	Beijing, China
Owner Country:	China
Owner Phone:	+86-010-51659311
Owner Website: <input type="checkbox"/>	www.cnnic.cn
All Owner IP Ranges:	42.62.0.0 – 42.62.127.255, 125.254.128.0 – 125.254.191.255, 124.243.192.0 – 124.243.255.255
All Owner IP Reverse DNS (Host)s:	42.62.0.45, 125.254.166.0, 124.243.198.166
Whois Record Updated: <input type="checkbox"/>	29 Jun 2011

Obrázek 5 – Potenciální odesílání uživatelských dat na server, umístěný v Číně

3.2. Případy úniku uživatelských dat v České republice a prostředí tuzemského internetu

Případy úniku ať již osobních, či firemních dat, pochopitelně nejsou výjimkou ani na území České republiky, byť se oproti globální situaci pochopitelně nejedná o problém s tak masovými důsledky, jako v případě úniku v rámci globálních služeb s desítkami milionů uživatelů.

Tato skutečnost samozřejmě vyplývá už jen z velikosti tuzemského internetového trhu a uživatelské základny, která, dle výzkumu společnosti SPIR z roku 2013, zahrnuje asi 71% české populace věku od 10 let výše⁹⁶ (přičemž v roce 2014 to bylo již 79%⁹⁷), což, převedeno na číselný údaj, značí asi 6,7 milionu uživatelů. To je však proti celosvětové uživatelské základně pochopitelně pouhý zlomek, a tak i úniky dat se v našem prostředí odehrávají v mnohem menším měřítku. Přesto i zde lze najít případy, při nichž k úniku citlivých dat dochází a mají pro český prostor elektronických médií nějaké dopady.

Společnost Kaspersky, jež se vývojem nástrojů proti internetovým hrozbám zabývá již od roku 1997, při svém šetření, provedeném na vzorku 3900 IT profesionálů v 27 zemích včetně tuzemska zjistila, že za úniky dat v českém prostředí mohou, kromě bezpečnostních chyb v užívaných systémech a firemních mobilních zařízeních, především sami zaměstnanci (podíl 26%). Průzkum dále ukázal znepokojující trend, týkající se zvláště telekomunikačních firem, u kterých se takový typ ztráty dat zaměstnanci pohyboval kolem 42%, u firem ze segmentu energetiky šlo o 33% a u firem výrobních pak o 31% celkového podílu úniku citlivých dat těchto společností⁹⁸.

Vidíme tedy, že v tuzemském prostředí nejde jen o ztrátu způsobenou útoky hackerů/crackerů, či bezpečnostními chybami v interních firemních systémech, ale i nedostatečnou kompetencí zaměstnanců při manipulaci s nimi (data jsou například ponechávána v nezašifrované podobě na pevných discích k internetu připojených

⁹⁶ Trendy v návštěvnosti internetu ročenka 2013 (leden 2012 – únor 2014). *Netmonitor.cz*, dostupné z: http://www.netmonitor.cz/sites/default/files/iac_2014_-_netmonitor_rocenka_2013.pdf

⁹⁷ V Česku narostl počet uživatelů internetu, stoupl už na 79 procent. *Mam.ihned.cz*, dostupné z: <http://mam.ihned.cz/c1-63313870-v-cesku-narostl-pocet-uzivatelu-internetu-stoupl-uz-na-79-procent>

⁹⁸ V Česku uniká víc dat kvůli zaměstnancům než kvůli softwarovým chybám. *Kaspersky.com*, dostupné z: http://www.kaspersky.com/cz/about/news/virus/2015/V_Cesku_unika_vic_dat_kvuli_zamestnancum_nez_kvuli_softwarovym_chybam

notebooků a počítačů, či nezašifrovaných flash/externích discích. Zpravodajský server ihned.cz posléze přinesl ještě méně potěšitelné zprávy, když v lednu 2015, v odkazu na výzkum společnosti Safetica, uvedl, že o citlivá data přišlo až těžko uvěřitelných **75% českých firem**⁹⁹, přičemž až čtvrtina z nich na ztráty dat žádným způsobem nereaguje.

V pětině takových případů dosáhla škoda jednoho až pěti milionů korun a dle výsledků této studie zaměstnanec stojí až za více než polovinou případů. Otázkou ještě posléze zůstává rozlišit případy, kdy zaměstnanec únik zaviní špatnou manipulací s daty, či si firemní data například při odchodu z firmy jednoduše ponechá pro vlastní potřebu. Dle společnosti Safetica se v případě úmyslné krádeže jedná asi o 20% a zbylých 80% je způsobeno nechtěně¹⁰⁰. Vidíme tedy, že firmy v českém prostředí, spíše než hackeři a crackeři, kteří se zaměřují spíše na útoky na koncové uživatele prostřednictvím spamu a různých podvodných stránek včetně ransomwaru, sužují spíše nedisciplinovaní a v problematice nakládání s uživatelskými daty nedostatečně vzdělaní zaměstnanci.

3.2.1. Únik citlivých dat z Komerční banky

V červenci roku 2013 z této bankovní instituce uniklo více než 45 tisíc osobních dat zájemců o penzijní spoření. V tomto případě nešlo o potvrzenou krádež dat zvenčí v důsledku prolomení systémové ochrany útočníky, ale o zpřístupnění osobních údajů chybou v systému samotné banky, respektive jejího dodavatele IT řešení.

Prostřednictvím systému internetového bankovníctví Komerční banky posléze bylo možné se k těmto osobním údajům dostat a využít je pro vlastní potřebu. Tento balík

⁹⁹ Ochrana citlivých dat se v Česku příliš neřeší, přišlo o ně 75 procent firem. *Byznys.ihned.cz*, dostupné z: <http://byznys.ihned.cz/c1-63351190-ochrana-citlivych-dat-se-v-cesku-prilis-neresi-prislo-o-ne-75-procent-firem>

¹⁰⁰ Anticeny za úniky dat rozdány, „uspěly“ školství a Penta. *Tyden.cz*, dostupné z: http://www.tyden.cz/rubriky/domaci/anticeny-za-uniky-dat-rozdany-uspely-skolstvi-a-penta_267449.html#.VYqya_ntmko

osobních dat obsahoval záznamy například o jménech, adresách, rodných číslech (které jsou obecně považovány za zvláště citlivý osobní údaj) a číslech telefonních.

K údajům navíc nebyl možný pouze přístup, ale šlo je i volně editovat. Státní orgán, Úřad pro ochranu osobních údajů, jenž se dohledem nad správným nakládáním s citlivými osobními daty ze zmocnění státem zabývá, se posléze rozhodl udělit bance pokutu 1,8 milionu korun¹⁰¹. Banka pochybení přijala a proti pokutě nevznesla námitek. Tím však celá kontroverze skončila a nejsou známy případy veřejných hromadných žalob, jak je tomu obvyklé v případě tzv. *class-action lawsuit*¹⁰² v prostředí britském, americkém, či globálním.

3.2.2. Únik citlivých dat z České spořitelny

O další únik dat, jenž na pár dní rozvířil vody českého internetu, se postarala další bankovní instituce v pořadí – Česká spořitelna. Na veřejnost se dostaly údaje o příjmech nejvyššího managementu dceřiných společností banky a další strategické údaje. Za únikem opět nestál nikdo zvenčí, ale notebook jedné zaměstnankyně středního managementu. Za důvodem zveřejnění pak údajně stály vztahy uvnitř společnosti – sexuální obtěžování, konflikty zájmů a nespravedlivé odměňování jednotlivých zaměstnanců. Na webu magazínu iDNES se dokonce objevila následující citace: „*Vážené dámy a pánové, mrzí mě, že vás musím zatahovat do této záležitosti, ale ráda bych nasměrovala vaši pozornost k sexuálnímu obtěžování, střetu zájmů a možnému zneužití finančních prostředků.*”¹⁰³ Spor měl posléze ještě dohru v tom smyslu, že údajná autorka

¹⁰¹ ÚOOÚ udělil Komerční bance pokutu 1,8 milionu korun za červencový únik dat. *Byznys.ihned.cz*, dostupné z: <http://byznys.ihned.cz/c1-61453470-uouu-udelil-komercni-bance-pokutu-1-8-milionu-korun-za-cervencovy-unik-dat>

¹⁰² Jedná se o typ soudního sporu, v němž je jedna strana zastupována jedincem, jenž kolektivně zastupuje zájmy určité skupiny.

¹⁰³ Spořitelně unikla data o mzdách, zřejmě za tím je rozvod manažerky. *Ekonomika.idnes.cz*, dostupné z: http://ekonomika.idnes.cz/spotitelne-unikla-data-o-prijmech-vyssich-manazeru-fx7-/ekonomika.aspx?c=A140102_212135_ekonomika_vez

redakci iDNES uvedla, že mail nepsala a je upraven tak, aby odpovídal účelu svalit vinu právě na ní. Za důvod takového konání uvedla v té době probíhající rozvodové řízení.

Tento případ však neměl žádný dopad na citlivé údaje klientů banky, přičemž mluvčí společnosti, Helena Matuszná z tiskového oddělení banky dokonce potvrdila, že informace, které unikly, byly neúplné a neaktuální.¹⁰⁴ Jistě však takové úniky hrozí poškodit dobré jméno společnosti a tím oslabit její konkurenceschopnost. Prozatím však není známo, že by se právě konkurenční firmy měly ve zvýšené míře podílet na cílené snaze o únik dat za tímto účelem, či rovnou provádět systematický data-mining¹⁰⁵ databází jiných firem – takové tvrzení by vyžadovalo podpoření nějakou dlouhodobější podrobnější analýzou, což je doména společností, jako je například v našem prostředí působící Safetica.

Tedy – ačkoliv úniky citlivých uživatelských dat nejsou ojedinělé ani v českém prostředí, povětšinou se kolem nich nestrhnou veliká míra internetové kontroverze mezi koncovými uživateli a ve srovnání se světem jsou i jejich dopady spíše minimální.

Z části je to dáno řádově menším okruhem postižených uživatelských účtů, z části tím, že se na podobné úniky často vůbec nepříjde, či se zřídka podniknou nějaké následné kroky a o událostech se tak dozví veřejnost, či alespoň mediální sféra. Firmy, pokud se jim již taková situace přihodí, ve snaze zachovat svůj merit vůči zákazníkům a vůbec celé společnosti, se snaží raději vše vyřešit uvnitř firmy samotné.

Výsledkem tedy celá situace vypadá, jakoby se tuzemské firmy k problematice osobních údajů stavěly podobně liknavě, jako někteří jejich zahraniční kolegové, ovšem

¹⁰⁴ V České spořitelně unikla citlivá data o platech lidí v managementu. *Byznys.ihned.cz*, dostupné z: <http://byznys.ihned.cz/c1-61511760-v-ceske-sporitelne-unikla-citliva-data-o-platech-lidi-v-managementu>

¹⁰⁵ Tedy získávání netriviálních, skrytých a potenciálně užitečných informací z datových databází, či balíků dat.

zároveň je u nich ještě těžší vzbudit o problematiku zájem, právě díky konečným dopadům, které povětšinou nejsou pro jejich byznys kritické.

Když v roce 2012 v sousedním Slovensku unikly investiční skupině Penta Investments z firemní databáze životopisy 2200 lidí, kteří se u skupiny ucházeli o zaměstnání, vina byla skupinou Penta přenesena na externí firmu dodávající IT řešení¹⁰⁶ a tím pro ně celá záležitost v podstatě skončila. Firmy, zdá se, jsou velice aktivní v samotném sběru citlivých dat uživatelů, ale jejich obraně věnují jen pramálo prostředků a úsilí a v případě jejich ztráty nesahají k podobným odškodňujícím řešením v rámci zachování dobrého jména, jak je tomu zvykem v západních společnostech.

ZÁVĚR

Nacházíme se na samém závěru této práce, která se věnovala proměně povahy metod dohlížení a jejím důsledkům – od klasického dohledu tváří v tvář, jenž je s výjimkami založen na symetrickém vztahu (dohlížitel je pro dohlíženého viditelný), přes Foucaultovskou racionalizaci a systematizaci osobních dat s využitím kartoték a archivů, až po ryze současný sběr a třídění informací a dat pomocí prostředků interface – elektronických systémů, jejichž práce je do značné míry již automatizována.

Zaměřili jsme se především na dohled, vyskytující se coby součást elektronického média, na nějž se pozvolna přesouvá valná část současné, tzv. informační společnosti – internetu. Na příkladu fór, chatovacích programů a posléze sociálních sítí (které jsou nejen nástrojem sběru dat a jejich třídění, ale především i všeobjímající socializace, původcem zcela pozměněného konceptu identity a náhledu na problematiku soukromí)

¹⁰⁶ Pentě unikly na web životopisy tisíců lidí, upozornili slovenští Anonymous. *Ihned.cz*, dostupné z: <http://zahranicni.ihned.cz/evropa-slovensko/c1-54947360-pente-unikly-na-web-zivotopisy-tisicu-lidi-upozornili-slovensti-anonymous>

jsme se snažili ukázat, že například koncem 90. let Pierrem Lévyem uvažovaná *nová demokracie*, jež měla společnost zbavit všech okovů institucionalizované reality a vytvořit nové prostředí bez kontroly, se postupem času mění v pravý opak – v prostředí, kde nic jiného, než nějaká forma dohledu (ať už laterální, komerční, či právě institucionální) neexistuje a v případě, že uživatel skutečně chce být svobodný, musí se uchýlit do prostředí **mimo** internet – například do prostředí intranetu, či dark webu - jednoduše daleko od možnosti indexování webových prohlížečů.

Zjistili jsme, že ne všechny služby, které jsou vydávány za bezplatné, jsou ve skutečnosti zdarma a že současný jedinec – tedy jeho fyzická schránka, není pro současné ICT firmy tak zajímavý, jako jeho digitální stín, datový otisk, či, chcete-li – datový dvojník, ze kterého lze automaticky a téměř ihned vytěžit zajímavé informace k rozšiřování dalšího internetového podnikání.

Na praktickém příkladu firmy Microsoft jsme se snažili ukázat, že při určité snaze ze strany uživatelů lze dopad firemního sledování uživatelů zmírnit, což ovšem neznamená, že lze zcela zastavit různé tajné vládní projekty typu PRISM, které prostředí internetu špiclují již celá desetiletí a na souhlas uživatele s čímkoliv se vůbec neptají.

Na příkladu podmínek pro užití služby a smluv EULA bylo ukázáno, že uživatel má rovněž ve vztahu mezi ním a poskytovatelem internetových a softwarových služeb v podstatě jen dvě možnosti – buď bezvýhradně souhlasit se vším, co je napsáno ve smluvních podmínkách těchto služeb (což se děje i v případě, že podmínky nečetl a pouze klikl na tlačítko Souhlasím), či služby vůbec nepoužívat a tím se ochudit o jeden z největších výdobytků současného vrcholu interakce – webu 2.0 a s ním spojeného masivního nástupu sociálních sítí a vůbec sociálních médií.

Predikovat další vývoj v tomto odvětví více, než pár let dopředu, je pak pochopitelně velice složité, stejně, jako je tomu v celém prostředí elektronické komunikace. Užívání stále většího množství elektronických médií a Hi-Tech telekomunikačních přístrojů, akumulace nepřehledného množství dat, jež hrozí brzy zcela přerůst kapacity jakýchkoliv datových center a koncept z toho vyplývající permanentní viditelnosti – to vše jsou vzrůstající problémy současného mediálního prostoru, jenž je dohledu a řízení ve velké míře nakloněn. Internet se ze svobodného média pozvolna stává jen dalším pokračovatelem postmoderní institucionalizované společnosti, jen na rozdíl od minulosti jsou již tyto instituce, slovy Zygmunta Baumana, tekuté, rozpuštěné v online prostředí vysoce interaktivního internetu.

Pokud současní badatelé v oborech Surveillance studies a elektronických médií vzhlížejí k nějakým projektům, které by znovu mohly učinit revoluci v systémech komunikace (a tím vést i k efektivnějšímu sběru uživatelských dat a sociální kontrole) – jedná se nepochybně o zařízení, schopné vytváření virtuálních realit, tedy například technologii Oculus Rift, jež byla v roce 2014 za 2 miliardy dolarů odkoupena společností Facebook¹⁰⁷ a především pak Microsoft HoloLens, která slibuje přinést skutečné holografické zobrazování vizuálních informací do reálného prostoru, což bylo dosud známé jen z některých filmů žánru science fiction. Desítky let uvažované teoretické koncepty tak pod vedením těch nejlepších IT firem světa konečně dostávají zřetelnější obrysy, což znovu vede k přehodnocování dalších konceptů a úvah z řad odborníků na tuto problematiku.

Je na obzoru doba elektronických utopií? Budou hologramy svítit na každé ulici, přinášející zcela jasně zacílenou a personalizovanou reklamu kolemjdoucímu, na základě

¹⁰⁷ Facebook closes its \$2 bn Oculus Rift acquisition. What next? *Theguardian.com*, dostupné z: <http://www.theguardian.com/technology/2014/jul/22/facebook-oculus-rift-acquisition-virtual-reality>

rychlého skenu jeho uživatelských informací, získaných ze sociálních médií a do nekonečna se rozpínajících datových center budoucnosti? Změní se způsob socializace, kdy primárním nástrojem učení a habituace již bude rychlá sensorická informace, způsobená diktátem, určeným obrazovou holograficko - prostorovou vizualizací? To jsou otázky, na které současní vědci chtějí znát odpovědi, jelikož ty mohou zcela změnit námi percipovanou realitu. Na ně si však bude třeba ještě pár let počkat a mezitím se snažit spíše se vyrovnat se současnými problémy a výzvami ryze současných elektronických médií a technologií.

SEZNAM POUŽITÉ LITERATURY A OSTATNÍCH ZDROJŮ

LITERATURA

ANDREJEVIC, M.: iSpy – Surveillance and Power in the Interactive Era, The University of Kansas, 2007.

ANDREJEVIC, M.: Reality TV, The Work of Being Watched, Rowman and Littlefield Publishers Inc, Maryland 2004.

BALL;HAGGERTY; LYON: Routledge Handbook of Surveillance Studies, Routledge, 2014.

BAUMAN, Z.; LYON, D.: Tekutý dohled, Arch-polygrafické práce, Brno, 2013.

BAUMAN, Z.: Tekutá modernita, Mladá Fronta, Praha, 2002.

BIGO, D.: Globalized (in)security: The field and the banopticon. [autor knihy]

SOLOMON; SAKAI: Traces: A Multilingual Series of Cultural Theory and Transition, University of Hong Kong Press, 2005.

BOGARD, W.: The Simulation of Surveillance: Hypercontrol in telematic societies, Cambridge University Press, 1996.

CAVANAGH, A.: Sociology In The Age of the Internet (Sociology and Social Change), Open University Press, 2007.

CLARKE, R. – Information Technology and Dataveillance, Communications of the ACM, 1998.

DANDEKER, CH.: Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day, Polity, 1994.

DELEUZE G.; GUATTARI R.: Tisíc plošin, Hermann & synové, 2010.

DELEUZE, G.: Rokovania 1972-1990, Archa, Bratislava 1998.

ERICSON, R.; HAGGERTY, K.: Policing the Risk Society, University of Toronto Press, 1997.

FOUCAULT, M.: Dohlížet a trestat – kniha o zrodu vězení, Daulphin, Praha 2000.

FOUCAULT, M.: Myšlení vnějšku, Hermann a synové, 2003.

GANDY, O.: Panoptic Sort: A Political Economy of Personal Information, Westview, 1993.

GIDDENS, A.: Důsledky modernity, Sociologické nakladatelství, 2010.

HAGGERTY, K; ERICSON, R.: The New Politics of Surveillance and Visibility, University of Toronto Press, 2006.

HIER; GREENBERG: The Surveillance Studies Reader, Open University Press, 2007.

CHRISTENSEN; JANSSON: Media, Surveillance and Identity: Social Perspectives (Digital Formations), Peter Lang Publishing, 2013.

KENNEDY, T.: „Gender and the Household Internet” in the Gender and Information Technology Encyclopedia, (ed) Eileen M. Trauth, Information Science Publishing, 2006.

KOTLER, P.: Moderní Marketing, Grada Publishing, Přeborn, 2007.

LÉVY, P.: Kyberkultura, Nakladatelství Karolinum, 2000.

- LYON, D.: *Surveillance Society, Monitoring Everyday Life*, Open University Press, Buckingham, 2001.
- LYON, D.: *Surveillance Studies, an Overview*, Polity Press, Cambridge, 2007.
- LYON, D.: *The Electronic Eye, the Rise of Surveillance Society*, University of Minnesota Press, Minneapolis, 1994.
- LYOTARD, J.F.: *O postmodernismu (Postmoderno vysvětlované dětem, Postmoderní situace)*, Filosofický ústav AV ČR, nakladatelství Filosofia, 1993.
- MCLUHAN, M.: *Člověk, média a elektronická kultura*, Jota, Brno 2008.
- MONAHAN, T.: *Surveillance and Security*, Routledge, 2006.
- MONAHAN, T.: *Surveillance in the Time of Insecurity (Critical Issues in Crime and Society)*, Rutgers University Press, 2010.
- POSTER, M.: *Critical Theory and Poststructuralism: In Search of Context*, Cornell University Press, 1989.
- SLAVÍČEK, D.: *Dohled a etika*, Disertační práce na Fakultě humanitních studií Univerzity Karlovy v Praze. Vedoucí práce doc. PhDr. Zdeněk Pinc, 2012.
- TALBOT, M.: *Media Discourse: Representation and Interaction (Media Topics)*, Edinburgh University Press, 2007.
- TAYLOR; HARRIS: *Critical Theory of Mass Media – Then and Now*, Open University Press, 2008.
- THOMPSON, J.: *Média a modernita*, Nakladatelství Karolinum, 2004.
- TROTTIER, D.: *Identity Problems in the Facebook Era*, Routledge, 2013.

TROTTIER, D.: *Social Media As Surveillance: Rethinking Visibility in a Converging World*, Ashgate Publishing, 2012.

VIRILIO, P.: *Informatická bomba*, Nakladatelství Pavel Mervart, 2004.

WEBER, M.: *Metodologie, sociologie a politika*, OIKOYMENH, 1998

ZUREIK, E et al.: *Surveillance, Privacy and Globalization of Personal Information*, McGill-Queen's University Press, 2010

ONLINE ZDROJE

„Mc Donald's Is Closing Hundreds of Stores This Year.“ *Time.com* [online]. 2015 [cit. 2015-06-20]. Dostupné z: <http://time.com/3832101/mcdonalds-closing-stores-2015/>

2014 Report – Adblocking Goes Mainstream. *Blog.pagefair.com* [online]. 2014 [cit. 2015-06-20]. Dostupné z: <http://blog.pagefair.com/2014/adblocking-report/>

AGRE P. E.: The Market Logic of Information. *Polaris.gseis.ucla.edu* [online]. 2000 2014 [cit. 2015-06-19]. Dostupné z: <http://polaris.gseis.ucla.edu/pagre/hamburg.html>

Amazon zvýšil zisk i tržby. Investory ale zklamal, čekali ještě lepší čísla. *Byznys.ihned.cz* [online]. 2014 [cit. 2015-06-20]. Dostupné z: <http://byznys.ihned.cz/c1-61639880-amazon-zvysil-zisk-i-trzby-investory-ale-zklamal-cekali-jeste-lepsi-cisla>

Anticeny za úniky dat rozdány, „uspěly“ školství a Penta. *Tyden.cz* [online]. 2013 [cit. 2015-06-23]. Dostupné z: http://www.tyden.cz/rubriky/domaci/anticeny-za-uniky-dat-rozdany-uspely-skolstvi-a-penta_267449.html#.VYqya_ntmko

Building for the next moment. *Adwords.blogspot.co.uk* [online]. 2015 [cit. 2015-06-21]. Dostupné z: <http://adwords.blogspot.co.uk/2015/05/building-for-next-moment.html>

By the Numbers: 12 Amazing Gmail Statistics. *ExpandedRamblings.com* [online]. 2015 [cit. 2015-06-20]. Dostupné z: <http://expandedramblings.com/index.php/gmail-statistics>

CDR SecUpdate 23 – Důkazy o špehování uživatelů: Google, Facebook, Apple, Yahoo, Skype. *Cdr.cz* [online]. 2013 [cit. 2015-06-22]. Dostupné z: <http://cdr.cz/clanek/cdr-security-update-projekt-prism-umozuje-vladam-spehovat-komunikaci-obcanu>

CLARKE, R.: Introduction to Dataveillance and Information Privacy, and Definitions of Terms. *Rogerclarke.com* [online]. 1997 [cit. 2015-06-18]. Dostupné z: <http://www.rogerclarke.com/DV/Intro.html#DV>

- Co je kyberšikana. *E-bezpeci.cz* [online]. 2009 [cit. 2015-06-20]. Dostupné z: <http://cms.e-bezpeci.cz/content/view/14/39/lang,czech/>
- DINUCCI, D.: Fragmented Future [online]. 1999 [cit. 2015-06-18]. Dostupné z: http://darcy.com/fragmented_future.pdf
- Dissecting Big Tech's Denial of Involvement in NSA's PRISM Spying Program. *Abcnews.go.com* [online]. 2013 [cit. 2015-06-23]. Dostupné z: <http://abcnews.go.com/Technology/nsa-prism-dissecting-technology-companies-adamant-denial-involvement/story?id=19350095#.UcNRdTvVBNs>
- EULA. *Rovio.com*. [online]. 2015 [cit. 2015-06-22]. Dostupné z: <http://www.rovio.com/eula>
- Facebook closes its \$2 bn Oculus Rift acquisition. What next? *Theguardian.com* [online]. 2014 [cit. 2015-06-23]. Dostupné z: <http://www.theguardian.com/technology/2014/jul/22/facebook-oculus-rift-acquisition-virtual-reality>
- Facebook wants solar drone to bring internet far and wide. *Cnet.com* [online]. 2015 [cit. 2015-06-24]. Dostupné z: <http://www.cnet.com/news/facebooks-solar-powered-drones-to-take-flight-this-summer/>
- Google admits its reading your emails. *theinquirer.net* [online]. 2014 [cit. 2015-06-20]. Dostupné z: <http://www.theinquirer.net/inquirer/news/2340003/google-admits-its-reading-your-emails-because-advertising>
- How the Playstation Network was Hacked. *Extremetech.com* [online]. 2011 [cit. 2015-06-22]. Dostupné z: <http://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked>
- Internet users by country (2014). *Internetlivestats.com* [online]. 2014 [cit. 2015-06-22]. Dostupné z: <http://www.internetlivestats.com/internet-users-by-country/>
- Kazuo Hirai's Letter to the U.S. House of Representatives. *flickr.com* [online]. 2011 [cit. 2015-06-22]. Dostupné z: <https://www.flickr.com/photos/playstationblog/sets/72157626521862165/>
- Když dírou do systému, tak přes Adobe Reader, Flash, nebo Javu. *Viry.cz* [online]. 2013 [cit. 2015-06-21]. Dostupné z: <http://www.viry.cz/kdyz-dirou-systemu-tak-pres-adobe-reader-flash-nebo-javu/>
- Larry Page „dreams of a place with no privacy laws“, Axel Springer CEO claims in open letter to Google. *TheDrum.com cz* [online]. 2014 [cit. 2015-06-18]. Dostupné z: <http://www.thedrum.com/news/2014/04/19/larry-page-dreams-place-no-privacy-laws-axel-springer-ceo-claims-open-letter-google>

Leading social networks worldwide as of March 2015, ranked by number of active users (in millions). *Statista.com* [online]. 2015 [cit. 2015-06-19]. Dostupné z: <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>

Most of the Web is Invisible to Google. Here's what it contains. *Popsoci.com* [online]. 2015 [cit. 2015-06-20]. Dostupné z: <http://www.popsoci.com/dark-web-revealed>

Ochrana citlivých dat se v Česku příliš neřeší, přišlo o ně 75 procent firem. *Byznys.ihned.cz* [online]. 2015 [cit. 2015-06-23]. Dostupné z: <http://byznys.ihned.cz/c1-63351190-ochrana-citlivych-dat-se-v-cesku-prilis-neresi-prislo-o-ne-75-procent-firem>

Pentě unikly na web životopisy tisíců lidí, upozornili slovenští Anonymous. *Ihned.cz* [online]. 2012 [cit. 2015-06-23] Dostupné z: <http://zahranicni.ihned.cz/evropa-slovensko/c1-54947360-pente-unikly-na-web-zivotopisy-tisicu-lidi-upozornili-slovensti-anonymous>

Prohlášení o právech a povinnostech. *Facebook.com* [online]. 2015 [cit. 2015-06-20]. Dostupné z: <https://cs-cz.facebook.com/legal/terms>

Silk Road Creator Ross Ulbricht Sentenced to Life In Prison. *Wired.com* [online]. 2015 [cit. 2015-06-21]. Dostupné z: <http://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/>

Sony fined over 'preventable' PlayStation data hack. *Bbc.com* [online]. 2013 [cit. 2015-06-22]. Dostupné z: <http://www.bbc.com/news/technology-21160818>

Sony odškodní uživatele PlayStation Network hrami za 15 milionů dolarů. *Lupa.cz* [online]. 2014 [cit. 2015-06-22]. Dostupné z: <http://www.lupa.cz/clanky/sony-odskodni-dalsi-uzivatele-playstation-network-hrami-za-15-milionu-dolaru/>

Spořitelně unikla data o mzdách, zřejmě za tím je rozvod manažerky. *Ekonomika.idnes.cz* [online]. 2014 [cit. 2015-06-23]. Dostupné z: http://ekonomika.idnes.cz/sporitelne-unikla-data-o-prijmech-vyssich-manazeru-fx7-/ekonomika.aspx?c=A140102_212135_ekonomika_vez

The Essex Cybersurvey. *Essexprimaryheads.co.uk* [online]. 2010 [cit. 2015-06-21]. Dostupné z: <http://www.essexprimaryheads.co.uk/sites/essexprimaryheads.co.uk/files/Essex%20Cybersurvey%20Spring%202011%20Executive%20summary.pdf>

The Xbox One will always be listening to you, in your own home (update). *The Verge.com* [online]. 2013 [cit. 2015-06-22]. Dostupné z: <http://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening>

TJX hack the biggest in history. *Computerweekly.com* [online]. 2007 [cit. 2015-06-23]. Dostupné z: <http://www.computerweekly.com/news/2240080607/TJX-hack-the-biggest-in-history>

Top 10 Big Data Companies (By Revenues). *Information-management.com* [online]. [cit. 2015-06-21]. Dostupné z: <http://www.information-management.com/gallery/top-10-big-data-companies-revenues-10026248-1.html>

Top Earning Blogs – Make Money Online Blogging. *Incomediary.com* [online]. 2010 [cit. 2015-06-22]. Dostupné z: <http://www.incomediary.com/top-earning-blogs>

Trendy v návštěvnosti internetu ročenka 2013 (leden 2012 – únor 2014). *Netmonitor.cz* [online]. 2014 [cit. 2015-06-21]. Dostupné z: http://www.netmonitor.cz/sites/default/files/iac_2014_-_netmonitor_rocenka_2013.pdf

ÚOOÚ udělil Komerční bance pokutu 1,8 milionu korun za červencový únik dat. *Byznys.ihned.cz* [online]. 2013 [cit. 2015-06-23]. Dostupné z: <http://byznys.ihned.cz/c1-61453470-uouu-udelil-komercni-bance-pokutu-1-8-milionu-korun-za-cervencovy-unik-dat>

V České spořitelně unikla citlivá data o platech lidí v managementu. *Byznys.ihned.cz* [online]. 2014 [cit. 2015-06-23]. Dostupné z: <http://byznys.ihned.cz/c1-61511760-v-ceske-sporitelne-unikla-citliva-data-o-platech-lidi-v-managementu>

V Česku narostl počet uživatelů internetu, stoupl už na 79 procent. *Mam.ihned.cz* [online]. 2014 [cit. 2015-06-21]. Dostupné z: <http://mam.ihned.cz/c1-63313870-v-cesku-narostl-pocet-uzivatelu-internetu-stoupl-uz-na-79-procent>

V Česku uniká víc dat kvůli zaměstnancům než kvůli softwarovým chybám. *Kaspersky.com* [online]. 2015 [cit. 2015-06-23]. Dostupné z: http://www.kaspersky.com/cz/about/news/virus/2015/V_Cesku_unika_vic_dat_kvuli_zamestnancum_nez_kvuli_softwarovym_chybam

Xbox One dumps Kinect requirement, no sensor required to play. *Nbcnews.com* [online]. 2013 [cit. 2015-06-22]. Dostupné z: <http://www.nbcnews.com/technology/xbox-one-dumps-kinect-requirement-no-sensor-required-play-6C10904079>

Xiaomi allegedly sending your info to Chinese servers [UPDATED]. *Blog.gsmarena.com* [online]. 2014 [cit. 2015-06-23]. Dostupné z: <http://blog.gsmarena.com/xiaomi-secretly-sending-info-chinese-servers/>

Youtube reportedly not profitable. *Siliconbeat.com* [online]. 2015 [cit. 2015-06-22]. Dostupné z: <http://www.siliconbeat.com/2015/02/26/youtube/>

SEZNAM OBRÁZKŮ

Obrázek č. 1 – Příklad zrealizovaného konceptu Panoptikonu

Obrázek č. 2 – Schéma zapojení počítačů v síti, umožňující snadný synchronní dohled

Obrázek č. 3 – Predikce rostoucí mobilní komerce ve Spojených státech v letech 2012-2018

Obrázek č. 4 – Příklad nastavení soukromí na sociální síti Facebook

Obrázek č. 5 – Potenciální odesílání uživatelských dat na server, umístěný v Číně