Súkromie a jeho modifikácie v digitálnom prostredí

Jaroslav Šušol
jaroslav.susol@uniba.sk

V roku 2018 celá Európska únia veľmi intenzívne žila fenoménom nazývaným GDPR. General Data Protection Regulation, alebo Všeobecné nariadenie o ochrane údajov vstúpilo do platnosti 26. mája 2016 ako Nariadenie Európskeho Parlamentu a Rady EÚ 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušila smernica 95/46/ES. Norma nadobudla účinnosť dňom 25. mája 2018. Samotné GDPR v názve síce neobsahuje termín súkromie, hovorí explicitne o ochrane dát – napriek tomu však ťažiskovým konceptom, okolo ktorého sa rozvíja celá regulácia, je ochrana súkromia subjektov, ktoré sa – chtiac či nechtiac – stále intenzívnejšie zapletajú do technologickej pavučiny modernej komunikácie a zanechávajú za sebou stopy, ktoré v porovnaní s archivačnými funkciami tradičných komunikačných kanálov a nástrojov nie sú zanedbateľné či prehliadnuteľné.

Nariadeniu EÚ sa už aj na stránkach slovenskej odbornej tlače venovalo viacero článkov, pochopiteľne, prevažne s dôrazom na kontexty informačnej bezpečnosti a informačného, resp. knižnično-informačného systému (napr. Andrejčíková et al., 2019). Táto štúdia je postavená na spracovaní aktuálnej výskumnej literatúry k problematike súkromia a pokúša sa analyzovať pojem súkromia z pohľadu sociálno-vedného, filozofického i právneho. Načrtáva nárast významu súkromia s rozvojom modernej demokratickej spoločnosti a následne sa zameriava na otázky spojené s výzvami, prínosmi i hrozbami, ktoré pre súkromie jednotlivca predstavuje rozvoj digitálnej komunikácie. V záverečnej časti prezentuje základné východiská výskumov informačného správania používateľov v digitálnom svete, ktoré sú spojené s fenoménom paradoxu súkromia.

Súkromie ako sociálna a filozofická kategória

Súkromie v súčasnosti predstavuje jednu z najdiskutovanejších a zároveň najkomplikovanejšie definovateľných (a definovaných) sociálnych, filozofických či právnych kategórií. Dotýka sa takých dôležitých hodnôt ľudského bytia ako sú sloboda, dôstojnosť alebo identita a zároveň sa pri posudzovaní právnych súvislostí veľmi úzko prelína s iným, na prvý pohľad nie veľmi podobným fenoménom, ktorým je vlastníctvo. V súčasnom verejnom diskurze sa pojem *súkromie* a jeho odvodeniny, najmä adjektívum *súkromný*, používajú v pomerne širokej škále významov – individuálny, vlastný, ale aj rodinný, domáci, neoficiálny či skrytý, dôverný, tajný, intímny.

Prienik súkromia a *slobody* možno vidieť najmä v tom, že všetko to, čo sa považuje za súkromné, predstavuje sektor akejsi nezávislosti od štátnej moci, priestor, v ktorom človek realizuje svoju osobnú slobodu bez ohľadu na vplyv oficiálnej moci či vládnucej ideológie. Tento rozmer súkromia veľmi dôverne poznajú všetci tí, ktorí žili v dobách reálneho socializmu 70. a 80. rokov 20. storočia a vedeli, že v súkromí si môžu hovoriť a myslieť čo chcú, ale oficiálna, verejne prezentovaná a štátom podporovaná ideológia mala svoje jasne definované podoby.

Ľudská dôstojnosť sa považuje za nevyhnutnú podmienku slobodného rozvoja človeka ako indivídua tým, že sa mu práve v podobe súkromia priznáva určitý stupeň autonómie, nezávislosti či „samourčenia". V úzkej nadväznosti na to má *identita* – suma osobných identifikátorov, kvalít, charakteristík, výzoru, ale aj názorov a postojov, ktoré umožňujú odlíšiť jedného človeka od druhého – veľmi blízky vzťah k takým pojmom ako osobnosť, individualita alebo identifikácia.

Psychológovia v súvislosti s identitou často akcentujú skutočnosť, že tento fenomén má blízky vzťah ku kreovaniu sebaobrazu jednotlivca, ako akéhosi mentálneho modelu, ktorý si každý z nás vytvára o sebe a ktorý obsahuje nielen objektívne a pozorovateľné údaje o nás samých, ako sú výška či farba vlasov, ale aj poznatky, ktoré sme si o sebe vytvorili na základe vlastnej skúsenosti alebo internalizáciou názorov ľudí v našom okolí (Fearon, 1999; Stets, 2000). Na druhej strane však treba tiež zdôrazniť, že identita nie je singulárna a nie je úplne fixná. Môžeme ju považovať za typické „ja" v určitom štádiu života, situované v kontexte organizovaných sociálnych vzťahov (Peace, 1999). Takže to, ako sa svojmu okoliu prezentujeme, závisí od konkrétnej situácie alebo účelu a elektronické siete sú práve prostredím, ktoré nám dáva možnosť byť niekým iným alebo naopak, ešte viac sám sebou (Reymers, 1998). Sociálne a psychologické súvislosti tohto javu výstižne zachytil už v roku 1993 Peter

Steiner, ktorý v časopise The New Yorker publikoval dnes už klasickú karikatúru rozhovoru dvoch psov pri počítači, keď jeden hovorí tomu druhému: „Na internete nikto nevie, že si pes".

Obr. 1 Peter Steiner: Na internete nikto nevie, že si pes. New Yorker, 5. júl 1993

V elektronickom sieťovom prostredí sa tak dá hovoriť o ešte silnejších nástrojoch a prejavoch *manažovania identity*, než aké máme k dispozícii v reálnom, fyzickom svete – kde tiež dokážeme úmyselne zdôrazňovať alebo naopak potláčať určité črty svojho správania, tak ako na sieti vieme zdôrazňovať alebo zatajovať určité informácie o sebe.

Viacerí autori pri analýze problematiky súkromia oprávnene zdôrazňujú (napr. Fuster, 2014) dialektiku vzťahu súkromného a verejného – na to, aby človek mohol byť skutočne slobodným indivíduom, nemôže byť oddelený od toho, čo je sociálne a verejné. Napokon, aj z pohľadu širokej škály aktuálnych sociálno-psychologických, kognitívnych a ďalších teórií platí, že to, čo transformuje deti na špecifické indivíduá sú ich vzťahy k iným ľuďom. Rozličné štruktúry psychiky človeka, ktoré utvárajú individuálne vedomie, sa determinujú práve vzťahmi s vonkajším svetom.

Súkromie ako právna kategória

V súčasnej odbornej spisbe prevláda názor, že právo na súkromie ako všeobecne akceptované právo sa začalo presadzovať až na prelome 19. a 20. storočia, avšak koncept súkromia ľudia vnímali už dávno (Lukács, 2016). V prospech tohto tvrdenia je možné argumentovať niektorými všeobecne rozšírenými kultúrnymi stereotypmi a obrazmi (Adam a Eva si čoskoro po stvorení sveta začali zakrývať telo, ako prejav hľadania súkromia), ale aj odkazmi na najstaršiu známu legislatívnu teóriu i prax – Chammurapiho zákonník, ktorý sa v súčasnosti datuje do obdobia roku 1800 pred naším letopočtom, i rímske právo obsahovali paragrafy, ktoré sankcionovali vniknutie do cudzieho príbytku. Pochopiteľne, našli by sme asi značné množstvo právnych teoretikov, ktorí by v tomto historickom kontexte ako silnejšiu motiváciu takéhoto právneho usporiadania videli skôr snahu o ochranu majetku. V každom prípade však možno konštatovať, že myšlienka súkromia a oddelenia toho, čo je privátne, od toho, čo je verejné, zrejme vždy reflektovala prirodzenú potrebu jednotlivca vnímať a deklarovať rozdiel medzi *mnou* ako osobou, subjektom na jednej strane a okolitým svetom na strane druhej.

Sociálny, filozofický či politický význam *subjektu* sa v priebehu vývoja spoločnosti, prirodzene, menil. V zásade však platí, že až do začiatku obdobia novoveku bol jednotlivec vnímaný predovšetkým ako člen komunity, súčiastka v súkolí spoločenského mechanizmu, ktorá bola neustále monitorovaná ostatnými príslušníkmi relatívne malého spoločenstva. V priebehu 19. storočia sa postupne presadzujú zásadné sociálne a ekonomické zmeny, najmä industrializácia, urbanizácia a formovanie národných štátov, ktoré vedú k výraznejšiemu doceňovaniu (možno až preceňovaniu?) významu jednotlivca a následne aj významu súkromia. Dôvodom i dôsledkom týchto civilizačných trendov bola výraznejšia koncentrácia obyvateľstva ako v predchádzajúcich historických etapách, väčšia anonymizácia i demokratizácia spoločnosti. Človek sa začal strácať vo veľkých komunitách a zároveň mu táto zdanlivá strata individuality umožnila sa výraznejšie prejaviť ako nezávisle mysliaca a konajúca bytosť.

Prelomovým okamihom v úvahách o legislatívnom pozadí fenoménu súkromia sa podľa viacerých autorov (Baek, 2014; Lukács, 2016) stal rok 1890, kedy vyšiel článok Samuela Warrena a Louisa Brandeisa pod názvom *The right to privacy*, teda Právo na súkromie. Časopis Harvard Law Review začal vychádzať v roku 1887 a do súčasnosti je jedným z najvýznamnejších periodík v oblasti práva. Vo svojom článku Warren a Brandeis

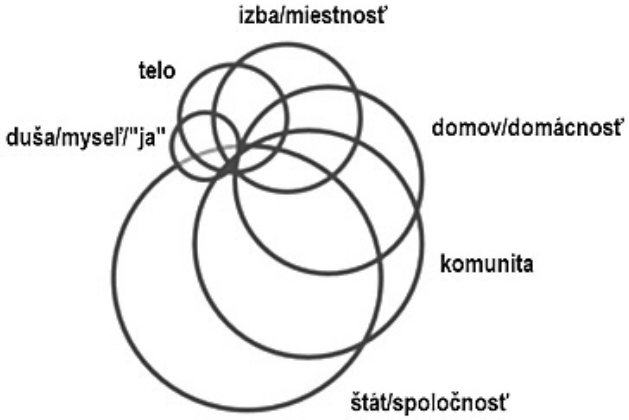
zdôrazňujú, že je nevyhnutné prispôsobovať vývoj legislatívy aktuálnym potrebám spoločnosti. V tomto období, teda na konci 19. storočia, autori identifikovali dva významné javy, ktoré podľa nich podstatne ohrozovali súkromie – technický vývoj, reprezentovaný najmä vynálezom fotografie, a klebety, ktoré sa začali „inštitucionalizovať" v podobe rodiacej sa bulvárnej tlače. Požiadavka práva na súkromie teda bola formulovaná pomerne výstižne, ako *právo nechať na pokoji* (the right to be let alone) a bola zameraná skôr proti emocionálnej ujme, nie proti ujme spojenej napríklad s odcudzením majetku. Išlo teda o právo na ochranu proti nechcenému zverejneniu súkromných faktov, myšlienok alebo emócií.

Od konca 19. storočia sa vnímanie fenoménu súkromia prirodzene posunulo ďalej a viedlo k vytvoreniu mnohých ďalších definícií a koncepcií – od tých jednoduchších či priamočiarejších (napr. Szabó: *súkromie je právo jednotlivca rozhodnúť o sebe*, Szabó, 2005) až po tie komplikovanejšie (Parker: *súkromie je kontrola nad tým, kto a kedy môže vnímať rozličné komponenty nás samých*, Parker, 1974). V 60. rokoch 20. storočia bol Alan Westin prvým autorom, ktorý prišiel s informačne orientovanou definíciou súkromia, keď ho charakterizoval, ako *právo jednotlivcov, skupín alebo inštitúcií určiť kedy, ako a do akej miery sa majú informácie o nich komunikovať iným subjektom* (Westin, 1967). Situácia okolo vnímania súkromia v súčasnom globalizovanom svete je zložitá aj kvôli tomu, že v rozličných kultúrach sa tradične kladie rôzny dôraz na význam jednotlivca a jeho súkromia – iné miesto má tento koncept v individualistických spoločnostiach Západu, a iné v kolektivistickejšie orientovaných kultúrach Východu.

O jeden z prvých systematickejších prístupov k zmapovaniu koncepcií súkromia sa začiatkom 21. storočia pokúsil Daniel Solove, podľa ktorého existuje 6 základných typov definícií súkromia (Solove, 2002):

1. právo „nechať na pokoji"
2. obmedzenie (fyzického) prístupu k osobe
3. utajovanie
4. kontrola osobných informácií
5. ochrana (integrity) osobnosti
6. intimita, dôvernosť, medziľudské vzťahy

Je faktom, že rozdiely v uvedených prístupoch sú niekedy ťažšie postihnuteľné, odlišnosť medzi prístupmi 1 a 2 (právo nechať na pokoji a právo obmedziť prístup) Solove napríklad špecifikuje tak, že druhý typ definície je vlastne len sofistikovanejšou formuláciou tej prvej. Z hľadiska priestorového záberu je možné koncipovať súkromie ako fenomén, ktorý je situovaný na rôznych úrovniach vzťahu človeka, indivídua a jeho okolia. Pri takomto pohľade na súkromie ide o to, s čím jednotlivec komunikuje alebo voči komu/čomu sa vymedzuje (Poulsen, 2019). Takýto model súkromia potom postupuje od jednotlivého „ja" ako osobnosti, mysle, cez telo, vlastný uzatvorený priestor, dom, komunitu, v ktorej človek žije, až po štát/spoločnosť.



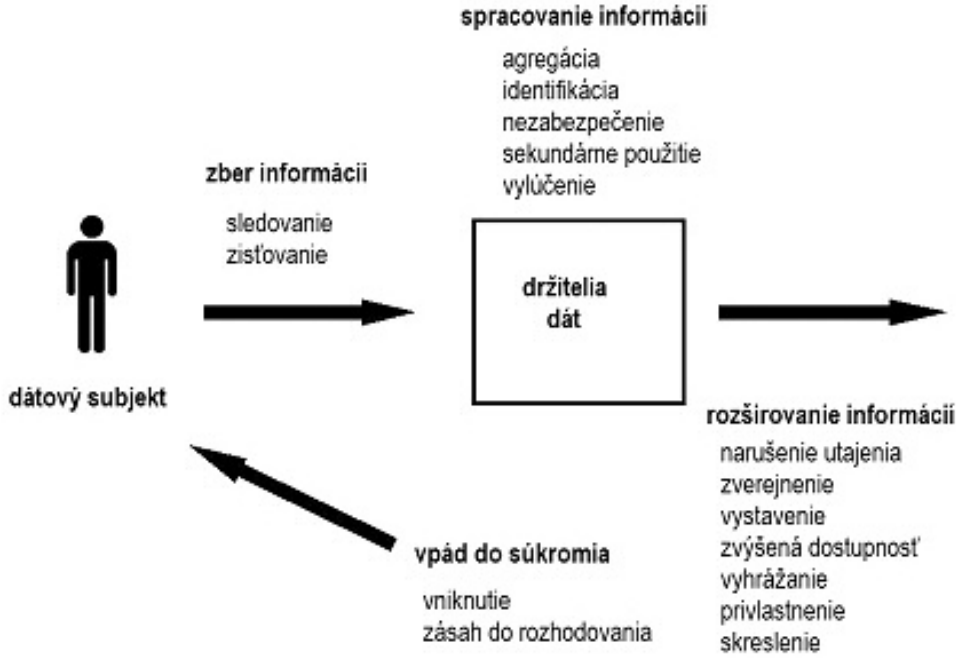
Obr. 2 Priestory/úrovne súkromia (Poulsen, 2019)

Daniel Solove len o pár rokov neskôr po zverejnení typológie definícií súkromia dospel k záveru, že snaha o logické usporiadanie vzťahov v rámci tohto konceptu si vyžaduje pragmatickejší a technologicky založený prístup, postavený na báze rôznych typov aktivít, ktoré môžu viesť k narušeniu súkromia. Jeho taxonómia súkromia (Solove, 2006) je vystavaná na existencii 4 typov potenciálne *škodlivých aktivít*, z ktorých väčšina (tri) súvisí s informáciami o človeku, resp. dátovom subjekte (obrázok 3). Ide o zber informácií, spracovanie informácií, rozširovanie informácií a vpád do súkromia.

Dátový subjekt je zdroj, od ktorého alebo o ktorom rôzne typy iných subjektov (iní ľudia, obchod, vláda a pod.) zbierajú informácie – pričom samotný *zber informácií* nemusí byť vždy aktivitou, ktorá dátový subjekt poškodzuje. K typickým negatívnym aktivitám tohto typu patria sledovanie alebo zisťovanie informácií. *Spracovanie informácií* je skupina aktivít, ktoré umožňujú na základe využitia rôznych metód odvodzovať z pôvodne zozbieraných dát nové informácie – zaraďujeme sem také aktivity ako agregácia dát, identifikácia jednotlivca, sekundárne využitie dát alebo porušenie povinností súvisiacich s ochranou dát. Do skupiny aktivít spojených s *rozširovaním informácií* patria napríklad, porušenie prísľubu o nezverejňovaní informácií zo strany spracovateľa, zverejnenie pravdivých či nepravdivých informácií o subjekte, privlastnenie si identity subjektu, vyhrážanie sa zverejnením informácií alebo zverejnenie intímnych obrazov tela subjektu. *Vpád do súkromia*, na rozdiel od predchádzajúcich troch typov aktivít, nemusí nevyhnutne zahŕňať osobné informácie – vniknutie predstavuje invazívny akt, ktorý porušuje niečí pokoj alebo samotu, zásah do rozhodovania je preniknutie štátnej moci do rozhodovania subjektu o osobných záležitostiach.

Tento pohľad na morfológiu súkromia jasne vypovedá o tom, že súkromie možno chápať v rozličných kontextoch, fyzických i mentálnych, a že jeho ochrana sa orientuje ani nie tak na škody, ktoré môžu byť spôsobené nášmu fyzickému telu, ako skôr na predchádzanie a riešenie poškodení či poranení psychickej, emocionálnej stránky osobnosti.

V duchu uvedených definícií a taxonómií bolo v priebehu 20. storočia prijatých niekoľko legislatívnych noriem, politických dokumentov a medzinárodných dohôd, ktoré deklarovali význam súkromia a jeho ochrany pre moderného človeka. K základným pilierom v tomto smere patrí *Všeobecná deklarácia ľudských práv*, ktorej článok 12 stanovuje, že „nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromia, rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na právnu ochranu proti takýmto zásahom alebo útokom." O niečo neskôr, v roku 1950 podobné princípy ukotvila aj Rada Európy v článku 8 *Dohovoru o ochrane ľudských práv a základných slobôd*. Podľa tohto dohovoru má každý občan „právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie" a „štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných."



Obr. 3 Taxonómia súkromia (Solove, 2006)

Charta základných práv EÚ bola prijatá v roku 2000 a v súlade s vývojom technológií v ostatných desaťročiach jej ustanovenia výraznejšie reflektujú predovšetkým informačnú stránku súkromia. Článok 8 tohto dokumentu deklaruje, že každý má právo na ochranu osobných údajov, ktoré sa ho/jej týkajú, pričom sa vyžaduje, aby takéto dáta boli spracované korektne na špecifikovaný účel a na základe súhlasu dotknutej osoby, alebo na inom legitímnom základe ustanovenom v zákone. Zároveň platí, že každý má právo prístupu k dátam, ktoré boli o ňom/nej zhromaždené, a právo požadovať opravu týchto dát.

Práve tieto princípy Charty základných práv EÚ sa stali jednými zo základných východísk už spomínanej európskej normy, GDPR, a možno ich sumarizovať v troch základných pilieroch (Gellert a Gutwirth, 2013):

- princíp špecifikácie účelu (dáta sa smú spracovať a využiť len na jasne špecifikované, explicitne odsúhlasené a zákonné účely);
- princíp férovosti (spracovanie dát musí byť férové a zákonné vo vzťahu k dátovému subjektu);
- princíp kvality dát (dáta musia byť adekvátne, relevantné a nepresahujúce účel použitia).

Ochrana súkromia v digitálnom svete

Nové rozmery vnímania limitov súkromia do spoločenskovedného i právneho uvažovania priniesli počítače a digitálne technológie. Jedným z prvých počítačových špecialistov, ktorý predvídal možné negatívne vplyvy počítačov na súkromie, bol Bernard S. Benson, ktorý už v roku 1961 konštatoval, že stále viac geograficky i technologicky „nesústredených" informácií o človeku sa cez počítače ukladá bez toho, aby si to ktokoľvek všimol – ale tieto dáta bude možné jedného dňa stiahnuť do nejakého výkonného prístroja a vtedy bude súkromie jednotlivca v rukách toho, kto bude ovládať tento stroj (Fuster, 2014).

Len o pár rokov neskôr, v roku 1964 iný významný počítačový technologický expert, Vance Packard, publikoval knihu *The Naked Society*, teda Nahá spoločnosť. V nej okrem iného vyslovuje obavu, že nové technológie sú potenciálnou hrozbou nielen pre súkromie jednotlivca, ale aj ďalšie jeho „práva", ktoré sú s vnímaním a fungovaním fenoménu súkromia spojené a ktoré v tradičnom, analógovom svete považujeme za samozrejmé. Ide napríklad o právo byť odlišný, právo dúfať v tolerantné odpustenie alebo prehliadnutie minulých hlúpostí a chýb, pokleskov alebo drobných prehreškov, či právo na nový začiatok. Problém podľa Packarda vo svete nových technológií spočíva práve v tom, že ich schopnosť zapamätať si, pripomínať i zverejňovať – a teda nezabúdať na naše minulé zlyhania, je mimoriadne silná (Fuster, 2014).

Aj viacerí ďalší autori upozorňujú na to, že obavy o online súkromie sa v spoločnosti objavovali postupne, s nástupom výkonnejších informačných a komunikačných technológií, ako boli databázové systémy (80. roky 20. storočia) a internet (90. roky 20. storočia) (Baek, 2014). Súvisiaca legislatíva sa však na dvoch stranách Atlantiku vyvíjala trocha odlišne. V krajinách budúcej EÚ zákony o ochrane osobných dát v tej dobe neboli explicitne spojené s právom na súkromie, ale vyvíjali sa samostatne. Prvým európskym zákonom tohto typu bol v roku 1970 prijatý Hessische Datenschutzgesetz, podľa ktorého záznamy, dáta a výsledky ich spracovania treba získavať, prenášať a ukladať tak, aby ich nemohla čítať, meniť, extrahovať alebo zničiť neoprávnená osoba. Primárnym záujmom teda bolo zabezpečenie dôvernosti, utajenia dát. Naproti tomu v USA sa dôraz kládol skôr na práva osôb dotknutých spracovaním dát – cez zabezpečenie súkromia, v podobe „kontroly" nad osobnými informáciami. Významnú úlohu zohrávala doktrína „fair information practices", správnej informačnej praxe, ktorá predpisuje, čo treba urobiť, keď sa informácia spracúva – ako protiklad voči prístupom, ktorých podstatou je zabrániť spracovaniu. (Fuster a Gutwirth, 2013).

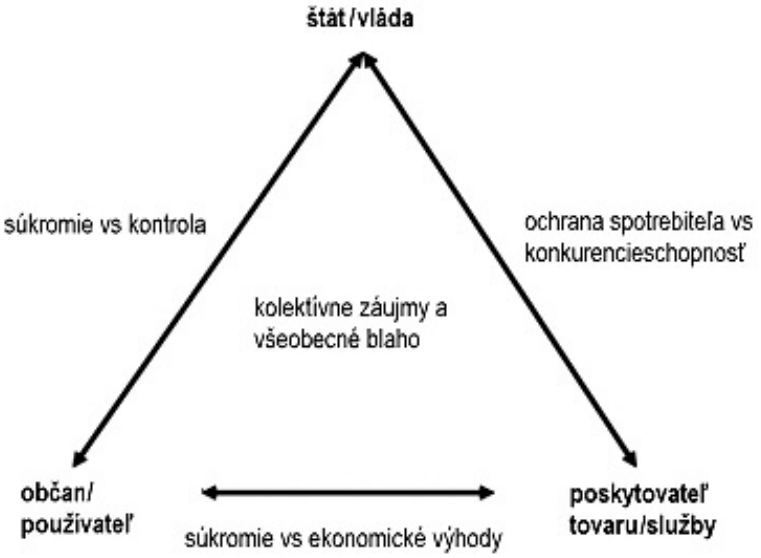
Vyššie uvedené úvahy o vplyve počítačov na súkromie, najmä tá Bensonova, nám zároveň ukazujú, ako sa reálny technologický vývoj často odlišuje od predstáv. Ak Benson pred cca 60 rokmi vo svojej vízii videl nejaký výkonný stroj, do ktorého bude možné uložiť a spracovať v ňom všetky zozbierané dáta o jednotlivcovi, dnes túto predstavu napĺňajú technológie veľkých dát a nástroje ich analýz – teda technológie, kde prvotnú úlohu nezohráva stroj, ale skôr usporiadanie nášho života postavené na neustálom zbieraní dát o našich aktivitách a našom správaní. Symptomatické pre dnešné technológie veľkých dát je to, že možné spôsoby ich využitia a výsledky, ku ktorým sa dá na základe ich analýzy dospieť, sa často dajú len ťažko predvídať v čase, keď sa tieto dáta zbierajú. Príkladov by sa dalo v tomto smere uviesť nepreberné množstvo, Tene a Polonetsky uvádzajú zaujímavý prípad vývoja okolo lieku Vioxx, ktorý bol uvedený na trh koncom 20. storočia ako prípravok s protizápalovými účinkami a využíval sa na liečenie osteoartritídy. Vedľajšie účinky lieku odhalili až podrobné analýzy klinických a nákladových dát, ktoré uskutočnila firma Kaiser Permanente a ktoré ukázali neúmerne vysoké množstvo prípadov úmrtia pacientov spojené so zlyhaním srdca medzi rokmi 1999 a 2003 (Tene a Polonetsky, 2012).

Za jednu z najvýznamnejších zmien vo fungovaní súkromia v digitálnom sieťovom prostredí možno považovať koncept *práva na zabudnutie*, alebo *práva na vymazanie*. Ako už bolo povedané, internet so sebou priniesol zásadnú technologickú zmenu. K dispozícii sú rozsiahle, takmer neobmedzené kapacity pamäťových médií, rozptýlené po celom svete v podobe distribuovaného, amorfného *cloudu*, v dôsledku čoho sa stále väčšie množstvo dát ukladá a sú dostupné na spracovanie. Zapamätanie sa tak v novej konštelácii pamäťových technológií stáva štandardom a zabúdanie, ktoré bolo inherentnou súčasťou a zároveň kvalitou (?) ľudskej i spoločenskej analógovej pamäte, sa dostáva skôr do polohy nechcenej výnimky či poruchy. Aj preto sa princíp práva na zabudnutie dostáva do modernej legislatívy spojenej s ochranou súkromia, hoci aj tu sa vynára niekoľko diskutabilných otázok: na aké kategórie dát by sa malo právo na vymazanie vzťahovať; či by mali používatelia mať možnosť vymazať alebo žiadať o vymazanie dát, ktoré sami zverejnili online; čo s dátami, ktoré používatelia zverejnili,

ale iní medzičasom zdieľali; alebo či môže niekto (napríklad súd) nariadiť stiahnutie informácie, ktorá je síce pravdivá, ale pre niekoho (možno samotného pôvodcu) nepríjemná? (Warso, 2013)

Analýza akýchkoľvek zozbieraných údajov, nielen tých, ktoré môžeme označiť ako veľké dáta, so sebou nesie riziko narušenia súkromia jednotlivca – predovšetkým z hľadiska jeho identifikácie v množine subjektov a následného zneužitia tejto informácie. Pochopiteľne, v reálnom živote sa dáta dajú využiť na rôzne stupne identifikácie subjektov, ktoré možno aplikovať v rôznych situáciách. Hovoríme napríklad o profilovaní (zisťovanie/zhromažďovanie základných charakteristík jednotlivcov s ohľadom na konkrétne, často adresné marketingové zámery), o diskriminácii či rozlišovaní medzi rôznymi subjektmi, o vylúčení osôb z určitých dátových množín či aktivít, alebo o strate kontroly nad dátami (Tene a Polonetsky, 2012).

Dôsledkom môže byť to, že napríklad zamestnávateľ si dokáže o zamestnancovi zistiť informácie, ktoré mu zamestnanec nechcel a nemusel poskytnúť. Weber ako príklad uvádza situáciu, keď sa k potenciálnemu zamestnávateľovi pred výberovým konaním dostane zo sociálnej siete informácia o tom, že uchádzačka je tehotná, alebo vyliečenému alkoholikovi sa za „minulé hriechy" nepodarí získať zamestnanie v školstve (Weber, 2015). Zoznam potenciálnych dôsledkov spojených s únikom osobných údajov alebo odhalením informácií osobného charakteru (napríklad identifikáciou konkrétneho subjektu vo výskumnej vzorke) môže byť obsiahly – okrem straty možnosti na zamestnanie či poistenie to môže byť napríklad cenová diskriminácia na trhu, zneistenie, rozpaky prípadne iný emočný stres, strata dobrého mena v kruhu rodiny, známych a kolegov, alebo dokonca konflikt s občianskym alebo trestným právom (Altman et al., 2018). Ako zdôrazňujú niektorí autori, čím viac dát sa o správaní subjektu nazbiera, tým je človek prediktabilnejší a takéto poznanie má obrovskú cenu vo sfére marketingu, najmä z hľadiska využívania princípov adresnej ponuky produktov, bez toho aby firma musela investovať prostriedky do masovej, často nákladnej reklamy (Weber, 2015).



Obr. 4 Vzťah osobných, verejných a ekonomických záujmov v doméne súkromia (podľa Baumann a Schünemann, 2017)

Napriek tomu, že sa pri zbere i spracovaní dát v súčasnosti využíva široká škála rozličných prístupov a techník, ktorých cieľom je zakryť identitu jednotlivých dátových subjektov a ktoré sa vo všeobecnosti označujú ako metódy deidentifikácie (anonymizácia, pseudonymizácia, kódovanie dát a ďalšie), informatici nám stále úspešnejšie dokazujú, že za určitých (nie príliš komplikovaných) podmienok je možná aj reidentifikácia, teda obnovenie možnosti určiť to, ktorý subjekt sa skrýva za konkrétnymi dátami.

V širokej verejnosti sa pomerne často možno stretnúť s pochybnosťou o tom, do akej miery treba považovať za citlivý či súkromný taký údaj ako je napríklad rodné číslo, bez spojenia s menom človeka. Treba si však uvedomiť, že rodné číslo v súčasnej podobe jednak obsahuje zakódované dáta, z ktorých možno odvodiť vek alebo pohlavie človeka. Na druhej strane, riziko zverejnenia rodného čísla spočíva aj v tom, že ide o údaj, ktorý je využívaný v rôznych evidenciách a veľmi ľahko tak umožňuje prepojiť údaje z rôznych databáz, ktoré zdanlivo medzi sebou nesúvisia. Žijeme v dobe, kedy si aj sami používatelia vytvárajú v digitálnom prostredí rozličné identity v rôznych typoch sietí a zdieľajú v nich rôzne typy informácií o sebe, pracovné, profesionálne, i súkromné. Často si neuvedomujú, že tieto dva póly digitálneho sveta sa nedajú od seba striktne oddeliť a informácie dokážu prúdiť od jedného pólu k druhému.

Teoretické koncepty a modely súkromia v digitálnom prostredí sa rozpracovávajú do stále väčších detailov. *Diferenciálne súkromie* je silný matematický model a definícia súkromia postavená na využití nástrojov štatistickej a strojovej analýzy, ktorá je aplikovateľná najmä v prostredí súborov výskumných dát, napríklad sociologických prieskumov. Zatiaľ, čo tradičné prístupy vnímajú súkromie ako vlastnosť výstupu analýzy, teda zabezpečiť, aby na výstupe nebolo možné zistiť údaje o konkrétnom jednotlivcovi, v tomto prípade ide o takú (štatistickú) modifikáciu výpočtov, aby sa zabezpečilo súkromie, resp. ochrana údajov v procese samotnej analýzy (Wood et al., 2018).

Detailnejšie sa prepracúvajú aj terminologické základy konceptu súkromia. *Kontrolu súkromia* (v podobe intervencií, zásahov) možno definovať, ako metódy a mechanizmy, ktoré sa dajú využiť v konkrétnom prípade zverejnenia dát na zvýšenie úrovne súkromia a bezpečnosti. Ide o široký pojem zahŕňajúci všeobecnejšie orientované zásahy, ako napr. vzdelávanie v oblasti súkromia, ale aj kontrolu informačnej bezpečnosti, ako je napríklad kódovanie, certifikácia autorizovaných používateľov alebo trestné postihy. Riziká spojené so súkromím sa potom dajú klasifikovať na *ohrozenia* súkromia (potenciálne nežiaduce udalosti alebo okolnosti ktoré môžu spôsobiť problém dátovému subjektu), *škody* na súkromí (dokonané ujmy) a *zraniteľnosť* súkromia (charakteristiky, ktoré zvyšujú pravdepodobnosť realizácie hrozieb) (Altman et al., 2016).

Pri všetkej pozornosti a dôraze, ktorý sa v súčasnosti kladie na otázky súkromia, však netreba zabúdať na to, že podobne ako v celej doterajšej histórii vzťahu jednotlivca a spoločnosti, aj v digitálnej ére platí, že princípy súkromia a ochrany osobných elektronických dát musia byť v rovnováhe vo vzťahu k ďalším celospoločenským hodnotám, ktoré treba brať do úvahy pri nastavovaní sily ochrany súkromia – ide o také hodnoty, ako verejné zdravie, národná bezpečnosť, presadzovanie práva, ochrana prostredia či ekonomická efektívnosť (Tene a Polonetsky, 2012).

Paradox súkromia na internete

Výskumy informačného správania používateľov v digitálnom prostredí sa realizujú už niekoľko desaťročí, s ohľadom na rozličné kontexty práce s informáciami. Viaceré takéto výskumy sa uskutočnili aj na Slovensku, so zameraním na informačné a publikačné správanie používateľov knižníc, vysokoškolských študentov či vedeckých pracovníkov (Steinerová a Šušol, 2004; Šušol, 2005; Šušol, 2011; Ondrišová, 2014; Steinerová, 2016 a ďalšie). V súčasnosti sa na interdisciplinárnej úrovni v spolupráci odborníkov z informatiky, informačnej vedy a psychológie rieši výskumný projekt Informačné správanie človeka v digitálnom prostredí, za účasti Fakulty informatiky a informačných technológií STU a Filozofickej fakulty UK v Bratislave. Projekt sa zameriava na implicitnú spätnú väzbu, návrh novších funkcií rozhraní systémov a návrhy nových modelov s využitím kvalitatívnych aj kvantitatívnych metód výskumu a experimentov s dôrazom na ekologické a etické aspekty spracovania informácií na úrovni jednotlivcov aj skupín (sociálnych sietí) v digitálnom prostredí. Cieľom je zlepšenie poznania v oblasti predikcie informačného správania, identifikácie bariér a personalizácie služieb v digitálnom prostredí.

V celosvetovom meradle je už dlhšiu dobu jedným z ťažiskových smerov výskumu v tejto oblasti aj otázka vnímania dôležitosti súkromia a jeho premena na komoditu – tak zo strany poskytovateľov informačných služieb, ako aj zo strany používateľov, teda dátových subjektov. Ako sme už uviedli, výskumy naznačujú, že používatelia najčastejšie majú tri hlavné typy obáv ohľadom ochrany ich súkromia a osobných dát na internete (Ginosar a Ariel, 2017):

- to, že sa ich osobné údaje budú zbierať bez ich explicitného a informovaného súhlasu;
- ak aj udelia súhlas, že tieto dáta sa budú posúvať ďalej na spracovanie či využitie „tretími stranami";
- že ich osobné dáta sa použijú na sekundárne účely, teda na také, na ktoré používatelia pôvodne nedali svoj súhlas.

Celý tento komplex problémov a súvislostí sa zvykne označovať ako *paradox súkromia* na internete, pričom paradoxnosť tejto situácie spočíva v dvoch rovinách:

1. Používatelia zvyčajne deklarujú, že si svoje súkromie vysoko cenia, ale nemajú problém s tým, aby v prostredí, ktoré sa im javí ako „súkromné" (napríklad sociálne siete) často zverejňovali veľmi intímne informácie zo svojho života.
2. Napriek deklaráciám o dôležitosti súkromia sú používatelia v digitálnom prostredí náchylní „prepustiť" viac a dôvernejších informácií, ako v podobnej situácii v reálnom svete. Niektorí tak robia preto, lebo si neuvedomujú možné riziká, iní preto, lebo zvažujú eventuálne výhody spojené s takýmto krokom a sú si vedomí toho, že druhá strana, teda poskytovatelia služieb, sú ochotní poskytnúť svoje služby výmenou za osobné dáta, ktoré pre nich majú význam najmä z marketingového hľadiska.

Na ten druhý prístup – teda vedomé poskytnutie súkromných údajov v snahe o dosiahnutie určitých výhod – sa v literatúre už vžil terminus technicus *kalkulácia so súkromím* (privacy calculus), hoci anglický termín *calculus* by sa dal preložiť aj ako výpočet. A skutočne, niektorí autori zdôrazňujú, že kalkulus je nielen snahou

o vysvetlenie, ale eventuálne aj o viac či menej exaktné „vypočítanie" používateľovho zámeru vyjaviť svoje osobné informácie, na základe troch premenných (Ginosar a Ariel, 2017):

- výhody, ktoré môže používateľ získať;
- rôzna úroveň dôvery – voči konkrétnym webovým stránkam a sídlam, alebo špecifické aktivity, v rámci ktorých sa informácie využívajú;
- rôzna úroveň povedomia používateľov o podstate internetu a rizík, ktoré sú s ním spojené – teda to, čo zvykneme súhrnne označovať ako online, sieťová alebo digitálna gramotnosť.

Niektoré prepracovanejšie prístupy tento model ešte detailnejšie špecifikujú do podoby tzv. *dvojitej kalkulácie* (dual-calculus model), ktorá sa skladá z *kalkulácie súkromia* (privacy calculus), posudzujúcej benefity a riziká konkrétnej transakcie, a *kalkulácie rizík* (risk calculus), zameriavajúcej sa na posúdenie vážnosti rizík transakcie a efektívnosť mechanizmov, ktoré má používateľ k dispozícii na ich zvládanie.

Ďalšie prístupy ku skúmaniu faktorov, ktoré ovplyvňujú postoj používateľov k svojmu súkromiu a jeho zverejňovaniu, sa pokúšajú brať do úvahy aj širšie sociálne a psychologické súvislosti týchto procesov. Podľa niektorých výskumníkov (Li et al., 2017) je v tomto prípade efektívne aplikovať viacrozmernú vývojovú teóriu a na jej základe možno tieto faktory rozdeliť do 3 dimenzií:

- osobnostné charakteristiky jednotlivca, reflektujúce jeho osobnostný vývoj a zahŕňajúce aj všeobecný postoj k otázkam ochrany súkromia;
- prostredie, ktoré je podnetom pre kognitívne i afektívne zhodnotenie konkrétnej komunikačnej/transakčnej situácie, produktu (ako na mňa pôsobí stránka?, páči sa mi?, je užitočná? atď.);
- interpersonálne vzťahy v konkrétnej situácii, vrátane zhodnotenia pomeru ziskov a nákladov pri danej výmene – ide teda hlavne o vnímanie kontroly súkromia v danom okamihu.

V súvislosti s rozvojom výskumu paradoxu súkromia na internete sa objavovali aj viaceré pokusy o načrtnutie typológie používateľov s ohľadom na ich správanie vo vzťahu k vlastnému súkromiu. Z pohľadu ochoty dať k dispozícii svoje osobné informácie napríklad možno používateľov rozdeliť do troch skupín (Ginosar a Ariel, 2017). Najväčšia skupina, ktorá zahŕňa cca 50 % populácie, je skupina *pragmatická* – tá je pripravená „vymeniť" svoje súkromie za určité benefity, ktoré môže získať. 25 % používateľov predstavujú *fundamentalisti*, ktorí nikdy a za žiadnych podmienok prístup k svojim dátam neposkytnú. Posledná štvrtina používateľov sa zaraďuje do skupiny *indiferentných*, teda takých, ktorí nemajú na túto vec vyhranený názor.

K trojstupňovej typológii používateľov internetu s ohľadom na vzťah k súkromiu dospel vo svojom výskume aj Oliver Murphy, ktorý sa v roku 2007 zaoberal konceptom tzv. *monitorovanej spoločnosti / spoločnosti dozoru* (surveillance society). Ide o takú spoločnosť, ktorá do určitej miery funguje na základe rozsiahleho zberu, zaznamenávania, ukladania, analýzy a využívania informácií o jednotlivcoch a skupinách v tejto spoločnosti. Jedným zo základných argumentov, ktoré sa používajú v prospech rozsiahleho monitorovania aktivít v spoločnosti, je faktor bezpečnosti. Z uvedenej definície je jasné, že za monitorovanú spoločnosť môžeme v súčasnosti označiť takmer každú krajinu na svete. Na základe kvalitatívneho výskumu vzťahu k využívaniu monitorovania v spoločnosti Murphy identifikoval tri typy respondentov (podľa Hallinan et al., 2012):

- libertariáni – predstavujú menšinu, sú rozhľadenejší vo svojich obavách, premýšľajú o spoločnosti a svojom mieste v nej, viac si uvedomujú potrebu rovnováhy medzi bezpečnosťou a súkromím, zdôvodňujú ju princípmi založenými na demokratických a sociálnych argumentoch;
- autoritariáni – súkromie je pre nich striktne individuálnym právom, nie sociálnym dobrom, takže všetko spoločenské/kolektívne má prednosť. Ich mottom je „Nevinným nikto neuškodí ani ich neznevýhodní";
- akceptátori – právo na súkromie vidia z užšej, individuálnej perspektívy, typické je pre nich paternalistické vnímanie štátu ako nástroja na boj proti zlu, nástroja, ktorý sa postará o najlepšie záujmy občanov.

Iné výskumy zasa vo svojich záveroch dospeli k poznaniu, že kategórie používateľov na základe ich vzťahu k ochrane vlastných dát a súkromia nemožno definovať na základe úrovne ich ochoty zdieľať informácie všeobecne, ale vždy túto otázku treba posudzovať s ohľadom na rôzne konkrétne druhy osobných informácií – podľa toho možno hovoriť o rozličných *profiloch poskytnutia prístupu k informáciám* (disclosure profiles) u používateľov.

Záver

Výskumy zamerané na používateľov informácií sú dôležitou oblasťou rozvíjania poznania vo sfére knižničnej a informačnej teórie i praxe. Na jednej strane umožňujú priblížiť sa k pochopeniu správania používateľov informácií a vytváraniu relevantných modelov, ktoré na druhej strane majú potenciál prispieť k úspešným predikciám požiadaviek a očakávaní používateľov v budúcnosti. V oboch prípadoch takýto výskum napomáha zlepšovať

prácu knižníc a informačných systémov v ich primárnom poslaní, ktorým je uspokojovanie potrieb používateľov v podobe poskytovania kvalitných a relevantných služieb.

Presunom stále výraznejšej časti organizačnej komunikácie i samotných služieb do digitálneho prostredia sa knižnično-informačné systémy musia prispôsobovať štandardom a požiadavkám, ktoré sa vyžadujú vo vzťahu k súkromiu jednotlivca/používateľa. Je dôležité pochopiť podstatu problematiky ochrany súkromia a s ním súvisiacich osobných údajov, riziká, s ktorými sa používateľ i knižnično-informačná inštitúcia v tejto oblasti môže stretnúť, vedieť tieto riziká klasifikovať a vyhodnotiť. Fenomén paradoxu súkromia na internete napovedá, že napriek deklaráciám o dôležitosti súkromia sú používatelia v digitálnom prostredí náchylní zdieľať viac a dôvernejších informácií o sebe, ako je to v podobnej situácii v reálnom svete. Často je dôvodom najmä pragmatická kalkulácia spočívajúca vo výmene osobných dát za služby, ktoré pre používateľov majú význam.

Literatúra

ALTMAN, M., WOOD, A., O'BRIEN, D. R. a U. GASSER. Practical approaches to big data privacy over time. *International Data Privacy Law*, 2018, Vol. 8, No. 1.

ALTMAN, M., WOOD, A., O'BRIEN, D. R., VADHAN, S. a U. GASSER. 2016. Towards a Modern Approach to Privacy-Aware Government Data Releases, 30 *Berkeley Tech. L.J.* 1967 (2016).

ANDREJČÍKOVÁ, N., PIŠKULA, L. a H. GÁBRIŠOVÁ. 2019. Informačná bezpečnosť a GDPR z pohľadu tvorcu knižnično-informačného systému. *IT Lib*, 2019, 2, 24-29.

BAEK, Y. M. 2014. Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behaviour*, 38, 2014, 33-42.

BAUMANN, M.O. a W.J. SCHÜNEMANN. 2017. Introduction: Privacy, Data Protection and Cybersecurity in Europe. In Schünemann W., Baumann M.O. *Privacy, Data Protection and Cybersecurity in Europe.* Springer, Cham 2017, ISBN 978-3-319-53633-0. https://doi.org/10.1007/978-3-319-53634-7_1

FEARON, J. D. 1999. *What Is Identity (As We Now Use the Word)?* [online]. California: Stanford University. [cit. 2019-11-10]. Dostupné na: http://www.stanford.edu/~jfearon/papers/iden1v2.pdf

FUSTER, G. G. 2014. *The emergence of personal data protection as a fundamental right of the EU.* Springer Cham 2014. ISBN 2352-1902.

FUSTER, G. G. a S. GUTWIRTH. 2013. Opening up personal data protection: a conceptual controversy. *Computer Law and Security Review*, 29, 531-539.

GELLERT, R. a S. GUTWIRTH. 2013. The legal construction of privacy and data protection. *Computer Law and Security Review*, 29, 522-530.

GINOSAR, A a Y. ARIEL. 2017. An analytical framework for online privacy reserach: What is missing? *Information and management*, 54, 948-957.

HALLINAN, D., FRIEDEWALD, M. a P. MCCARTHY. 2012. Citizens' perceptions of data protection and privacy in Europe. *Computer Law and Security Review*, 28, 263-272.

LI, H., LUO, X., ZHANG, J. a H. XU. 2017. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information and Management*, 54, 2017, 1012-1022.

LUKÁCS, A. 2016. What is privacy: The history and definition of privacy. In: Keresztes, Gábor (ed.): *Tavaszi Szél 2016 Tanulmánykötet I.*, [online]. Budapest, Doktoranduszok Országos Szövetsége, 2016. [cit. 2019-11-10]. Dostupné na: https://www.academia.edu/31980162/What_is_Privacy_The_History_and_Definition_of_Privacy

ONDRIŠOVÁ, M. 2014. Vedecká komunikácia v prostredí tradičných a nových médií. *Žurnalistika, médiá, spoločnosť* 3-4 [online]. - Bratislava: STIMUL, 2014. - ISBN 978-80-8127-116-8. - S. 50-68.

PARKER, R. B. 1974. A Definition of Privacy, *Rutgers Law Review* 27, 1974, 281.

PEACE, M. 1999. *A Chatroom Ethnography.* Dissertation. [online]. [cit. 2019-11-10]. Dostupné na: http://www.aber.ac.uk/media/Students/mbp9702.doc.

POULSEN, F.E. 2019. *Towards a history of privacy: conceptual and methodological considerations* [online]. Centre for Privacy Studies, A Centre of Excellence Funded by the Danish National Research Foundation. [cit. 2019-11-10]. Dostupné na: https://privacy.hypotheses.org/189

REYMERS, K. 1998. *Identity and the Internet. A symbolic interactionist perspective on computer-mediated social networks*. [online] [cit. 2009-10-18]. Dostupné na: http://www.acsu.buffalo.edu/~reymers/identity.html.

SOLOVE, D. J. 2002. Conceptualizing Privacy. *California Law Review*, [online]. 90, 4, July 2002; 1087-1155. [cit. 2019-11-10]. Dostupné na: https://doi.org/10.15779/Z382H8Q

SOLOVE, D. J. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, [online]. 154, 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129. [cit. 2019-11-10]. Dostupné na SSRN: https://ssrn.com/abstract=667622

STEINEROVÁ, J. 2016. Information behaviour of researchers: contexts of digital scholarship. In: *WiKT/DaZn. 11th Workshop on Intelligent and Knowledge Oriented Technologies*. [online]. 35th Conference on Data and Knowledge. Eds. M. Bieliková, I. Srba. Bratislava: Nakl. STU 2016, 159-165. ISBN 978-80-227-4619-9. [cit. 2019-11-10]. Dostupné na https://wikt-daz2016.fiit.stuba.sk

STEINEROVÁ, J. a J. ŠUŠOL. 2004. Human information behaviour: electronic resources, digital library use and evaluation. *Human information behaviour & competences for digital libraries*. - Osijek: University J.J. Strossmayer, 2004. - S. 39-49.

STETS, J. E., a P.J. BURKE. 2000. Identity Theory and Social Identity Theory. *Social Psychology Quarterly* [online]. 63, 3, 2000, 224-237. *JSTOR*, [cit. 2019-11-10]. Dostupné na: www.jstor.org/stable/2695870.

SZABÓ M. D. 2005. *Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival.* Információs Társadalom 2, 2005. p. 45. cit. podľa Lukács, A. 2016.

ŠUŠOL, J. 2005. Elektronické informačné zdroje - vzťah používateľských a autorských preferencií. *Ikaros* [online]. - Roč. 9, září (2005), s. 1-9 ISSN 1212-5075

ŠUŠOL, J. 2011. Library data in higher education institution management publishing behaviour research as a factor of academic assessment. In: *Bezpieczna, innowacyjna i dostępna informacja, perspektywy dla sektora usług informacyjnych w społeczeństwie wiedzy Katowice*: PTIN, 2011. ISBN 978-83-904561-9-5 S. 77-91.

TENE, O. a J. POLONETSKY. 2012. Privacy in the age of big data. A time for big decisions. *Stanford Law Review*, February 2012.

WARSO, Z. 2013. There's more to it than data protection – fundamental rights, privacy and the personal/household exemption in the digital age. *Computer Law and Security Review*, 29, 491-500.

WEBER, R. H. 2015. The digital future – a challenge for privacy? *Computer Law and Security Review*, 31, 234-242.

WESTIN, A. 1967. *Privacy and Freedom*. New York: Atheneum. p. 7.

WOOD, A., ALTMAN, M., BEMBENEK, A., BUN, M., GABOARDI, M., HONAKER, J., NISSIM, K., O'BRIEN,D. R., STEINKE, T. a S. VADHAN. 2018. Differential Privacy: A Primer for a Non-Technical Audience. *The Vanderbilt Journal of Entertainment & Technology Law (JETLaw)* [online]. 21, 1, 209-276. [cit. 2019-11-10]. Dostupné na http://www.jetlaw.org/journal-archives/volume-21/volume-21-issue-1/differential-privacy-a-primer-for-a-non-technical-audience/

Príspevok bol spracovaný v rámci riešenia výskumnej úlohy APVV 0508-15 HIBER, Human Information Behavior in the Electronic Environment – Informačné správanie človeka v informačnom prostredí.

prof. PhDr. Jaroslav Šušol PhD.

jaroslav.susol@uniba.sk ■

(Katedra knižničnej a informačnej vedy, Filozofická fakulta, Univerzita Komenského v Bratislave)