Efekt filtračných bublín: Defenzívne stratégie a taktiky

Problematika filtračných bublín označuje efekt uzatvárania sa používateľov do vlastných intelektuálnych bublín v internetovom prostredí. Informačné filtračné bubliny sa v tomto prostredí vytvárajú jednak vďaka automatickej filtrácii obsahu v personalizovaných vyhľadávacích nástrojoch a na sociálnych sieťach, ale aj vplyvom kognitívnych skreslení samotných používateľov. V príspevku sa zameriavame najmä na intelektuálne, ale aj technologické možnosti riešenia problematiky. Pre úspešný boj proti tomuto fenoménu je na základe našich zistení potrebná kombinácia viacerých riešení tak na individuálnej, ako aj na celospoločenskej úrovni.

Informačné filtračné bubliny sa v súčasnosti považujú za negatívny dôsledok personalizácie obsahu na sociálnych sieťach a vo vyhľadávacích nástrojoch (Parizer, 2011). Personalizácia je súbor funkcií informačného systému, ktoré ho umožňujú prispôsobiť používateľovi a jeho preferenciám, jeho informačnému a kognitívnemu štýlu, či povahe riešeného problému. Silnou stránkou personalizácie je zníženie informačného preťaženia používateľa a zvýšenie efektivity interakcie v zmysle vyššej relevancie a šetrenia času (Steinerová, 2017). Problémom je, že adaptívne personalizačné systémy týmto spôsobom uzatvárajú používateľa do jeho vlastnej informačnej bubliny, vo vnútri ktorej dochádza k oslabeniu kontaktu s rôznorodými postojmi, prístupmi, myšlienkami či názormi. Informačné správanie používateľa tak v konečnom dôsledku definuje jeho informačný horizont v rámci určitej personalizovanej služby. Existuje viacero spôsobov, ako sa čiastočne vyhnúť tomuto negatívnemu javu, preto sa ich pokúsime zhrnúť v tomto príspevku.

Rozširovanie informačného horizontu a obzoru

Jednou z najúčinnejších metód prevencie intelektuálnej izolácie je snaha o aktívne rozširovanie vlastného obzoru. Dôležité je budovanie kritického myslenia, snaha vykročiť zo svojej zóny komfortu a „otváranie si mysle" aj iným uhlom pohľadu na rozličné témy (Pariser, 2011). To je možné zabezpečiť samostatným aktívnym informačným správaním, najmä komunikáciou s ľuďmi s odlišnými názormi a pohľadmi na svet, ale vplyv na postoj voči prijímaným informáciám má aj zázemie používateľa v oblasti informačnej gramotnosti.

V tomto zmysle je pre dosiahnutie čo najobjektívnejšieho obrazu o dostupných zdrojoch a informáciách dôležité neupínať sa len na jednu oblasť prístupu k informáciám, ale kombinovať viaceré vyhľadávacie nástroje a informačné kanály a získané informácie vzájomne porovnávať a hodnotiť (Winter, 2015). Vyhľadávacími nástrojmi, ktoré spracovávajú výsledky vyhľadávania bez využitia personalizácie, sú napríklad *DuckDuckGo* alebo *Ixquick*. Nápomocné môžu byť aj nástroje na syndikáciu a agregáciu obsahov z rôznych webových zdrojov, ako napríklad RSS kanály a ich čítačky *(Rich Site Summary* alebo aj *Really Simple Syndication)*. Používatelia s aktívnym informačným správaním majú tiež možnosť manuálne nastaviť obsahové preferencie na Facebooku v jeho nastaveniach. Ani RSS kanály či nastavenie prijímaných informácií však používateľa z jeho intelektuálnej bubliny dokonale nevytiahnu. Automatickú filtráciu obsahov totiž zastúpia vlastné intelektuálne obmedzenia používateľa s cieľom predísť informačnému preťaženiu. Dochádza tak k takzvanej selektívnej expozícii, pri ktorej sa používatelia nevedome vystavujú a vyberajú si iba také informačné zdroje, ktoré korešpondujú s ich doterajšími znalosťami, názormi či postojmi (Mutz, Young, 2011).

Opatrnosť pri zabezpečovaní súkromia používateľských údajov na internete

Verejné údaje zo sociálnych sietí hrajú pri personalizácii dôležitú rolu. Je preto na zvážení každého jednotlivca, či prípadné použitie zverejnených informácii pre neho nebude potenciálne škodlivé. Najmä v prostredí sociálnych sietí možno zdieľané údaje nastaviť ako súkromné, a tak zabrániť ostatným službám čerpať informácie, ako napríklad záujmy a kontakty. Navyše, k údajom, označeným ako verejné, má prístup ktokoľvek (Prakash, 2016).

Súčasťou aktívneho zabezpečovania vlastných údajov je oboznamovanie sa s politikami a podmienkami používania webových aplikácií a služieb. Je síce veľmi ťažké odhaliť, akým spôsobom sú používateľské údaje v skutočnosti využívané, no zvyšovanie informovanosti a záujmu o problematiku môže pomôcť zvýšiť aj vlastnú ochranu (Cardona et al., 2016; Well a Royakkers, 2004).

Riešenia na celospoločenskej úrovni

Zvýšeniu informačnej gramotnosti používateľov ohľadom súkromia a filtračných bublín na internete pomôže najmä celospoločenská debata a zvyšovanie povedomia o problematike (Well a Royakkers, 2004). Používatelia by mali byť dôsledne varovaní o možných rizikách automatického filtrovania informácií a o spôsoboch zmien obsahových preferencií v najrozšírenejších internetových službách. Používatelia sami by však mali klásť otázky, kritizovať nedostatky a celkovo sa viac zaujímať o problematiku.

Personalizačné algoritmy nie sú transparentné, a preto dohľad nad personalizáciou a web-data miningom[1] by mali realizovať nestranné subjekty. Na získanie prístupu k jednotlivým systémom je tiež potrebná legislatívna opora a názorová jednota spoločností vykonávajúcich zber dát.

[1] *Web-data mining* je zbieranie informácií z dokumentov na webe a z webových služieb za pomoci automaticky pracujúcich algoritmov a nástrojov, formulujúcich hypotézy a hľadajúcich relevantné stopy. V kontextoch môžu tieto procesy viesť k vytváraniu nového poznania (Well a Royakkers, 2004).

Používanie nástrojov na ochranu súkromia

Súkromie používateľa na internete úzko súvisí s personalizáciou aj s informačnými filtračnými bublinami, pretože v prípade absencie údajov od používateľov nie je možné informácie v informačnom systéme prispôsobovať. V súčasnosti existuje množstvo nástrojov na ochranu súkromia, pričom najpoužívanejšími sú doplnky webových prehliadačov ako *Privacy Badger či Disconnect.* (Cardona et al., 2016).

Používatelia môžu pri ochrane svojho súkromia využiť aj takzvané PETs technológie (Privacy-Enhancing Technologies). Môže ísť o zabezpečené prehliadače (*Tor Browser*) a ich doplnky (*Beef Taco, Blur*...), špeciálne operačné systémy a „anonymizéry" (*Tails, Orbot, Anonymizer, CyberGhost VPN*...), či sieťové decentralizátory (*Hyperboria, GNUnet*...) a ďalšie typy nástrojov (Epic, 2018; Well a Royakkers, 2004).

Lepšie zabezpečenie súkromia používateľov možno na internete dosiahnuť aj deaktivovaním JavaScriptu a Flashu. Práve vďaka JavaScriptu možno zbierať veľkú časť informácií o používateľovi („browser fingerprint", cookies a iné). Jeho zakázaním sa dá zberu a používaniu týchto údajov jednoducho a účinne zabrániť, daňou je však zhoršený používateľský zážitok. Hoci vypnutie Flashu nemusí spôsobiť problémy, zakázanie JavaScriptu môže, pretože ten tvorí pevnú súčasť množstva webových stránok. Riešením je doplnok prehliadača, napríklad *NoScript.* Ten umožňuje manuálne nastaviť, na ktorej stránke sa JavaScript spustiť môže a na ktorej nie (Browser, 2016).

Čiastočne možno zabrániť zbieraniu údajov aj používaním inkognito režimu. Pri prehliadaní tak nebude zaznamenávaná história ani cookies, teda záznamy používateľských interakcií počas prehliadania webu internetovým prehliadačom (Winter, 2015). Práve tieto záznamy bývajú najčastejšie používané na personalizáciu obsahu, napríklad vo vyhľadávači Google. Okrem vzniku filtračných bublín je ďalším úskalím to, že k týmto údajom majú okrem webového servera prístup aj tretie strany, ako napríklad reklamné alebo dcérske spoločnosti, čo je v súčasnosti po zavedení GDPR možné lepšie regulovať. Je žiaduce, aby online služby vo svojich podmienkach používania jasne vymedzili, koho považujú za tretiu stranu a koho nie (Winter, 2015), a tiež aby sa používatelia sami zamysleli, s akými podmienkami pri využívaní služieb súhlasia.

Cookies a históriu prehliadania je okrem využívania inkognito režimu možné aj priebežne odstraňovať a vo väčšine najpoužívanejších internetových prehliadačov (*Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Apple Safari*) možno zbieranie cookies manuálne zakázať v nastaveniach. Účinnosť blokovania možno overiť, napríklad prostredníctvom stránky *Cookie-Checker*. Tá dokáže odhaliť všetky použité cookies, aj tie tretích strán. Navyše používateľa informuje, na čo každé z cookies slúži a aký subjekt ho zbiera. Stránka tiež upozorní pri porušení európskeho práva[2] (Prakash, 2016).

K celospoločenským technologickým riešeniam možno zaradiť zjednotenie prístupu k používateľskému súkromiu. Ako jedno z riešení sa objavuje myšlienka vytvorenia nového webového štandardu „disallow mining", respektíve jeho začlenenia do HTML. Každá stránka by si tak sama mohla zadefinovať, či techniky web data miningu povolí alebo nie.

Špeciálne riešenia na zmiernenie efektu filtračných bublín

V poslednom období začali vznikať špeciálne pomôcky na zmiernenie efektu filtračných bublín. Napríklad mobilná aplikácia *Read Across the Aisle,* ktorá združuje množstvo obľúbených informačných zdrojov a upozorňuje používateľa v prípade, že čítal príliš veľa informácií z jednej strany politického spektra. Podobne funguje stránka *AllSides,* ktorá ku zdieľaným témam a aktualitám pripája tri rôzne prístupy prezentácie (pohľad zo strany ľavice, pravice a zo stredu, podľa zdroja, z ktorého články pochádzajú) (Lum, 2017).

Doplnok prehliadača *Escape Your Bubble* zas dokáže v prostredí Facebooku zviditeľniť pozitíva a úspechy časti politického spektra, ktorej si používateľ želá lepšie porozumieť (Lum 2017). Dôležité je poznamenať, že uvedené aplikácie fungujú najmä pre americké prostredie a v slovenskom prostredí je v tejto oblasti stále medzera na trhu.

Záver

Technologické riešenia, zabezpečujúce minimalizáciu zbieraných informácií s cieľom personalizácie, sú len čiastočnými riešeniami a problém v podstate obchádzajú. Za najdôležitejšie v boji proti intelektuálnej izolácii, nielen v internetovom prostredí, preto pokladáme snahu o aktívne rozširovanie vlastného obzoru, budovanie kritického myslenia a celkovo úsilie o zvyšovanie vlastnej informačnej gramotnosti. Keďže ani jedno z menovaných riešení nie je samo o sebe dostatočné, ako najúčinnejšia alternatíva sa javí kombinácia viacerých riešení – intelektuálnych aj technologických.

Poďakovanie: Tento príspevok bol pripravený v rámci projektu APVV-15-0508.

Použitá literatúra

Is your browser safe against tracking?, 2016. In: Panopticlick [online]. San Francisco: Electronic Frontier Foundation [cit. 2018-03-10]. Dostupné na: https://goo.gl/DgWVVR

CARDONA, Tatiana et al., 2016. *Ethical issues with customer data collection* [online]. Missouri: Missouri University of Science and Technology [cit. 2018-02-25]. Dostupné na: https://goo.gl/vFUCiD

[2] Európske zákony hovoria, že informácie nesmú byť použité na iné účely, než na aké boli získané. Uvádzajú tiež, že používateľ musí byť dopredu informovaný o účele zberu údajov. V praxi však zákon používateľa nedokáže ochrániť. Pri web-data miningu nie je vždy dopredu jasné, aké informácie systém nájde, aké vzťahy medzi blokmi dát odhalí, a teda na aký účel budú nájdené informácie neskôr slúžiť. V takom prípade je takmer nemožné používateľa dopredu informovať o účele zberu údajov. Rovnaký problém sa týka prehľadávania starších báz dát, ktoré boli zaznamenané v minulosti (Rubinstein, Lee a Schwartz, 2008; Well a Royakkers, 2004).

EPIC online guide to practical privacy tools, 2018. In: *epic.org* [online]. Washington: Electronic Privacy Information Center [cit. 2018-03-06]. Dostupné na: https://goo.gl/LPf2nM

LUM, Nick, 2017. Tools for bursting your filter bubble. In: *Medium* [online]. *Medium [cit. 2018-03-12].* Dostupné na: https://goo.gl/WByPv3

MUTZ, Diana a Lori YOUNG, 2011. Communication and public opinion: plus ca change? In: *Public opinion Quarterly* [online]. *Oxford: Oxford University Press,* **75**(5), s. 1018–1044 [cit. 2018-01-30]. ISSN 1537-5331. Dostupné na: https://goo.gl/m4VnoF

PARISER, Eli, 2011. *The filter bubble: what the internet is hiding from you.* London: Penguin Books [cit. 2017-12-15]. ISBN 978-0-670-92038-9.

PRAKASH, Sneha, 2016. Filter bubble: how to burst your filter bubble. In: *International Journal Of Engineering And Computer Science* [online]. Mandsaur: Valley International, **5**(10), s. 18321-18325 [cit. 2018-02-27]. ISSN 2319-7242. Dostupné na: https://goo.gl/6PcFGr

RUBINSTEIN, Ira, Ronald LEE a Paul SCHWARTZ, 2008. Data mining and internet profiling: emerging regulatory and technological approaches. In: *University of Chicago Law Review* [online]. Chicago: University of Chicago Law School, s. 261-285 [cit. 2018-03-02]. ISSN 1939-859X. Dostupné na: https://goo.gl/ZMNnn2

STEINEROVÁ, Jela. Personalizácia. In: *Informačná veda. Terminologický slovník* [CD-ROM]. Verzia 1.0. Bratislava: Katedra knižničnej a informačnej vedy FiF UK, 2017, heslo 223.

WELL, Lita van a Lambèr ROYAKKERS, 2004. Ethical issues in web data mining. In: *Ethics and Information Technology* [online]. Dordrecht: Kluwer Academic Publishers, **6**(2), s. 129-140 [cit. 2017-12-20]. ISSN 1572-8439. Dostupné na: https://goo.gl/ja2bxs

WINTER, Annet, 2015. *How to escape the Filter bubble: are you at the helm?* [online]. [cit. 2018-03-04]. Dostupné na: https://goo.gl/eQk3dD

Mgr. Andrea Hrčková, PhD. **Bc. Tomáš Mirga**

(Katedra knižničnej a informačnej vedy FiF UK v Bratislave) ■