Veľké údaje v osídlach Veľkého brata

S v á k, J., S a k o l c i o v á, S.*

SVÁK, J., SAKOLCIOVÁ, S.: Veľké údaje v osídlach Veľkého brata. Právny obzor, *103,* 2020, č. 2, s. 119 – 131.

Big data in the trap of the Big Brother. In the past, the existing technology did not make it possible to store and process such vast amounts of data as the technology today. Data had to be selected according to their necessity and were collected only about specific persons or small groups of people. Nowadays, the technologies manage to predict "patterns" of people's behaviour and significantly improve the effectiveness of decision-making. The question we are dealing with in the article is whether the "traditional" individual right to privacy is still fit in the era of Big Data where the individuality ceases to be of importance or whether other solutions need to be sought.

Key words*: Right to privacy, Big Data, European Court of Human Rights, group rights*

Edward Snowden s veľkou pravdepodobnosťou čítal a pochopil odkaz antiutopického románu Georgea Orwella s názvom 1984 (Nineteen Eighty – Four) z roku 1984 a ocitol sa zrejme „v koži" úradníka Ministerstva pravdy Oceánie Winstona Smitha v štáte, kde samotná ľudská individualita je trestaná ako myšlienkový zločin. Keď tento bývalý zamestnanec CIA zverejnil informácie o hromadnom sledovaní elektronickej komunikácie tajnými službami v Spojenom kráľovstve a Spojených štátoch amerických, tak nielenže odkryl z tváre masku Veľkého brata, ale zároveň odhalil bezvýznamnosť nášho súkromia ako ľudskej entity. S hrôzou sme zistili, že človek ako jedinečná ľudská bytosť prestáva mať súkromie pred štátom reprezentovaným Veľkým bratom. Ale čo keď sa za maskou Veľkého brata neskrýva štát? Pre súkromných zberateľov našich údajov na rozdiel od štátu totiž prestáva mať hodnotu naše súkromie ako také. Jednotlivec vo svete veľkých údajov (Big Data) nemá už hodnotu subjektu, ale objektu. Predmetom ich záujmu nie je jednotlivec ako taký (jeho súkromie), ale jeho záujmy a správanie. Nešpehuje nás preto, aby mohol zneužiť informácie z nášho súkromia, ale preto, aby ich využil s cieľom ovplyvniť naše správanie ako spotrebiteľov, aj ako voličov. Samotný zber, zhromažďovanie a triedenie našich osobných údajov sa stáva samostatným obchodným modelom v digitálnom hospodárstve. Otázka je, či sa tým vytvára aj nové kolektívne súkromie ľudí, ktorých súčasné dátové analytické technológie zatrieďujú do určitých skupín, ktoré sú však svojou podstatou tekuté, a teda ťažko fixovateľné a definovateľné. Navyše voľne sa prelievajúce z jednej skupiny do druhej bez toho, aby sme to mohli ovplyvniť, a spravidla aj bez toho, aby sme sa o tom vôbec dozvedeli.

Doteraz sme naše skupinové (kolektívne) zatriedenie poznali a niekedy sme ho mohli aj ovplyvniť. Ťažko sa nám mohlo dať ovplyvniť našu rasu, ľahšie národnosť či štátnu identitu, a niekedy zaradenie do určitej skupiny (napríklad právnikov) záležalo výlučne

* Prof. JUDr. Ján S v **á** k, CSc., Katedra medzinárodného práva a medzinárodných vzťahov, Právnická fakulta UK, Bratislava; Mgr. Sandra S a k o l c i o v á, Katedra medzinárodného práva a medzinárodných vzťahov, Právnická fakulta UK, Bratislava

na našom rozhodnutí. V takto definovanej skupine sme pomerne ľahko dešifrovali naše práva a s určitými obmedzeniami sme si ich mohli uplatňovať či ochraňovať. Vo svete internetu a veľkých dát to však prestáva platiť.

V oblasti ľudských práv bola kolektívna ochrana zásadným spôsobom obmedzená tým, že ľudské práva v západnej filozofii sa stali individuálnymi subjektívnymi právami prirodzenoprávneho pôvodu.[1] Tento výdobytok liberálnej filozofie moderných európskych dejín sa po 2. svetovej vojne začal presadzovať aj na nadštátnej úrovni, ktorej vlajkovou loďou sa stali Rada Európy a Európsky súd pre ľudské práva (ďalej ESĽP) pri aplikácii Dohovoru o ochrane ľudských práv a základných slobôd (ďalej Dohovor). Ľudské práva v ňom obsiahnuté boli založené v duchu tejto filozofie na princípe individuálnej ochrany a ESĽP permanentne deklaroval, že poskytuje ochranu len individuálnym ľudským právam na základe individuálnej sťažnosti. Vylučoval *actio popularis*, kde by mohlo dôjsť len potenciálne k porušeniu ľudských práv neurčitej skupiny, ktorá mohla byť ohrozená zásahom štátu.[2] Toto sa však tiež malo zmeniť nástupom internetu a veľkých údajov.

Big Brother nastupuje

Všeobecné pravidlo, či dokonca princíp je, že Dohovor nepripúšťa abstraktný prieskum určitého rozhodnutia alebo opatrenia štátu bez toho, aby bolo predmetné opatrenie aj konkrétne a dokázateľne použité proti individuálne poškodenej osobe.[3] Určitým prielomom do zásady individuálnosti a možnosti podať sťažnosť aj osobou, ktorá nebola konkrétnym opatrením štátu priamo zasiahnutá (a to ani ako nepriama obeť v prípade, keď by napríklad sťažovateľ umrel a mal by právneho nástupcu), bolo rozhodnutie vo veci *Centre Legel Resources* v zastúpení *Valentina Câmpeana proti Rumunsku (zo 17. júla 2014, č. 47848/08),* kde išlo o porušenie práva na život. Pán Câmpeanu bol mladý Róm, ktorý nepoznal svojich príbuzných a od narodenia trpel viacerými telesnými aj duševnými chorobami. Jeho smrť bola dôsledkom zanedbania pozitívnych povinností štátu v oblasti práva na život chráneného článkom 2 Dohovoru. Jeho prípadu sa ujala nezisková organizácia, ktorá napokon úspešne obhájila svoj štatút „obete" v zmysle článku 34 Dohovoru bez toho, aby musela preukázať, že bola predmetným opatrením priamo dotknutá na svojich právach. Stále však išlo o porušenie individuálneho, a nie kolektívneho ľudského práva.

[1] Súčasný veľký kritik doktríny ľudských práv Alain de Benoist k tomu píše *„...túžba a vôľa každého jednotlivca určuje mieru toho, čo je dobré, a každý jednotlivec je zvrchovaným posudzovateľom svojho vlastného šťastia. Prirodzené moderné práva sa už nezaoberajú spoločenskými bytosťami, ale jednotlivcami, t. j. ľuďmi považovanými za sebestačných. Právo v súvislosti s prirodzeným moderným právom už nie je výsledkom právnych vzťahov, ale sa stáva vlastníctvom každého človeka - každý môže, „ak sám chce, uplatniť svoju právomoc, aby si tým zachoval svoju prirodzenosť." Toto vlastníctvo bolo nastolené ako sloboda, čo následne umožnilo, aby sloboda splynula so slobodou vlastniť. Prirodzené práva sú teda súčasne vlastníctvo aj právomocou: sú vlastné každému človeku, ktorý je schopný ich uplatňovať tým, že ich vlastní."* BENOIST, A. de: Za horizontem lidských práv. Sol Noctis. Zvolen, 2019, s. 36.

[2] Pozri napríklad rozhodnutie vo veci *Athanassoglou a ostatní proti Švajčiarsku (zo 6. apríla 2000, č. 27644/95),* kde mohlo dôjsť k porušeniu ľudských práv rozhodnutím o výstavbe jadrovej elektrárne.

[3] Pozri napríklad rozhodnutie vo veci *N. C. proti Taliansku (z 18. decembra 2002, č. 24952/94*).

Vráťme sa však k tajnému sledovaniu, resp. zberu, zhromažďovaniu a triedeniu osobných údajov. Práve táto oblasť bola akoby predurčená na to, aby sa pripustila aj, povedzme ústavnoprávnou terminológiou, abstraktná kontrola ústavnosti.

Dlhodobo precedentným bolo rozhodnutie vo veci *Klass a ostatní proti Nemecku (zo 6. septembra 1978, č. 5029/71)*, kde plénum ESĽP naznačilo, že za určitých okolností prípadu by si vedelo predstaviť, že „obeťou" môže byť osoba len z dôvodu samotnej existencie tajných opatrení, resp. zákonnej úpravy, ktorá takéto opatrenia umožňuje vykonávať bez toho, aby musela preukazovať aj to, že boli proti nemu použité. Práve tajné zbieranie a zhromažďovanie údajov je tým prípadom, keď by abstraktná kontrola mala racionálne jadro z dôvodu, že v opačnom prípade by bola vlastne ochrana práva na súkromie iluzórna. Takéto *de facto* zbavenie ochrany práva na súkromie by bolo možné len vďaka tomu, že právo na súkromie je porušované prostredníctvom utajených metód zberu, zhromažďovania a triedenia osobných údajov, o ktorých existencii sa nemajú dotknuté osoby ako dozvedieť.[4]

Po prijatí rozhodnutia vo veci *Klass a ostatní* sa začala prax ESĽP zásadne rozchádzať do troch smerov.

Prvý smer viedol ESĽP k tomu, že postaveniu „obete" sa nemôže dovolávať každá osoba v príslušnom štáte, ktorá má neurčitú obavu, že o nej mohla tajná polícia zbierať a zhromažďovať osobné údaje. Od tejto osoby však nemožno spravodlivo požadovať, aby preukázala, že bola utajovanými prostriedkami skutočne aj sledovaná. Postačí, aby ESĽP získal presvedčenie o tom, že v danom štáte bola uplatňovaná prax tajného sledovania osôb spolu so zvýšenou mierou pravdepodobnosti, že týmito opatreniami mohol byť sťažovateľ dotknutý.[5]

V druhom smere, naopak, ESĽP konštatoval, že samotná existencia zákonnej úpravy, ktorá pripúšťa tajné sledovanie prakticky všetkých osôb na danom území, predstavuje zásah do ich práv, a to aj bez existencie konkrétnych opatrení, ktoré by mali byť voči nim namierené.[6]

V prípade *Kennedy* ESĽP upozornil na to, že pri skúmaní, či si sťažovateľ môže nárokovať postavenie obete, je potrebné prihliadať aj na dostupnosť prostriedkov nápravy na vnútroštátnej úrovni a na mieru rizika, že na neho bolo utajované opatrenie použité a došlo tak k zberu, zhromažďovaniu a triedeniu údajov.

Vzhľadom na neujasnenosť a rôznorodosť prístupov znižujúcich právnu istotu rozhodovania pre sťažovateľov sa ESĽP rozhodol pre stanovenie unifikovaných a jednoznačných podmienok na uplatňovanie postavenia „obete" porušenia práva na súkromie bez toho, aby sťažovatelia museli preukázať, že boli vystavení tajnému sledovaniu. Príhodným sa mu zdala byť právna situácia v Rusku a v zložení Veľkej komory ESĽP v rozhod-

[4] Pozri k tomu bod 124 rozhodnutia vo veci *Kennedy proti Spojenému kráľovstvu (z 18. mája 2010, č. 26839/05)*

[5] K tomu pozri najmä rozhodnutia vo veciach *Esbester proti Spojenému kráľovstvu (z 2. apríla 1993, č. 18601/91, Iliya Stefanov proti Bulharsku (z 22. mája 2008, č. 65755/01).*

[6] Pozri rozhodnutia vo veciach *Malone proti Spojenému kráľovstvu (z 2. augusta 1984, č. 8691/79), Weber a Saravia proti Nemecku (z 29. júna 2006, č. 54934/00), Iordachi proti Rumunsku (z 10. februára 2009, č. 25198/02).*

nutí vo veci *Roman Zakharov proti Rusku (zo 4. decembra 2015, č. 47143/06)*[7] určil podmienky uplatnenia *actio popularis* v súvislosti s tajným zberom, zhromažďovaním a triedením osobných údajov štátnou mocou.

Prvou skutočnosťou, ktorú je pri takejto sťažnosti potrebné zohľadniť, je rozsah zákonnej úpravy umožňujúcej tajné sledovanie a posúdiť, či ňou mohol byť sťažovateľ dotknutý, a to z dôvodu, že

- patrí ku skupine osôb, voči ktorej je právna úprava namierená alebo
- posudzovaná úprava dopadá na všetkých užívateľov komunikačných služieb, pretože vytvára možnosť zachytiť akúkoľvek korešpondenciu.

Druhou dôležitou skutočnosťou sú prostriedky nápravy dostupné na vnútroštátnej úrovni. Ak také prostriedky nápravy pre osoby, ktoré majú podozrenie zo sledovania, nie sú k dispozícii, tak je opodstatnená obava a znepokojenie širokej verejnosti, že predmetné nástroje môžu byť zneužívané. Potom sa všetci užívatelia telekomunikačných sietí môžu považovať za potenciálne priamo dotknutých na svojich právach a môžu potom namietať zásah do svojho práva na rešpektovanie súkromného života a korešpondencie. V prípade, že sú dostupné účinné prostriedky nápravy na vnútroštátnej úrovni, tak bude obava z tajného sledovania menej odôvodnená. Vtedy si môžu sťažovatelia nárokovať na postavenie „obete", len ak preukážu, že vzhľadom na svoju osobnú situáciu sú potenciálne v ohrození, že mohli byť ich osobné údaje zbierané a zhromažďované.

Pri aplikovaní predmetných kritérií na prípad *Zakharov* došiel ESĽP k záveru, že ruská právna úprava zakladá systém, v ktorom môže byť fakticky každý užívateľ mobilu sledovaný bez toho, aby sa o tejto skutočnosti vôbec dozvedel. Neobsahuje ani žiadne prostriedky nápravy, ktorých prostredníctvom by sa dotknuté osoby mohli domáhať prieskumu, či boli ich osobné údaje aj naozaj zbierané a zhromažďované. Preto podľa ESĽP sa mohol sťažovateľ domáhať postavenia „obete", aj keď nebol schopný preukázať, že bol vystavený odpočúvaniu. Právna úprava sama osebe tak predstavovala zásah do výkonu sťažovateľových práv chránených článkom 8 Dohovoru.

Potom už prišiel na rad sám Veľký brat v rozhodnutí *Big Brother Watch a ostatní proti Spojenému kráľovstvu (z 13. septembra 2018, č. 58170/13, 62322/14 a 24960/15)*. V tomto prípade už sťažovateľom nebola individuálna osoba, ale neziskové, charitatívne a iné organizácie, jednotlivci a novinári. Boli presvedčení o tom, že vzhľadom na povahu ich aktivít bolo vysoko pravdepodobné, že ich komunikáciu monitorovali buď britské

[7] Sťažovateľom bol riaditeľ vydavateľstva a šéfredaktor novín, ktorý využíval služby niekoľkých mobilných operátorov. Proti trom z nich podal žaloby z dôvodu, že boli nútení nainštalovať zariadenia, ktoré spravodajským službám a policajným orgánom umožňujú sledovať celú telefónnu komunikáciu bez povolenia súdu. Sťažovateľ v žalobách žiadal odstránenie týchto zariadení, avšak vnútroštátne súdy tieto žaloby zamietli z dôvodu, že sťažovateľ nepreukázal, že by mobilní operátori aj reálne tieto informácie poskytli tajnej službe, či polícii. Samotná inštalácia takých zariadení podľa ich názoru nepredstavuje porušenie dovolávaných práv, pretože slúži len na to, aby príslušné orgány mohli využívať zákonným spôsobom operatívno-pátracie spôsoby práce.

tajné služby samotné, alebo tajné služby cudzích štátov, ktoré ich odovzdávali Spojenému kráľovstvu. Dôvodom týchto obáv boli informácie zverejnené Edwardom Snowdenom o hromadnom sledovaní elektronickej komunikácie tajnými službami v Spojenom kráľovstve a USA. Na základe kritérií stanovených v kauze *Zakharov* ESĽP priznal sťažovateľom status „obete" a potom posudzoval to, či predmetný hromadný proces zberu, zhromažďovania a triedenia osobných údajov porušil právo na súkromie chránené článkom 8 Dohovoru.

Po vzore prípadu *Zakharov* aplikoval šesť základných zákonných záruk brániacich zneužitiu moci tajným sledovaním v kontexte trestného konania[8] aj na prípady, keď tajné sledovanie je vykonávané s cieľom ochrany národnej bezpečnosti. Týmito zárukami sú:

- upresnenie povahy trestných činov vedúcich k vydaniu príkazu na tajné odpočúvanie,
- vymedzenie okruhu osôb, ktorých komunikácia sa sleduje,
- časové obmedzenie trvania odpočúvania,
- dodržanie určitého postupu pri zaobchádzaní so získanými údajmi,
- zakotvenie záruk pre odovzdávanie údajov ďalším stranám,
- vymedzenie podmienok na zmazanie alebo zničenie záznamov.

Prieskum a dozor sa uplatňuje v troch fázach sledovania, a to pri zadávaní, pri výkone a po jeho skončení. Prvé dve fázy sa celkom logicky nevykonávajú s vedomím sledovanej osoby, a preto musia obsahovať také záruky, ktoré chránia práva tejto osoby. Vzhľadom na nebezpečenstvo zneužitia je najvhodnejším orgánom dohľadu súd. V tretej fáze sú záruky proti zneužitiu a prostriedky nápravy úzko spojené s mechanizmami upozornenia jednotlivca, že bol objektom sledovania.

ESĽP pri aplikácii týchto pravidiel proti zneužitiu moci neakceptoval názor sťažovateľov, že každú žiadosť na sledovanie musí schváliť nezávislý súd. Nemožno totiž predpokladať, že hromadné sledovanie automaticky zakladá väčší zásah do súkromia ako cielené individuálne sledovanie osoby.

Samotný proces zachytávania a monitorovania komunikácie v prípade *Big Brother Watch* pozostával zo štyroch fáz, a to:

a) zachytávanie komunikácie z niektorých nosičov z infraštruktúry internetu,
b) filtráciu a vyradenie zachytenej komunikácie, ktorá nemala informačnú hodnotu pre spravodajské služby,
c) použitie vyhľadávačov na zostatok zachytenej komunikácie,
d) následná analýza tejto komunikácie analytikmi.

ESĽP v tomto procese našiel dva problematické body. Prvým bol nedostatočný nezávislý dohľad nad vyhľadávacími procesmi vrátane výberu komunikácie postúpenej analytikom. Druhým potom absentujúce záruky, ktoré by sa na výber komunikácie uplatnili. Z toho ESĽP vyplynul záver, že v týchto bodoch zákon nedosahuje dostatočnú kvalitu

[8] ESĽP ich skompletizoval v rozhodnutí o neprijateľnosti sťažnosti v prípade *Weber a Saravia proti Nemecku (z 29. júna 2006, č. 54934/00)*

a nie je spôsobilý udržať zásahy do súkromia v medziach, ktoré sú „nevyhnutné v demokratickej spoločnosti“, a preto bolo porušené právo na súkromie chránené článkom 8 Dohovoru.

Keď je Big Brother kapitalista

Tajné sledovanie spočívajúce v zbere, zhromažďovaní a triedení údajov sa však v internetovej dobe nevyužíva len štátom a nie s cieľom ochrany národnej bezpečnosti. V ére veľkých údajov údaje zbiera, zhromažďuje a triedi nie štát, ale „kapitalista“. Hĺbka zásahov do súkromia je ešte oveľa širšia a využitie našich údajov je ešte variabilnejšie v celom spektre od podnikateľského biznisu až po ten politický. Má štát právo do toho zasiahnuť, alebo je to jeho povinnosť? Alebo máme túto sféru „tradične“ ponechať na samoreguláciu a etiku?

Hlavný problém je v tom, že kým štát zaujíma človek ako individualita a tak chápe aj jeho identitu, tak kapitalistu nezaujíma človek ako identifikovateľný jednotlivec, ale „len“ jeho identita algoritmicky odvodená z údajov (z týchto údajov je hádam najmenej podstatné meno a priezvisko) jednotlivca. Rôzne sú aj ciele, pre ktoré je človek zaujímavý pre štát a pre kapitalistu. Pre štát je to riadenie (ovládanie) človeka a pre kapitalistu je to obchod. Obchod s osobnými údajmi je dnes jeden z najvýnosnejších a najdynamickejšie sa rozvíjajúcich. A dnes už pravdepodobne aj nezastaviteľný. Najnepravdepodobnejšie by ho mohlo zastaviť, paradoxne, práve právo na súkromie, pretože konečným užívateľom služieb a výhod je človek ako spotrebiteľ. Blaho spotrebiteľa je v kapitalistickom svete konečnou métou spokojnej spoločnosti, a teda aj záujmom štátu.

Nemožno však tvrdiť, že by štát tento obchod s osobnými údajmi úplne ignoroval. Najvýraznejším symbolom európskeho boja za ochranu osobných údajov sa stalo nariadenie Európskej únie o ochrane osobných údajov fyzických osôb – GDRP, ktoré na území Slovenskej republiky nahradilo zákon č. 122/2013 Z. z. o ochrane osobných údajov. Predmetné nariadenie však chráni údaje, ktoré sa týkajú identifikovanej alebo identifikovateľnej fyzickej osoby. Predmetom príslušnej regulácie sú tak údaje, ktoré obsahujú identifikátory, akými sú napríklad meno, priezvisko či rodné číslo. Táto koncepcia ochrany osobných údajov vychádza z tradičného chápania práva na súkromie (osobné údaje sú súčasťou práva na súkromie) ako individuálneho práva, ktorého stredobodom záujmu je jednotlivec a ochrana jeho osobnej autonómnej dôstojnosti, osobnej slobody a záujmov týkajúcich sa jeho osobného rozvoja a individuality.[9]

Tento individualistický prístup má svoje korene v minulosti, keď ešte úroveň technológií a finančná nákladnosť neumožňovali ukladať a spracúvať obrovské množstvá informácií, ale bolo potrebné urobiť selekciu na základe potrebnosti údajov. Údaje sa zbierali iba o konkrétnych osobách alebo o malých skupinách ľudí. V súčasnej dobe však už

[9] Európsky súd pre ľudské práva pri svojom extenzívnom a evolučnom výklade práva na súkromie objavil v článku 8 Dohovoru však aj také práva, ktorých porušenie nezasahuje len individuálneho človeka ale celé spoločenstvo v jeho okolí. Typickým príkladom je právo na životné prostredie. Toto právo však naďalej nechápe ako kolektívne právo, ale len ako individuálne právo a v prípade porušenia práva napríklad skládkou komunálneho odpadu, musí každý sťažovateľ preukázať individuálnu ujmu.

existujú také technológie, pre ktoré sa dôležitými stávajú „vzorce" správania veľkého počtu jednotlivcov, pričom samotný jednotlivec ako jedinečná bytosť prestáva byť dôležitý. Súčasné dátové analytické technológie sa na jednotlivca ako takého sústredia už len výnimočne preto, lebo predmetom ich záujmu je život a správanie ľudí na úrovni veľkých *skupín*. Tieto technológie využívajú algoritmy, ktorých pomocou zoskupujú jednotlivcov do určitých skupín, pričom dokážu zacieliť na jednotlivcov v skupine bez toho, aby ich potrebovali identifikovať. Slovo „skupina" je však kľúčovým a ústredným pojmom, pretože v sebe zhmotňuje podstatu problému, ktorý tu načrtneme, a to, že právna úprava chráni jednotlivca – obeť porušenia práva na súkromie, a nie skupinu, navyše v praxi spravidla ťažko definovateľnú.

V súčasnosti pritom už nemožno o Big Data hovoriť ako o nejakom fenoméne, prelome vo vede, novinke, ktorú zatiaľ objavili najväčšie a najbohatšie firmy sveta, a je potrebné sa na tento zlom v nakladaní s údajmi pripraviť. Už teraz ide o trend a úplne bežný biznis model mnohých spoločností a je jasné, že firmy, ktoré nebudú držať krok vo využívaní Big Data, budú prevalcované konkurenciou. Navyše tu dochádza k sofistikovanému využívaniu praktík zameraných proti tradičnému chápaniu hospodárskej súťaže. Fúzie medzi internetovými gigantami, ako napríklad Facebook /WhatsApp či Microsoft/LinkedIn, už nie je možné merať klasickými metódami „blahobytu" spotrebiteľa a o GDPR ako o hodnotiacom kritériu sa len veľmi opatrne uvažuje.[10]

Vzhľadom na to, že téme Big Data nebol ešte v Právnom obzore venovaný širší priestor, nebude na škodu pripomenúť si jeho fungovanie v praxi. Analytické systémy využívajú algoritmickú klasifikáciu a zoskupovanie jednotlivcov, a to s jednoduchým cieľom – urýchliť rozhodovanie – pretože kto sa vie rýchlo rozhodnúť a efektívne zacieliť na potrebnú množinu jednotlivcov, má na trhu najväčšiu šancu na úspech. Hovoríme tu teda o vzniku určitých *skupín*, ktoré algoritmy vytvárajú na základe analýzy dát.

Proces vytvárania takýchto skupín je možné znázorniť na jednoduchom príklade: Poisťovňa X za posledné dva roky vyplácala svojim klientom nepomerne viac poistných plnení v oblasti zdravotnej starostlivosti ako v predošlom období a jej zisk sa výrazne znížil. Z tohto dôvodu sa akcionári rozhodli investovať do nových zamestnancov a zriadili oddelenie dátových odborníkov, ktorí mali za úlohu zistiť, ako by mohla poisťovňa vyriešiť neuspokojivú finančnú situáciu. Títo odborníci disponovali rôznymi údajmi o klientoch – vek, hmotnosť, pohlavie, údaje o prekonaných chorobách a chorobách v rodine a podobne. Na základe týchto údajov sa im podarilo vytvoriť skupiny ľudí, u ktorých je najväčšia pravdepodobnosť, že im bude potrebné vyplácať poistné plnenia, pretože sú napríklad náchylnejší na ochorenia. Týmto *skupinám* najrizikovejších klientov ponúkne poisťovňa najdrahšie poistenie, aby tak kompenzovala svoje výdavky na prípadné poistné plnenie.

Na základe algoritmickej klasifikácie sa teda vytvárajú *skupiny* ľudí, ktorí, hoci neboli identifikovaní, boli predmetom určitých opatrení, ktoré zasiahli alebo mohli zasiahnuť aj do sféry ich súkromného života. Navyše, tradičné identifikátory, ako napríklad

[10] Pozri FUNTA, R. Fúzie a ich vplyv na ochranu osobných údajov spotrebiteľov, *Justičná revue,* 3/2020, v tlači.

meno či adresa, boli pri tomto „spoznávaní“ ľudí takmer nepodstatné. Jednotlivci sú tak zatrieďovaní/klasifikovaní na základe ich preferencií, správania a iných prejavov bez toho, aby boli identifikovaní[11] (napríklad ako milovníkov drahých áut, športovcov, zberateľov obrazov a pod.). Klasifikácia sa uskutočňuje aj na základe prepojenia a vzťahov jednotlivcov s inými jednotlivcami, ktoré nám odhaľujú ich záujmy a typy ich správania.[12] Samozrejme, v niektorých prípadoch, v závislosti od konkrétnej situácie a od toho, čo je potrebné zistiť, sa v *machine-learningu* využívajú také metódy, ktoré skupiny nevytvárajú, ale priraďujú váhu určitým aspektom, ktoré prezentujú jednotlivé subjekty.[13]

Pri takomto spracovávaní osobných údajov je ochrana identifikovateľných osôb nedostatočná. Nepokrýva totiž všetky situácie, keď dochádza k zásahu do práva na súkromie. Inak povedané, existujú situácie, keď je skupina vystavená riziku napriek tomu, že právo každého člena je chránené? Opäť jednoduchý príklad: Ak chce marketingové oddelenie firmy X zacieliť na potenciálnych zákazníkov spomedzi užívateľov sociálnej siete Facebook, musí získať údaje o ich preferenciách/záujmoch a analýzou zistiť, ktorým užívateľom danej sociálnej siete sa oplatí zobraziť reklamu. Vzhľadom na to, že Facebook má milióny užívateľov, z finančného hľadiska nie je rozumné a výhodné cieliť na všetkých. Algoritmus však dokáže na základe zozbieraných údajov vyfiltrovať skupinu takých užívateľov, u ktorých je najväčší predpoklad, že si službu firmy X zakúpia. V tomto prípade pre firmu X vôbec nebolo dôležité vedieť, či zacieli na Ing. Jána Nového, narodeného 14. 8. 1962 v Lučenci. Táto osoba bola pre ňu iba jeden z bodov v určitej množine, ktorá sa do nej dostala na základe svojej aktivity na internete.[14] Ľudia po sebe (najmä na internete) zanechávajú až roztopašne veľké množstvo stôp (údajov), ktoré stačí „pozbierať“, vyhodnotiť a použiť vo svoj prospech. Predstavme si sami seba a náš profil na sociálnej sieti, všetko čo si pozeráme, kam klikneme, čo komu napíšeme – všetko z toho sú údaje, ktoré môžu firme X priniesť benefit vo forme úspešného zacielenia na zákazníkov.

Fakt, že jednotlivec už nie je centrom záujmu pri Big Data procesoch, podkopáva základy prevažnej existujúcej právnej, etickej a spoločenskej teórie a praxe[15] minimálne v troch smeroch, a to pri:

a) identifikovaní legitimity zásahu,
b) vzniku ujmy,
c) vedomosti o spôsobenej ujme.

Ad a) V prípade tradičných zásahov do práva na súkromie sa predpokladá jasný a zrejmý verejný záujem. Napríklad v prípade domovej prehliadky osoby podozrivej zo

[11] MITTELSTADT, B. From Individual to Group Privacy in Big Data Analytics, 2017, SpringerLink s. 478. Dostupné online: https://link.springer.com/article/10.1007/s13347-017-0253-7, cit. dňa 21. 2. 2020.

[12] Ibid.

[13] Ibid., s. 477.

[14] Pripomína to povestného Jozefa Maka, ktorého ako príklad vybral R. Procházka pre svoju právnickú etudu. PROCHÁZKA, R. *Mak proti Gatsbymu*. Edition Ryba, 1. júl 2009

[15] TAYLOR, L. et al. Introduction: a new perspective on privacy. In Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies. Dordrecht : Springer, s. 13-14.

spáchania zločinu ide o zachovanie poriadku a boj proti trestnej činnosti. V prípadoch Big Data procesov je vzťah medzi zberom a spracúvaním údajov konkrétnej osoby a verejným záujmom často vágny a abstraktný, pretože údaje sa často nezbierajú s vopred vytýčeným cieľom, ale až v neskoršej fáze sa rozhodne, ako najlepšie zozbierané údaje využiť.[16] V uvedenom príklade s poisťovňou to bolo presne tak. Poisťovňa už disponovala údajmi svojich klientov a až neskôr, v čase krízy, sa rozhodla analyzovať ich s určitým cieľom. V druhom prípade s marketingovou spoločnosťou nastáva podobná situácia. Facebook o užívateľoch zbiera údaje neustále bez vopred vytýčeného cieľa. V podmienkach Facebooku nie je nikde uvedené, že zbiera vaše údaje za tým účelom, aby firma X mohla zhodnotiť, či ste perspektívnym klientom a či investuje prostriedky do toho, aby vám sprostredkovala reklamu na svoje finančné služby.

Ad b) Pri posudzovaní porušenia práva na súkromie sa ďalej skúma, či došlo k vzniku ujmy. Vznik ujmy je predpokladom na porušenie práva na súkromie. Osoba môže tvrdiť, že jej právo na súkromie bolo porušené iba vtedy, ak utrpela ujmu na svojich záujmoch. Pojem a chápanie ujmy bolo vždy problematické, rovnako aj zdôvodnenie, respektíve dokázanie, že určitú ujmu spôsobilo konkrétne porušenie práva. Ešte v druhej polovici dvadsiateho storočia sa kládla otázka, aká ujma bola spôsobená v prípade odpočúvania telefónneho rozhovoru alebo neoprávneného vniknutia do domu, ak žiadny predmet nebol ukradnutý a získané informácie neboli zverejnené tretím stranám?[17]

Problematickejšie je potom preukázať, že jednotlivec utrpel ujmu v kontexte Big Data procesov. Opäť príklad. Tentoraz nepôjde o hypotetickú situáciu (hoci sme presvedčení, že podobné praktiky ako v prípade s Facebook-om sa dejú každý deň), ale pôjde o konkrétnu situáciu, ktorá bola aj medializovaná. V roku 2013 sa na Ukrajine konal protest, tzv. Euromaidan, na ktorom obyvatelia protestovali proti korupcii a zneužitiu moci zo strany vlády, ako aj proti porušovaniu ľudských práv na Ukrajine. Tento protest vyvolalo rozhodnutie vlády pozastaviť podpísanie asociačnej dohody s Európskou úniou a, naopak, posilniť väzby s Ruskom. Účastníci tohto protestu dostali varovné SMS správy, o ktorých mnohí predpokladali, že išlo o aktivitu zo strany vlády, hoci táto to odmietala.[18] Ktokoľvek tieto SMS správy zasielal (pravdepodobne hackeri), cielil na určitú skupinu ľudí (protestujúcich), ktorú chcel zastrašiť – nešlo o identifikáciu konkrétnych jednotlivcov za účelom ich potrestania z dôvodu účasti na proteste. Na to, aby sa dosiahol požadovaný cieľ, nemuseli byť konkrétni účastníci protestu vôbec identifikovaní alebo identifikovateľní (SMS sa mohli zasielať na základe GPS signálu v mobile). Zdá sa, že tu ide skôr o ohrozenie záujmu na úrovni spoločnosti ako záujmu konkrétnych jednotlivcov.

[16] VAN DER SLOOT, B. How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one. Draft version. Final version published in Information & Communications Technology Law 2015, s. 2. Dostupné online: https://bartvandersloot.com/onewebmedia/How_to_assess_privacy_violations_in_the.pdf, cit. dňa 21. 2. 2020.

[17] Ibid., s. 1.

[18] Pozri napríklad: https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot, cit. dňa 21. 2. 2020.

Ad c) Dokázanie, že jednotlivcovi vôbec vznikla ujma pri Big Data procesoch, je problematické. Častejší prípad je však ten, že jednotlivec sa *vôbec nedozvie*, že údaje o ňom boli predmetom určitej analýzy a algoritmus ho zatriedil do konkrétnej skupiny a vytvoril mu určitý profil, na ktorého základe bude posudzovaný. V súčasnej dobe technologického pokroku sa otázka ujmy stáva čoraz nejasnejšou a komplikovanejšou. Jednotlivec si často ani neuvedomuje, že jeho osobné údaje sú zbierané, a teda uplatňovanie porušenia práva na súkromie je v rovine hypotetickej. Aj keby však vedomosť mal, vzhľadom na rozsah zbierania a vyhodnocovania dát je takmer nemožné, aby jednotlivec dokázal sledovať všetky takéto aktivity a zároveň posúdil, či sú v súlade s právom a v prípade, že nie, podal sťažnosť proti konkrétnemu subjektu, či domáhal sa nápravy v štátnych orgánoch. V prípade, ak by človek podal žalobu na súd, musel by dokázať, že utrpel konkrétnu ujmu, čo je v prípade Big Data procesov viac ako otázne.[19]

Pôvodná otázka smerovala k tomu, či existujú situácie, keď je skupina vystavená riziku napriek tomu, že právo každého člena je chránené. Kladná odpoveď vychádza z uvedených príkladov, pri ktorých algoritmy ľudí zatrieďujú do skupín bez toho, aby ich vôbec identifikovali. Nepotrebujú na to ani citlivé údaje, úplne im postačia informácie, ako napríklad, na aký post ste dali „like". Samozrejme, mnohé inštitúcie disponujú aj citlivými údajmi ako vek, pohlavie a podobne, ktoré musia zo zákona chrániť, avšak vedia ich využiť pri algoritmickej klasifikácii (príklad s poisťovňou). V niektorých prípadoch sa profily vytvorené na základe neutrálnych znakov, ako je napríklad poštové smerové číslo, môžu prelínať s inými profilmi vzťahujúcimi sa na národnosť, pohlavie, sexuálnu orientáciu a podobne.[20] Algoritmickú klasifikáciu možno považovať za zásah do súkromia, pričom táto skutočnosť zostáva v právnom vákuu.[21]

V súčasnosti sa preto vynára z oblakov teórie myšlienka vytvoriť *skupinové právo na súkromie*. Podobne ako záujmy jednotlivcov, aj algoritmicky zoskupení ľudia majú kolektívny záujem vedieť, ako sa informácie, ktoré charakterizujú a vytvárajú uvedené skupiny, zbierajú a používajú.[22] Mittelstadt napríklad uvádza, že by malo byť vytvorené ekvivalentné právo na súkromie aj pre takéto *ad hoc* skupiny – takzvané kolektívne právo, aby tak bola vytvorená rovnováha s individuálnym právom na súkromie na jednej strane a spoločenskými, obchodnými a inými výhodami analytiky na druhej strane.[23] Kolektívne súkromie vníma v zmysle konceptu informačnej identity Floridiho, ako súkromie informácií, ktoré vytvára identitu. Identita je teda tvorená informáciami popisujúcimi daný subjekt (jednotlivca alebo skupinu) a integrita tejto identity je porušená v momente, keď sa nejaký údaj alebo informácia pridá k identite bez súhlasu zodpovedajúce-

[19] VAN DER SLOOT, B. How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one. Draft version. Final version published in Information & Communications Technology Law 2015, s. 2. Dostupné online: https://bartvandersloot.com/onewebmedia/How_to_assess_privacy_violations_in_the.pdf, cit. dňa 21. 2. 2020.

[20] MITTELSTADT, B. From Individual to Group Privacy in Big Data Analytics, 2017, SpringerLink, s. 479. Dostupné online: https://link.springer.com/article/10.1007/s13347-017-0253-7, cit. dňa 21. 2. 2020.

[21] Ibid., s. 478.

[22] Ibid., s. 476.

[23] Ibid.

ho subjektu. Podľa neho by mal mať jednotlivec aj skupina právo na zaobchádzanie s informáciami, ktoré sa na nich vzťahujú, a to predovšetkým vykonávanie kontroly nad informáciami.[24] Z tohto dôvodu by malo byť právo na súkromie (právo na identitu) chránené nezávisle od možnosti alebo nemožnosti zistiť a napraviť nežiaduce efekty spracúvania údajov.[25] Existuje však vôbec skupinové/kolektívne právo na súkromie (respektíve kolektívne právo na identitu), odlišné od individuálneho práva?

Sú tri možnosti, a to:[26]
- právo môžu mať iba jednotlivci,
- skupina môže mať právo, ale iba preto, že ho majú jednotlivci – členovia skupiny,
- skupina má vlastné práva, ktoré môže aj uplatniť a mala by sa vnímať podobne ako jednotlivec.

Skupinové právo vnímané ako *súbor individuálnych práv* nie je riešením, pretože by sa situácia v podstate nezmenila a naďalej by si právo na súkromie mohli uplatniť iba jednotlivci. Taylor prirovnáva údaje o jednotlivcoch k ingredienciám. Keď varíme, používame určité ingrediencie (údaje o jednotlivcoch), ale jedlo, ktoré získame (informácia) nie je kópiou ingrediencií. Takisto, keď staviame dom pomocou určitých materiálov, tak postavený dom nie je kópiou tehiel, ktoré sme použili.[27] Ak by niekto ohrozoval náš dom, nebolo by praktické snažiť sa chrániť každú tehlu zvlášť, ale chrániť dom ako celok.

Samozrejme, otázkou je, či by bolo riešením také skupinové právo, ktoré by bolo vnímané ako *právo patriace (algoritmicky vytvorenej) skupine ako takej*. Súčasný prístup Európskej únie je tradičný: zaruč právo každému jednotlivcovi osobitne a skupina tým pádom bude tiež v poriadku.[28] Tento prístup Európskej únie ilustroval Floridi na výstižnom príklade s veľrybami a sardinkami. Málokto z nás je veľryba, väčšina z nás sme sardinky. Sardinka si môže myslieť, že obrovská sieť sa ju snaží uloviť. Sieť sa však nesnaží uloviť konkrétnu sardinku, ale celý húf sardiniek. Preto by nemala byť chránená sardinka, ale húf sardiniek ako celok. To, že ochrana jednotlivcov je veľmi silná, ako keby každý z nás bol Moby-Dick, môže byť síce lichotivé a v niektorých prípadoch aj opodstatnené, ale tento prístup by mal byť podľa Floridiho urgentne zmenený.[29]

V prípade, že by sa priznalo skupine právo na súkromie, bude potrebné vyrovnať sa s mnohými otázkami a problémami. Po prvé, ak má mať skupina práva, je potrebné ju ako subjekt práv zadefinovať. Takáto skupina sa však oproti napríklad obchodnej spoločnosti odlišuje tým, že:[30]

[24] Ibid, s. 481-482.

[25] Ibid, s. 482.

[26] FLORIDI, L.: Group Privacy: a Defence and an Interpretation. In Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies.* Dordrecht : Springer, s. 111.

[27] Ibid., s. 107.

[28] Ibid., s. 120.

[29] Ibid., s. 121.

[30] VAN DER SLOOT, B. Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under Article 8 ECHR. In Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies.* Dordrecht : Springer, s. 272.

– nie je jasné, kto do nej patrí,
– väčšinou nejde o vedomé alebo chcené členstvo,
– je ťažké určiť, čo je jej záujmom,
– je otázne, kto ju reprezentuje alebo má reprezentovať,
– je dynamická a nestála, zmení sa po zmene určovateľov alebo kritérií, podľa potrieb toho, kto dáta analyzuje – teda postmoderným slovom, je tekutá.

Je preto nevyhnutné, aby sa viac preskúmalo fungovanie Big Data procesov a využívanie algoritmov. Výsledkom analýzy údajov algoritmom môžu byť skupiny, avšak pred získaním určitého výsledku nevyhnutne prebieha určitý proces (v niektorých procesoch nemusia byť výsledkom skupiny, ale napríklad odpoveď áno/nie). Príkladom môže byť banka, ktorá chce vytvoriť skupinu potenciálnych zákazníkov, aby im ponúkla úver. Kým sa k tomuto výsledku dátový odborník banky dostane, musí do algoritmu vložiť určité vstupy – napríklad vek, pohlavie, úroveň vzdelania zákazníkov a iné faktory, ktoré môžu zohrať úlohu pri klasifikácii. Už v tejto fáze pracuje dátový odborník so skupinami – skupina ľudí od 50 rokov a starších, skupina žien, skupina mužov a tak ďalej. Otázne je, či je v poriadku využívať všetky možné relevantné faktory, respektíve relevantné skupiny. Je síce pravda, že v priemere zarábajú ženy menej ako muži, no otázkou je, či by tento faktor mal ovplyvňovať to, kto dostane úver a kto nie. Nepôjde o nemorálnu a diskriminačnú praktiku, ak šanca získať úver bude pre ženy nižšia ako pre mužov? V prípade, ak algoritmus nevytvára skupiny, ale dáva odpoveď áno/nie (dať úver/nedať úver), je možné tiež dôjsť k podobnej dileme. So skupinami sa pracuje už na začiatku analytického procesu. Sú napríklad skupiny i) vydaté ženy s deťmi a ii) slobodní bezdetní muži, pričom túto kategorizáciu mohol uskutočniť človek – analytik. Algoritmus dá odpoveď k prvej skupine „nie – nedať úver“ a k druhej skupine „áno – dať úver“ (samozrejme, ide o zjednodušený extrémny príklad). V tomto prípade nejde o algoritmicky vytvorené skupiny (na výstupe), ktorým sa doteraz venovala pozornosť, ale o skupiny, ktoré algoritmus vyhodnocuje (skupiny na vstupe) a na ich základe poskytne určitý výsledok.

Základnou otázkou je teda definícia pojmu „skupiny“ ako potenciálneho nositeľa práv. Druhou otázkou je, ako by skupina dokázala svoje právo uplatniť. Je možné uplatniť „actio popularis“? Je možné ísť po trajektórii práva na súkromie zasiahnutého tajným odpočúvaním zo strany štátu? Alebo tu dochádza k úplne protikladnému postupu? Aby sa mohol ochrániť pred zásahom do práva na súkromie jednotlivec, je potrebné poskytnúť ochranu skupine, v ktorej sa nachádza. Úspechom by bolo už dosiahnutie práva byť informovaný, v akej skupine sa človek nachádza.[31]

[31] O tom, že to nemusí byť také jednoduché, svedčí peripetia rakúskeho študenta Maximiliana Schremsa, ktorý sa obrátil na Facebook s požiadavkou, aby mu zaslal všetky údaje, ktoré o ňom má. Po niekoľkých týždňoch a desiatkach e-mailov mu napokon vo Facebooku vyhoveli a zaslali mu CD, ktoré obsahovalo 496 MB údajov, čo sa rovná 1 222 stranám. Neprekvapuje, že medzi nimi boli aj záznamy, ktoré vymazal. Písal sa rok 2011.

Literatúra

BENOIST, A. de: Za horizontem lidských práv, Zvolen : Sol Noctis, 2019, ISBN 9788097329242
FLORIDI, L. Group Privacy: a Defence and an Interpretation. In Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies. Dordrecht : Springer
FUNTA, R. Fúzie a ich vplyv na ochranu osobných údajov spotrebiteľov. In Justičná revue, 3/2020, v tlači
MITTELSTADT, B. From Individual to Group Privacy in Big Data Analytics, 2017, SpringerLink. Dostupné online: https://link.springer.com/article/10.1007/s13347-017-0253-7, cit. dňa 21. 2. 2020
PROCHÁZKA, R. Mak proti Gatsbymu. Edition Ryba, 2009, ISBN 9788089250066
TAYLOR, L. et al. Introduction: a new perspective on privacy. In: Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies. Dordrecht : Springer
VAN DER SLOOT, B. How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one. Draft version. Final version published in Information & Communications Technology Law 2015. Dostupné online: https://bartvandersloot.com/onewebmedia/How_to_assess_privacy_violations_in_the.pdf, cit. dňa 21. 2. 2020
VAN DER SLOOT, B. Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under Article 8 ECHR. In: Taylor, L. – Floridi, L. – van der Sloot, B. eds. (2017) Group Privacy: new challenges of data technologies. Dordrecht : Springer

Judikatúra Európskeho súdu pre ľudské práva

Athanassoglou a ostatní proti Švajčiarsku (zo 6. apríla 2000, č. 27644/95)
Esbester proti Spojenému kráľovstvu (z 2. apríla 1993, č. 18601/91
Iliya Stefanov proti Bulharsku (z 22. mája 2008, č. 65755/01)
Iliya Stefanov proti Bulharsku (z 22. mája 2008, č. 65755/01)
Iordachi proti Rumunsku (z 10. februára 2009, č. 25198/02)
Kennedy proti Spojenému kráľovstvu (z 18. mája 2010, č. 26839/05)
Malone proti Spojenému kráľovstvu (z 2. augusta 1984, č. 8691/79)
N.C. proti Taliansku (z 18. decembra 2002, č. 24952/94)
Weber a Saravia proti Nemecku (z 29. júna 2006, č. 54934/00)

Internetové linky:

https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot, cit. dňa 21. 2. 2020