Analýza ohrození pri spracovaní osobných údajov

EISI, o.z.

Európska únia

Európsky sociálny fond

Operačný program
Efektívna verejná správa

EISI European Information Society Institute

Realizované občianskym združením European Information Society Institute v rámci projektu Priateľské dátové prostredie v zdravotníctve. Tento projekt je podporený z Európskeho sociálneho fondu v rámci operačného programu Efektívna verejná správa.

Obsah

Úvod

Zhromažďovanie údajov nie je novinka. Zhromažďujeme odjakživa, spracúvanie samotné a metódy spracúvania sa však menia.
Čo má však etika spoločné s požiadavkami na spracovanie osobných údajov? K dôvodom, prečo je nutné stanoviť obmedzenia na spracovanie osobných údajov, nás privedie definícia osobného údaju – „informácia týkajúca sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"). Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby."[1]

A druhým dôvodom je prirodzená túžba ľudí zefektívniť, zrýchliť a zvýšiť zisk zo svojej činnosti. A tu sa stretávame s pojmom BigData alebo pojmom „profilovanie" – ktorým je „akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom."[2] S pojmom Big Data však okrem profilovania súvisí aj mnoho ďalších činností, ktoré nemajú zákonnú definíciu a často ani slovenský ekvivalent, ako – mining, scraping, sampling, AI, machine learning, natural language, image processing, simulation, computer modeling a cloud computing.

Prečo je teda spracovanie osobných údajov nutne previazané s etickými aspektmi? Pretože zaobchádzanie s údajmi človeka a ich využívanie, či už pre dobromyseľné alebo nedobromyseľné konanie, ovplyvňuje jeho/jej konanie – autonómiu. Účelom etiky je ponúknuť najlepší variant toho, ako žiť dobre. Na to, aby sme žili dobre, nemôžeme zasahovať neoprávnene do autonómie iných.

[1] Nariadenie Európskeho Parlamentu A Rady (Eú) 2016/679, Čl. 4
[2] Tamtiež,

1 Ohrozenia pri nepochopení etických aspektov

Zber údajov, ktoré nám dokážu osvetliť čo a ako funguje, ak ich dokážeme sledovať a správne interpretovať, čím viac o svete vieme, tým viac ho dokážeme ovplyvňovať. Vďaka údajom vieme pochopiť zložité javy týkajúce sa ľudského správania, ktoré by sme bez ich zaznamenávania nedokázali spojiť a pochopiť. Bez zaznamenávania by sme nemali kolektívnu pamäť. S veľkými benefitmi prichádzajú aj veľké ohrozenia. Aký prospech a aké ohrozenia vyplývajú z ne/pochopenia a ne/zvládnutia etických výziev, ktorým čelíme pri ochrane osobných údajov?

Ohrozenia:

a) **Ohrozenia súkromia jednotlivca** aj pseudonymizované datasety prepojené s inými o nás vypovedajú veľa.

Príklad: Naša sexuálna história a preferencie, záznamy o duševnom zdraví, súkromné rozhovory v práci a doma, genetická výbava a predispozície, návyky na čítanie a vyhľadávanie na internete, politické, náboženské názory môžu byť súčasťou dátových profilov, ktoré boli vytvorené a uložené niekde **neznáme**, často bez nášho vedomia alebo informovaného súhlasu.

Pred GDPR existovali len regionálne, nekonzistentné a slabo vynútené predpisy a politiky nás chránili pred ekonomickými a emocionálnymi škodami, ktoré by mohli spôsobiť uvoľnenie takýchto intímnych údajov do nesprávnych rúk. Príkladom je existencia údajov identifikujúcich obete domáceho násilia alebo politických protestujúcich, alebo sexuálnych menšín žijúcich v represívnych režimoch. Potenciálne škody môžu znamenať stratu života alebo slobody.

b) **Ohrozenie nedotknuteľnosti** – zmena a zneužitie údajov

- očakávame, že prístup k nám bude spravodlivý – teda na rovnaké prípady rovnaký prístup bez ohľadu na to, o koho ide. Avšak všetky súčasné systémy začínajú pracovať s analýzou dát.

A nie všetky tieto systémy sú kvalifikované pre splnenie etických štandardov - poskytujú priestor pre arbitrárnosť, chyby, predsudky v datasetoch. Takisto sa môžu objaviť kvantitatívne nedostatky vyhodnocovacích systémov – málo údajov, ktoré neponúknu relevantný výsledok.

Takéto zlyhania v oblasti etických údajov, či už pri používaní malých súborov údajov alebo pri analýze veľkých údajov, môžu viesť

k ekonomickej škode, psychickej škode, poškodeniu reputácie a poškodeniu zdravia.

c) **Ohrozenie rovnosti ako etickej a právnej základnej požiadavky**

- Napr. datamining, automatizované spracúvanie a profilovanie, ktorého výsledkom môže byť diskriminácia a nerovnosť.

d) **Ohrozenie transparentnosti a autonómie**
Transparentnosť: schopnosť ponúknuť „insight" ako spoločenský systém alebo inštitúcia funguje.
Autonómia: schopnosť viesť život podľa vlastnej vôle. Rovnako tu patrí aj zodpovednosť za vlastné rozhodnutia.

- Ako sú prepojené? Na to, aby som mohol robiť dobré rozhodnutia, musím mať kvalitné informácie, na základe ktorých ich mám robiť – teda transparentnosť je kľúčová pre moju autonómiu.
- Čo ak nerozhoduje človek – ale program? A čo ak taký, ktorý sa učí vyhodnocovať na základe nových údajov? – machine learning – ak stroj zamietne moju liečbu, tak mi lekár nedokáže úplne povedať, prečo tak urobil.
- Algoritmus, na základe ktorého to rozhodujú, nezverejnia, lebo je to ich know how.

Napr. proces automatizovaného spracovania údajov a ich vyhodnocovanie na základe algoritmu nemusí byť zverejnený (napr. pre iné právne prekážky – ako obchodné tajomstvo, know how, atď.).
Preto môžeme podľa nového zákona požiadať o to, aby som nepodliehal automatizovanému rozhodnutiu.

1.1 Benefity vyplývajúce zo spracúvania údajov

Prospech, ktorý nadobúdame ako spoločnosť vďaka moderným technológiám, prepájaním systémov a porovnávaním získaných údajov, je natoľko veľký, že prevyšuje škody, ktoré by jeho zneužitím mohli vzniknúť. Pre zachovanie ľudskej dôstojnosti je preto nutné nastaviť dostatočný štandard odvrátenia neželaného stavu, ako aj postup pre napravenie vzniknutých škôd, ako zavrhnutie využitia a benefitov zo systematického zbierania a spracovania osobných údajov.

a) Rozširovanie ľudského poznania - **dáta nám dokážu osvetliť čo a ako funguje, ak ich dokážeme sledovať a správne interpretovať**, čím viac o svete vieme, tým viac ho dokážeme ovplyvňovať.
b) **Vďaka** dátam vieme pochopiť zložité javy, ktoré by sme bez ich zaznamenávania nedokázali spojiť a pochopiť.

c) Udržiavanie dosiahnutej úrovne vedomosti - bez zaznamenávania nemáme pamäť.
d) Ekonomický prínos - procesy, ako sa ovplyvňujú navzájom, napr. big data, nám dokážu pomôcť pri riešení dopravy, služieb, posilnenia služieb.
e) Personalizované riešenie problémov – „na mieru". Napríklad v oblasti personalizovanej medicíny.

2 Etické výzvy

a) Problém zbierania a spracovania údajov

- Ako dodržiavame požiadavku, aby údaje boli spracúvané iba v súlade s účelom, pre ktorý nám boli dané?
- Aké dáta zbierame? Potrebujeme ich vôbec?
- Máme analýzu toho, čo sa deje s údajmi, ktoré zdieľame s 3. osobami?
- Majú dotknuté subjekty vedomosť o údajoch, ktoré o nich zbieram?
- Majú možnosť sa k nim vyjadriť, resp. ich obmedziť?
- Pristupujeme rovnako/nediskriminačne k tým, ktorí poskytli svoje údaje ako k tým, ktorí obmedzili rozsah svojich údajov, ktoré zbieram?
- Sú zrozumiteľné naše podmienky alebo zneužívame technický a právnický jazyk?
- Sú dotknutí poučení dostatočne o tom, ako sa narába a čo sa deje s ich údajmi?
- Čo dostaneme výmenou za poskytnutie našich údajov?
- Akú kontrolu máme nad disponovaním so svojimi dátami?

b) Problém ukladania a skladovania údajov

- Prijali sme opatrenia na bezpečné ukladanie údajov? Sú subjekty informované o tom, ako sú uchovávané a kto je zodpovedný?
- Máme scenáre – worst scenario? Aké budú krátkodobé a dlhodobé dôsledky zneužitia údajov?
- Aké postupy máme pripravené pre worst scenario prípady? Máme nejaké?
- Dosiahli sme bezpečnú infraštruktúru prúdu údajov? Pr. Datacentrá.
- Aké postupy používame pre bezpečnosť údajov? – Postup pseudonymizácie/anonymizácie údajov. Čomu tým chceme predísť?
- Aké sú hrozby pri dlhodobom uchovávaní údajov? Ako dlho môžeme uchovávať konkrétne údaje? Ak nie je limitované zákonom, koľko je vhodné?
- Máme plán a postup systematizovaného mazania údajov?
- Máme postupy pre dotknuté osoby pre žiadosť na vymazanie, opravu a doplnenie údajov?

c) Problém vymazávania nadbytočných údajov

- Máme postupy pre zistenie, nakoľko sú naše údaje usporiadané, spoľahlivé, pravdivé, aktuálne? – Dátový audit.
- Ako vyhodnocujeme spoľahlivosť, pravdivosť a aktuálnosť údajov?

- Ak využívame viacero systémov s podobnými údajmi: Máme postupy pre zistenie kompatibility? Kto je oprávnený vykonať opravu? Ako zabezpečiť integritu údajov? Napr. pri prenose a po prenose. Každý zásah do údajov je zmena údajov – čo s tým?
- Aké postupy máme prijaté pre tzv. scrubbing údajov – česanie. Aké riziká nám z nich vyplývajú?
- Sú údaje, ktoré spracúvame relevantné pre problém, ktorý riešime?
- Čo s údajmi, ktoré sú neaktuálne, nespoľahlivé?

d) Problém vyhodnocovania citlivých osobných údajov a identifikovania možnej diskriminácie pri automatizovanom vyhodnocovaní

- Máme postupy pre odhalenie možnej automatizovanej zaujatosti pri spracúvaní údajov?
- Čo je vhodná a nevhodná zaujatosť? Čo hľadáme a, naopak, čo nesmieme dopustiť?
- Aké metódy sme zvolili na odlíšenie?
- Máme expertízu možných následkov, ak budú výsledky ovplyvnené automatizovanou predpojatosťou?
- Ako môžu byť tieto výsledky zneužité?

e) Problém transparentnosti spracovania a vyhodnocovania údajov

- Aké informácie o skutočnostiach, ktoré mali vplyv na vyhodnocovanie údajov, je nutné poskytnúť verejnosti a dotknutým osobám?
- Ako preukázať, že modely, ktoré sme využili pre vyhodnocovanie, sú v súlade s etikou?
- Aké sú riziká nesprávneho vyhodnotenia údajov?
- Aké dopady môže mať netransparentnosť konania?
- Ako postupovať pri námietkach voči netransparentnosti?

f) Výzvy pre vyhodnotenie zodpovednosti

- **Dirty hands** – riešenie dilemy, porušenia etického štandardu za účelom menej škodlivého následku.
- **Many hands** – problém prisúdenia zodpovednosti za porušenie základného práva na súkromie.

- Kto je poverený a kto je zodpovedný? Kto je zodpovedný za akú úroveň spracovania údajov?
- Máme vytvorené postupy a politiky pre vyvodzovanie zodpovednosti?
- Každý musí vedieť, za ktorú fázu je zodpovedný on/ona.
- Máme postup pre kontrolu? Kto, ako, kedy, aké oprávnenia?

- Liberačné dôvody?
- Pripustiť verejnú kontrolu? Teda zverejniť interné predpisy? – transparentnosť, na druhej strane ohrozenie.

g) Problém potrebnej prípravy osôb pracujúcich s osobnými údajmi

- Ako prebieha oboznamovanie zamestnancov s ochranou osobných údajov?
- Je zabezpečená ochrana údajov aj po tom, ako opustia zodpovednosť našej inštitúcie? Máme mechanizmy pre kontrolu štandardu spolupracujúcich inštitúcií?

2.1 Benefity vyplývajúce zo spracúvania údajov

Právne požiadavky – GDPR – všeobecné, je na odborníkoch vytvoriť vhodné podmienky – nech nie je ochrana údajov iba formalita vyžadovaná zákonom, ale nech je v centre pozornosti a zmyslom každodennej práce s údajmi.[3]

Cieľ: Best practices – Code of Conduct pre zamestnancov zariadení poskytujúcich zdravotnú starostlivosť:

a) Spracovávanie údajov podlieha vždy etickým otázkam – majú vplyv na život dotknutých osôb. Je nutné podrobiť etickej analýze jednotlivé situácie a nepodľahnúť lákadlám redukcionizmu.

b) Nielen právne požiadavky, ale aj etické aspekty mať na zreteli vždy pri ochrane osobných údajov (vyšší štandard ochrany).

c) Za dátami je vždy konkrétny jednotlivec – Kantove kategorické imperatívy musia byť dodržané.

d) Sledovať, čo sa s dátami po ich spracovaní ďalej deje. Proces nekončí etickým zbieraním; v súlade s etickými štandardmi musia byť aj ďalšie fázy práce s osobnými údajmi.

e) Byť si vedomý toho, kde sú zajtra dáta, s ktorými dnes pracujem, preto potrebujem poznať aj celý kontext, prečo a ako to mám robiť takto a ako by to bolo lepšie.

[3] Nariadenie Európskeho Parlamentu A Rady (Eú) 2016/679, Čl. 40

f) Kontrolovať, ako pracuje s osobnými údajmi zmluvná strana, ktorej ich sprístupňujeme.

g) Rozdiel v očakávaniach a realite – ak je norma na papieri, neznamená to, že sa tak dodržiava aj v praxi – preto je nutné oboznamovanie jednotlivcov nielen s normou samotnou, ale aj s jej podstatou.

h) Dáta nie sú tovar v pôvodnom zmysle – ak ich nepotrebujeme a účel je naplnený, treba ich mazať. Nenechávať ich pre prípad možného použitia v budúcnosti.

i) Prehodnoť hranice riešenia pomocou dátovej analýzy, nie každý problém je nutné riešiť analýzou osobných údajov.

j) Postaviť jasnú štruktúru zodpovednosti pri pochybení pri ochrane osobných údajov.

k) Pripraviť scenáre krízových situácií a zistiť ako sa mení režim práce a ochrany osobných údajov pri mimoriadnych situáciách.

l) Podpora a oceňovanie transparentnosti a dôveryhodnosti.

m) Pohľad zvonku. Niekedy sa vnútorný pohľad môže otupiť, nevidí les pre stromy, vidí veci účelovo, nutný vonkajší feedback.

n) Nutná je etická reflexia a prax. Nekončiaci cyklus. Etický prístup musí byť pochválený.

Bibliografia

Všeobecne záväzné právne predpisy

[1] Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

[2] Vyhláška Úradu na ochranu osobných údajov SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

[3] 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 zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

Metodické pokyny a usmernenia

[1] ODPORÚČANIE KOMISIE z 11. marca 2005 týkajúce sa Európskej charty výskumných pracovníkov

Iná použitá literatúra

[1] European Handbook on European data protection law. 2018 edition, ISBN 978-92-871-9849-5.

[2] Rubinstein, I.S. Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 2013, Vol 3, No 2.

[3] Stahl, B.C et al. Identifying the Ethics of Emerging Information and Communication Technologies: An Essay on Issues, Concepts and Method. International Journal of Technoethics 1(4), 2010. 20-38.

[4] Vallor, S et al. An Introduction to Cybersecurity Ethics. Santa Clara University

[5] Kenneally, E. et al. A Framework for Understanding and Applying Ethical Principles in Network and Security Research.

[6] Stahl, B.C et al. From Computer Ethics to Responsible Research and Innovation in ICT.

Európska únia

Európsky sociálny fond

Operačný program
Efektívna verejná správa

EISI European Information Society Institute