

Analýza právnych aspektov využívania IoT zariadení pri automatizovanej správe verejných športovísk

Termín internet vecí (Internet of Things - ďalej ako IoT) bol prvýkrát použitý v roku 1999 britským technologickým priekopníkom Kevinom Ashtonom na opis systému, v ktorom by sa objekty vo fyzickom svete mohli pripojiť k internetu snímačmi. Ashton vytvoril termín na ilustráciu výkonu spájania značiek rádiových frekvencií identifikácie používaných v podnikových dodávateľských reťazcoch na internete, aby bolo možné počítať a sledovať tovar bez potreby ľudskej intervencie.¹

Inteligentné zariadenia pripojené k internetu, ktoré sú určené na zlepšenie a obohacovanie nášho života, sa stali pravidelnou súčasťou nášho každodenného života. Napriek globálnemu hluku okolo internetu vecí ešte neexistuje jednotná, všeobecne akceptovaná definícia tohto pojmu. Používajú sa rôzne definície na opis a podporu konkrétneho pohľadu na to, čo autor vníma za najdôležitejšie atribúty pojmu IoT. Niektoré definície chápu IoT jednoducho ako objekty do ktorých bolo vložením technológií ako napríklad mikročipy, senzory alebo ovládače, ktoré komunikujú a zdieľajú dáta s inými zariadeniami cez internet.² Iné vymedzujú IoT odkazom na schopnosť denných objektov pripojiť sa k internetu a odosielať a prijímať dáta. Takými sú kamery pripojené k internetu, ktoré umožňujú odosielanie obrázkov online, systémy domácej automatizácie alebo implantovateľné zdravotnícke pomôcky.³ Pojem IoT vo všeobecnosti označuje trend, v ktorom veľké množstvo zariadení využíva komunikačné služby, ktoré ponúkajú internetové protokoly. Mnohé z týchto zariadení, často nazývané inteligentné objekty, nie sú priamo ovládané ľuďmi, ale existujú ako súčasť budov alebo vozidiel, alebo sú rozmiestnené po okolí.⁴ Spoločným ukazovateľom v týchto definíciách je skutočnosť že popisujú scenáre v ktorých sa: „*Sieťová konektivita a výpočtová schopnosť*

¹ Rose, Eldridge, Chapin: The Internet of Things: an Overview, 2015 Dostupné na: https://www.researchgate.net/profile/Ananth_Saradhiz/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

²K Britton.: Handling privacy and security in the Internet of Things Journal of Internet Law, 2016 Dostupné na: <https://www.coursehero.com/file/16667577/Handling-Privacypdf/>

³ Federal Trade Commission: Internet of things: Privacy & security in a connected world. FTC Staff Report, 2015 Dostupné na: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staffreport-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

⁴ D Thaler, M Tschofenig: Architectural Considerations in Smart Object Networking, 2015 Dostupné na: <https://www.ietf.org/proceedings/92/slides/slides-92-ia6-techplenary-2.pdf>

*zariadení sa rozširuje na konšteláciu objektov, zariadení, senzorov a každodenných položiek, ktoré sa bežne nepovažujú za počítače čo umožňuje zariadeniam generovať, vymieňať a konzumovať dáta, často s minimálnym zásahom človeka.*⁵ Nesúrodé definície by mohli byť zdrojom nejasností v otázkach vecí internetu. Rôzne definície však nemusia nevyhnutne navzájom oponovať, ale skôr zdôrazňujú rôzne aspekty fenoménu z rôznych pohľadov a spôsobov použitia. Otázkou času však ostáva či je potrebné vypracovať jednotnú definíciu IoT. Pre ďalšiu identifikáciu IoT z pohľadu tejto práce sa budem prikláňať k definícií podľa ktorého IoT je systém zariadení, mechanických a digitálnych strojov, ako aj každodenných objektov, ktoré sú schopné prenosu údajov cez informačnú sieť aj bez interakcie človeka.

Rozsiahla implementácia IoT prístrojov sľubuje transformáciu mnohých aspektov spôsobu života. IoT zariadenia menia náš životný štýl tým, že šetria čas a zdroje, pričom vytvárajú nové šance na rast, inováciu a prenos vedomostí⁶. Technologický vývoj je hodnotou, a preto je dôležité predchádzať akémukoľvek pokusu podvodného zneužitia.⁷ Nové produkty, ako sú internetové zariadenia, komponenty domácej automatizácie a zariadenia na správu energie, nás posúvajú k vízii inteligentnej domácnosti, ktoré ponúkajú väčšiu bezpečnosť a energetickú účinnosť. Osobné IoT zariadenia, ako nositeľné zariadenia na sledovanie zdravotného stavu a zdravotnícke pomôcky pre zdravotne postihnutých, transformujú spôsob poskytovania zdravotnej starostlivosti. Systémy IoT, ako sú inteligentné vozidlá, dopravné systémy a senzory zabudované do ciest, nás približujú k myšlienke inteligentných miest. Technológia IoT ponúka možnosť transformovať aj poľnohospodárstvo, priemysel, výrobu a energetiku. IoT „*umožňujú organizáciám spravovať aktíva, maximalizovať výkonnosť a rozvíjať nové obchodné modely, má tiež potenciál zvýšiť energetickú účinnosť a optimalizovať rôzne druhy dopravy a mobility.*“⁸ Zatiaľ čo prínosy internetu vecí sú nepopierateľné, ich ostrá

⁵ Rose, Eldridge, Chapin: The Internet of Things: an Overview, 2015 Dostupné na: https://www.researchgate.net/profile/Ananth_Saradhiz/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

⁶ Tamtiež

⁷ N Fabiano: Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation, 2017 Dostupné na: <https://www.athensjournals.gr/law/2017-3-3-2-Fabiano.pdf>

⁸ P Vermesan, O Friess: Internet of things-From research and innovation to market development (ed.), 2014 Dostupné na: https://www.researchgate.net/publication/263970385_Internet_of_Things_-_From_Research_and_Innovation_to_Market_Deployment_Chapter_4_-_Internet_of_Things_Global_Standardisation_-_State_of_Play

kritika spočíva v skutočnosti, že vývoj bezpečnosti v tejto oblasti nie je v súlade s tempom inovácií⁹. Koncept sféry IoT je veľmi široký a zahŕňa aj kritickú infraštruktúru.

Zodpovednosť zariadení IoT

Zodpovednosť ako právny pojem je vo všeobecnosti vždy spájaná s porušením určitých práv alebo povinností ustanovenej v právnej norme. Každé takéto porušenie práv alebo povinností je spojený s určitým zodpovednostným následkom ktorú zákon predvída. „*Teória i prax sa prikláňa k názoru, že pod pojmom zodpovednosti treba rozumieť následnú (sekundárnu) povinnosť vznikajúcu subjektu, ktorý porušil primárnu právnu povinnosť vyplývajúcu mu zo zákona alebo z inej právnej skutočnosti.*“¹⁰ Obsahom právnej zodpovednosti je preto oprávnenie verejno-mocenského orgánu prejednávať porušenie zodpovednosti a následne možnosť ukladania sankcií.

Predpoklady vzniku právnej zodpovednosti sú:

- a) Protiprávne konanie subjektu - t.j. porušenie práv alebo povinností zakotvených v právnych normách,
- b) Nepriaznivý následok - t.j. škoda na majetku, ujma na zdraví, atď.,
- c) Kauzálny nexus - t.j. príčinná súvislosť medzi protiprávnym konaním subjektu a vzniknutým nepriaznivým následkom,
- d) Zavinenie (vyžaduje sa iba v prípadoch subjektívnej zodpovednosti).

Je však treba podotknúť, že tieto zariadenia fungujú oveľa komplexnejšie ako jednoduché obyčajné produkty, z čoho vyplýva, že bude potrebné zvážiť komplexnejšie scenáre

⁹ DHS: Strategic principles for securing the internet of things (IoT), 2016 Dostupné na: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

¹⁰Krajský súd Košice(S Zborovjanová): 5Co/336/2016, 2017 Dostupné na: <http://judikatura.jinepravo.cz/5f03b217-edd5-43f3-a9ca-257deb3a90bo:b2d8e2ff-6796-4dbf-b91d-d220d4f35c7f.xml>

zodpovednosti¹¹. Tieto skutočnosti viedli k nahromadeniu otázok medzi odborníkmi akými sú Peppet¹², Clubb a kol.¹³ Rose a kol.¹⁴, McMahon¹⁵ alebo Booz Allen Hamilton¹⁶.

Najdôležitejšou otázkou pri zodpovednosti zariadení IoT však ostáva určenie subjektu, ktorý bude musieť zniesť následky, ak dôjde ku škode alebo k poškodeniu osoby v dôsledku konania alebo nečinnosti zariadenia IoT. Odpoveď v mnohých prípadoch je veľmi komplikovaná a ešte nie je ani dostatok judikatúry, ktorá by pomohla pri riešení tejto otázky. Vzhľadom na to že zariadenia IoT sa dokážu navzájom prepojiť zariadenia od rôznych výrobcov, je možné aby používateľ vlastnil inteligentnú chladničku od výrobcu A, inteligentný kávovar od výrobcu B a inteligentný vysávač od výrobcu C, pričom je všetko ovládané inteligentným telefónom od výrobcu A, ktorý prevádzkuje softvér IoT, ktorý vytvoril vývojár softvéru tretej strany. *„Takéto prepojenie zariadení IoT vytvára komplexný reťazec, pri ktorom je oveľa ťažšie určiť, kto je zodpovedný podľa tradičných zákonov a predpisov, keď sa niečo pokazí.“*¹⁷

Aj pri najjednoduchšom zodpovednostnom scenári, ak sa chytrý hriankovač prehreje a spáli dom, má majiteľ domu rad potenciálnych kandidátov o ktorých môže tvrdiť, že sú zodpovední. Možné subjekty sa pohybujú od predajcu, výrobcu až po vývojárov aplikácie na telefóne alebo hriankovači¹⁸. Problematickou ostáva aj otázka, či bude jedna strana plne zodpovedná? Alebo budú do určitej miery zodpovedné všetky strany zapojené do vytvárania a spracovania integrovaných dátových komponentov hriankovača.

¹¹ Rose, Eldridge, Chapin: The Internet of Things: an Overview, 2015 Dostupné na: https://www.researchgate.net/profile/Ananth_Saradhiz/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

¹² S Peppet: Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent 2014 Dostupné na: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>

¹³ Clubb, Kirch, Patwa: The ethics, privacy, and legal issues around the internet of things, 2015 Dostupné na: <https://www.ischool.berkeley.edu/sites/default/files/projects/w231-internetofthingsfinalpaper.pdf>

¹⁴ Rose, Eldridge, Chapin: The Internet of Things: an Overview 2015 dostupné na : https://www.researchgate.net/profile/Ananth_Saradhiz/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

¹⁵ McMahon : Internet of things: A privacy law case study, 2015 Dostupné na: https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?referer=https://www.google.sk/&httpsredir=1&article=1000&context=stu_papers

¹⁶ Booz Allen Hamilton: The field guide to IoT security, 2017 Dostupné na: https://www.actiac.org/system/files/Booz_Allen_Hamilton_IoT_Field_Guide_Small_compressed.pdf

¹⁷ Nolan, Adair: Untangling the Web of liability in the Internet of Things, 2016 Dostupné na: <https://www.mhc.ie/latest/blog/untangling-the-web-of-liability-in-the-internet-of-things>

¹⁸ Tamtiež

Nolan a Adair argumentujú, že pri zodpovednostných scenároch zariadení IoT musíme hľadať zodpovednosť mimo tradičných hraníc zodpovednosti. Ako príklad uvádzajú dopravnú situáciu, keď sa pokazia inteligentné dopravné semaforey a inteligentné vozidlo idúce pod nimi je naprogramované sledovať tieto signály, čo znamená že vozidlo nedokáže zastaviť a spôsobí dopravnú nehodu. V takýchto prípadoch by sa zdalo neprimerané brať na (tradičnú) zodpovednosť vodiča za spôsobenie škody, keď „vinníkom“ bol čiastočne nefunkčný semafor a čiastočne aj nefunkčné vozidlo.¹⁹

Na druhej strane nemožno vnímať takéto zlyhanie zariadení ako zodpovednosť iba na strane výrobcov a vývojárov, keďže validným argumentom ostáva skutočnosť že: *„Zariadenia internetu vecí sa používajú a budú sa používať spôsobom a v situáciách, ktorú výrobca neočakáva. Výrobca zariadenia IoT nemôže primerane vykonávať testovanie zabezpečenia výrobku vo všetkých možných prípadoch a situáciách používania zariadení IoT.“*²⁰ Podľa Raffmana a Russoa závažnou prekážkou pri zodpovednosti zariadení IoT je aj skutočnosť, že vo väčšine krajín sveta je právna úprava zodpovednosti za výrobky upravené tak, že je zodpovednosť obmedzená na tie prípady, pri ktorých žalobca utrpel aspoň určitý stupeň hmatateľnej škody (t.j. fyzické zranenie alebo majetková ujma). Žalobca vo všeobecnosti neuspje so žalobou na náhradu škody ak výrobok spôsobil iba hospodárske alebo iné nehmotné škody. V dôsledku toho, ak spotrebitelia utrpeli iba ekonomickú ujmu (napr. kúpnu cenu chybného výrobku), budú sa pokúšať podať iné žaloby za iné právne porušenie (ako porušenia záruky, podvod alebo nekalú súťaž).²¹

Ochrana súkromia a osobných údajov

Zariadenia internetu vecí (Internet of Things - ďalej ako „IoT“) vytvárajú jedinečné problémy ktoré presahujú tradičné chápanie a problémy súkromia a ochrany osobných údajov²². Je

¹⁹ Tamtiež

²⁰ Rose, Eldridge, Chapin: The Internet of Things: an Overview, 2015 Dostupné na: https://www.researchgate.net/profile/Ananth_Saradhiz/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

²¹ M Raffman a A Russo: Mitigating Transactional Risk in the Internet of Things, 2018 Dostupné na <https://www.goodwinlaw.com/-/media/files/publications/the-journal-of-private-equity-mitigating-transacti.pdf>

²² Pre súvislosť ochrany súkromia a ochrany osobných údajov pozri bližšie: O. Lynskey: Foundations of Eu Data protection Law, 2015 Dostupné na <https://books.google.sk/books?hl=sk&lr=&id=jCXYCgAAQBAJ&oi=fnd&pg=PP1&dq=Lynskey:+Foundations+o>

preto potrebné položiť nové kľúčové otázky pri reevaluácii modelov ochrany súkromia a ochrany osobných údajov v kontexte internetu vecí.²³

Kumulácia inteligentných zariadení okolo človeka vytvára falošný pocit bezpečia, čím povzbudzuje jednotlivcov k tomu, aby odhalili citlivé alebo súkromné informácie bez toho, aby si boli plne vedomí alebo dokázali odhadnúť potenciálny dopad a dôsledky takejto situácie. Zariadenia IoT dokážu zhromažďovať informácie s nevídaným stupňom špecifickosti a prenikavosti, a následná agregácia a korelácia týchto údajov môže vytvoriť podrobné profily jednotlivcov, ktoré vytvárajú potenciál pre profilovanie, diskrimináciu ako aj iným hrozbám.²⁴

Netradičný model

*„V dobe kedy sa informácie prenášajú a spracúvajú elektronicky a digitálne prostredníctvom informačných a komunikačných technológií sa problematika bezpečnosti spája najmä s pojmami **informačná bezpečnosť a kybernetická bezpečnosť**“*²⁵ Otázky bezpečnosti dát a ochrany osobných údajov sú pri zariadeniach IoT úzko prepojené, keďže zariadenia IoT pracujú najmä s osobnými informáciami o používateľoch.

Jedinečnosť zariadení IoT spôsobuje, že keď nastane kybernetický bezpečnostný incident²⁶, pri ktorom dôjde k narušeniu integrity dát, ktoré zariadenie spracovávalo (ktoré obsahovali

[f+Eu+Data+protection+Law,+&ots=iWjo65HBFa&sig=nony27JofPHormaawBX_8d_z6fM&redir_esc=y#v=onepage&q=Lynskey%3A%20Foundations%20of%20Eu%20Data%20protection%20Law%2C&f=false](https://www.researchgate.net/profile/Sandra-Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf)

²³N Fabiano: Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation 2017 Dostupné na: <https://www.athensjournals.gr/law/2017-3-3-2-Fabiano.pdf>

²⁴S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 Dostupné na : https://www.researchgate.net/profile/Sandra-Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

²⁵J Andraško: Bezpečnosť a ochrana súkromia, 2019 Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Publikacne_vystupy/2019/Monografia_DVSEI_2019.pdf

²⁶J Andraško : Bezpečnosť informačných systémov verejnej správy vo svetle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe, 2019 Dostupné z: https://journals.muni.cz/revue/issue/view/issue/20/pdf_18

osobné údaje používateľa), zároveň dochádza aj k porušeniu osobných údajov²⁷(t.j. „je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchováajú alebo inak spracúvajú, alebo neoprávnený prístup k nim;“)²⁸ „V tomto kontexte je nutné poznamenať, že teória aj prax má tendenciu aplikovať definíciu osobného údajú značne extenzívne a dochádza tak k situácií, keď každá informácia má potenciál figurovať ako osobný údaj“²⁹

Tradičný model ochrany osobných údajov, ktorý je postavený na systéme „**oznámení a súhlasu**“ kde používatelia uplatňujú svoje preferencie ochrany osobných údajov tým, že priamo komunikujú s informáciami prezentovanými na obrazovke počítača alebo mobilného telefónu (napríklad kliknutím na položku „Súhlasím“) je však u zariadení IoT neefektívny, keďže zariadenia IoT často nemajú žiadne používateľské rozhranie na konfigurovanie preferencií ochrany osobných údajov. Navyše pri mnohých konfiguráciách zariadení IoT nie je jednoduché získať vedomosti (ani kontrolu nad spôsobom), akým sa osobné údaje zhromažďujú a používajú.³⁰

Problémom je aj fakt že zariadenia IoT často fungujú aj v kontextoch a spôsobom, v ktorých blízkosť ľudí spôsobuje zhromažďovanie údajov všetkých subjektov.³¹ (Napríklad, senzor geolokácie vo vozidlách zaznamenáva údaje o polohe všetkých cestujúcich vo vozidle, bez ohľadu na to, či všetci cestujúci chcú svoju polohu sledovať alebo nie.) V takýchto situáciách je nemožné rozlišovať individuálne preferencie jednotlivcov ohľadne ochrany ich osobných údajov.

²⁷Pozri bližšie stanovisko WP29, dostupné na : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

²⁸GDPR článok 4 ods 12, 2018 Dostupné na : <https://gdpr.algolia.com/gdpr-article-4>

²⁹M, Mesarčík: Výkon verejnej správy prostredníctvom údajov - výzva digitálnej ekonomiky a štátu? 2018, Dostupné na : https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/milniky_zborniky_2011_2018/Zbornik_Milniky_2018.pdf

³⁰Pozri bližšie stanovisko WP29, Dostupné na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

³¹Rose, Eldridge, Chapin: The Internet of Things: an Overview, 2015 Dostupné na: https://www.researchgate.net/profile/Ananth_Saradhiz/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

Výzvy z pohľadu zariadení IoT v oblasti súkromia a ochrany osobných údajov

Najvýznamnejšie výzvy z pohľadu zariadení IoT v oblasti ochrany súkromia a osobných údajov predstavujú³²

- a) Diskriminácia a Profilovanie;
- b) Udelenie súhlasu;
- c) Dôvera a Transparentnosť

Diskriminácia a Profilovanie

Inteligentné zariadenia potrebujú zhromažďovať dáta a následne vyvodzovať závery, aby mohli fungovať správne. Súčasne ale takéto zhromažďovanie informácií môže viesť k narušeniu súkromných životov užívateľov.

Zatiaľ čo väčšina získaných údajov zo zariadení internet vecí sú neškodné, a majú slúžiť iba pre poskytnutie osobnejšieho zážitku používateľa, nemožno vylúčiť, že iné získané informácie nebudú zneužit napríklad práve na diskrimináciu. *„Súčasná antidiskriminačná zákony nie sú pripravené riešiť diskrimináciu na základe zariadení internetu vecí, v ktorej sa odhalia informácie ohľadne užívateľov. Tento druh získavania informácií o užívateľoch otvorí dvere novým formám diskriminácie.“*³³

Používatelia zariadení internet vecí sú často bezmocní pri prevencii potenciálnych hrozieb, akým je aj diskriminácia kvôli nedostatočne možnej kontrole. V súčasnosti pri zariadeniach internet vecí používatelia nemajú takmer žiadnu schopnosť definovať obmedzenia ohľadne zverejňovania totožnosti alebo citlivých informácií.

Všeobecné obavy o ochranu osobných údajov sú u zariadení internet vecí znásobené o spôsob, akým tieto zariadenia rozširujú možnosť a dosah sledovania a získavanie informácií.

³² S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 Dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

³³S Peppet: Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent, 2014 Dostupné na: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>

„Charakteristiky zariadení internetu vecí a spôsobov ako sa používajú, predefinujú celú otázku akým spôsobom sa zbierajú, analyzujú, používajú a chránia osobné údaje.“³⁴

Podľa S. Wachterovej existujú najmenej tri možné spôsoby monitorovania a profilovania vo sfére internet vecí, ktoré môžu slúžiť ako základ pre diskrimináciu:³⁵

- a) Zhromažďovanie údajov, ktoré vedú k záverom o osobe (napríklad správanie pri prehliadaní internetu);
- b) Profilovanie vo všeobecnosti, prostredníctvom prepojenia údajov zo zariadení IoT (tiež nazývaná ako "senzorová fúzia");
- c) Profilovanie, ku ktorému dochádza keď sú údaje zdieľané s tretou stranou, ktorá kombinuje údaje s inými dátovými súbormi (napr. zamestnávateľ, poisťovňa).

Najväčšiu výzvu pre tému diskriminácie predstavuje efekt senzorovej fúzie, kde okrem toku zozbieraných údajov z jedného zariadenia môžu byť vyvodené širšie závery v kombinácii s inými údajmi. Ako príklad senzorovej fúzie môžeme uviesť „Smart-watches“ zariadenia, ktoré vytvárajú prehľad o zdravotnom stave užívateľa (najmä srdcovej frekvencie), pričom zaznamenávajú aj údaje o pohybe používateľa (geolokácia, vykonané kroky za deň atď.).

Tieto údaje by mohli byť relevantné napríklad pre potenciálnych budúcich zamestnávateľov, ktorí by na základe tých informácií mohli vyvodiť závery ohľadne návykov uchádzača *ako sú*: životospráva, požívanie alkoholu alebo drog, fajčenie, nedostatok spánku (práve tieto skutočnosti boli spájané so zlým psychickým stavom, zdravotnými problémami a slabým kognitívnym výkonom).

Tieto obavy sa odrážajú aj v Nariadení Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe

³⁴Rose, Eldridge, Chapin: The Internet of Things: an Overview, 2015 Dostupné na: https://www.researchgate.net/profile/Ananth_Saradhiz/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

³⁵S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 Dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej ako GDPR), najmä v článku 21 (Právo na námietku) a v článku 22 (Automatizované individuálne rozhodovanie vrátane profilovania). Článok 21 zavádza právo dotknutých osôb kedykoľvek namietat' proti spracovaniu údajov. Ak je účelom spracovania údajov priamy marketing, subjekt údajov má absolútne právo na námietku³⁶. Vo všetkých ostatných prípadoch sa spracovanie údajov musí zastaviť, pokiaľ správca údajov nemôže preukázať **nevyhnutné oprávnené dôvody** na spracúvanie (ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby). Problematickou však ostáva skutočnosť že GDPR bližšie nedefinuje pojem „nevyhnutné oprávnené dôvody“. Článok 22 zavádza dodatočné záruky proti automatizovanému rozhodovaniu vrátane profilovania.³⁷

Udelenie súhlasu

Systém sa považuje za dôveryhodnú ak umožňuje používateľom dohľad a voľbu nad spôsobom ako zariadenia komunikujú a podnikajú kroky v mene používateľa, a teda aj to ako sa zdieľajú ich osobné údaje generované zo zariadenia.³⁸

Aby udelenie súhlasu za účelom komunikácie, zdieľania alebo spracovania údajov mohlo byť efektívne, musí nejakým spôsobom odrážať preferencie a záujmy používateľa.³⁹ Udelenia súhlasu v praxi je možné nastaviť mnohými spôsobmi (pri niektorých spôsoboch si používatelia môžu vybrať z nastavených predvolieb, ktoré sa automaticky premietajú do oprávnení špecifických pre zariadenie alebo používateľa. Je tiež možné zakomponovať používateľské nastavenia pri prístupe explicitnejšie a presnejšie, takéto systémy kontroly prístupu sú založené na úlohách. Takéto nastavenia môžu napríklad poskytnúť používateľom

³⁶GDPR článok 21, 2018 Dostupné na: <https://gdpr.algolia.com/gdpr-article-21>

³⁷M Mesarčík. : Policačné profilovanie v kontexte základných ľudských práv a slobôd, 2019 Dostupné na : <http://alis.uniba.sk:9909/lib/item?id=chamo:361987&fromLocationLink=false&theme=EPC>

³⁸S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

³⁹Roman, Najera a Lopez,: Securing the Internet of Things, 2011 Dostupné na: <https://www.nics.uma.es/pub/papers/1633.pdf>

kontrolu jednotlivo nad oprávneniami zariadenia)⁴⁰, nehladiac však na spôsob alebo formu udelenia súhlasu, najdôležitejším faktom ostáva to, aby používateľ udelil súhlas slobodne a plne rozumejúc na čo udeľuje súhlas.

Problematické sa môže stať situácia ak „schopnosť dotknutých osôb slobodne súhlasiť bude spochybnená, ak nemôžu úplne pochopiť rozsah pôsobnosti súhlasu, kvôli zložitosti politík ochrany osobných údajov.“⁴¹ Pokiaľ ide o ochranu súkromia a informovaný súhlas, GDPR stanovila nové normy v celej Európe. Článok 25 vytvára pre prevádzkovateľov údajov všeobecnú povinnosť implementovať ochranu osobných údajov a ochrany súkromia podľa stanovených mechanizmov⁴². V článku 25 sa uvádza, že správcovia údajov musia vziať do úvahy *"So zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb"*⁴³ pri spracúvaní osobných údajov.

Všeobecné zásady uvedené v článku 5 sa musia tiež riadiť technickými a organizačnými opatreniami akým je minimalizácia údajov (t.j. *„primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú“*)⁴⁴ a Obmedzené vzhľadom na účel (t.j. *„získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi“*)⁴⁵

⁴⁰S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR 2017 dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

⁴¹„Pojem "politika ochrany osobných údajov" je zavádzajúca, ktorá sa používa iba pod zámenou, ako sa správcovia údajov snažia zbaviť novej zodpovednosti" Dostupné : O Tene a J Polonetsky: Big Data for All: Privacy and User Control in the Age of Analytics, 2013 Dostupné na: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip>

⁴²M Mesarčík : Naozaj sa bojím tmy? Zopár úvah o technologickom determinizme v kontexte ochrany osobných údajov, 2017 Dostupné na : <http://alis.uniba.sk:9909/lib/item?id=chamo:339467&fromLocationLink=false&theme=EPC>

⁴³ GDPR, 2018 Dostupné na: <https://gdpr.algolia.com/sk/gdpr-article-25>

⁴⁴ Tamtiež, písmeno C

⁴⁵ Tamtiež, písmeno B

S cieľom informovať o potenciálnych rizikách zhromažďovania údajov vytvoril GDPR prísnejšie normy týkajúce sa informovaného súhlasu uvedené v článku 7 a 4 a oznamovacej povinnosti článku 13 a 14. Popri potrebe oznamovať možné riziká v spojitosti so spracovaním údajov *"v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho"*⁴⁶ je cieľom článku 7 aj zabrániť nadmernému zhromažďovaniu údajov.

Ako sa uvádza v odseku 4 článku 7 posúdenie, či bol súhlas poskytnutý voľne, bude tiež závisieť od toho *"či sa plnenie zmluvy (...) podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný."* Nadmerné zhromažďovanie údajov môže preto spôsobiť neplatnosť súhlasu⁴⁷.

Obdobné obmedzenie sa nachádza aj v článku 13 ods. 2 písm. e) v ktorom sa uvádza, že pred zberom údajov musí prevádzkovateľ uviesť *"či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov"*, a v článku 5 ods. 1 písmeno C „ primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú"⁴⁸. Tieto ustanovenie vytvárajú právnu požiadavku minimalizovať nadmerné zhromažďovanie údajov.

Dôvera a Transparentnosť

*„Pojem dôvera užívateľa je definovaná ako komplikovaný koncept zakladajúci sa na dôvere, očakávaníach, spoľahlivosti, integrity, bezpečnosti, schopností a iných znakov entity."*⁴⁹ Správa informácií sa zameriava na vytvorenie a udržiavanie dôvery medzi objektmi IoT a užívateľmi

⁴⁶ Tamtiež, ods. 2

⁴⁷ S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 Dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

⁴⁸ GDPR, 2018 Dostupné na : <https://gdpr.algolia.com/sk/gdpr-article-5>

⁴⁹ S Chakraborty, H Choi a MB Srivastava: Demystifying Privacy in Sensory Data: A QoI Based Approach, 2016 Dostupné na: http://www-inf.telecom-sudparis.eu/COURS/CILS-IAAIO/Articles/qoc_and_privacy.pdf

týchto vecí⁵⁰. Dôvera medzi objektmi a subjektmi, ktorí tieto zariadenia používajú sa zakladá autentizáciou používateľa pred komunikáciou alebo prístupom k dátam. Zabránenie prístupu neoprávnených objektov alebo používateľov k systému má za následok zvýšenie dôvery používateľov⁵¹

Transparentnosť zohráva dôležitú úlohu pri zvyšovaní dôvery užívateľov, zvýšenie transparentnosti by sa mohlo doceliť pomocou niekoľko krokov⁵²:

- a) Poskytnite informácií o zbieraní, ukladaní a/alebo spracovaní údajov;
- b) Poskytnúť prehľad o tom, aké osobné údaje boli sprístupnené správcovi údajov a podľa akých pravidiel;
- c) Poskytovať on-line prístup k osobným údajom a ako boli spracované;
- d) Poskytujú možnosti na porovnávanie profilov, ktoré pomáhajú používateľovi predvídať, ako sa dáta zhodujú s príslušnými skupinovými profilmi, čo môže ovplyvniť budúce príležitosti alebo riziká.

GDPR obsahuje niekoľko ustanovení, ktoré zvyšujú dôveru a transparentnosť. Príkladom je článok 35, ktorý hovorí o povinnosti riadiacich pracovníkov vykonať hodnotenie vplyvu ochrany údajov (data protection impact assessment - DPIA) ak budú používať nové technológie alebo metódy akým je aj posúdenie vplyvu na ochranu údajov.

DPIA môže byť veľmi užitočné na zvýšenie dôvery užívateľov, najmä ak sú výsledky zverejnené verejne. V ideálnom prípade by DPIA mala vyhodnotiť súvisiace riziká spracovania údajov a navrhnúť riešenia na zmiernenie identifikovaných rizík.⁵³

⁵⁰C Perera: Context Aware Computing for The Internet of Things: A Survey', 2014 Dostupné na: <https://arxiv.org/pdf/1305.0982.pdf>

⁵¹S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 Dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

⁵²O Tene a J Polonetsky: Big Data for All: Privacy and User Control in the Age of Analytics, 2013 Dostupné na: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip>

⁵³S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 Dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

Okrem toho článok 13 ods. 2 písm. f) a článok 14 ods. 2 písm. g) majú za cieľ informovať subjekty o „*existencii automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a aspoň v týchto prípadoch zmysluplné informácie o použítom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.*“ Tieto ustanovenia sú určené na to, aby subjekty údajov mohli posúdiť riziká ak sa používajú algoritmické metódy pri spracovávaní osobných údajov.

Problematickou sa stáva skutočnosť že v článku 13 ods. 2 písm. f) a článku 14 ods. 2 písm. g) sa výslovne vyžaduje iba vysvetlenie systému ex ante, pričom oznamovacie povinnosti predchádzajú rozhodovaniu. K oznámenie dôjde pred prijatím rozhodnutia v okamihu, keď sa údaje iba zbierajú na spracovanie, potom logicky je potom možné podať vysvetlenie len pred rozhodnutím. Články 13 - 14 sa preto nemôžu použiť ako dôkaz ex post na vysvetlenie konkrétnych rozhodnutí.⁵⁴

GDPR tiež odkazuje na dôveru v štandardoch počítačovej bezpečnosti.⁵⁵ Na tento účel článok 5 definuje všeobecnú zásadu integrity a dôvernosti. Podobne články 33 a 34 opisujú, ako musia prevádzkovatelia údajov reagovať na porušenie bezpečnosti údajov. Každé z týchto ustanovení môže prispieť k transparentnosti a dôveryhodnému vzťahu medzi používateľmi a poskytovateľmi zariadení ako aj samotnými zariadeniami IoT. Keďže sa však oznámenie vyžaduje len v prípadoch „*porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb*“ určenie prahu „vysokého rizika“ bude mať významný vplyv na skutočnú ochranu ponúkanú používateľom zariadení IoT.

Na záver by som iba dodal že otázky ochrany súkromia a ochrany osobných údajov pri zariadeniach IoT by boli náročné, aj keby boli záujmy a motivácie všetkých účastníkov dobre zosúladené. Vieme však, že medzi subjektmi, ktoré sú vystavené zhromažďovaniu osobných

[entification in the Internet of Things Privacy Profiling Discrimination and the GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiling-Discrimination-and-the-GDPR.pdf](https://academic.oup.com/idpl/article/7/2/76/3860948)

⁵⁴ Wachter, Mittelstadt, Floridi: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 2017 Dostupné na : <https://academic.oup.com/idpl/article/7/2/76/3860948>

⁵⁵C Naden: Tackling privacy information management head on: first international standard just published, 2019 Dostupné z : <https://www.iso.org/news/ref2419.html>

údajov (používateľia), a tí ktorí zhromažďujú, analyzujú a používajú údaje (predajca, výrobca, vývojár) existujú nevyvážené vzťahy a záujmy.

Pre zvládnutie týchto otázok je preto primárnou záležitosťou, aby sa dosiahla rovnováha medzi identifikáciou a kontrolou prístupu (informácií) potrebnými na fungovanie zariadení internetu vecí a používateľskými právami na súkromie a ochranou na strane používateľa. Dosiahnutie rovnováhy však nie je jednoduchou úlohou kvôli slabým stránkam v technike kybernetickej bezpečnosti a možnostiam anonymizácie.

Transparentnosť a povedomie o možných rizikách a dôsledkoch používania zariadení IoT je kľúčom pre to, aby si užívatelia mohli urobiť kvalifikované rozhodnutie ako chcú využívať tieto služby.

Záver z praxe

Doterajší výklad vychádzal prevažne z právno-teoretickej roviny, ktorá je pre pochopenie jedinečnosti právnych aspektov zariadení internetu vecí nevyhnutná. Napriek tomu však jestvuje potreba overiť, do akej miery sa identifikované výzvy prejavujú v konkrétnom vnútroštátnom prostredí. Slovenská republika nemá k dispozícii špeciálnu právnu úpravu zameranú výlučne na zariadenia IoT. Fungovanie týchto zariadení je rámčované vo viacerých sekundárnych režimoch a najmä z práva ochrany osobných údajov, kybernetickej bezpečnosti, zodpovednosti za škodu a spotrebiteľského práva.

Základným predpisom zostáva zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“), ktorý však od 1. januára 2025 prešiel zásadnou novelou transponujúcou smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555, známu ako NIS 2. Z hľadiska zariadení IoT je kľúčová povinnosť nahlásiť kybernetický bezpečnostný incident. Podľa § 24 ZoKB je povinný subjekt povinný bez zbytočného odkladu, najneskôr však do stanovenej lehoty, nahlásiť Národnému bezpečnostnému úradu (ďalej len „NBÚ“) kybernetický bezpečnostný incident, ktorý má vplyv na ním poskytovanú službu alebo prevádzkované siete a informačné systémy.

Táto povinnosť je taktiež v súlade s čl. 33 GDPR, ktorý ukladá prevádzkovateľovi povinnosť oznámiť Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „ÚOOÚ SR“)

porušenie bezpečnosti osobných údajov bez zbytočného odkladu, a ak je to uskutočniteľné, do 72 hodín od momentu, keď sa o ňom dozvedel. Praktickým dôsledkom je, že v prípade incidentu týkajúceho sa zariadenia IoT, ktoré spracúva osobné údaje, vzniká prevádzkovateľovi súbežná oznamovacia povinnosť voči dvom rôznym úradom, čo v praxi komplikuje koordináciu a zvyšuje riziko formálnej chyby.

Na vnútroštátnej úrovni implementuje GDPR zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „ZoOOÚ“). § 40 ZoOOÚ ukladá prevádzkovateľovi povinnosť oznamovať ÚOOÚ SR porušenie bezpečnosti osobných údajov v súlade s čl. 33 GDPR, pričom § 41 ZoOOÚ upravuje oznámenie dotknutej osobe podľa čl. 34 GDPR. Špecifikum slovenského prostredia nespočíva v obsahu týchto ustanovení, ale v ich aplikácii. ÚOOÚ SR doteraz nevydal v oblasti IoT zamerané metodické usmernenie, ktoré by jednoznačne vymedzilo, kedy sa má u zariadení s obmedzeným používateľským rozhraním považovať súhlas za platný.

Z hľadiska zodpovednosti za škodu spôsobenú vadným výrobkom zostáva kľúčovým zákon č. 294/1999 Z. z. o zodpovednosti za škodu spôsobenú vadným výrobkom (ďalej len „ZoZŠV“). Podľa § 1 ods. 1 ZoZŠV výrobca zodpovedá za škodu na zdraví spôsobenú vadou jeho výrobku; podľa § 1 ods. 2 ZoZŠV zodpovedá aj za škodu na veci inej ako je vadný výrobok, ak je škoda vyššia ako hodnota stanovená osobitným predpisom. Výrobcom sa podľa § 2 ZoZŠV rozumie aj osoba, ktorá zariadenie zostavila alebo ho označila svojím menom alebo obchodnou značkou.

Vedľajšou, no nemenej dôležitou rovinou je všeobecná zodpovednosť za škodu podľa § 420 ods. 1 Občianskeho zákonníka č. 40/1964 Zb. (ďalej len „OZ“), podľa ktorého každý zodpovedá za škodu, ktorú spôsobil porušením právnej povinnosti. V praxi to znamená, že ak používateľ zariadenia IoT spôsobí konaním (napr. neodborným nastavením zariadenia) škodu, môže byť volaný na zodpovednosť podľa § 420 OZ, no, ako už bolo vyššie uvedené, určenie skutočného pôvodcu škody v komplexnom reťazci výrobca–vývojár–prevádzkovateľ–používateľ zostáva jednou z najzložitejších otázok aj v slovenskom kontexte. Tento problém sa zhoršuje skutočnosťou, že § 5 ods. 1 písm. b) ZoZŠV umožňuje výrobcovi zbaviť sa zodpovednosti, ak preukáže, že chyba, ktorá spôsobila škodu, vznikla až po uvedení výrobku

do obehu, čo v prípade IoT zariadení, ktoré sa neustále aktualizujú, môže viesť k možnosti obrany, ktorá spochybňuje účinnosť tohto režimu.

Pre vzťah medzi používateľom-spotrebiteľom a predajcom zariadenia IoT je určujúci zákon č. 108/2024 Z. z. o ochrane spotrebiteľa (ďalej len „ZoSP“), ako aj nariadenie (EÚ) 2023/988 o všeobecnej bezpečnosti výrobkov (GPSR), resp. zákon č. 56/2018 Z. z. o posudzovaní zhody výrobku (ďalej len „právne predpisy v oblasti bezpečnosti výrobkov“). Tie ukladajú výrobcovi a dovozcom povinnosť uvádzať na trh len bezpečné výrobky t. j. výrobky, ktoré za obvyklých alebo predvídateľných podmienok použitia nepredstavujú riziko pre zdravie a bezpečnosť osôb. V kontexte IoT je pojem „predvídateľné podmienky použitia“ problematický: ako už bolo uvedené, používatelia zariadenia často používajú spôsobom, ktorý výrobca nemohol predvídať, čo komplikuje posudzovanie „bezpečnosti“ v zmysle uvedenej legislatívy.

Dôležitým vývojom je pripravovaná transpozícia nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 o požiadavkách na kybernetickú odolnosť produktov s digitálnymi prvkami (Cyber Resilience Act), ktoré priamo upravuje bezpečnostné požiadavky na výrobky IoT a ukladá výrobcovi povinnosť zabezpečiť bezpečnosť výrobku počas jeho celého životného cyklu. Jeho aplikácia na slovenskom národnom prostredí bude vyžadovať novelizáciu ZoBP a pravdepodobne aj ZoRVV, čím by sa rozptýlená fragmentácia, ktorá doteraz znemožňovala komplexný pohľad na IoT, čiastočne prekonala.

Analýza slovenského právneho kontextu potvrdzuje závery komparatívnej časti: jedinečnosť právnych aspektov zariadení IoT sa prejavuje tromi spôsobmi. Po prvé, fragmentácia právnej úpravy medzi štyrmi a viacerými zákonmi s rozdielnymi účelmi (ochrana osobných údajov, kybernetická bezpečnosť, zodpovednosť za škodu, ochrana spotrebiteľa) vedie k tomu, že žiadny z nich neposkytuje komplexnú odpoveď na otázky, ktoré IoT vyvoláva. Po druhé, absencia cielenej judikatúry a metodických usmernení znamená, že teoretické problémy zostávajú v aplikačnej rovine nevyriešené. Po tretie, dynamický vývoj práva EÚ najmä smernica NIS 2 a Cyber Resilience Act sa premietne do slovenskej úpravy oneskorane, ale zásadne, čím sa osobitosti dnes ešte nezavriešaného národného rámca stanú v nasledujúcom období predmetom častejších úprav.

Bibliografia

Booz Allen Hamilton: The field guide to IoT security, 2017 Dostupné na: https://www.actiac.org/system/files/Booz_Allen_Hamilton_IoT_Field_Guide_Small_compressed.pdf

C Naden: Tackling privacy information management head on: first international standard just published, 2019 Dostupné z : <https://www.iso.org/news/ref2419.html>

C Perera: Context Aware Computing for The Internet of Things: A Survey', 2014 Dostupné na: <https://arxiv.org/pdf/1305.0982.pdf>

Clubb, Kirch, Patwa: The ethics, privacy, and legal issues around the internet of things, 2015 Dostupné na: <https://www.ischool.berkeley.edu/sites/default/files/projects/w231-internetofthingsfinalpaper.pdf>

D Thaler, M Tschofenig: Architectural Considerations in Smart Object Networking, 2015 Dostupné na <https://www.ietf.org/proceedings/92/slides/slides-92-iab-techplenary-2.pdf>

DHS: Strategic principles for securing the internet of things (IoT), 2016 Dostupné na: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Federal Trade Commission: Internet of things: Privacy & security in a connected world. FTC Staff Report, 2015 Dostupné na: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staffreport-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

GDPR, 2018 Dostupné na: <https://gdpr.algolia.com/sk/gdpr-article-25>

J Andraško : Bezpečnosť informačných systémov verejnej správy vo svetle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe , 2019 Dostupné z : https://journals.muni.cz/revue/issue/viewissue/20/pdf_18

K Britton.: Handling privacy and security in the Internet of Things Journal of Internet Law, 2016 Dostupné na: <https://www.coursehero.com/file/16667577/Handling-Privacypdf/>

Krajský súd Košice(S Zborovjanová): 5Co/336/2016, 2017 Dostupné na: <http://judikatura.jinepravo.cz/5f03b217-edd5-43f3-a9ca-257deb3a90bo:b2d8e2ff-6796-4dbf-b91d-d220d4f35c7f.xml>

M Mesarčík : Naozaj sa bojím tmy? Zopár úvah o technologickom determinizme v kontexte ochrany osobných údajov, 2017 Dostupné na : <http://alis.uniba.sk:9909/lib/item?id=chamo:339467&fromLocationLink=false&theme=EPC>

M Mesarčík. : Policajné profilovanie v kontexte základných ľudských práv a slobôd, 2019 Dostupné na : <http://alis.uniba.sk:9909/lib/item?id=chamo:361987&fromLocationLink=false&theme=EPC>

M Raffman a A Russo: Mitigating Transactional Risk in the Internet of Things, 2018 Dostupné na <https://www.goodwinlaw.com/-/media/files/publications/the-journal-of-private-equity-mitigating-transacti.pdf>

M, Mesarčík: Výkon verejnej správy prostredníctvom údajov - výzva digitálnej ekonomiky a štátu? 2018, Dostupné na : https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/milniky_zborniky_2011_2018/Zbornik_Milniky_2018.pdf

N Fabiano: Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation, 2017 Dostupné na: <https://www.athensjournals.gr/law/2017-3-3-2-Fabiano.pdf>

Nolan, Adair: Untangling the Web of liability in the Internet of Things, 2016 Dostupné na: <https://www.mhc.ie/latest/blog/untangling-the-web-of-liability-in-the-internet-of-things>

Tene a J Polonetsky: Big Data for All: Privacy and User Control in the Age of Analytics, 2013 Dostupné na: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip>

O. Lyskey: Foundations of Eu Data protection Law, 2015 Dostupné na https://books.google.sk/books?hl=sk&lr=&id=jCXYCgAAQBAJ&oi=fnd&pg=PP1&dq=Lynsk ey:+Foundations+of+Eu+Data+protection+Law,++&ots=iWjo65HBFa&sig=nony27JofPHor maawBX_8d_z6fM&redir_esc=y#v=onepage&q=Lynskey%3A%20Foundations%20of%20Eu%20Data%20protection%20Law%2C&f=false

P Vermesan, O Friess: Internet of things-From research and innovation to market development (ed.), 2014 Dostupné na: https://www.researchgate.net/publication/263970385_Internet_of_Things_-

From Research and Innovation to Market Deployment Chapter 4 -

Internet of Things Global Standardisation - State of Play

Roman, Najera a Lopez,: Securing the Internet of Things, 2011 Dostupné na: <https://www.nics.uma.es/pub/papers/1633.pdf>

Rose, Eldridge, Chapin: The Internet of Things: an Overview 2015 dostupné na : https://www.researchgate.net/profile/Ananth_Saradhia/post/What_are_the_latest_developments_in_IOT_architectures/attachment/59d6387d79197b8077995b29/AS:397885586853893@1471874724774/download/57.pdf

S Chakraborty, H Choi a MB Srivastava: Demystifying Privacy in Sensory Data: A QoI Based Approach, 2016 Dostupné na: http://www-inf.telecom-sudparis.eu/COURS/CILS-IAAIO/Articles/qoc_and_privacy.pdf

S McMahon : Internet of things: A privacy law case study, 2015 Dostupné na: https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?referer=https://www.google.sk/&httpsredir=1&article=1000&context=stu_papers

S Peppet: Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent 2014 Dostupné na: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>

S Wachter: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017 Dostupné na: https://www.researchgate.net/profile/Sandra_Wachter2/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR/links/5baab8bfa6fdccd3cb73321e/Normative-Challenges-of-Identification-in-the-Internet-of-Things-Privacy-Profiles-Discrimination-and-the-GDPR.pdf

Stanovisko WP29, dostupné na : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Wachter, Mittelstadt, Floridi: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 2017 Dostupné na : <https://academic.oup.com/idpl/article/7/2/76/3860948>