INTERNET VĚCÍ A OCHRANA DAT V EVROPSKÉM KONTEXTU

FRANTIŠEK KASL[*]

ABSTRAKT

Příspěvek je věnován vybraným aspektům Obecného nařízení o ochraně osobních údajů v kontextu internetu věcí. Po úvodním vymezení tohoto technologického trendu je pozornost zaměřena na tři dílčí oblasti úpravy a to s ohledem na specifika internetu věcí. Prvně je otevřena otázka ochranných opatření a pseudonymizace údajů a problémů s tím spojených. Následně je pojednáno o významu posunu k samoregulaci v podobě posouzení vlivu a omezeních, která v tomto směru vyplývají z jiných souvisejících ustanovení úpravy. Jako třetí je zmíněna nově zavedená obecná mandatorní oznamovací povinnost v případě narušení bezpečnosti osobních údajů a také je představen kontext této problematiky v širším než evropském měřítku. V závěru je pojednáno o rizicích, kterým čelí efektivní prosazení nově přijaté úpravy, a výzvách, které je zapotřebí zdolat před jeho účinností.

KLÍČOVÁ SLOVA

internet věcí, ochrana dat, Obecné nařízení o ochraně údajů

ABSTRACT

The contribution is dedicated to selected aspects of the General Data Protection Regulation in the context of the Internet of Things. Following the introductory definition of this new technological trend, the attention is turned to its three par-

[*] Autor je absolventem Právnické fakulty Univerzity Karlovy. Příspěvek byl odpřednášen dne 29. dubna 2016 na X. ročníku konference pro doktorandy a mladé právní vědce COFOLA 2016 v rámci sekce Právní ochrana dat a jejich kontrola. Autorův kontaktní e-mail je frantisek.kasl@gmail.com

tial aspects while taking into account the specifics of the Internet of Things. Firstly is opened the question of protection measures and data pseudonymization and the related problems. Next is addressed the significance of the shift towards self-regulation represented by the impact assessment and restrictions, which follow in this regard from related provisions. As third is mentioned the new general mandatory obligation to notify a personal data breach and the broader than European context of this issue is introduced. In conclusion are addressed the risks, which stand against the putting of the newly adopted regulation into effect, and the challenges, which need to be overcome until its coming into force.

KEYWORDS

Internet of Things, data protection, General Data Protection Regulation

1. ÚVOD DO PROSTŘEDÍ INTERNETU VĚCÍ

Pojem internet věcí je v současné době jedním z často zmiňovaných hesel spojovaných s nejmodernějšími technologickými trendy. Souvisí s ním pokrok ve všech klasických oblastech elektroniky, díky kterému je již nejen technologicky možné, ale především komerčně dostupné, instalovat komunikační moduly do předmětů každodenní potřeby. Na trhu se tedy objevují první řady chytrých zařízení schopných komunikovat dodatečné informace, zpracovávat dodatečné údaje a nabízet díky tomu dosud nedostupné funkce. Předpokládá se, že internet věcí postupně propojí skrze globální síť i předměty, u kterých se takové připojení vymyká našemu běžnému vnímání okolního světa. Analytici předvídají, že internet věcí bude jedna z nejzásadnějších změn v ICT v následující dekádě.[1] Internet věcí slibuje vytvoření globální sítě propojených zařízení od ledničky či termostatu ve vašem domě přes čidla ve vašem voze až po senzory přímo ve vašem těle.[2] To je však pouze část možností, které tento technologický posun přináší. Významné využití se již dnes rýsuje v podobě snížení nákladů výroby a po-

[1] Tech Trends 2014, Inspiring Disruption. [online]. In *Deloitte's annual Technology Trends report 2014*. Delloite, str. 55 [cit. 28.02.2016]. Dostupné z: http://dupress.com/wp-content/uploads/2014/02/Tech-Trends-2014-FINAL-ELECTRONIC_single.2.24.pdf.

[2] KROES, N. Ethical implications of tomorrow's digital society. In SMITH, Ian G. (ed.) *Internet of Things*, New Horizons, 2012, ISBN: 978-0-9553707-9-3, str. 7.

skytování služeb, především v podobě zefektivnění logistiky (např. formou *just-in-time* dodávek), lepšího managementu skladování a distribuce, a obecně eliminace řady funkcí či činností, které bude možné přenechat automatické komunikaci mezi zařízeními a výrobky nebo uživateli služeb.

V tomto lze spatřovat pouze počátek tohoto trendu, jelikož se jedná o využití, která jsou již v současné době aplikována a rozšiřována. Ke globální internetové síti jsou již dnes připojeny nejen v podstatě všechny podstatné infrastrukturní prvky, osobní počítače, mobilní telefony, tablety a nejrůznější další technologické příslušenství, ale také rostoucí výčet běžných předmětů a zařízení od spotřebičů a hraček po zdravotní zařízení[3] či sensory pohybu domácích mazlíčků. Průzkum z roku 2013 odhadl počet připojených zařízení na 4 miliardy v roce 2010, 15 miliard v roce 2012 a predikoval 80 miliard do roku 2020.[4] Tyto dříve futuristické vize jsou dnes vysoce relevantní, a to i v naší české realitě. O tom svědčí například skutečnost, že právě touto dobou je v České republice významnými tržními subjekty spouštěna specifická síť pro internet věcí.[5]

Lze vycházet z toho, že součástí internetu věcí může být prakticky jakýkoliv předmět bez ohledu na jeho rozměry nebo výrobní náklady. O tom, které předměty budou mít komerčně dostupnou „chytrou" verzi zřejmě často rozhodne ekonomická úvaha, zda taková verze skýtá potenciál snížení nákladů např. v logistice nebo zda slibuje zvýšení výnosů např. jako nový produkt nebo lépe cílená reklama.[6] S rostoucí konektivitou a za trvající

[3] Health care. Things are looking app. *The Economist* [online]. 12. 3. 2016, z tištěné edice: Business. [cit. 15. 3. 2016]. Dostupné z: http://www.economist.com/news/business/21694523-mobile-health-apps-are-becoming-more-capable-and-potentially-rather-useful-things-are-looking?fsrc=scn/fb/te/pe/ed/thingsarelookingapp.

[4] *Internet of things: Outlook for the top 8 vertical markets* [online]. IDATE, 2013. [cit. 29. 2. 2016]. Dostupné z: http://www.idate.org/fr/Research-store/Collection/In-depth-market-report_23/Internet-of-Things_785.html.

[5] ÚŠELA, Jan. T-Mobile a SimpleCell v dubnu spouští síť pro internet věcí. Pomůže s parkováním i hlídáním domácích mazlíčků. *Hospodářské noviny* [online]. 22. 2. 2016. [cit. 12. 3. 2016] Dostupné z: http://byznys.ihned.cz/c1-65174540-t-mobile-bude-pomahat-parkovat-a-sledovat-mazlicky-v-dubnu-spusti-sit-pro-internet-veci.

[6] ANDERSON, Janna; RAINIE, Lee. *The Internet of Things Will Thrive by 2025* [online]. Pew Internet Project report, 2014 [cit. 28. 2. 2016]. Dostupné z: http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.

platnosti tzv. *Mooreova zákona*[7] se současně otevírají nové možnosti funkcí a autonomních činností, které tyto předměty v internetu věcí mohou vykonávat. Mluví se o prolomení hranice mezi reálným a virtuálním světem, tedy o konceptu rozšířené reality („*augmented reality*“[8] či „*enhanced reality*“[9]), který se vyznačuje stavem všudypřítomného pokrytí informační sítí, která se stává neopominutelnou (a neodstranitelnou) součástí běžného vnímání světa. U cílených urbanistických infrastrukturních řešení s významným zapojením nejrůznějších senzorů za účelem zvýšení efektivity se mluví o tzv. chytrých městech („*smart cities*“[10]). Tyto moderní prvky zvažují zavést mimo jiné i některá česká města.[11]

V tomto okamžiku je na místě pojem internetu věcí vymezit a klasifikovat nad rámec výše popsaných možných uplatnění a projevů v rámci ekonomiky. Definice pojmu internet věcí je nesnadná, a to především s ohledem na neustálý vývoj technických možností, které lze pod něj podřadit.

---

[7] COFFMAN, Kerry; G. ODLYZKO, Andrew M. Internet growth: Is there a “Moore’s Law” for data traffic?. [online]. In *Handbook of massive data sets*. Springer US, 2002, [cit. 14. 3. 2016]. Dostupné z: http://www.dtc.umn.edu/~odlyZko/doc/internet.moore.pdf.

[8] BARFIELD, Woodrow. *Fundamentals of Wearable Computers and Augmented Reality*. CRC Press. Taylor & Francis Group. 2016. ISBN: 978-1-4822-4351-2; FLORIDI, Luciano. *The Onlife Manifesto*. Being Human in a Hyperconnected Era. Springer International Publishing. 2015. ISBN: 978-3-319-04092-9.

[9] BOWSKILL, Jerry; DOWNIE, John. Extending the capabilities of the human visual system: an introduction to enhanced reality. *ACM SIGGRAPH Computer Graphics - Special focus: modular visualization environments (MVEs)* [online]. Ročník 29. Číslo 2. květen 1995. str. 61-65 [cit. 9. 6. 2016]. Dostupné z: http://dl.acm.org/citation.cfm?id=204378.

[10] Pro více informací viz např. BATTY, M.; AXHAUSEN, K. W.; GIANNOTTI, F.; POZDNOUKHOV, A.; BAZZANI, A.; WACHOWICZ, M.; OUZOUNIS, G.;PORTUGALI, Y. *Smart cities of the future*. [online]. The European Physical Journal Special Topics. listopad 2012. Ročník 214. Číslo 1. str. 481-518. [cit. 9. 6. 2016]. Dostupné z: http://link.springer.com/article/10.1140%2Fepjst%2Fe2012-01703-3 nebo CHOURABI, Hafedh; NAM, Taewoo; WALKER, Shawn; GIL-GARCIA, Ramon J. et al. *Understanding Smart Cities: An Integrative Framework*. [online]. System Science (HICSS), 2012 45th Hawaii International Conference. ISBN: 978-0-7695-4525-7 [cit. 9. 6. 2016]. Dostupné z: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6149291.

[11] LUKÁČ, Petr. Prvním "chytrým" městem v Česku se stane Písek. Firma Schneider Electric bude řídit dopravu i vytápění. *Hospodářské noviny* [online]. 8. 1. 2016 [cit. 15. 3. 2016]. Dostupné z: http://archiv.ihned.cz/c1-65066210-prvnim-chytrym-mestem-v-cesku-bude-pisek-rika-sef-tuzemske-pobocky-schneider-electric; ČERNÝ, Aleš. Firmy začínají kroužit kolem „chytrých měst“. Cítí zakázky za miliardy. *iDnes/Ekonomika* [online]. 12. 3. 2016 [cit. 15. 3. 2016]. Dostupné z: http://ekonomika.idnes.cz/smart-cities-v-cesku-0lm-/ekonomika.aspx?c=A160310_2231323_ekonomika_rny.

Pro účely tohoto příspěvku vycházím z následujícího vymezení: *Internet věcí je koncept, dle kterého každý předmět může být připojen k internetu a sdílet data, čímž se zvyšuje jeho hodnota a využitelnost.*[12] Jedná se tedy o široký pojem, který zahrnuje *komunikační zařízení*, *interakci strojů* (M2M, tzn. *machine to machine*), jakož i tzv. *internet objektů* (*Internet of Objects*). Komunikační zařízení jsou přístroje, pro které je konektivita klíčovou vlastností (např. smartphone, tablet), zatímco M2M jsou předměty se samostatným určením, které jsou vylepšeny komunikačním modulem pro účely automatické komunikace se serverem nebo jinými předměty (např. „chytré" ledničky, gadgety, televizní obrazovky, vozidla, termostaty nebo zdravotní zařízení). Tyto dvě skupiny jsou míněny pod pojmem internet věcí v tomto příspěvku. Nad jeho rámec lze mluvit i o internetu objektů, který je označením pro předměty, které neshromažďují data, ale obsahují identifikační technologii (nejčastěji RFID nebo 2D čárový kód), což jim umožňuje otevřenou komunikaci přednastavených informací (např. obaly, znovupoužitelné přepravní předměty, přístupové karty).[13]

Neopominutelnou složkou internetu věcí, která je výsledkem nových technických možností, ale zároveň předpokladem jejich funkce, je permanentní a rozsáhlý sběr, zpracování a shromažďování údajů. Tyto údaje mohou být vytvářeny senzory, které představují součást internetu věcí, mohou být vnášeny uživatelem nebo mohou být poskytovány z jiných zdrojů dostupných skrze konektivitu zařízení (např. z internetu). Může se jednat o čistě technické údaje, o metadata způsobilá za určitých okolností nebo v kombinaci identifikovat jednotlivce (např. pohyb před senzorem, druh odebraného výrobku ze zařízení apod. v kombinaci se vzorcem chování daného uživatele nebo jeho virtuálním profilem) nebo přímo o osobní údaje (v souladu s jejich vymezením evropským právem). Není zároveň vyloučeno, že shromažďování údajů shodným předmětem při plnění

[12] *Internet of things: Outlook for the top 8 vertical markets* [online]. IDATE, 2013. [cit. 6. 5. 2016]. str. 9. Dostupné z: http://www.sbdi.co.kr/cart/data/info/IDATE_Internet_of_Things_sample.pdf?ckattempt=2.

[13] *Internet of things: Outlook for the top 8 vertical markets* [online]. IDATE, 2013. [cit. 6. 5. 2016]. str. 9. Dostupné z: http://www.sbdi.co.kr/cart/data/info/IDATE_Internet_of_Things_sample.pdf?ckattempt=2.

shodné funkce může v různých situacích představovat odlišnou míru zásahu do soukromí jednotlivce (např. při použití v jednočlenné domácnosti v kontrastu s použitím ve veřejně přístupném zařízení). Je tudíž možné dovodit, že zařízení propojená pomocí internetu věcí mají potenciál zásadně zasahovat do osobní sféry jednotlivců.[14]

Je nad rámec tohoto příspěvku zabývat se navazujícími aspekty, které souvisí se zprostředkovanými důsledky internetu věcí pro soukromí a identitu subjektů osobních údajů. Tím je především míněno další nakládání s údaji shromážděnými a vytvořenými předměty internetu věcí a jejich užití v rámci databází pro účely profilování uživatelů. Zde se jedná o problematiku tzv. *big data*. Tento pojem označuje velké objemy strukturovaných, semi-strukturovaných nebo nestrukturovaných a zároveň personalizovaných, pseudonymizovaných nebo anonymizovaných dat, která jsou shromážděna v databázi a umožňují *data mining.* Tento pojem označuje filtrování nebo kombinování dat za účelem identifikace vzorců chování a vztahových řetězců mezi jednotlivými daty. To může být následně využito pro nejrůznější účely, mimo jiné pro profilování uživatelů, analýzu chování zákazníků, zvyšování efektivity výrobního řetězce, krádež online identity, online sledování nebo hospodářskou špionáž.

Internet věcí představuje zcela novou oblast technologických možností, které je zapotřebí zkoumat ze všech možných úhlů pohledu. Tento příspěvek se však omezuje pouze na částečné řešení otázky: „Jak zohledňuje unijní právo specifické aspekty internetu věcí?“, přičemž cílem je nastínit, do jaké míry nově přijatá úprava ochrany osobních údajů v Evropské unii ve vybraných oblastech reaguje na určité vlastnosti sběru, shromažďování nebo zpracovávání údajů předměty, které spadají pod výše uvedené vymezení internetu věcí.

[14] *IoT Privacy, Data Protection, Information Security* [online]. Fact Sheet of the European Commission, [cit. 28. 2. 2016]. Dostupné z: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753.

2. POTŘEBA NOVÉHO VNÍMÁNÍ OCHRANY OSOBNÍCH ÚDAJŮ

Shromažďování a zpracovávání údajů v rámci internetu věcí představuje zřejmě nejvýznamnější právní aspekt tohoto nového fenoménu. Klíčovým prvkem je totiž permanentní přenos dat, která mohou v řadě případů přímo nebo nepřímo identifikovat subjekt údajů. Zároveň se potenciálně jedná o údaje, které v případě kombinace s jinými údaji (tzv. profilování) mohou zpřístupnit citlivé osobní údaje nebo osobní údaje o vzorci chování, které subjekt údajů může považovat za významný zásah do jeho soukromí. *„Cílem stran zúčastněných na internetu věcí je nabízet nové aplikace a služby prostřednictvím shromažďování a dalšího kombinování těchto údajů o fyzických osobách – ať již za účelem „pouhého“ měření údajů specifických pro prostředí daného uživatele, nebo konkrétního sledování a analýzy jeho zvyklostí. Jinými slovy, internet věcí s sebou zpravidla přináší zpracovávání údajů, které se týkají identifikovaných nebo identifikovatelných fyzických osob, a jsou proto považovány za osobní údaje ve smyslu článku 2 směrnice EU o ochraně údajů.“*[15] (dále jen „Směrnice“[16]).

Skutečnost, že předměty v rámci internetu věcí často zpracovávají údaje, na které se vztahují požadavky na ochranu osobních údajů, nepředstavuje sama o sobě zásadně novou problematiku, na kterou by nebylo možné vztáhnout dosavadní teoretické či praktické závěry a poznatky. To, čím internet věcí představuje novou výzvu v této oblasti, je především nepřeberná různorodost dat, která za různých situací mohou představovat různou formu údajů. Tato variabilita se potenciálně umocňuje v případě, že zařízení pro své funkce užívá autonomní komunikace s jinými předměty, čímž může docházet k akumulaci údajů, které ve své kombinaci představují nepřímý identifikátor osobních údajů.

---

[15] *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. 29 Pracovní skupina, přijaté dne 16. září 2014. [cit. 28. 2. 2016]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_cs.pdf, str. 4.

[16] Směrnice Evropského parlamentu a Rady (ES) č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:31995L0046.

Dále je významný prvek potenciální všudypřítomnosti předmětů internetu věcí, čímž dochází prakticky k situaci, kdy subjekt údajů nemá nejen kontrolu, ale (za určitých okolností) ani povědomí o zařízeních, která o něm sbírají, shromažďují a zpracovávají údaje (a potenciálně v důsledku toho ani o rozsahu sbíraných údajů). Zde lze uvažovat nejen o veřejně přístupných prostorách, popř. cizích či sdílených prostorách nebo zařízeních, ale též např. o dočasně poskytnutých prostorách a pronajatých či vypůjčených předmětech. Nejproblematičtější situace z hlediska současné koncepce práva ochrany osobních údajů nastává, pokud si uživatel ani není vědom skutečnosti, že jsou o něm určitým předmětem sbírány údaje.[17] *„Taková nedostatečná informovanost představuje významnou překážku projevení platného souhlasu podle práva EU vzhledem k tomu, že subjekt údajů musí být náležitě informován. Za těchto okolností nelze podle práva EU takový souhlas využít jako právní základ pro příslušné zpracování údajů.“*[18] Dnes platná úprava oprávněného zpracování údajů v těchto situacích naráží na své limity, které lze jen stěží překonat extenzivním výkladem.[19] *„Pokud není možná účinná kontrola způsobu interakce předmětů ani určení virtuálních hranic na základě určení aktivních nebo neaktivních zón konkrétních věcí, stane se kontrola vytvořeného toku údajů mimořádně obtížnou. Ještě obtížnější bude kontrolovat jejich následné využití, a zabránit tak možnému riziku neplánovaných funkcí.“*[20] Problematikou předvídatelnosti shromažďování osobních údajů

[17] ABDMEZIEM, Riad; TANDJAOUI, Djamel. *Internet of Things: Concept, Building blocks, Applications and Challenges*. [online]. Cornell University Library, 2014. [cit. 28. 2. 2016]. Dostupné z: http://arxiv.org/pdf/1401.6877v1.pdf.

[18] *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. 29 Pracovní skupina, přijaté dne 16. září 2014. [cit. 28. 2. 2016]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_cs.pdf, str. 8.

[19] Pro bližší vymezení nedostatků evropské koncepce práva ochrany osobních údajů, především s ohledem na přílišný důraz na souhlas subjektů viz RUBINSTEIN, Ira. Big Data: The End of Privacy or a New Beginning? NYU School of Law, Public Law Research Paper No. 12-56. [online] 5. 10. 2012 [cit. 6. 5. 2016]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659.

[20] *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. 29 Pracovní skupina, přijaté dne 16. září 2014. [cit. 28. 2. 2016]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_cs.pdf, str. 8.

pro subjekt údajů a vymezením rovnováhy mezi ochranou subjektů osobních údajů a efektivním využitím těchto údajů se zabývalo již několik autorů.[21]

Do budoucna není vyloučeno, že jakýkoliv předmět mimo svého běžného určení (např. žehlička, šatní skříň, sprcha, nádobí) bude také navíc sbírat a sdílet údaje o svém stavu či činnosti, ke které byl využit. Bude tedy zřejmě nad možnosti (nejen) běžného uživatele rozpoznat, v jaké míře je jeho konání v reálném světě transponováno do specifické digitální stopy bez jeho aktivního přičinění. Toto inherentní riziko internetu věcí je navíc nutno vnímat v kontextu dalších, rapidně se rozmáhajících, technologií (např. *cloud computingu*,[22] shromažďování databází *big data*,[23] *data miningu* těchto databází[24] či *self-learning* vlastností moderních algoritmů[25]) a především pak při zohlednění současné podoby nakládání s osobními údaji uživatelů ze strany poskytovatelů nejrůznějších online služeb, kteří si skrze značně jednostranné všeobecné smluvní podmínky zajišťují přístup k rozsáhlým souborům uživatelských dat, která jsou následně běžným předmětem na trhu agregovaných dat pro nejrůznější účely.[26] *„Nárůst množství údajů vytvářených internetem věcí v kombinaci s moderními technikami souvisejícími s analýzou údajů a jejich křížovým přiřazováním může vést k sekundární-*

[21] Např. NISSENBAUM, Helen. *Privacy as contextual intergrity*. [online]. Washington Law Review. 2004. [cit. 9. 6. 2016]. Dostupné z: https://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf nebo CUSTERS, Bart; URŠIČ, Helena. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law* [online] 7. 1. 2016 [cit. 6. 5. 2016]. Dostupné z: http://data-reuse.eu/wp-content/uploads/2016/01/International-Data-Privacy-Law-2016-Custers.pdf.

[22] MELL, Peter, GRANCE, Tim. *The NIST definition of cloud computing*. [online] 2011. [cit. 28. 2. 2016]. Dostupné z: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

[23] MCAFEE, Andrew, et al. Big data. The management revolution. *Harvard Business Review* [online]. 2012, 90.10, str. 61-67. [cit. 29. 2. 2016]. Dostupné z: http://www.rosebt.com/uploads/8/1/8/1/8181762/big_data_the_management_revolution.pdf.

[24] FREITAS, Alex A. *Data mining and knowledge discovery with evolutionary algorithms*. Springer Science & Business Media, 2013, ISBN: 9783662049235.

[25] GORBENKO, Anna; POPOV, Vladimir. Self-learning algorithm for visual recognition and object categorization for autonomous mobile robots. In: *Computer, Informatics, Cybernetics and Applications*. Springer Netherlands, 2012, ISBN: 9789400718388. str. 1289-1295.

mu využívání těchto údajů, které může i nemusí souviset s účelem, k němuž bylo určeno jejich původní zpracování.“[27, 28] V tomto ohledu je nutno vycházet z toho, že ani převážná většina uživatelů internetu si stále není zdaleka vědoma rozsahu, v jakém po sobě zanechávají datovou stopu. Takovou, která je intenzivně a pečlivě analyzována ze strany nejrůznějších třetích subjektů. Bohužel je zřejmě nemístné domnívat se, že by datová stopa vyprodukovaná v rámci internetu věcí unikla stejné či dokonce větší pozornosti těchto subjektů.

Významným bodem je samotné zabezpečení údajů shromažďovaných, zpracovávaných a sdílených zařízeními spadajícími pod internet věcí. V tomto ohledu jde o zařízení, která často obsahují limitované možnosti zabezpečení, vzhledem k (mimo jiné) tlaku na minimální náklady, omezené kapacitě baterií a nízkému výkonu miniaturních procesorů. Zároveň jsou omezené možnosti aktualizace jejich firmwallu a softwaru, jelikož tato zařízení běžně fungují na základě jednoduchých přednastavených algoritmů, které neumožňují dodatečné aktualizace.[29]

---

[26] SPIEKERMANN, Sarah, et al. The challenges of personal data markets and privacy. Electronic Markets. *Electronic Markets* [online]. červen 2015, 161-167. [cit. 28. 2. 2016]. Dostupné z: https://www.researchgate.net/profile/Sarah_Spiekermann2/publication/276129671_The_challenges_of_personal_data_markets_and_privacy/links/55c4c7fb08aeca747d617e4d.pdf.

[27] *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. 29 Pracovní skupina, přijaté dne 16. září 2014. [cit. 28. 2. 2016]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_cs.pdf, str. 9.

[28] V tomto směru se otevírá prostor pro diskusi o uplatnění a vymezení zásady omezení účelu, dle které je zákonnost zpracování vázána na omezení pro účel, pro který byly osobní údaje shromážděny. Tato zásada doznala v Nařízení (viz dále) úpravy, které předcházela rozsáhlá debata, jejímž výsledkem je znění článku 6 odst. 4 Nařízení. Rozbor této problematiky je však nad rámec tohoto příspěvku. Blíže viz např. Opinion 03/2013 on purpose limitation [online]. 29 Pracovní skupina, přijaté dne 2. dubna 2013. [cit. 9. 6. 2016]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[29] Pro podrobnější rozbor viz např. HUI, Suo; JIAFU, Wan; CAIFENG, Zou; JIANQI, Liu. Security in the Internet of Things: A Review. *Computer Science and Electronics Engineering (ICCSEE), 2012* [online]. 23. 3. 2012 [cit. 6. 5. 2016]. Dostupné z: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6188257 nebo ROMAN, Rodrigo; ZHOU Jianying; LOPEZ, Javier. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*. [online]. Ročník 57, Číslo 10, 5. 7. 2013, str. 2266-2279 [cit. 6. 5. 2016]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S1389128613000054.

S ohledem na skutečnost, že již současná síť komunikačních zařízení v podobě počítačů či smartphonů čelí častým a významným případům narušení bezpečnosti, přičemž rozsáhlé úniky osobních údajů[30] nejsou zdaleka tak výjimečné, jak by se z médií zdálo,[31] lze řadu nově připojovaných zařízení označit za články dále oslabující již tak poměrně slabě chráněnou strukturu. Pokud nebude dosaženo celkového zlepšení bezpečnosti v rámci této globální sítě zařízení, může mít tato skutečnost dalekosáhlé důsledky nejen pro subjekty osobních údajů.

3. EVROPSKÉ PRÁVO OCHRANY OSOBNÍCH ÚDAJŮ

Současný stav ochrany osobních údajů v Evropské unii charakterizují různorodé národní úpravy, které do značné míry nesourodě implementují a prosazují evropské snahy o zajištění minimálního standardu ochrany a celkově nepružně reagují na výzvy, které jim kladou nové technologie. Základ byl na evropské úrovni položen již v roce 1995 výše představenou Směrnicí,[32] která byla později v různých dílčích směrech doplňována, např. směrnicí o soukromí a elektronických komunikacích.[33] Značný význam mají v rámci vývoje výkladu evropské úpravy ochrany osobních údajů stanoviska Pracovní skupiny podle čl. 29 Směrnice, která poskytují podrobný vý-

[30] PERLROTH, Nicole; GELLES, David. Russian Hackers Amass over a Billion Internet Passwords. *New York Times.* [online]. 5. 8. 2014 [cit. 16. 3. 2016]. Dostupné z: http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0 ; JOHNSON, Steve. Target Now Says up to 110 Million Consumers Victimized in Breach. *MercuryNews.com* [online]. 1. 10. 2014 [cit. 16. 3. 2016]. Dostupné z: http://www.mercurynews.com/news/ci_24889060/target-now-says-up-to-110.

[31] STUART, Keith; ARTHUR, Charles. PlayStation Network Hack: Why It Took Sony Seven Days to Tell the World. *Guardian*. [online] 27. 1. 2011. [cit. 16. 3. 2016]. Dostupné z: http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony.

[32] Směrnice Evropského parlamentu a Rady (ES) č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:31995L0046.

[33] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:cs:HTML.

klad řady dílčích aspektů Směrnice, jakož i situační aplikací její úpravy (zde je na místě zmínit již několikrát citované Stanovisko 29 Pracovní skupiny č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí).

Pro posledních několik let je typická značná aktivita ze strany Evropské Komise v oblasti ochrany osobních údajů. Část lze připsat naplňování iniciativ v rámci Digitální Agendy pro Evropu, která se zaměřuje na vytvoření Jednotného digitálního trhu a komplexní řešení stěžejních oblastí v souvislosti s informačními a komunikačními technologiemi.[34] Za zásadnější lze ovšem shledat skutečnost, že evropským legislativním procesem prochází posledních několik let návrh nařízení, které má zajistit modernizaci práva ochrany osobních údajů tak, aby bylo schopné dostát požadavkům současnosti i blízké budoucnosti.

4. REFORMA EVROPSKÉHO PRÁVA V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ

V nedávné době dospěl do finále proces modernizace evropské úpravy ochrany údajů, který by měl mít za cíl zapracovat mimo jiné i výše zmíněná rizika spojená s nejnovějšími technologickými trendy v ICT. Dne 4. května 2016 bylo v Úředním věstníku Evropské unie uveřejněno znění Obecného nařízení o ochraně osobních údajů ze dne 27. dubna 2016 (dále jen „Nařízení“).[35] V platnost tudíž vstoupilo dnem 24. května 2016 a účinnost lze očekávat po uplynutí dvouleté legisvakanční lhůty ke dni 25. května 2018.[36]

---

[34] Digitální agenda pro Evropu: klíčové iniciativy [online] MEMO/10/200, Evropská Komise, 19. května 2010. [cit. 16. 3. 2016]. Dostupné z: http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm.

[35] Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS.

[36] Outcome of the Council meeting [online]. 3445th Council meeting, Economic and Financial Affairs, Brussels, 12. 2. 2016 [cit. 13. 2. 2016]. Dostupné z: http://www.consilium.europa.eu/en/.../meetings/, str. 17.

Nařízení představuje cestu k zajištění jednotnějšího standardu ochrany osobních údajů v rámci Evropské unie, přičemž upravuje obecný základ, který je na evropské úrovni i v jednotlivých národních úpravách již nyní dále doplňován a rozšiřován zvláštními právními předpisy jako např. předpisy týkajícími se boje proti praní špinavých peněz.

5. VYBRANÉ BODY ÚPRAVY OBECNÉHO NAŘÍZENÍ O OCHRANĚ ÚDAJŮ

Úprava obsažená v Nařízení je velmi komplexní a bezpochyby nad rámec tohoto stručného pojednání. V následujících oddílech je tudíž poskytnut pouze krátký vhled do tří vybraných aspektů této nové právní úpravy s přihlédnutím ke specifikům internetu věcí. Cílem je identifikovat významné prvky, nikoliv poskytnout řešení nastíněných dílčích otázek.

5.1 OPATŘENÍ OCHRANY OSOBNÍCH ÚDAJŮ A PSEUDONYMIZACE

Nařízení obsahuje velmi flexibilní vymezení požadavků na ochranu osobních údajů, které bude nutno blíže vymezit pro jednotlivé situace, lze však uvítat důraz na minimalizaci údajů jako nosnou myšlenku ochrany údajů.[37] Dvěma výslovně zmíněnými prostředky zajištění zabezpečení jsou pseudonymizace a šifrování osobních údajů.[38] Pojem pseudonymizace osobních údajů je v Nařízení oproti předchozí právní úpravě výslovně definován jako: *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“*[39]

[37] Článek 25 odst. 1 Nařízení.

[38] Článek 32 odst. 1 písm. a) Nařízení.

[39] Článek 4 bod 5 Nařízení.

Pseudonymizace není formou anonymizace.[40] Na rozdíl od anonymizovaných údajů,[41] jde o údaje, které obsahují tzv. nepřímé identifikátory,[42] které mohou sloužit k opětovné identifikaci subjektu údajů, a proto je s nimi nutno i nadále nakládat jako s osobními údaji.[43] Pseudonymizace představuje formu zabezpečení osobních údajů, která vede ke snížení rizika ohrožení osobních údajů za současného uchování vlastností těchto údajů, čímž je (na rozdíl od anonymizace) umožněno jejich další efektivní využití. *„Použití pseudonymizace osobních údajů může omezit rizika pro dotčené subjekty údajů a napomoci správcům a zpracovatelům splnit jejich povinnosti týkající se ochrany údajů.“*[44]

Nařízení v řadě ohledů podporuje její uplatnění,[45] které má zdůrazněný význam např. při posuzování přípustnosti zpracování osobních údajů pro jiný než původně stanovený účel,[46] při naplnění požadavků záměrné a standardní ochrany osobních údajů (*„data protection by design and by default“*)[47] či pro zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.[48]

Skutečnost, že Nařízení takto široce rozeznává tuto formu zabezpečení osobních údajů, lze uvítat jako pragmatickou reakci na současný vývoj nakládání s osobními údaji a na technické možnosti jejich zabezpečení. Vý-

[40] Opinion 05/2014 on Anonymisation Techniques [online]. 29 Pracovní skupina, přijaté dne 10. dubna 2014. [cit. 14. 6. 2016]. Dostupné z: http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf , str. 3.

[41] Anonymizovaný údaj lze vymezit jako osobní údaj, který byl nenávratně změněn tak, že subjekt údajů není možné nadále identifikovat přímo ani nepřímo, a to jak správcem osobních údajů samotným, tak ve spolupráci s kýmkoliv jiným. Blíže viz např. ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework. [online] [cit. 14. 6. 2016] Dostupné z: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123.

[42] Opinion 05/2014 on Anonymisation Techniques [online]. 29 Pracovní skupina, přijaté dne 10. dubna 2014. [cit. 14. 6. 2016]. Dostupné z: http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf , str. 20.

[43] Bod 26 Preambule Nařízení.

[44] Bod 28 Preambule Nařízení.

[45] Bod 29 Preambule Nařízení.

[46] Článek 6 odst. 4 písm. e) Nařízení.

[47] Článek 25 Nařízení.

[48] Článek 89 odst. 1 Nařízení.

znam zohlednění této formy zabezpečení zdůrazňuje ve svém doporučení o variantách reformy EU v oblasti ochrany údajů i Evropský inspektor ochrany údajů (EIOÚ).[49]

Pseudonymizace hraje již dnes významnou roli v rámci medicíny, klinického výzkumu a databází obsahujících údaje o zdravotním stavu.[50] Značná pozornost jí je věnována také v kontextu internetu věcí, big data či cloud computingu,[51] jelikož představuje jedno z možných řešení zabezpečení osobních údajů při současném uchování možnosti jejich komerčního využití.

S ohledem na výše zmíněnou podporu uplatnění pseudonymizace v režimu Nařízení lze očekávat, že značná část osobních údajů shromažďovaných a zpracovávaných v rámci internetu věcí bude takto zabezpečena. Zde bude dle mého názoru hrát významnou roli i zakotvení koncepce záměrné a standardní ochrany osobních údajů v článku 25 Nařízení. Ta požaduje začlenění prvků ochrany osobních údajů již ve fázi vývoje výrobku, namísto dnes

[49] Stanovisko EIOÚ 3/2015, Velká příležitost pro Evropu, Doporučení EIOÚ o variantách reformy EU v oblasti ochrany údajů ze dne 28. července 2015 [online]. Evropský inspektor ochrany údajů. [cit. 12. 3. 2016]. Dostupné z: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_CS.pdf, str. 6.

[50] Např. ARNING, Marian; FORGÓ, Nikolaus; KRÜGEL, Tina. Data protection in grid-based multicentric clinical trials: killjoy or confidence-building measure? [online]. *Philosophical Transactions of the Royal Society A*. The Royal Society Publishing. 1. června 2009. Ročník 367. Číslo 1898. [cit. 9. 6. 2016]. Dostupné z: http://rsta.royalsocietypublishing.org/content/367/1898/2729.

[51] Např. ARYAN, Anoop; SINGH, Sanjay. *Protecting location privacy in Augmented Reality using k-anonymization and pseudo-id* [online]. Computer and Communication Technology (ICCCT), 2010 International Conference, 17-19. 9. 2010. str. 119-124. [cit. 9. 6. 2016] Dostupné z: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5640424&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5640424 ; GOUVAS, Panagiotis; ZAFEIROPOULOS, Konstantinos Perakis; BOURAS, Thanasis: An Innovative Approach for the Protection of Healthcare Information Through the End-to-End Pseudo-Anonymization of End-Users. In: *Internet of Things. User-Centric IoT*. Springer International Publishing. 2015. str. 210-216. ISBN: 978-3-319-19656-5 ; JANG, Sung-Bong; KO, Young-Woong. Efficient multimedia big data anonymization. [online]. Multimedia Tools and Applications. 1. prosince 2015. str. 1-18 [cit. 9. 6. 2016]. Dostupné z: http://link.springer.com/article/10.1007/s11042-015-3123-2#/page-1 nebo MOTRO, Amihai; PARISI-PRESICCE, Francesco. Blind Custodians: A Database Service Architecture That Supports Privacy Without Encryption. In: *Data and Applications Security XIX*. 19th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Storrs, CT, USA, August 7-10, 2005, Proceedings. ISBN 978-3-540-31937-5.

standardního následného doplnění, přičemž pseudonymizace je výslovně zmíněna jako jeden z možných přístupů. Požadavek na tuto formu koncepce vývoje výrobků je často zdůrazňován právě ve spojení s úvahami o bezpečnosti předmětů internetu věcí, jejichž technické řešení často nabízí pouze omezené možnosti následného rozšíření, aktualizace či přenastavení ochranných opatření.

Ohrožení údajů zpracovávaných jednotlivými předměty v internetu věcí zřejmě nebude samo o sobě představovat významné riziko pro subjekty údajů, následná kombinace těchto údajů a její ohrožení však může vést k rozsáhlým a nenávratným zásahům do osobního života a soukromí jednotlivců.[52] Většina senzorů v předmětech nebude sama o sobě shromažďovat a zpracovávat data, která by bylo možné jednotlivě označit za citlivá, ba ani personifikovatelná, avšak následná analýza a kombinace dat z různých zdrojů (např. v jiném, centrálním, zařízení internetu věcí) může odhalit specifické vzorce jednání,[53] které představují významný zásah do soukromí jednotlivce. V řadě případů lze toto profilování uživatelů (tzv. *behavioral targeting*, popř. *predictive targeting*)[54] vysledovat již v současném online prostředí, kdy jsou data z vyhledávačů, sociálních sítí či jiných online aktivit agregována a kombinována za účelem vytváření cílených marketingových profilů uživatelů.[55] Z těchto důvodů je zabezpečení osobních

[52] Pro bližší vymezení a analýzu dat a údajů primárně generovaných a shromažďovaných předměty v rámci internetu věcí viz např. kapitolu 12 The Internet of Things: A Survey from the Data-Centric Perspective v AGGARWAL, Charu C. *Managing and Mining Sensor Data*. Springer Science & Business Media, 2013. ISBN: 9781461463092.

[53] COOK, Diane J.; KRISHNAN, Narayanan C. *Activity Learning: Discovering, Recognizing, and Predicting Human Behavior from Sensor Data*. John Wiley & Sons, 2015, ISBN: 978-1-118-89376-0.

[54] CHEN, Ye; PAVLOV, Dmitry; CANNY, John F. Large-scale behavioral targeting. In: *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*. [online]. ACM, 2009. str. 209-218. [cit. 12. 3. 2016]. Dostupné z: http://www.cc.gatech.edu/~zha/CSE8801/ad/p209-chen.pdf.

[55] MARWICK, Alice E. How Your Data Are Being Deeply Mined, *New York Review of Books*, 9. 1. 2014; SINGER, Natasha. Acxiom, the Quiet Giant of Consumer Database Marketing, *New York Times*, 16. 6. 2012; PARISER, Eli. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* New York: Penguin Press, 2012, ISBN: 9780143121237, str. 43; SINGER, Natasha. A Data Broker Offers a Peek Behind the Curtain, *New York Times*, 31. 7. 2013.

údajů, byť v pseudonymizované podobě, v rámci internetu věcí potřeba věnovat náležitou pozornost.

Alternativou k pseudonymizaci jsou různé metody šifrování. Ty mohou představovat řešení řady situací, pro internet věcí je zde však limitace omezenými výpočetními možnostmi jednotlivých předmětů, jakožto i jinými technickými požadavky včetně kompatibility zařízení a datových toků, které ji mohou činit nevhodnou pro tento druh zařízení.[56]

Samostatným bodem je problematika anonymizace osobních údajů v kontextu neustálého pokroku technologických možností a nalézání nových postupů tzv. *de-anonymizace*.[57] Limity jednotlivých forem anonymizace se zabývala i Pracovní skupina podle čl. 29 Směrnice.[58] K technologickému pokroku však nedochází jen na straně *de-anonymizace*, ale nabízí se i nové možnosti technických řešení anonymizace a lze identifikovat řadu projektů, které mohou překonat nedostatky dnešních přístupů.[59]

Otevřenou otázkou zůstává, jak zajistit dostatečnou úroveň ochrany údajů v rámci zařízení internetu věcí, resp. jaké požadavky budou ve směru

---

[56] BELL, C. Kapitola 1 The Internet of Things and Data. In *MySQL for the Internet of Things*. Apress, 2016. ISBN: 978-1-484212-94-3, str. 1-28.

[57] Pro lepší seznámení se se současnými možnostmi *de-anonymizace* viz např. NAINI, Farid M.; UNNIKRISHNAN, Jayakrishnan; THIRAN, Patrick; VETTERLI, Martin. Where You Are Is Who You Are: User Identification by Matching Statistics. *IEEE Transactions on Information Forensics and Security* [online]. Ročník 11, Číslo 2, str. 358-372 [cit. 6. 5. 2016]. Dostupné z: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7321027 ; GAMBS, Sebastien; KILLIJIAN, Marc-Olivier; CORTEZ, Miguel Nunez del Prado. De-anonymization attack on geolocated data. *Journal of Computer and System Sciences* [online]. Elsevier, 2014, 80 (8), str. 1597-1614. [cit. 10. 3. 2016]. Dostupné z: https://hal.archives-ouvertes.fr/hal-01242268/document ; NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust de-anonymization of large sparse datasets. In: *Security and Privacy* [online]. IEEE Symposium on. IEEE, 2008. str. 111-125. [cit. 12. 3. 2016]. Dostupné z: http://myspew.com/gallery/1/Robust%20De-anonymization%20of%20Large%20Datasets.pdf.

[58] Opinion 05/2014 on Anonymisation Techniques [online]. 29 Pracovní skupina, přijaté dne 10. dubna 2014. [cit. 14. 6. 2016]. Dostupné z: http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf , str. 8-9.

[59] Např. projekt řešící možnosti hierarchických anonymizačních algoritmů, viz AMIRI, Fatemeh; YAZDANI, Nasser; SHAKERY, Azadeh; CHINAEI, Amir H. Chinaei. Hierarchical anonymization algorithms against background knowledge attack in data releasing. *Knowledge-Based Systems 101*, 1. 6. 2015, str. 71-89, popř. studie možností autonomních postupů v rámci internetu věcí k omezení rizika porušení bezpečnosti údajů, viz ASHRAF, Qazi Mamoon; Habaebi, Mohamed Hadi. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications 49*, 1. 3. 2015, str. 112-127.

bezpečnostních opatření na tato zařízení kladena. Nařízení sice poskytuje obecný právní rámec, ten však je nyní nutné aplikovat na reálie tržní ekonomiky a okolního světa. Významná role je v tomto směru přikládána kodexům chování, které mají být vypracovány členskými státy, dozorovými orgány a Komisí.[60] Nadto se očekávají kodexy chování vypracované sektorovými sdruženími a dalšími subjekty, které by mohly mimo jiné upřesnit formy opatření k zajištění bezpečnosti zpracování osobních údajů či specifikovat postupy pseudonymizace osobních údajů.[61] Obecně pak problematika zabezpečení osobních údajů (nejen v rámci internetu věcí) zůstává i nadále velmi živé téma, které je předmětem řady odborných studií.[62]

5.2 POSUN OD OZNAMOVACÍ POVINNOSTI K POSOUZENÍ VLIVU

Zřejmě nejproblematičtější částí úpravy ochrany osobních údajů je nalezení vhodné rovnováhy mezi povinnostmi správců a zpracovatelů a ochranou subjektů osobních údajů. Cílem je tedy zakotvení dostatečných ochranných opatření při současném zachování přijatelné míry administrativní zátěže a srozumitelné podoby regulace. „*Ochranná opatření by se neměla zaměřovat za formality. Hrozí, že nadměrná detailnost nebo pokusy o mikrořízení podnikových procesů se v budoucnu přežijí.*“[63]

Současná úprava na základě Směrnice ukládá správci za účelem transparentnosti především předběžnou oznamovací povinnost vůči dozorovému orgánu se stanoveným minimálním rozsahem oznamovaných informací.[64]

---

[60] Článek 40 odst. 1 Nařízení.

[61] Článek 40 odst. 2 Nařízení.

[62] Lze zmínit např. BANDYOPADHYAY, Debasis; SEN, Jaydip. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications* [online]. Ročník 58, Číslo 1 [cit. 6. 5. 2016]. str. 49-69. Dostupné z: http://link.springer.com/article/10.1007/s11277-011-0288-5 nebo WEBER, Rolf H. Internet of Things – New security and privacy challenges. *Computer Law & Security Review* [online]. Ročník 26, Číslo 1, leden 2010 [cit. 6. 5. 2016]. str. 23-30. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0267364909001939.

[63] Stanovisko EIOÚ 3/2015, Velká příležitost pro Evropu, Doporučení EIOÚ o variantách reformy EU v oblasti ochrany údajů ze dne 28. července 2015 [online]. Evropský inspektor ochrany údajů. [cit. 12. 3. 2016]. str. 7. Dostupné z: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_CS.pdf.

[64] Článek 18 a násl. Směrnice.

Nařízení odbourává tuto povinnost, avšak přináší zároveň řadu jiných nástrojů, které ji nahrazují. Nový mechanismus je do značné míry vytvořen po vzoru samoregulace obsažené v evropské úpravě soutěžního práva. Správce bude nově povinen před zahájením zpracování osobních údajů provést posouzení vlivu na ochranu osobních údajů,[65] které obsahuje systematickou analýzu, posouzení rizik z hlediska práv a svobod subjektů údajů, test proporcionality a posouzení nezbytnosti zpracování po deklarovaný účel. Následně se vyžaduje definování bezpečnostních opatření a záruk pro zajištění dostatečné ochrany osobních údajů a případnou eliminaci identifikovaného vysokého rizika.[66]

Na tento koncepční posun lze nahlížet jako na vhodnou reakci na rostoucí množství připojených zařízení a tím i situací, při kterých dochází ke zpracování údajů pro nejrůznější účely. S ohledem na internet věcí lze odbourání předběžné oznamovací povinnosti ve prospěch samoregulačního přístupu shledat za únosné řešení pro správce a zpracovatele, jakož i pro dozorčí orgány.

Je však otázkou, zda v kontextu všech povinností správce na základě Nařízení jde o administrativní ulehčení. Zde je myšlena především skutečnost, že v případě, že z posouzení vlivu vyplyne vysoké riziko a omezené možnosti jeho zmírnění,[67] což jsou opět pojmy, které vyžadují konkrétnější vymezení pro sektor nebo typ údajů, má standardně navazovat předběžná konzultace s dozorčím orgánem. Zároveň je dosavadní oznamovací povinnost pro řadu správců (pokud zpracovávají citlivé údaje, případně pokud mají nad 250 zaměstnanců) do značné míry pouze transformována do povinnosti vést záznamy o všech zpracováních, za která nesou odpovědnost.[68] Tyto záznamy lze přirovnat k informacím poskytovaným dozorovému orgánu na základě současné předběžné oznamovací povinnosti,[69] přičemž do budoucna k nim bude mít dozorčí orgán na žádost přístup přímo u správce.

[65] Článek 35 Nařízení.

[66] Článek 35 odst. 7 písm. d) Nařízení.

[67] Článek 36 odst. 1 Nařízení.

[68] Článek 30 Nařízení.

Výše popsané činnosti by sice mělo správcům usnadnit jmenování pověřence pro ochranu údajů,[70] to lze však dle mého názoru považovat za řešení pro subjekty střední či větší velikosti, nikoliv za obecně přijatelné zdůvodnění komplexnosti požadavků.

Klíčovým i pro případného pověřence bude, zda dostupné prováděcí předpisy či sektorové instrukce poskytnou dostatečně srozumitelné a jednoznačné pokyny a požadavky pro konkrétní činnosti. Národní dozorové orgány mají dle Nařízení vypracovat seznam zpracování, na která se vztahuje povinnost provést posouzení vlivu (a případně i seznam takových, na která se povinnost nevztahuje) a poskytnout je Evropskému sboru pro ochranu osobních údajů, který nahradí dosavadní Pracovní skupinu podle čl. 29 Směrnice.[71] Je však otevřenou otázkou, v jakém časovém horizontu a v jak komplexní podobě lze tyto a další oficiální vodítka pro aplikaci ustanovení Nařízení očekávat.

Jako pozitivum lze na druhou stranu v tomto ohledu shledat zakotvení bližších pravidel pro proces analýzy rizik a okruh zpracování, na která se má vztahovat. Tu má správce za povinnost provést ve většině členských států i za současné právní úpravy na základě vnitrostátní konkretizace podmínek pro zpracování osobních údajů,[72] v případě českého práva na základě § 5 odst. 2 písm e) zákona č. 101/2000 Sb., o ochraně osobních údajů, v aktuálním znění, pro případy zpracování bez výslovného souhlasu subjektu údajů na základě řádného právního titulu a v přiměřeném rozsahu.[73]

---

[69] BURIAN, David; RADIČOVÁ, Zuzana, K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR), *Právní prostor* [online]. 25. 2. 2016 [cit. 14. 3. 2016]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr.

[70] Článek 37 a násl. Nařízení.

[71] Bod 139 Preambule Nařízení.

[72] Článek 5 Směrnice.

[73] § 5 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů, v aktuálním znění; *„Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat, (…) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.“*

5.3 POVINNOSTI PŘI NARUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

Narušení bezpečnosti osobních údajů (tzv. *data breach*) představuje jedno z nejzávažnějších rizik, kterému jsou dnes a denně vystavováni především významní správci a zpracovatelé osobních údajů (státní orgány, banky, obchodní řetězce, telekomunikační společnosti, online portály apod.). ISO/IEC 27040[74] pro něj obsahuje následující definici: "*Narušení bezpečnosti, které vede k náhodnému nebo nezákonnému poškození, ztrátě, změně, neoprávněnému zveřejnění nebo přístupu k přenášeným, uchovávaným nebo jinak zpracovávaným údajům.*" *Ponemon Institute*[75] dělí jeho příčiny do tří skupin: nezákonný útok; systémová chyba; a lidský omyl, přičemž první příčina je značně dominantní.

Bohužel jsou informace o narušeních bezpečnosti z velké části nedostupné, což je případ téměř všech států, nejen členských států Evropské unie. Důvodem je nejen častý nedostatek národní legislativy, která by zakládala povinnost poskytovat informace dozorčím orgánům, ale především významné riziko pro reputaci a podnikatelskou činnost subjektu, které je spojené s případným zveřejněním této skutečnosti a častá absence či nedostatečnost bezpečnostních auditů dozorčích orgánů, které by byly schopny neoznámená narušení odhalit.

Přesto je k dispozici řada studií, které se snaží o aktuální zhodnocení bezpečnostních rizik z různých pohledů (četnost, význam, náklady, čas potřebný k proniknutí do systému, čas potřebný k odhalení narušení atd.). Tyto studie však často trpí statisticky neprůkazným vzorkem společností, který tudíž nemůže sloužit jako údaj pro další analýzy, ale pouze k přiblížení stavu v situaci, kdy lepší informace nejsou dostupné. Následující údaje pocházejí od subjektů z různých vzorků pokrývající různé části světa, ale vzhledem k omezenému počtu jurisdikcí, které mají zavedenu obecnou mandatorní ohlašovací povinnost (ze členských států Evropské unie mají tuto povinnost pro správce údajů obecně v současné době v účinnosti pouze

[74] ISO/IEC 27040:2015 Information technology — Security techniques — Storage security. [online] [cit. 26. 4. 2016] Dostupné z: http://www.iso.org/iso/catalogue_detail?csnumber=44404.

[75] *2015 Cost of Data Breach Study: Global Analysis* [online]. Ponemon Institute [cit. 26. 4. 2016]. Dostupné z: https://www-03.ibm.com/press/us/en/pressrelease/47022.wss.

Německo[76], Nizozemí[77] a Irsko[78]), je zřejmě převažující část údajů od subjektů inkorporovaných ve Spojených státech amerických (ty jsou také státem, ze kterého pochází myšlenka obecné mandatorní ohlašovací povinnosti správců osobních údajů o narušení bezpečnosti osobních údajů).

Verizon ve své zprávě zahrnuje informace od 70 subjektů z 61 zemí (relativní význam zemí však není udán), které v roce 2014 ohlásili 79 790 bezpečnostních incidentů, z nichž 2,122 byly potvrzeny jako narušení bezpečnosti osobních údajů.[79] Dále je mimo jiné poskytnuta zajímavá prediktivní kalkulace očekávaných nákladů spojených s určitým počtem neoprávněně zpřístupněných záznamů (složek osobních údajů jednotlivce), kde je ztráta 1000 záznamů ohodnocena s přesností 95 % v rozmezí od 52 260 USD do 87 140 USD.[80]

Ve studii *The Internet Security Threat Report* informuje *Symantec* o dosud historicky největším porušení bezpečnosti osobních údajů z prosince 2015, kdy bylo zpřístupněno 191 miliónů záznamů. Taktéž poskytuje odhad, že v minulém roce bylo celkově zpřístupněno okolo 429 miliónů virtuálních identit (profilů uživatelů obsahujících jejich osobní údaje).[81] Z této studie také vyplývá, že jen v roce 2015 bylo odhaleno a oznámeno 9 narušení bezpečnosti, při kterých došlo ke zpřístupnění 10 miliónů nebo více záznamů o uživatelích.[82] *Ponemon Institute* zpracoval informace od 350 společností,

---

[76] *Data protection laws of the world* [online] DLA Piper, staženo dne 22. 4. 2016 [cit. 22. 4. 2016]. str. 150. Dostupné z: https://www.dlapiperdataprotection.com/#handbook/world-map-section.

[77] *Data protection laws of the world* [online] DLA Piper, staženo dne 22. 4. 2016 [cit. 22. 4. 2016]. str. 322. Dostupné z: https://www.dlapiperdataprotection.com/#handbook/world-map-section.

[78] *Data protection laws of the world* [online] DLA Piper, staženo dne 22. 4. 2016 [cit. 22. 4. 2016]. str. 209. Dostupné z: https://www.dlapiperdataprotection.com/#handbook/world-map-section.

[79] *2015 Data Breach Investigations Report* [online] Verizon [cit. 26. 4. 2016]. str. 5. Dostupné z: http://www.verizonenterprise.com/DBIR/2015/.

[80] *2015 Data Breach Investigations Report* [online] Verizon [cit. 26. 4. 2016]. str. 34. Dostupné z: http://www.verizonenterprise.com/DBIR/2015/.

[81] *Internet Security Threat Report* [online]. Symantec. duben 2016 [cit. 26. 4. 2016]. str. 6. Dostupné z: https://www.symantec.com/security-center/threat-report.

[82] *Internet Security Threat Report* [online]. Symantec. duben 2016 [cit. 26. 4. 2016]. str. 8. Dostupné z: https://www.symantec.com/security-center/threat-report.

aby analyzoval rozdíly v nákladech spojených s narušením bezpečnosti osobních údajů v závislosti na zemi inkorporace a sektoru činnosti. Zároveň vymodeloval pravděpodobnost, s jakou se bude náhodná společnost potýkat s narušením bezpečnosti v následujících 24 měsících, ta např. představuje 22 % pro narušení střední velikosti (tzn. zpřístupnění min. 10 000 záznamů).[83] *McAfee* zdůrazňuje, že v důsledku nedostatečných údajů se predikce a analýzy často významně liší v odhadovaných nákladech na kyberkriminalitu a rozsah jejího dopadu.[84]

Současná unijní úprava vychází z implementace Směrnice o soukromí a elektronických komunikacích,[85] která se však vztahuje pouze na omezený okruh subjektů, které představují poskytovatele veřejně dostupných služeb elektronických komunikací. Byla jí založena oznamovací povinnost o narušení bezpečnosti vůči dozorčímu orgánu, přičemž technické otázky ohlášení včetně sjednocení ohlašovací lhůty (na 24 resp. 72 hodin) upravuje Nařízení č. 611/2013.[86] Uložena je zároveň, v případě vysokého rizika pro její práva a svobody, i povinnost ohlásit tento případ narušení bezpečnosti osobních údajů jednotlivé dotčené osobě.[87]

Nařízení počítá s mohutným rozšířením povinnosti ohlašování případů narušení bezpečnosti osobních údajů vůči dozorčímu orgánu, a to v podstatě na všechny správce, přičemž lhůta pro ohlášení činí 72 hodin od

---

[83] *2015 Cost of Data Breach Study: Global Analysis* [online]. Ponemon Institute [cit. 26. 4. 2016]. str. 19. Dostupné z: https://www-03.ibm.com/press/us/en/pressrelease/47022.wss.

[84] *Net Losses: Estimating the Global Cost of Cybercrime* [online] McAfee [cit. 26. 4.2016]. str. 4. Dostupné z: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[85] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:cs:HTML.

[86] Nařízení Evropského parlamentu a Rady (ES) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32013R0611&from=EN.

[87] § 88 zákona č. 127/2005, o elektronických komunikacích.

okamžiku, kdy se o něm správce dozvěděl.[88] Tím se ohlašovací povinnost vztáhne i na případy narušení zabezpečení zařízení v rámci internetu věcí, které se budou, vzhledem k značně omezeným možnostem implementovat a především aktualizovat ochranné prvky na senzorech a předmětech, vyskytovat zřejmě velmi často. Vyjmuty jsou případy, které pravděpodobně nepředstavovaly riziko z hlediska práv a svobod jednotlivce.[89] V tomto směru je ale otázka dodatečné podrobnější úpravy, do jaké míry budou narušení bezpečnosti složek internetu věcí považovány za tuto formu rizika. Vzhledem k výše nastíněným parametrům takto připojených zařízení lze však mít za to, že nebude jejich exempce ani v zájmu subjektů údajů, ani v zájmu dozorčích orgánů.

Nadto Nařízení zakládá pro případy, kdy je pravděpodobné, že porušení ochrany osobních údajů bude představovat vysoké riziko pro práva a svobody fyzických osob, povinnost oznámit tyto případy porušení bez zbytečného odkladu přímo jednotlivému subjektu údajů.[90] I zde je otázka budoucího výkladu, jak bude toto ustanovení aplikováno ve vztahu k internetu věcí a shromažďování kombinovatelných souborů pseudonymizovaných údajů. Úprava obsahuje z hlediska funkčnosti vítané a smysluplné výjimky pro případy, kdy správce je schopen prokázat, že zavedl příslušná technická a organizační ochranná opatření, popř. následná opatření, která zajistí, že riziko pro práva a svobody jednotlivce se pravděpodobně již nebude opakovat.[91] Tento bod je však do jisté míry negován skutečností, která byla zmíněna již výše, tedy že není v současné době zřejmé, co především v kontextu internetu věcí představuje ona dostatečná ochranná opatření.

S nedodržením výše zmíněných oznamovacích povinností je obdobně jako u porušení převážné většiny povinností ve vztahu ke zpracování osobních údajů dle Nařízení odpovědný subjekt vystaven riziku sankce až do výše 10.000.000 EUR, resp. 2 % ročního celosvětového obratu

[88] Článek 33 odst. 1 Nařízení.

[89] Článek 33 odst. 1 Nařízení.

[90] Článek 34 odst. 1 Nařízení.

[91] Článek 34 odst. 3 Nařízení.

podniku.[92] Zkušenosti s plněním této povinnosti, která se v současné době vztahuje pouze na poskytovatele veřejně dostupných služeb elektronických komunikací a za jejíž porušení jim dle současné právní úpravy hrozí pokuta za správní delikt do výše 20.000.000 Kč,[93] jsou nejen ze strany ÚOOÚ značně nepřesvědčivé: „*Dosavadní zkušenosti s ohlašováním narušení bezpečnosti údajů nejen z ČR ale i z ostatních států EU však ukazují, že povinné subjekty plní tuto zákonem danou povinnost pouze velmi sporadicky. Většinou se jedná řádově o několik podání za rok. (…) Jeden z hlavních důvodů nezájmu správců oznamovat případy narušení lze určitě shledat v obavách oznamovatelů z případných sankcí, pokud by se přiznali, že k narušení bezpečnosti osobních údajů v jejich společnosti došlo.*“[94] Je tedy otázkou, jaké důsledky na činnost dozorčích orgánů bude mít významné rozšíření povinných subjektů, resp. situací, kdy vzniká ohlašovací povinnost, za současného skokového zvýšení potenciální sankce.

Pouze proaktivní přístup dozorčích orgánů může dle mého názoru zajistit, aby povinné subjekty náležitě plnili tuto, z pohledu subjektů údajů velmi významnou, povinnost, která by zároveň měla plnit funkci ekonomické motivace pro zvýšené investice do zabezpečení systémů před vnějším zásahem a ohrožením, což je klíčový krok ke snižování rizika, které představují současné a o to více budoucí technologie, především pak zapojení systému internetu věcí do podnikové struktury. Značnou roli v tomto směru může hrát vytvoření centrálního dozorčího orgánu v podobě Evropského sboru pro ochranu osobních údajů, od kterého si lze slibovat zvýšenou koordinaci a systematičtější bezpečností audity zaměřené na kontrolu dodržování předepsaných povinností, jakožto i efektivnější prosazování případných sankcí, což by mělo vést ke zvýšenému zájmu správců a zpracova-

[92] Článek 83 odst. 4 Nařízení.

[93] § 88 a 118 odst. 12 písm. a) a odst. 22 písm. c) zákona č. 127/2005, o elektronických komunikacích.

[94] BURIAN, David; RADIČOVÁ, Zuzana, K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR), *Právní prostor* [online]. 25. 2. 2016 [cit. 14. 3. 2016]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr.

telů o dodržování jejich povinností ve vztahu k ochraně osobních údajů podle Nařízení.

5.4 RIZIKO NEFUNKČNOSTI SYSTÉMU

Přestože Nařízení reaguje na výzvy kladené moderními technologickými trendy a vytváří komplexní systém omezení a povinností s důrazem na minimalizaci údajů a transparentnost, je otevřenou otázkou, do jaké míry lze očekávat funkčnost tohoto systému. Nařízení představuje obecný rámec nové úpravy, jde tedy o nespecifická ustanovení, která je zapotřebí analyzovat, definovat a vymezit ve vztahu ke specifickým situacím. V případě, že nebudou zpracovatelům a správcům včas poskytnuty srozumitelné požadavky, lze jen stěží očekávat funkčnost a vymahatelnost nově přijatého souboru práv a povinností.

Bert-Jaap Koops ve svém příspěvku *The Trouble with European Data Protection Law*[95] výstižně vymezuje tři klíčová rizika koncepce evropského práva ochrany osobních údajů, která se mohou plně projevit se vstupem Nařízení v účinnost. Prvně polemizuje nad tím, zda je možné vytvořit regulatorní systém, ve kterém budou mít subjekty osobních údajů kontrolu nad svými údaji. Tento boj je více než aktuální právě v kontextu výše popsaného a vymezeného internetu věcí, který je do značné míry charakterizován všudypřítomným shromažďováním údajů bez přičinění subjektů údajů. V druhém bodě poskytuje důvody, proč významná reforma úpravy osobních údajů nevede k usnadnění, ale naopak ztížení situace pro všechny zúčastněné. To je dle mého názoru riziko, které je inherentní každé zásadnější úpravě nebo novele právní úpravy. Je proto, jak bylo výše několikrát zmíněno, zásadní, do jaké míry budou včas a podrobně vytvořeny prováděcí předpisy, výkladová stanoviska a implementační manuály, které umožní správcům, zpracovatelům, pověřencům i dozorčím orgánům uvést ustanovení Nařízení v život v prostředí reálné ekonomiky a jejích specifických výzev a požadavků. V třetím bodě je polemizováno nad efek-

[95] KOOPS, Bert-Jaap. The Trouble with European Data Protection Law. *International Data Privacy Law* [online] 29. 8. 2014 [cit. 6. 5. 2016]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692.

tivností komplexní úpravy ochrany osobních údajů, v kontrastu dílčích sektorových úprav. Zde je na místě zohlednit i obecný účel a myšlenku unijního práva a Evropské unie vůbec, čímž je do značné míry ospravedlněna jednotící všeobjímající koncepce, na kterou však dle mého názoru nyní musí navazovat ony dílčí sektorové prováděcí úpravy.[96]

6. ZÁVĚR

Internet věcí lze vnímat jako významný prvek moderních technologických trendů, který přináší nové výzvy pro aplikaci práva ochrany osobních údajů. Ty jsou dány především rozmanitostí údajů, které předměty v internetu věcí mohou sbírat, shromažďovat a zpracovávat, což vede k potřebě lepšího vymezení hranic mezi osobními údaji, pseudonymizovanými údaji a technickými metadaty, jakož i zohlednění důsledků kombinací a souběhu různých údajů z různých zdrojů. Značnou roli bude pro aplikaci úpravy hrát i skutečnost, že předměty internetu věcí budou zřejmě do značné míry všudypřítomné a subjekt údajů se může stát předmětem jejich činnosti i bez vlastního přičinění či dokonce vědomí. V neposlední řadě pak, s ohledem na omezené technické možnosti ochranných opatření, skýtají novou formu rizikových bodů pro zabezpečení ochrany nejen sítí, ale i zpracovávaných osobních údajů.

Na unijní úrovni dospělo do finální podoby Nařízení, které má zajistit plošné přizpůsobení ochrany osobních údajů a schopnost čelit výzvám, které přináší mimo jiné i internet věcí. Tento právní předpis však představuje pouze obecný právní rámec, který bude zapotřebí ve značné míře specifikovat pro jednotlivá práva a povinnosti, a to specificky ve vztahu k jednotlivým (často značně odlišným) formám zpracování, za pomoci prováděcích předpisů a výkladových stanovisek.

---

[96] *Bert-Jaap Koops* není jediným, kdo polemizuje nad současným směrem vývoje unijního práva ochrany osobních údajů. Dále lze zmínit např. BUITELAAR, J.C. Privacy: Back to the Roots. *German Law Journal*. Ročník 13, Číslo 3, 2012. ; ROOSENDAAL, Arnold. *Digital Personae and Profiles in Law: Protecting Individuals' Rights in Online Contexts* [online]. 21. 8. 2013 [cit. 6. 5. 2016]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2313576 nebo HILDEBRANDT, Mireille. *Profiling and the Identity of the European Citizen*. Springer Netherlands. 2008 ISBN: 978-1-4020-6914-7.

V tomto příspěvku byla věnována pozornost třem dílčím oblastem úpravy v rámci Nařízení a to s ohledem na specifika internetu věcí. Prvně byla otevřena otázka ochranných opatření a pseudonymizace údajů a problémů s tím spojeným. Následně bylo pojednáno o významu posunu k samoregulaci v podobě posouzení vlivu a omezeních, která vyplývají v tomto směru z jiných souvisejících ustanovení úpravy. Jako třetí byla zmíněna nově zavedená obecná mandatorní oznamovací povinnost v případě narušení bezpečnosti osobních údajů a byl představen kontext této problematiky v širším než evropském měřítku. V závěru bylo pojednáno o rizicích, kterým čelí efektivní prosazení nově přijaté úpravy, a výzvách, které je zapotřebí zdolat před jeho účinností.

V mezidobí, než se nově navrhovaná úprava prosadí v praxi, může vzhledem k akcelerujícímu trendu vývoje dojít k posunu v technologických možnostech, které se budou následkem toho opět vymykat účinné právní úpravě. Je tedy nutno prosazovat adaptabilní výklad účinných norem, který bude postihovat též technologie, které nebylo možné vědomě zahrnout do vlastní podoby úpravy. Funkční právní zakotvení ochrany osobních údajů a soukromí totiž představuje vzhledem k internetu věcí výzvu, která bude mít zásadní dopad na kvalitu života v Evropské unii v nadcházejících letech.

7. POUŽITÁ LITERATURA

7.1 MONOGRAFIE, ODBORNÉ ČLÁNKY, SBORNÍKY

[1] AGGARWAL, Charu C. *Managing and Mining Sensor Data*. Springer Science & Business Media, 2013. ISBN: 9781461463092.

[2] AMIRI, Fatemeh; YAZDANI, Nasser; SHAKERY, Azadeh; CHINAEI, Amir H. Chinaei. Hierarchical anonymization algorithms against background knowledge attack in data releasing. *Knowledge-Based Systems 101*, 1. 6. 2015, str. 71-89.

[3] ASHRAF, Qazi Mamoon; Habaebi, Mohamed Hadi. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications 49*, 1. 3. 2015, str. 112-127.

[4] BARFIELD, Woodrow. *Fundamentals of Wearable Computers and Augmented Reality*. CRC Press. Taylor & Francis Group. 2016. ISBN: 978-1-4822-4351-2.

[5] BELL, C. Kapitola 1 The Internet of Things and Data. In *MySQL for the Internet of Things*. Apress, 2016. ISBN: 978-1-484212-94-3, str. 1-28.

[6] BUITELAAR, J.C. Privacy: Back to the Roots. German Law Journal. Ročník 13, Číslo 3, 2012.

[7] COOK, Diane J.; KRISHNAN, Narayanan C. *Activity Learning: Discovering, Recognizing, and Predicting Human Behavior from Sensor Data*. John Wiley & Sons, 2015, ISBN: 978-1-118-89376-0.

[8] FLORIDI, Luciano. *The Onlife Manifesto*. Being Human in a Hyperconnected Era. Springer International Publishing. 2015. ISBN: 978-3-319-04092-9.

[9] FREITAS, Alex A. *Data mining and knowledge discovery with evolutionary algorithms*. Springer Science & Business Media, 2013, ISBN: 9783662049235.

[10] GORBENKO, Anna; POPOV, Vladimir. Self-learning algorithm for visual recognition and object categorization for autonomous mobile robots. In: *Computer, Informatics, Cybernetics and Applications*. Springer Netherlands, 2012, ISBN: 9789400718388.

[11] GOUVAS, Panagiotis; ZAFEIROPOULOS, Konstantinos Perakis; BOURAS, Thanasis: An Innovative Approach for the Protection of Healthcare Information Through the End-to-End Pseudo-Anonymization of End-Users. In: *Internet of Things. User-Centric IoT*. Springer International Publishing. 2015. str. 210-216. ISBN: 978-3-319-19656-5

[12] HILDEBRANDT, Mireille. *Profiling and the Identity of the European Citizen*. Springer Netherlands. 2008 ISBN: 978-1-4020-6914-7.

[13] MARWICK, Alice E. How Your Data Are Being Deeply Mined, *New York Review of Books*, 09.01.2014.

[14] MOTRO, Amihai; PARISI-PRESICCE, Francesco. Blind Custodians: A Database Service Architecture That Supports Privacy Without Encryption. In: *Data and Applications Security XIX*. 19th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Storrs, CT, USA, August 7-10, 2005, Proceedings. ISBN 978-3-540-31937-5

[15] KROES, N. Ethical implications of tomorrow's digital society. In SMITH, Ian G. (ed.) *Internet of Things*, New Horizons, 2012, ISBN: 978-0-9553707-9-3.

[16] PARISER, Eli. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think,* New York: Penguin Press, 2012, ISBN: 9780143121237.

[17] SINGER, Natasha. Acxiom, the Quiet Giant of Consumer Database Marketing, *New York Times*, 16.06.2012.

[18] SINGER, Natasha. A Data Broker Offers a Peek Behind the Curtain, *New York Times*, 31.07.2013.

7.2 PRÁVNÍ PŘEDPISY

[19] Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS.

[20] Nařízení Evropského parlamentu a Rady (ES) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32013R0611&from=EN.

[21] Směrnice Evropského parlamentu a Rady (ES) č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:31995L0046.

[22] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:cs:HTML.

[23] Zákon č. 101/2000 Sb., o ochraně osobních údajů.

[24] Zákon č. 127/2005, o elektronických komunikacích.

7.3 JUDIKATURA

[25] Rozsudek Soudního dvora ze dne 13. května 2014. Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mario Costeja González. Věc C-131/12.

7.4 ELEKTRONICKÉ ZDROJE

[26] *2015 Cost of Data Breach Study: Global Analysis* [online]. Ponemon Institute [cit. 26. 4. 2016]. Dostupné z: https://www-03.ibm.com/press/us/en/pressrelease/47022.wss.

[27] *2015 Data Breach Investigations Report* [online] Verizon [cit. 26. 4. 2016]. str. 5. Dostupné z: http://www.verizonenterprise.com/DBIR/2015/.

[28] ABDMEZIEM, Riad; TANDJAOUI, Djamel. *Internet of Things: Concept, Building blocks, Applications and Challenges*. [online]. Cornell University Library, 2014. [cit. 28. 2. 2016]. Dostupné z: http://arxiv.org/pdf/1401.6877v1.pdf.

[29] ANDERSON, Janna; RAINIE, Lee. *The Internet of Things Will Thrive by 2025* [online]. Pew Internet Project report, 2014 [cit. 28. 2. 2016]. Dostupné z: http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.

[30] ARNING, Marian; FORGÓ, Nikolaus; KRÜGEL, Tina. Data protection in grid-based multi-centric clinical trials: killjoy or confidence-building measure? [online]. *Philosophical Transactions of the Royal Society A*. The Royal Society Publishing. 1. června 2009. Ročník 367. Číslo 1898. [cit. 9. 6. 2016]. Dostupné z: http://rsta.royalsocietypublishing.org/content/367/1898/2729.

[31] ARYAN, Anoop; SINGH, Sanjay. *Protecting location privacy in Augmented Reality using k-anonymization and pseudo-id* [online]. Computer and Communication Technology (ICCCT), 2010 International Conference, 17-19. 9. 2010. str. 119-124. [cit. 9. 6. 2016] Dostupné z: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5640424&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5640424.

[32] BANDYOPADHYAY, Debasis; SEN, Jaydip. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications* [online]. Ročník 58, Číslo 1 [cit. 6. 5. 2016]. str. 49-69. Dostupné z: http://link.springer.com/article/10.1007/s11277-011-0288-5.

[33] BARFIELD, Woodrow. *Fundamentals of Wearable Computers and Augmented Reality*. CRC Press. Taylor & Francis Group. 2016. ISBN: 978-1-4822-4351-2.

[34] BATTY, M.; AXHAUSEN, K. W.; GIANNOTTI, F.; POZDNOUKHOV, A.; BAZZANI, A.; WACHOWICZ, M.; OUZOUNIS, G.;PORTUGALI, Y. *Smart cities of the future*. [online]. The European Physical Journal Special Topics. listopad 2012. Ročník 214. Číslo 1. str. 481-518. [cit. 9. 6. 2016]. Dostupné z: http://link.springer.com/article/10.1140 2Fepjst%2Fe2012-01703-3.

[35] BOWSKILL, Jerry; DOWNIE, John. Extending the capabilities of the human visual system: an introduction to enhanced reality. *ACM SIGGRAPH Computer Graphics - Special focus: modular visualization environments (MVEs)* [online]. Ročník 29. Číslo 2. květen 1995. str. 61-65 [cit. 9. 6. 2016]. Dostupné z: http://dl.acm.org/citation.cfm?id=204378.

[36] BURIAN, David; RADIČOVÁ, Zuzana, K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR), *Právní prostor* [online]. 25. 2. 2016 [cit. 14. 3. 2016]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr.

[37] CHEN, Ye; PAVLOV, Dmitry; CANNY, John F. Large-scale behavioral targeting. In: *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*. [online]. ACM, 2009. str. 209-218. [cit. 12. 3. 2016]. Dostupné z: http://www.cc.gatech.edu/~zha/CSE8801/ad/p209-chen.pdf.

[38] CHOURABI, Hafedh; NAM, Taewoo; WALKER, Shawn; GIL-GARCIA, Ramon J. et al. *Understanding Smart Cities: An Integrative Framework*. [online]. System Science (HICSS), 2012 45th Hawaii International Conference. ISBN: 978-0-7695-4525-7 [cit. 9. 6. 2016]. Dostupné z: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6149291.

[39] COFFMAN, Kerry G. ODLYZKO, Andrew M. Internet growth: Is there a "Moore's Law" for data traffic?. [online]. In *Handbook of massive data sets*. Springer US, 2002, [cit. 14. 3. 2016]. Dostupné z: http://www.dtc.umn.edu/~odlyZko/doc/internet.moore.pdf.

[40] CUSTERS, Bart; URŠIČ, Helena. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law* [online] 7. 1. 2016 [cit. 6. 5. 2016]. Dostupné z: http://data-reuse.eu/wp-content/uploads/2016/01/International-Data-Privacy-Law-2016-Custers.pdf.

[41] ČERNÝ, Aleš. Firmy začínají kroužit kolem „chytrých měst". Cítí zakázky za miliardy. *iDnes/Ekonomika* [online]. 12. 3. 2016 [cit. 15. 3. 2016]. Dostupné z: http://ekonomika.idnes.cz/smart-cities-v-cesku-0lm-/ekonomika.aspx?c=A160310_2231323_ekonomika_rny.

[42] *Data protection laws of the world* [online] DLA Piper, staženo dne 22. 4. 2016 [cit. 22. 4. 2016]. str. 209. Dostupné z: https://www.dlapiperdataprotection.com/#handbook/world-map-section.

[43] Digitální agenda pro Evropu: klíčové iniciativy [online] MEMO/10/200, Evropská Komise, 19. května 2010. [cit. 16. 3. 2016]. Dostupné z: http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm.

[44] GAMBS, Sebastien; KILLIJIAN, Marc-Olivier; CORTEZ, Miguel Nunez del Prado. De-anonymization attack on geolocated data. *Journal of Computer and System Sciences* [online]. Elsevier, 2014, 80 (8), str. 1597-1614. [cit. 10. 3. 2016]. Dostupné z: https://hal.archives-ouvertes.fr/hal-01242268/document.

[45] Health care. Things are looking app. *The Economist* [online]. 12. 3. 2016, z tištěné edice: Business. [cit. 15. 3. 2016]. Dostupné z: http://www.economist.com/news/business/21694523-mobile-health-apps-are-becoming-more-capable-and-potentially-rather-useful-things-are-looking?fsrc=scn/fb/te/pe/ed/thingsarelookingapp.

[46] HUI, Suo; JIAFU, Wan; CAIFENG, Zou; JIANQI, Liu. Security in the Internet of Things: A Review. *Computer Science and Electronics Engineering (ICCSEE), 2012* [online]. 23. 3. 2012 [cit. 6. 5. 2016]. Dostupné z: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6188257.

[47] JANG, Sung-Bong; KO, Young-Woong. Efficient multimedia big data anonymization. [online]. Multimedia Tools and Applications. 1. prosince 2015. str. 1-18 [cit. 9. 6. 2016]. Dostupné z: http://link.springer.com/article/10.1007/s11042-015-3123-2#/page-1.

[48] JOHNSON, Steve. Target Now Says up to 110 Million Consumers Victimized in Breach. *MercuryNews.com* [online]. 1. 10. 2014 [cit. 16. 3. 2016]. Dostupné z: http://www.mercurynews.com/news/ci_24889060/target-now-says-up-to-110.

[49] *Internet of things: Outlook for the top 8 vertical markets* [online]. IDATE , 2013. [cit. 6. 5. 2016]. Dostupné z: http://www.sbdi.co.kr/cart/data/info/IDATE_Internet_of_Things_sample.pdf?ckattempt=2.

[50] *Internet Security Threat Report* [online]. Symantec. duben 2016 [cit. 26. 4. 2016]. str. 6. Dostupné z: https://www.symantec.com/security-center/threat-report.

[51] ISO/IEC 27040:2015 Information technology — Security techniques — Storage security. [online] [cit. 26. 4. 2016] Dostupné z: http://www.iso.org/iso/catalogue_detail?csnumber=44404.

[52] ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework. [online] [cit. 14. 6. 2016] Dostupné z: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123.

[53] *IoT Privacy, Data Protection, Information Security* [online]. Fact Sheet of the European Commission, [cit. 28. 2. 2016]. Dostupné z: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753.

[54] KOOPS, Bert-Jaap. The Trouble with European Data Protection Law. *International Data Privacy Law* [online] 29. 8. 2014 [cit. 6. 5. 2016]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692.

[55] Legislativní usnesení Evropského parlamentu ze dne 12. března 2014 o návrhu nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) [online]. P7_TA(2014)0212. [cit. 13. 2. 2016]. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//CS.

[56] Legislativní usnesení Evropského parlamentu ze dne 12. března 2014 o návrhu směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů [online]. P7_TA(2014)0219. [cit. 13. 2. 2016]. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0219+0+DOC+XML+V0//CS.

[57] LUKÁČ, Petr. Prvním "chytrým" městem v Česku se stane Písek. Firma Schneider Electric bude řídit dopravu i vytápění. *Hospodářské noviny* [online]. 8. 1. 2016 [cit. 15. 3. 2016]. Dostupné z: http://archiv.ihned.cz/c1-65066210-prvnim-chytrym-mestem-v-cesku-bude-pisek-rika-sef-tuzemske-pobocky-schneider-electric.

[58] MCAFEE, Andrew, et al. Big data. The management revolution. *Harvard Business Review* [online]. 2012, 90.10, str. 61-67. [cit. 29. 2. 2016]. Dostupné z: http://www.rosebt.com/uploads/8/1/8/1/8181762/big_data_the_management_revolution.pdf.

[59] MELL, Peter, GRANCE, Tim. *The NIST definition of cloud computing*. [online] 2011. [cit. 28. 2. 2016]. Dostupné z: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

[60] NAINI, Farid M.; UNNIKRISHNAN, Jayakrishnan; THIRAN, Patrick; VETTERLI, Martin. Where You Are Is Who You Are: User Identification by Matching Statistics. *IEEE Transactions on Information Forensics and Security* [online]. Ročník 11, Číslo 2, str. 358-372 [cit. 6. 5. 2016]. Dostupné z: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7321027.

[61] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust de-anonymization of large sparse datasets. In: *Security and Privacy* [online]. IEEE Symposium on. IEEE, 2008. str. 111-125. [cit. 12. 3. 2016]. Dostupné z: http://myspew.com/gallery/1/Robust%20De-anonymization%20of%20Large%20Datasets.pdf.

[62] Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) [první čtení] – politická dohoda [online]. Výbor stálých zástupců, Brusel, 28. 1. 2016, Interinstitucionální spis: 2012/0011 (COD) (OR. en), 5455/16, DATAPROTECT 3, JAI 44, MI 27, DIGIT 2, DAPIX 13, FREMP 5, COMIX 39, CODEC 55 [cit. 12.03.2016]. Dostupné z: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/cs/pdf.

[63] Návrh směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů [první čtení] – politická dohoda [online]. Výbor stálých zástupců, Brusel, 28. 1. 2016, Interinstitucionální spis: 2012/0010 (COD) (OR. en), 5463/16, DATAPROTECT 4, JAI 46, DAPIX 14, FREMP 6, COMIX 40, CODEC 56 [cit. 12. 3. 2016]. Dostupné z: http://data.consilium.europa.eu/doc/document/ST-5463-2016-INIT/cs/pdf.

[64] *Net Losses: Estimating the Global Cost of Cybercrime* [online] McAfee [cit. 26. 4. 2016]. str. 4. Dostupné z: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[65] NISSENBAUM, Helen. *Privacy as contextual intergrity*. [online]. Washington Law Review. 2004. [cit. 9. 6. 2016]. Dostupné z: https://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf.

[66] Opinion 03/2013 on purpose limitation [online]. 29 Pracovní skupina, přijaté dne 2. dubna 2013. [cit. 9. 6. 2016]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[67] Opinion 05/2014 on Anonymisation Techniques [online]. 29 Pracovní skupina, přijaté dne 10. dubna 2014. [cit. 14. 6. 2016]. Dostupné z: http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf.

[68] Outcome of the Council meeting [online]. 3445th Council meeting, Economic and Financial Affairs, Brussels, 12. 2. 2016. [cit. 13. 2. 2016]. Dostupné z: http://www.consilium.europa.eu/en/.../meetings/.

[69] PERLROTH, Nicole; GELLES, David. Russian Hackers Amass over a Billion Internet Passwords. *New York Times.* [online]. 5. 8. 2014. [cit. 16. 3. 2016]. Dostupné z: http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0.

[70] PODESTA, John. a kol. *Big Data: Seizing Opportunities. Preserving Values* [online]. Excutive Office of the President, 2014 [cit. 14. 3. 2016]. Dostupné z: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[71] ROMAN, Rodrigo; ZHOU Jianying; LOPEZ, Javier. On the features and challenges of security and privacy in distributed internet of things. Computer Networks. [online]. Ročník 57, Číslo 10, 5. 7. 2013, str. 2266-2279 [cit. 6. 5. 2016]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S1389128613000054.

[72] ROOSENDAAL, Arnold. *Digital Personae and Profiles in Law: Protecting Individuals' Rights in Online Contexts* [online]. 21. 8. 2013 [cit. 6. 5. 2016]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2313576.

[73] RUBINSTEIN, Ira. Big Data: The End of Privacy or a New Beginning? NYU School of Law, Public Law Research Paper No. 12-56. [online] 5. 10. 2012 [cit. 6. 5. 2016]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659.

[74] SPIEKERMANN, Sarah, et al. The challenges of personal data markets and privacy. Electronic Markets. *Electronic Markets* [online]. červen 2015, 161-167. [cit. 28. 2. 2016]. Dostupné z: https://www.researchgate.net/profile/Sarah_Spiekermann2/publication/276129671_The_challenges_of_personal_data_markets_and_privacy/links/55c4c7fb08ae-ca747d617e4d.pdf.

[75] Společné prohlášení Evropského parlamentu, Rady a Komise o praktických opatřeních pro postup spolurozhodování (článek 251 Smlouvy o ES) ze dne 30.6.2007. 2007/C145/02. In *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32007C0630%2801%29&from=EN.

[76] Stanovisko EIOÚ 3/2015, Velká příležitost pro Evropu, Doporučení EIOÚ o variantách reformy EU v oblasti ochrany údajů ze dne 28. července 2015 [online]. Evropský inspektor ochrany údajů. [cit. 12. 3. 2016]. Dostupné z: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_CS.pdf.

[77] *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. 29 Pracovní skupina, přijaté dne 16. září 2014. [cit. 28. 2. 2016]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_cs.pdf.

[78] STUART, Keith; ARTHUR, Charles. PlayStation Network Hack: Why It Took Sony Seven Days to Tell the World. *Guardian*. [online] 27. 1. 2011. [cit. 16. 3. 2016]. Dostupné z: http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony.

[79] Tech Trends 2014, Inspiring Disruption. [online]. In *Deloitte's annual Technology Trends report 2014*. Delloite. [cit. 28. 2. 2016]. Dostupné z: http://dupress.com/wp-content/uploads/2014/02/Tech-Trends-2014-FINAL-ELECTRONIC_single.2.24.pdf.

[80] ÚŠELA, Jan. T-Mobile a SimpleCell v dubnu spouští síť pro internet věcí. Pomůže s parkováním i hlídáním domácích mazlíčků *Hospodářské noviny* [online]. 22. 2. 2016. [cit. 12. 3. 2016] Dostupné z: http://byznys.ihned.cz/c1-65174540-t-mobile-bude-pomahat-parkovat-a-sledovat-mazlicky-v-dubnu-spusti-sit-pro-internet-veci.

[81] WEBER, Rolf H. Internet of Things – New security and privacy challenges. *Computer Law & Security Review* [online]. Ročník 26, Číslo 1, leden 2010 [cit. 6. 5. 2016]. str. 23-30. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0267364909001939.