František Kasl

PORUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ V KONTEXTU INTERNETU VĚCÍ

MASARYKOVA UNIVERZITA

ACTA UNIVERSITATIS BRUNENSIS IURIDICA
EDITIO SCIENTIA

MUNI PRESS

MUNI LAW

PORUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ V KONTEXTU INTERNETU VĚCÍ

František Kasl

Masarykova univerzita
Brno 2021

Vzor citace
KASL, František. *Porušení bezpečnosti osobních údajů v kontextu internetu věcí*. 1. vyd. Brno: Masarykova univerzita, 2021, 346 s. Spisy Právnické fakulty Masarykovy univerzity, Edice Scientia, 717.
ISBN 978-80-210-9985-2 (brož.), 978-80-210-9986-9 (online).

CIP - Katalogizace v knize

Kasl, František
Porušení bezpečnosti osobních údajů v kontextu internetu věcí / František Kasl. – 1. vydání. -- Brno: Masarykova univerzita, 2021. 346 stran. – Spisy Právnické fakulty Masarykovy univerzity, Edice Scientia, sv. č. 717. ISBN 978-80-210-9985-2 (brož.), 978-80-210-9986-9 (online)

342.721* 004.89:621.398* (048.8)
- ochrana osobních údajů
- internet věcí
- monografie

342 - Ústavní právo. Správní právo [16]

Tato publikace vznikla na Masarykově univerzitě v rámci projektu Právo a technologie IX č. MUNI/A/1292/2020 podpořeného z prostředků účelové podpory na specifický vysokoškolský výzkum, kterou poskytlo MŠMT v roce 2021.
Právní stav byl zohledněn ke dni 30. 9. 2021.
Překlady anglických termínů a textů v této monografii jsou dílem autora monografie, pokud není uvedeno jinak.

Recenzenti:
doc. JUDr. Pavel Mates, CSc.
JUDr. Tomáš Rychlý, Ph.D.

Gratis Open Access – https://www.press.muni.cz/open-access

ISBN 978-80-210-9986-9 (online ; pdf)
https://doi.org/10.5817/CZ.MUNI.M210-9986-2021

OBSAH

ABSTRAKT A KLÍČOVÁ SLOVA / ABSTRACT AND KEYWORDS

Abstrakt

Cílem této monografie bylo zkoumat, zda má současná právní úprava povinností při porušení zabezpečení osobních údajů dle Obecného nařízení účelné uplatnění i v prostředí internetu věcí, a pokud ano, pak jakými úpravami lze překonat případné zjištěné výzvy a překážky. Na tuto problematiku je nahlíženo ze čtyř perspektiv. Úvod do tématu je z perspektivy kyberbezpečnosti. Je zde provedeno zakotvení pojmu porušení bezpečnosti osobních údajů a vyložen jeho vztah k pojmu bezpečnostní incident. Následně jsou představeny možné podoby porušení bezpečnosti, doložen rozsah a četnost tohoto jevu a nastíněn trend jeho vývoje. Poté je vysvětlena možná újma jednotlivců v důsledku porušení bezpečnosti. Následně je přistoupeno k tématu z právní perspektivy. V jejím rámci je nabídnut celostní rozbor právních rámců s povinnostmi směřujícími k zabránění či zmírnění dopadů porušení bezpečnosti jak v rámci Evropské unie, tak ve Spojených státech amerických. Ty jsou následně diskutovány s cílem identifikovat jejich překážky a limity. Další kapitola přibližuje dopad technologické proměny prostředí, které vymezuje pojmem internet věcí. Pozornost je věnována novým výzvám, které toto prostředí přináší pro zpracování osobních údajů. Rozmanitost situací, které pod tento pojem spadají je zachycena za pomoci tří dílčích scénářů: automatizované komunikace mezi zařízeními, prostředí chytrého města a proměny postavení mikropodniků. Tyto pohledy jsou doplněny o perspektivu ekonomickou. Ta je využita k modelování rozhodování povinných subjektů ohledně dodržování uložených povinností ve spojení s porušením bezpečnosti. Poté je přistoupeno k propojení představených perspektiv, jsou shrnuty získané poznatky o porušení bezpečnosti v kontextu internetu věcí a jsou diskutována možná řešení pro odhalené překážky dodržování příslušných povinností.

Klíčová slova

Porušení bezpečnosti osobních údajů; ohlašovací povinnost; oznamovací povinnost; internet věcí; ochrana osobních údajů; Obecné nařízení; kyberbezpečnost.

Abstract

The goal of this research publication was to assess, if the current legal framework of obligations related to personal data breach under GDPR are purposefully applicable also in the context of internet of things and if so, then which changes can help to overcome eventual discovered challenges or obstacles to it. This issue is studied from four perspectives. The introduction to the topic is from the cyber security perspective. The term personal data breach is defined and explained in relation to the term security incident. Next are presented possible forms of personal data breach, offered evidence for the scope and frequency of this phenomenon and outlined the future trend of its development. Pursuant to that the potential harm for individuals from personal data breach is explained. After that, the topic is approached from the legal perspective. Within it is presented a comprehensive analysis of the legal frameworks with obligations aimed at prevention or mitigation of personal data breach in the EU, as well as in the United States. These are then discussed with the aim to identify challenges and limits applicable to them. The next chapter introduces the impact of technological change of the context, which is defined by the term internet of things. The attention is focused on the new challenges, which are brought by it to personal data processing. The variety of situations, which fall under this term, is captured through three partial scenarios: automated machine-to-machines communication, smart city environment and change in the role of microenterprises. These views are completed with an economic perspective. This is used for modelling the decision-making of the obliged parties regarding their compliance with the obligations related to personal data breach. Subsequently, the presented perspectives are merged, the obtained findings regarding personal data breach in the context of internet of things are summarized and then the possible solutions for the discovered challenges of compliance with the respective obligations are discussed.

Keywords

Personal Data Breach; Notification Obligation; Communication Obligation; Internet of Things; Personal Data Protection; GDPR; Cyber Security.

PODĚKOVÁNÍ

Tato kniha vychází z mého disertačního výzkumu a na tomto místě bych velmi rád poděkoval všem, bez jejichž pomoci, podpory či inspirace by nevznikla.

Předně děkuji Martinu Škopovi za podnětné rozpravy a nasměrování v klíčových chvílích. Za zpětnou vazbu k textu, podnětné připomínky a nesčetné předchozí konzultace děkuji Pavlu Loutockému, Jakubu Haraštovi, Jakubu Míškovi a Matěji Myškovi. Radimu Polčákovi děkuji za diskuse a náměty k zamyšlení, ale též příležitosti pro akademický rozvoj a růst, které mi umožnily podnětná a obohacující setkání.

Za ta, při kterých jsem měl příležitost diskutovat problematiku představenou v této knize, si zaslouží mé poděkování především Roger Clarke, Christof Tschohl, Michael Froomkin, Federica Casarosa, Fabrizio Esposito, Denitsa Kozhuharova a Damian Klimas.

Děkuji všem kolegyním a kolegům z Ústavu práva a technologií za podnětné diskuse a nové obohacující náměty.

Děkuji mým rodičům, prarodičům a sestře za veškerou pomoc při hledání mé životní cesty a neutuchající podporu při každém kroku.

Velké poděkování patří mé ženě Sabině za andělskou toleranci a láskyplnou péči.

Na závěr si pak zvláštní poděkování zasluhuje můj syn Martínek za mnoho klidných chvil, kdy mi bylo umožněno soustředit se na psaní a za věčně dobrou náladu, která pro mě byla vždy velkým povzbuzením.

SEZNAM NEJVÝZNAMNĚJŠÍCH POJMŮ

Bezpečnostní incident

V rámci této monografie jde o pojem užitý ve smyslu zavedeném pro oblast kyberbezpečnosti, tedy jako porušení nebo hrozba porušení provozu ICT. Blíže viz podkapitola 1.2 a následně druhá kapitola.

Externalita

Jedná se o přínos či náklad způsobený danou činností, který se však neprojeví u subjektu, který danou činnost vykonal, ale jinde. Viz pátá kapitola.

Funkční výklad

Přístup k výkladu unijního práva, který zahrnuje teleologický výklad a historický výklad za současného reflektování mezinárodněprávních aspektů unijního práva. Blíže viz podkapitola 1.5.

Chytré město

Koncept chytrého města je příkladem synergie nových technologií, které zahrnují internet věcí, *big data* a *cloud computing* do modelu propojeného městského prostředí, které slibuje zlepšení udržitelnosti a kvality života. Blíže viz oddíl 4.4.2.

Chytrá regulace

Jedná se o regulatorní techniku obsahující mechanismy pro shromažďování informací o aktuálním stavu regulovaného prostředí, tak aby na ně bylo možné vrchnostensky reagovat. Blíže viz oddíl 3.2.3.

Incentiva

Pobídka, která subjekt motivuje k dané aktivitě či volbě. Blíže viz pátá kapitola.

Internet věcí

Trend implementace prvků informačních a komunikačních technologií do širokého spektra zařízení vytvářející nové kontexty propojenosti a zpracování osobních údajů. Blíže viz podkapitola 4.1.

Kyberbezpečnost

Označení pro oblast věnovanou zajištění bezpečnosti informačních a komunikačních technologií zahrnující kybernetickou bezpečnost i související roviny včetně technických.

Kybernetická bezpečnost

Oblast upravená zákonem č. 181/2014 Sb., o kybernetické bezpečnosti.

Kybernetický bezpečnostní incident

Bezpečnostní incident v rámci definice obsažené v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti.

Mikropodnik

Podnik s méně než 10 zaměstnanci a ročním obratem či rozvahou nižší než 2 miliony €. Blíže viz oddíl 4.4.3.

Notifikační povinnost

V rámci této monografie jde o obecný pojem pro povinnost sdělení informací o porušení bezpečnosti bez ohledu na právní rámec či příjemce.

Ohlašovací povinnost

Povinnost sdělení informací o porušení bezpečnosti dozorovému orgánu. Směrodatná je v tomto směru úprava dle článku 33 Obecného nařízení, kterou představuji v podkapitole 3.2.

Osobní údaje

Veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tedy subjektu údajů. Jde o pojem vymezený Obecným nařízením. Blíže viz oddíl 3.2.2.

Oznamovací povinnost

Povinnost sdělení informací o porušení bezpečnosti dotčeným fyzickým osobám. Vymezení se váže především na úpravu dle článku 34 Obecného nařízení, kterou představuji v podkapitole 3.2.

Performativní pravidlo

Obecně uložená povinnost, kdy je povinnému subjektu zákonodárcem ponechána volnost při volbě konkrétního postupu, který vede k dosažení regulací sledovaného cíle. Blíže viz oddíl 3.2.3.

Porušení bezpečnosti osobních údajů

V rámci této monografie je pojem porušení bezpečnosti osobních údajů, či zkráceně porušení bezpečnosti, užíván ve smyslu ústředního diskutovaného jevu bez ohledu na související úpravu v konkrétním předpise. Srov. podkapitola 1.2.

Porušení zabezpečení osobních údajů

V rámci této monografie je pojem porušení zabezpečení osobních údajů, či zkráceně porušení zabezpečení, užit pro zúžení závěrů či diskuse na kontext právní úpravy dle Obecného nařízení. Srov. podkapitola 1.2.

Subjekt údajů

Fyzická osoba přímo či nepřímo identifikovaná za pomoci osobních údajů. Jde o pojem vymezený Obecným nařízením.

Údaje o jednotlivci

V rámci této monografie je pojem užit pro zachycení odlišného vnímání okruhu relevantních údajů o fyzické osobě v řešeném kontextu v americkém prostředí. Blíže viz oddíl 3.3.1.

Zpracovávané údaje

V rámci této monografie jde o obecný pojem přemosťující odlišnosti jednotlivých vymezení okruhu relevantních údajů o fyzické osobě, tedy zahrnující jak osobní údaje, tak údaje o jednotlivci.

SEZNAM UŽITÝCH ZKRATEK

BYOD *Bring your own device* je podniková politika podpory zaměstnanců v užívání vlastních ICT zařízení při práci. Blíže viz oddíl 4.4.3.

CERT *Computer emergency response team*, tj. skupina pro reakci na počítačové hrozby, blíže viz podkapitola 6.5.

CSIRT *Computer security incident response team*, tj. skupina pro reakce na počítačové bezpečnostní incidenty, blíže viz podkapitola 6.5.

DDoS *Distributed denial-of-service* je typ útoku na server, při kterém je pro přehlcení cílové služby požadavky využito velké množství rozptýlených zařízení.

EU Evropská unie

ENISA *European Network and Information Security Agency*, tj. Evropská agentura pro bezpečnost sítí a informací.

FTC *Federal Trade Commission*, tj. Federální obchodní komise.

HHS *Department of Health and Human Services*, blíže viz oddíl 3.3.5.

HIPAA *Health Insurance Portability and Accountability Act,* blíže viz oddíl 3.3.5.

HITECH *Health Information Technology for Economic and Clinical Health Act*, blíže viz oddíl 3.3.5.

ICT Informační a komunikační technologie

ISAC *Information sharing and analysis centre,* tj. centrum pro analýzu a sdílení informací. Blíže viz podkapitola 6.3.

ISRA *Information security risk assessment*, tj. hodnocení informačních bezpečnostních rizik, blíže viz podkapitola 5.1.

Komise Evropská komise

M2M *Machine-to-machine* je označení pro přímou komunikaci a datový přenos mezi zařízeními.

MSP Malé a střední podniky

NIST *National Institute of Standards and Technology*, tj. americký Národní úřad pro standardy a technologie.

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

Obecné nařízení

Nařízení Evropského parlamentu a Rady (EU) 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. In: EUR-Lex.

Pracovní skupina dle článku 29

Pracovní skupina pro ochranu osobních údajů zřízení podle článku 29 zrušené směrnice 95/46/ES.

PPP *Public-private partnership*, tj. spolupráce veřejného a soukromého sektoru.

Sbor Evropský sbor pro ochranu osobních údajů zřízený dle článku 68 Obecného nařízení.

SC USA *Supreme Court of the United States*, tj. Nejvyšší soud Spojených států amerických.

SDEU Soudní dvůr Evropské unie

UDAP *Unfair and deceptive acts or practices*, tj. zakázaná nekalá a klamná jednání nebo praktiky. Blíže viz oddíl 3.3.5.

Úřad Úřad pro ochranu osobních údajů

VoKB Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti. In: ASPI.

ZoKB Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. In: ASPI.

1 ÚVOD*

Trendy digitalizace moderní společnosti směřují k rostoucímu všudypřítomnému zpracovávání a shromažďování osobních údajů o každém z nás. Naše virtuální identity se již nevytvářejí pouze v rámci využívání služeb informační společnosti, ke kterým přistupujeme přes webové prohlížeče a jiná tradiční rozhraní pro vstup uživatele do kyberprostoru. Jejich formování se stále intenzivněji přenáší i do kontextu našeho fyzického jednání, které je zaznamenáváno, hodnoceno a sledováno za účelem profilování a poskytování služeb propojujících virtuální a fyzickou realitu. Chytré náramky tak trvale sledují naši fyzickou aktivitu, polohu či duševní rozpoložení, chytří osobní asistenti jsou v soukromých prostorách vždy připraveni naslouchat našim projevům, aby zachytili pokyn či dotaz a dnešní automobily jsou běžně vybaveny prvky neustálého sledování pozornosti řidiče a jeho aktivit během řízení.

Toto jsou přitom pouze nejběžnější náznaky technologických trendů, které nás stále intenzivněji obklopují, do jisté míry bez ohledu na naše osobní volby či preference. Zintenzivňování snah o shromažďování údajů za účelem zlepšování a rozšiřování služeb, snižování nákladů či zvyšování bezpečnosti k nám nepřichází pouze skrze nabídku spotřebního zboží. V různých fázích a podobách totiž vstupuje do kontextu našich pracovních prostředí, veřejné sféry či osobní sféry druhotně skrze spotřebitelské a uživatelské volby osob, se kterými přicházíme do kontaktu. Tato plošná tendence k implementaci prvků komunikačních a informačních technologií do širokého spektra kontextů je v této monografii označována pojmem „internet věcí".

Jedná se o jev, který se realizuje nejen v rovině technologického vývoje, ale má dopady do řady dalších vrstev, ke kterým je na místě přihlížet pro jeho

* JUDr. Ing. František Kasl, Ph.D., Odborný pracovník, Centrum vzdělávání, výzkumu a inovací v informačních a komunikačních technologiích, Fakulta informatiky, Masarykova univerzita, Brno; Ústav práva a technologií, Právnická fakulta, Masarykova univerzita, Brno / Specialist, Centre for Education, Research and Innovation in Information and Communication Technologies, Faculty of Informatics, Masaryk University, Brno, Czech Republic; Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic / E-mail: frantisek.kasl@law.muni.cz / ORCID: 0000-0001-6675-9528

Monografie vychází z textu disertační práce nazvané „Právní a ekonomické aspekty porušení bezpečnosti osobních údajů v kontextu internetu věcí", jíž jsem v roce 2021 úspěšně obhájil na půdě Právnické fakulty Masarykovy univerzity v Brně.

komplexní uchopení.[1] Aspektem, který je určující pro nahlížení na tento trend v rámci představované monografie, je proměna a zintenzivňování shromažďování a zpracování osobních údajů dotčených jednotlivců, a zvláště pak otázka bezpečnosti takto zpracovávaných osobních údajů.

Právní prostředí ochrany osobních údajů přitom samo zaznamenává významnou dynamiku a rozvoj. Přesto nelze odhlédnout od paradoxu, který *Bygrave* popsal jako *„silný kontrast mezi de facto erozí soukromí a stále složitějšími právními strukturami zaměřenými zdánlivě na zabránění této erozi."*[2] Pozornost zde tudíž soustředím na problematiku, kde se protíná intenzita technologického vývoje s dynamikou proměny právního rámce. Unijní, a tudíž i české právo ochrany osobních údajů prošlo v nedávných letech zásadní aktualizací, která byla cíleně připravována ve snaze čelit novým technologickým výzvám.[3] Tato úprava právního rámce upoutala značnou pozornost právní vědy, která rozproudila řadu diskusí o aplikaci norem na nové technologie.[4] Cloudové služby, analýza velkých databází *(big data)*[5], umělá inteligence, technologie blockchain či algoritmické rozhodování jsou tak předmětem množství odborných statí upozorňujících na rostoucí mezeru mezi normativním rámcem a stavem techniky

1 Internet věcí má vedle technologických rovin projevy v rovině sociální, v oblastech obchodních modelů, managementu, bezpečnosti či soukromí. Blíže viz MINERVA, Roberto, Abyi BIRU a Domenico ROTONDI. *Towards a definition of the Internet of Things (IoT)* [online]. Torino: IEEE, 2015, s. 7 [cit. 1. 6. 2021].

2 *„Stark contrast between de facto privacy erosion and the increasingly elaborate legal structures aimed ostensibly at preventing that erosion."* Viz BYGRAVE, Lee A. Legal Scholarship on Data Protection: Future Challenges and Directions. In: *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde Liber Amicorum Yves Poullet*. 1. vyd. Brussels: Larcier, 2018, s. 495.

3 Srov. body odůvodnění 6 a 7 Obecného nařízení.

4 Příkladem uvádím nosná témata významné mezinárodní konference *Computers, Privacy & Data Protection* (CPDP) v letech 2016 *([In]visibilities and Infrastructures)*, 2017 *(The Age of Intelligent Machines)* či 2018 *(The Internet of Bodies);* Srov. COMPUTERS, PRIVACY & DATA PROTECTION. Previous editions of CPDP. *Archive CPDP Conferences* [online]. 2020 [cit. 12. 7. 2021]. Dostupné z: https://www.cpdpconferences.org/archive

5 V rámci této monografie bylo z převážné části vycházeno ze zahraniční literatury. U některých kontextů si přitom nejsem vědom zavedenosti odpovídajících českých odborných pojmů, často pak pokládám anglické termíny za lépe vystihující danou myšlenku. Za účelem vyšší srozumitelnosti proto často napříč textem uvádím touto formou v závorkách a kurzívou původní cizojazyčný termín, který je pro účely plynulosti textu přeložen do češtiny. Ze stejného důvodu je u přímých citaci zahraničního textu dáno k dispozici původní citované znění, tak jako výše v pozn. č. 2.

*(*tzv. *pacing problem)*, které se věnoval již *Hughes*.[6] Ani tato monografie v tomto směru není výjimkou, snažím se však neomezovat při zde prezentované analýze pozornost pouze na budoucno, ale v souladu s přístupem, který prosazuje *Bygrave*,[7] se snažím doplnit tento pohled vpřed o adekvátní historický přehled, jelikož si jsem vědom toho, že pro mnoho zdánlivě nových výzev lze nalézt inspiraci či návod řešení v minulých zkušenostech či úvahách.

1.1 Zaměření monografie

Reforma právního rámce ochrany osobních údajů v Evropské unii, symbolizovaná především nařízením 2016/679 o ochraně osobních údajů[8] (dále jen „Obecné nařízení") použitelném od 25. května 2018, přinesla zvýšený akcent na odpovědnost *(accountability)*[9] správců, a také důraz na transparentnost a bezpečnost osobních údajů v rámci jejich zpracování. Jedním z konkrétních projevů tohoto posunu bylo zavedení nových povinností ohlašování a oznamování případů porušení zabezpečení[10] osobních údajů dle článků 33 a 34 Obecného nařízení.

V těchto povinnostech, doplňujících požadavek na zajištění přiměřených technických a organizačních opatření na zabezpečení zpracovávaných osobních údajů dle článku 32 Obecného nařízení, spatřuji značně přehlížený prvek tohoto právního rámce. Přitom jimi může být dle mého názoru významně přispíváno k omezení škodlivých následků neoprávněného přístupu k osobním údajům na straně jedné a celkovému účelnému vynucování důsledné implementace přiměřených opatření na ochranu zpracovávaných osobních údajů na straně druhé. Není přitom přílišným tajemstvím, že proklamovaného

6 Viz HUGHES, Thomas P. Technological Momentum. In: SMITH, Merritt Roe a Leo MARX (eds.). *Does Technology Drive History?: The Dilemma of Technological Determinism*. Cambridge, Massachusetts: MIT Press, 1994.

7 Srov. BYGRAVE, Lee A. Legal Scholarship on Data Protection: Future Challenges and Directions. In: *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde Liber Amicorum Yves Poullet*. 1. vyd. Brussels: Larcier, 2018, s. 502.

8 Nařízení Evropského parlamentu a Rady (EU) 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).

9 K významovému přesahu pojmu *accountability* oproti českému termínu odpovědnost blíže viz MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. 1. vyd. Brno: Masarykova univerzita, 2020. s. 159–169.

10 Užití pluralitní terminologie pojmů porušení bezpečnosti osobních údajů a porušení zabezpečení osobních údajů je zdůvodněno a vysvětleno v následující podkapitole 1.2.

přínosu tato úprava v současné době zcela nedosahuje, ať již z důvodu omezené pozornosti ze strany dozorových úřadů[11] či v důsledku nevhodného nastavení a výsledné nízké motivace povinných subjektů k dodržování těchto povinností v předvídaných kontextech.[12]

Dle mého názoru se přitom jedná o prvek, který si zaslouží podrobnější pozornost, jelikož při zahrnutí určitých úprav či doplnění může představovat významný nástroj pro vyrovnávání se s rostoucí nezbytností zpracování osobních údajů ve všech aspektech fungování moderní společnosti. K tomu dále přispívají všudypřítomnost, vzájemná propojenost a častá nenápadnost kontextů zpracování v rámci prostředí internetu věcí, které s sebou přinášejí významnou proměnu interakce jedinců a technologií při zpracování osobních údajů, a s tím spojená rizika újmy, která je na místě brát v potaz.[13]

Tato monografie se zaměřuje na podrobné zkoumání povinností pojících se s porušením bezpečnosti osobních údajů za účelem funkčního právního výkladu příslušných ustanovení Obecného nařízení. Na to navazuje pohled z ekonomické perspektivy, která nám umožňuje zkoumat racionální motivace povinného subjektu (podniku) při rozhodování se o reakci na porušení bezpečnosti. To je významným doplněním funkčního právního výkladu, jelikož je tím možné normativní rámec diskutovat též v intencích předvídatelné či dosažitelné praktické aplikace. V tomto směru reflektuji technologický vývoj prostředí vymezený jako rozvoj internetu věcí a identifikuji vhodná řešení pro překonání překážek či omezení, která brání plné realizaci účelu předmětné normativní úpravy v diskutovaném kontextu.

---

11 Nedostatečné vynucování souladu s povinnostmi v důsledku omezených kapacit dozorových úřadů je obecným problémem spojovaným v dnešní době s Obecným nařízením. Srov. VINOCUR, Nicholas. 'We have a huge problem': European regulator despairs over lack of enforcement. *POLITICO* [online]. 27. 12. 2019 [cit. 12. 7. 2021]. Dostupné z: https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs--over-lack-of-enforcement/; Pro přehled o současném stavu implementace viz MASSÉ, Estelle. *Two Years under the EU GDPR. An Implementation Progress Report. State of Play, Analysis and Recommendations* [online]. New York: Access Now, 2020 [cit. 12. 7. 2021].

12 Tento aspekt bude podrobně rozebrán v následujících částech monografie, především pak v páté kapitole, již zde lze odkázat např. na BISOGNI, Fabio, Hadi ASGHARI a Michel J. G. VAN EETEN. Estimating the size of the iceberg from its tip. In: *16th Annual Workshop on the Economics of Information Security*: *WEIS 2017* [online]. San Diego: University of California, 2017 [cit. 12. 7. 2021].

13 Tato proměna bude podrobně představena v rámci čtvrté kapitoly.

Úprava dle Obecného nařízení je přímo použitelná v prostředí českého práva a vzhledem k absenci podstatných národních odchylek[14] je v monografii zásadně upřednostňován sjednocující pohled na úrovni unijní úpravy, který je motivován též širší potenciální využitelností dosažených závěrů.

Vzhledem k původu konceptu notifikačních povinností porušení bezpečnosti v právu Spojených států amerických věnuji přiměřenou pozornost i této perspektivě. Přestože je přenositelnost zkušeností z tohoto prostředí do kontextu současné unijní právní úpravy omezená, lze abstrahovat od dílčích odlišností a využít dostupné praktické zkušenosti i obecně platné závěry akademického diskurzu jak v právních, tak v ekonomických otázkách řešené problematiky, pro její celostní zachycení. To pokládám za hodnotné především vzhledem k délce a rozmanitosti amerických zkušeností s notifikačními povinnostmi, které stojí v kontrastu s nedávným zavedením těchto povinností na základě Obecného nařízení.

Soubor povinností pojících se k porušení bezpečnosti je v této monografii analyzován se záměrem konfrontování nedostatků jejich aplikace na kontext zpracování osobních údajů v nově vznikajícím prostředí internetu věcí. Jedná se přitom o nesnadno uchopitelný jev, který nemá zatím jednotně ustálenou definici. Přistoupím tedy k jeho výstižnému zachycení skrze řadu jeho dílčích projevů. V rámci monografie představím, jaká tento technologický vývoj přináší nová nastavení procesů zpracovávání osobních údajů a vzorce datových toků, které jsou relevantní pro aplikaci představované právní úpravy. Na základě celostní analýzy problematiky z kyberbezpečnostního, právního, technologického i ekonomického pohledu pak v závěru monografie diskutuji dostupná dílčí řešení a nástroje, které umožňují *de lege ferenda* čelit identifikovaným výzvám pro současnou unijní právní úpravu v kontextu internetu věcí.

1.2 Odůvodnění užité pluralitní terminologie

Pozorný čtenář si jistě povšiml zdánlivé terminologické nejednotnosti dosavadního textu monografie a jejího názvu. V rámci prezentované monografie jsem se musel vypořádat s problematikou uchopení terminologie klíčových

14 K tomuto blíže ke konci oddílu 3.2.1, kde podrobně sleduji vývoj relevantní právní úpravy.

pojmů v několika rovinách. Je nutné odlišení pojmů *notifikační povinnost*,[15] *ohlašovací povinnost*[16] a *oznamovací povinnost*[17] s ohledem na různé koncepce příjemce informací o daném incidentu. Taktéž zohledňuji odlišné vnímání ochrany zpracovávaných údajů v americkém a unijním právu, které zdůrazňuji užitím odlišujících pojmů *zpracovávané údaje*,[18] *osobní údaje*[19] a *údaje o jednotlivci*.[20]

Dále bylo pro přehlednost potřebné přistoupit k terminologickému odlišení širšího a užšího vymezení relevantního jevu jako incidentu z hlediska kyberbezpečnosti. Napříč publikací užívám zpravidla pojmu *bezpečnostní incident*,[21] přičemž pro následnou diskusi v intencích zákona č. 181/2014 Sb. o kybernetické bezpečnosti (dále jen „ZoKB“) je užit jím definovaný pojem *kybernetický bezpečnostní incident*.[22]

Výše uvedená rozlišování užitých pojmů jsou důsledkem odlišných právních zakotvení či obsahu, které vyžadují odlišování jednotlivých pojmů pro dodržení přesnosti a platnosti tvrzení a závěrů představených v textu.

Oproti tomu převažující užití pojmu *porušení bezpečnosti osobních údajů* či *porušení bezpečnosti* napříč monografií na úkor pojmu *porušení zabezpečení osobních údajů*, který nalezneme v závazném českém znění Obecného nařízení, je mým upozorněním na terminologickou nevhodnost druhého z těchto pojmů.

---

15 V rámci této monografie jde o obecný pojem pro povinnost sdělení informací o porušení bezpečnosti bez ohledu na právní rámec či příjemce.

16 Povinnost sdělení informací o porušení bezpečnosti dozorovému orgánu. Směrodatná je v tomto směru úprava dle článku 33 Obecného nařízení, kterou představuji v podkapitole 3.2.

17 Povinnost sdělení informací o porušení bezpečnosti dotčeným fyzickým osobám. Vymezení se váže především na úpravu dle článku 34 Obecného nařízení, kterou přibližuji v téže podkapitole.

18 V rámci této monografie jde o obecný pojem přemosťující odlišnosti jednotlivých vymezení okruhu relevantních údajů o fyzické osobě.

19 Pojem z prostředí unijního přístupu k ochraně informačního sebeurčení jednotlivce, definovaný Obecným nařízením a podrobněji přiblížený v oddílu 3.2.2.

20 V rámci této monografie je pojem užit pro zachycení odlišného vnímání okruhu relevantních údajů o fyzické osobě v řešeném kontextu v americkém prostředí. Blíže viz oddíl 3.3.1.

21 Vycházím přitom z pojmu *security incident*, užívaného za tímto účelem ENISA, srov. ENISA. Reference Incident Classification Taxonomy. *ENISA* [online]. 2018 [cit. 12. 7. 2021]; Americký NIST pak užívá v zásadě totožný pojem *computer security incident*, srov. CICHONSKI, Paul et al. *Computer Security Incident Handling Guide* [online]. NIST Special Publication (SP) 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology. 2012 [cit. 12. 7. 2021].

22 Blíže viz podkapitola 6.5.

Na základě mého podrobného rozboru užití obou termínů napříč právními předpisy i akademickým diskurzem[23] jsem dovodil, že není mezi pojmy obsahový rozdíl. Přestože pak pojem *zabezpečení* figuruje v dnes použitelných a účinných právních předpisech, jeho zanesení do českého znění unijních předpisů je nesystematické a neodůvodněné, jelikož v předchozích předpisech bylo pro srovnatelný účel užito pojmu *bezpečnost* a cizojazyčná znění unijních předpisů v mezičase nedostála žádné změny. Vedle tohoto pochybného původu užívání termínu *zabezpečení* na úkor *bezpečnosti* v českém znění Obecného nařízení jsem toho názoru, že z významového hlediska a provázaností s blízkými obory (především právo kybernetické bezpečnosti a kyberbezpečnost, ale též informační bezpečnost či bezpečnostní studia) je na místě v akademickém diskurzu zachovat preferenci termínu *bezpečnost*. Tento přístup ostatně podporuje i provedená analýza akademických publikací,[24] kde je tento termín stále široce užíván.

V rámci této publikace je tak pojem *porušení bezpečnosti osobních údajů*, či zkráceně *porušení bezpečnosti*, užíván ve smyslu ústředního diskutovaného jevu bez ohledu na související úpravu v konkrétním předpise. Pro vyšší terminologickou čistotu je v kontextu americké úpravy pojem upraven na *porušení bezpečnosti* údajů *o jednotlivci*. Oproti tomu užití pojmu *porušení zabezpečení osobních údajů*, či zkráceně *porušení zabezpečení*, vyznačuje zúžení závěrů či diskuse na kontext právní úpravy dle Obecného nařízení.

1.3 Cíl monografie a dílčí otázky

Jak vyplývá z výše nabídnutého popisu zaměření, cílem této monografie bylo zkoumat, zda má současná právní úprava povinností při porušení zabezpečení osobních údajů dle Obecného nařízení účelné uplatnění i v prostředí internetu věcí, a pokud má, pak jakými úpravami lze překonat případné zjištěné výzvy a překážky, které jí v tomto prostředí vyvstávají.

Takto stanovený cíl bylo následně potřebné specifikovat do souboru dílčích otázek, které umožnily systematicky postupovat v rámci této monografie

23 Podrobně jsem jej představil v příspěvku KASL, František. K pojmové nejednotnosti porušení zabezpečení/bezpečnosti osobních údajů v českém právu. *AUC IURIDICA* [online]. 2019, roč. 2019, č. 3, s. 120–125.

24 Ibid., s. 126–130.

jednotlivými rovinami řešené problematiky (kyberbezpečnostní, právní, technologickou a ekonomickou) se zachováním směřování k celostnímu zachycení relevantních aspektů. Podkladem pro jejich formulaci byla přitom úvodní rešerše, při které jsem se systematicky seznamoval s řešenou problematikou na základě dostupné odborné literatury a průběžně konfrontoval své utvářené teze s akademickým diskurzem.[25]

Výsledkem je soubor osmi dílčích otázek, které budou reflektovány z hlediska poznatků a tezí představených v jednotlivých kapitolách této publikace vždy v příslušném shrnutí kapitoly a následně ve vlastním závěru při diskusi cíle této monografie.

1. **Jak se proměnily notifikační povinnosti v Obecném nařízení ve srovnání s předchozí unijní a paralelní americkou právní úpravou?**

   Výchozím bodem pro diskusi důsledků technologické proměny na řešenou problematiku porušení bezpečnosti je studium použitelné právní úpravy, představené ve třetí kapitole. Na tu je přitom na místě nahlížet za pomoci funkčního výkladu relevantních ustanovení Obecného nařízení, který zahrnuje jak historický pohled vývoje unijní právní úpravy, tak určení účelu daných povinností. Jelikož je však tradice těchto povinností v evropském prostředí značně omezená, pokládám za vhodné přihlédnout také k paralelnímu vývoji v rámci americké úpravy. Ta je dostatečně blízká evropské tradici, aby nevznikala nepřemostitelná bariéra pro tento postup. Současně se potýká se srovnatelnými koncepčními výzvami u těchto povinností a nabízí notně obsáhlejší odborný diskurz, který je jim věnován.

25 Viz KASL, František. Internet of Things – Assessment of Incentives of Businesses to Fullfil the Personal Data Breach Obligation under the proposed General Data Protection Regulation. In: *The 33rd Annual Conference of the European Association of Law and Economics (EALE)*: *EALE* [online]. Bologna: EALE, 2016 [cit. 12. 7. 2021]; KASL, František. Internet věcí a ochrana dat v evropském kontextu. *Revue pro právo a technologie*, 2016, roč. 7, č. 13; KASL, František. Towards identification of cybersecurity principles for smart city cyber-physical environment. In: *Cyberspace Conference 2017*. 2017; KASL, František. Cybersecurity of Small and Medium Enterprises in the Era of Internet of Things. *The Lawyer Quarterly* [online]. 2018, roč. 8, č. 2 [cit. 12. 7. 2021]; KASL, František. Personal Data Breach in the Era of Internet of Things. In: *Internationales Rechtsinformatik Symposion IRIS 2018* [online]. 2018 [cit. 12. 7. 2021]; KASL, František. Towards Functioning Personal Data Breach Notification in the Age of Internet of Things. *Jusletter IT. Die Zeitschrift für IT und Recht* [online]. 2019 [cit. 12. 7. 2021].

2. **Přináší prostředí internetu věcí nové výzvy pro dodržování povinností souvisejících s porušením bezpečnosti osobních údajů?**

   Tato otázka je klíčová pro stanovení přínosu představované monografie. Právní rámec ochrany osobních údajů byl navržen a přijat s plným vědomím možného budoucího rozvoje nových technologií.[26] Záměrem tedy bylo vytvoření základního rámce pravidel, která odolají času a budou technologicky neutrální. Tato pevná základna však může vyžadovat dodatečnou specifikaci pro řešení výzev technologických posunů, pro které je výklad obecné úpravy příliš vágní a nepřiléhavý. Internet věcí pokládám za příklad takového jevu. Jak bude diskutováno v rámci podkapitoly 4.5, proměna procesů zpracování osobních údajů v tomto kontextu a nová kyberbezpečnostní rizika lze považovat za zdroj praktických překážek pro plnění povinností dle Obecného nařízení, mezi které se řadí i notifikační povinnosti.

3. **Dochází v tomto prostředí k navýšení četnosti a rozsahu porušení bezpečnosti?**

   Touto otázkou sleduji především očekávatelný rozsah proměn, které vyplynou z diskuse předchozí otázky. Výchozím bodem bude posouzení současného stavu v rámci podkapitoly 2.2. Ve čtvrté kapitole bude následně věnována pozornost předpokladům, že masové rozšíření internetu věcí do domácností, podnikových operací i veřejného sektoru povede k významnému nárůstu kybernetických hrozeb.[27] Díky propojenosti je toto prostředí označováno za „zesilovač hrozeb".[28] Budu tak zkoumat související proměny propojení prvků internetu věcí, nové formáty zpracování a sdílení osobních údajů a výsledný nárůst bezpečnostních zranitelností, před kterými varuje např. *Schneier*.[29]

---

26 Viz především body odůvodnění 6, 15, 89 a 91 Obecného nařízení.

27 Tyto předpoklady se zakládají především na ARBOR NETWORKS. *Worldwide Infrastructure Security Report* [online]. Burlington, MA: NETSCOUT, 2016, s. 76 [cit. 12. 7. 2021]; MARINOS, Louis, Adrian BELMONTE a Evangelos REKLEITIS. *ENISA Threat Landscape 2015* [online]. Heraklion: ENISA, 2015, s. 74 [cit. 12. 7. 2021]; SYMANTEC. *Internet Security Threat Report 2017 Volume 22* [online]. 2017, s. 64 [cit. 12. 7. 2021].

28 Srov. EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. The Hague: European Police Office, 2016, s. 52.

29 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018.

4. **Narůstá v tomto prostředí též intenzita a škodlivý dopad případů porušení bezpečnosti?**

   Vedle proměny četnosti incidentů je na místě se zabývat též jejich škodlivým dopadem, na což směřuje tato dílčí otázka. Vyšší škodlivost případů porušení bezpečnosti posiluje význam notifikačních povinností jako nástrojů k omezení hrozící újmy. K zachycení současného vnímání možné újmy směřuje podkapitola 2.3. Internet věcí pak v tomto směru přináší v řadě ohledů novou provázanost jednání v kyberprostoru s fyzickými důsledky, např. při selhání chytrého vozidla.[30] V rámci čtvrté kapitoly bude zkoumáno, nakolik je rozšiřování senzorů a aktivačních systémů významné i z hlediska neoprávněného zpracování osobních údajů, např. v důsledku utajené aktivace či manipulaci se vstupy do zařízení, která mají kameru či mikrofon. Zohledněno bude taktéž, jakou roli hraje skutečnost, že samotná všudypřítomná interakce s přizpůsobivými zařízeními vede nezbytně k bohatšímu a detailnějšímu sběru osobních údajů a profilování uživatelů.[31]

5. **Vyvstávají v tomto prostředí nové překážky znesnadňující odhalení případů porušení bezpečnosti?**

   Doplňující otázkou k proměně hrozeb porušení bezpečnosti v prostředí internetu věcí je proměna možností tyto hrozby v souladu s požadavky právní úpravy odhalit. Technologický posun přitom v tomto směru může situaci znesnadňovat[32] (např. pro malé podniky, jak bude diskutováno v oddílu 4.4.3), může však i přinášet nové možnosti řešení[33] (těm se věnuji v šesté kapitole).

6. **Přináší prostředí internetu věcí specifické výzvy pro určení povinných subjektů?**

   Jelikož významným funkčním aspektem aplikace regulatorního rámce, jako je Obecné nařízení, je spolehlivý mechanismus identifikace

30 Viz GREENBERG, Andy. Hackers Remotely Kill a Jeep on the Highway – With Me in It. *Wired* [online]. 2015 [cit. 5. 8. 2021].

31 Viz MARAS, Marie-Helen. Tomorrow's Privacy. Internet of Things: security and privacy implications. *International Data Privacy Law*, 2015, roč. 5, č. 2, s. 101.

32 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W. W. Norton & Company, 2018, s. 30–31.

33 Srov. FANG, Junbin et al. Position Paper on Recent Cybersecurity Trends: Legal Issues, AI and IoT. In: AU, Man Ho et al. (eds.). *Network and System Security*. New York: Springer International Publishing, 2018, Lecture Notes in Computer Science.

subjektů odpovědných za zajištění souladu s danou povinností, věnuji mu v rámci monografie adekvátní pozornost. Internet věcí, jako složitá síť zařízení a služeb na několika funkčních úrovních,[34] je často provozován a spravován různými subjekty nebo několika subjekty zároveň, případně v kombinacích závislých na dané situaci (příkladem je prostředí chytrého města, kterému je věnován oddíl 4.4.2). Lze tudíž předpokládat nárůst četnosti zpracování skrze společné správce dle článku 26 Obecného nařízení. Mnohostí zúčastněných subjektů však narůstá neurčitost přiřazení povinnosti konkrétnímu subjektu a s ním spojená vymahatelnost jejího plnění. To se tudíž může negativně odrážet na plnění povinností odhalovat a ohlašovat porušení bezpečnosti. Možnému řešení těchto situací je věnován oddíl 6.1.2.

7. **Odrážejí se tyto proměny prostředí v motivaci subjektů plnit povinnosti související s porušením bezpečnosti?**

   Regulatorní reakcí na případy porušení bezpečnosti bylo zakotvení povinností, které představuji ve třetí kapitole. Současně jsem si však vědom dostupných studií z amerického prostředí poukazujících na nedostatečné plnění těchto povinností vzhledem ke konfliktním zájmům povinných subjektů.[35] Ty jsou dále rozvíjeny do ekonomických modelů, které poukazují na klíčové proměnné v motivaci těchto subjektů pro racionální rozhodování směrem k plnění příslušných notifikačních povinností.[36] Těm je věnována pátá kapitola, přičemž je využito ekonomické perspektivy pro vyhodnocení vlivu rozvoje prostředí internetu

34 Lze např. odlišovat primární vrstvu, ve které dochází ke sběru informací senzory a provozu aktivačních systémů, od komunikační vrstvy, ve které dochází k přenosu informací za pomoci různých komunikačních protokolů a síťových nadstaveb. Specifické je pak zpracování osobních údajů a aktivace funkcionalit zařízení skrze aplikační vrstvu. Srov. YANG, Xue et al. A Multi-layer Security Model for Internet of Things. In: WANG, Yongheng a Xiaoming ZHANG (eds.). *Internet of Things*. Berlin/Heidelberg: Springer, 2012, s. 389, Communications in Computer and Information Science.

35 Viz např. BISOGNI, Fabio, Hadi ASGHARI a Michel J. G. VAN EETEN. Estimating the size of the iceberg from its tip. In: *16th Annual Workshop on the Economics of Information Security*: *WEIS 2017* [online]. San Diego: University of California, 2017 [cit. 12. 7. 2021]; BOASIAKO, Kwabena Antwi a Michael O'CONNOR KEEFE. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. *SSRN Electronic Journal* [online]. 2018 [cit. 5. 9. 2021].

36 Srov. především GARCIA, Michael E. *The Economics of Data Breach: Asymmetric Information and Policy Interventions*. Disertační práce. Columbus. The Ohio State University, 2013; LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1.

věcí na tyto proměnné a následně v rámci šesté kapitoly diskutuji možná řešení pro posílení motivace k plnění předmětných povinností.

8. **Jaký relativní význam lze přikládat notifikačním povinnostem porušení bezpečnosti v prostředí internetu věcí?**
   Přes primární zaměření této monografie na perspektivu právního rámce na ochranu osobních údajů si plně uvědomuji, že v moderním propojeném kontextu jako je internet věcí nelze vhodné řešení problematiky analyzovat izolovaně. To je zvláště platné pro povinnosti a opatření související se zajištěním bezpečnosti zpracovávaných údajů, jelikož zde dochází k úzkému prolínání s problematikou zajištění bezpečnosti sítí, systémů a zařízení, skrze která k tomuto zpracování dochází. Tím je nevyhnutelné přihlížet též k příslušnému právnímu rámci kybernetické bezpečnosti, jakož i širším standardům a požadavkům utvářeným v oblasti kyberbezpečnosti. Vnímám tak za podstatné klást si otázku, jaké je místo notifikačních povinností ve vztahu k nástrojům prosazujícím se skrze tyto související perspektivy a do jaké míry je možné koordinovat jejich rozvoj a výsledný účinek s povinnostmi při porušení bezpečnosti osobních údajů. K této otázce přistupuji částečně v páté kapitole, a následně napříč šestou kapitolou, především pak v podkapitole 6.1 ve vztahu k možnostem kyberbezpečnostní certifikace, v podkapitole 6.2 s ohledem na rodící se specifické kyberbezpečnostní standardy pro prostředí internetu věcí, a zvláště pak v podkapitole 6.5 při zkoumání propojitelnosti s hlášením kybernetických bezpečnostních incidentů.

1.4 Struktura monografie

Monografie sestává ze sedmi kapitol. Po této úvodní kapitole následují čtyři kapitoly představující jednotlivé perspektivy, ze kterých je na problematiku porušení bezpečnosti v rámci této monografie nahlíženo.

Druhá kapitola je obecným uvedením do tématu z perspektivy kyberbezpečnosti. Je zde provedeno zakotvení pojmu porušení bezpečnosti a vyložen jeho vztah k pojmu bezpečnostní incident. Následně jsou na základě dostupných analýz a statistik představeny možné podoby porušení bezpečnosti, doložen rozsah a četnost tohoto jevu a nastíněn trend jeho vývoje. Poté je vysvětlena možná újma jednotlivců v důsledku porušení bezpečnosti.

Třetí kapitola přináší právní perspektivu a nabízí rozbor právních rámců s povinnostmi směřujícími k zabránění či zmínění dopadů porušení bezpečnosti jak v rámci EU, tak ve Spojených státech amerických. Nejprve je pojednáno o úpravě před Obecným nařízením a poté je podrobně představena a analyzována tato dnes použitelná unijní právní úprava. Následně je stručně přiblížena americká úprava a jsou zachyceny poznatky, které jsou z ní přenositelné do diskuse úpravy dle Obecného nařízení.

Čtvrtá kapitola zahrnuje technologickou perspektivu a přibližuje dopad proměny prostředí, které vymezuje pojmem internet věcí. Pozornost je věnována novým výzvám, které toto prostředí pro zpracování osobních údajů přináší. Rozmanitost situací, které pod tento pojem spadají je zachycena za pomoci tří dílčích scénářů: automatizované komunikace mezi stroji, prostředí chytrého města a proměny postavení mikropodniků.

Pátá kapitola doplňuje diskusi o perspektivu ekonomickou. Ta je využita k modelování rozhodování povinných subjektů ohledně dodržování uložených povinností ve spojení s porušením bezpečnosti. Je přitom vycházeno z teorie racionálního rozhodování podniku a dostupné modely zahrnují nejen rozhodování o výši investic do bezpečnostních opatření, ale i vliv sdílení informací mezi podniky a podmínky motivace podniku k řádnému ohlašování odhalených porušení bezpečnosti dozorovému orgánu.

Šestá kapitola je vyústěním monografie a propojením poznatků shromážděným v rámci výše představených perspektiv. Jsou v ní shrnuty dosažené dílčí závěry o porušení bezpečnosti v kontextu internetu věcí a diskutována možná řešení pro odhalené překážky dodržování příslušných povinností.

V závěrečné sedmé kapitole je pak shrnut celkový výstup této monografie. Jsou diskutovány dílčí otázky a představeny dosažené výsledné závěry, ke kterým směřovala.

1.5 Metodologie

V představované monografii postupuji systematicky od obecnějších rovin problematiky ke konkrétním dílčím aspektům. To přitom platí jak v rámci každé ze čtyř převážně analytických kapitol, kde postupně představuji jednotlivé perspektivy (tzn. kyberbezpečnostní v druhé kapitole, právní ve třetí kapitole,

technologickou v čtvrté kapitole a ekonomickou v páté kapitole), tak i napříč celou prací, kdy z těchto dílčích aspektů následně skládám celostní pohled na problematiku při diskusi možných řešení odhalených překážek v šesté kapitole. Využívám přitom standardní postupy právní hermeneutiky, případně tradiční analytické metody právní vědy. Za hlavní využité analytické nástroje platí rozbor, klasifikace a popis dílčích aspektů a jejich interakce v rámci příslušné roviny normativní regulace. Jako vodítko pro propojení výkladu napříč představovanými perspektivami směrem k dosažení stanoveného cíle monografie užívám dílčí otázky představené v předcházející podkapitole.

Monografií silně rezonuje pragmatická metoda, kterou v českém prostředí pro oblast práva informačních technologií vymezil v zásadě za jedinou příhodnou *Polčák*.[37] Tento přístup jsem zvolil s ohledem na specifika řešených otázek z oblasti práva ochrany osobních údajů, které se nacházejí na průsečíku právně teoretického vymezení regulatorního rámce a praktických technologických výzev spojených s prostředím internetu věcí. V textu nadto posiluji komplexní zachycení řešeného problému prvkem interdisciplinarity monografie, tj. zohledněním ekonomických modelů racionálního rozhodování pro rozšíření analýzy na aspekty, které za pomoci čistě právního doktrinálního zkoumání nelze v rámci monografie adekvátně zachytit a argumentačně podložit.[38]

Druhá kapitola slouží jako úvod do problematiky porušení bezpečnosti, kde zdůrazňuji kyberbezpečnostní perspektivu. K utvoření představy o podobách, rozsahu a dopadech porušení bezpečnosti osobních údajů v dnešní společnosti čerpám z dostupných bezpečnostních zpráv a statistik, které pravidelně utvářejí přední společnosti působící v odvětví kyberbezpečnosti, jakož i některé instituce (např. ENISA). Představuji významné historické případy porušení bezpečnosti a hlavní dosud odhalené hrozby vztahující se k novým technologickým trendům. Tyto zdroje následně využívám i k přiblížení forem a intenzity újmy, která hrozí dotčeným subjektům údajů.

37 Srov. POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 76; POLČÁK, Radim. 1 Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 5.

38 Tedy především diskusi motivace subjektů k plnění notifikačních povinností a možných cest pro její posílení.

Ve třetí kapitole doktrinálně zkoumám právní povinnosti pojící se k porušení bezpečnosti zpracovávaných údajů. V první části soustředím pozornost na vývoj v rámci EU, přičemž ústředním bodem je funkční výklad[39] relevantních ustanovení Obecného nařízení. Sleduji přitom účelový přístup k výkladu, kdy skrze rozbor historických a teleologických aspektů úpravy nalézám její účel bez nezbytné vazby na úmysl vyjádřený normotvůrcem.[40] Ten totiž v řadě případů není možné spolehlivě stanovit,[41] a to i přesto, že v případě sekundárního unijního práva je postoj normotvůrce zpravidla zachycen v bodech odůvodnění, které jsou povinnou součástí každého unijního právního předpisu.[42] K tomuto přistupuji především za využití historické a systematické analýzy příslušných právních předpisů, legislativních dokumentů a souvisejících odborných akademických publikací. Přehled následně doplňuji o vývoj a hlavní parametry notně fragmentované právní úpravy ve Spojených státech amerických, kde nacházím významný zdroj zkušeností s fungováním notifikačních povinností.

Následující čtvrtá kapitola směřuje k vymezení proměny technologického prostředí, která vede k novým vzorcům ve zpracování osobních údajů a nese pro účely této monografie označení internet věcí. Jelikož se jedná o nesnadno uchopitelný jev, který nemá zatím jednotně ustálenou definici a lze výstižně popsat pouze skrze řadu jeho dílčích projevů, je mým záměrem v rámci této kapitoly vymezit prvky relevantní z hlediska řešené problematiky a představit je čtenáři na základě zvolených příkladů. V tomto směru jde tudíž především o popis technologického prostředí s prvky klasifikace.

---

39 K pojmu funkčního výkladu blíže viz SEHNÁLEK, David. *Specifika výkladu práva Evropské unie a jeho vnitrostátní důsledky*. Praha: C. H. Beck, 2019, s. 110 a násl.

40 Ibid., s. 110.

41 Srov. ŠKOP, Martin. Interpretace práva jako literární interpretace. In: *Dny práva*: *Dny práva – 2010 – Days of Law* [online]. Brno: Masarykova univerzita, 2010, s. 2981 [cit. 12. 7. 2021].

42 Viz SEHNÁLEK, David. *Specifika výkladu práva Evropské unie a jeho vnitrostátní důsledky*. Praha: C. H. Beck, 2019, s. 113;Odůvodnění unijních předpisů nejsou srovnatelná s důvodovou zprávou u českého právního předpisu, jelikož nezachycují pouze záměr předkladatele, ale jsou diskutována a upravována v rámci řádného legislativního procesu, a tudíž nalézají uplatnění nad rámec historického výkladu právě i ve výkladu funkčním. Blíže k tomu viz FRÖHLICH, Radek. Odůvodnění legislativních aktů Evropské unie. In: ŽATECKÁ, Eva et al. (eds.). *COFOLA 2011*: *Cofola 2011 The Conference Proceedings* [online]. Brno: Masarykova univerzita, 2011, s. 391 [cit. 12. 7. 2021].

V páté kapitole vystupuji z tradičního rámce monografie na poli práva a čerpám z oblasti ekonomických modelů racionálního rozhodování pro doplňkový rozbor rozhodování o investicích do bezpečnostních opatření a motivace povinných subjektů (podniků) k dodržování notifikačních povinností. Smyslem zahrnutí této perspektivy je rozšíření diskuse řešení v duchu pragmatické metody o multidisciplinární přesah, díky kterému lze postihnout otázky přesahující čistě právní rovinu problematiky. Ty směřují především na nástroje k motivaci povinných subjektů plnit normativně uložené povinnosti, resp. analýzu praktických překážek či racionálních preferencí, které je od toho odrazují.

V šesté kapitole propojuji roviny představené v předcházejících kapitolách k zachycení celostního pohledu na problematiku porušení bezpečnosti v prostředí internetu věcí. Jádrem je přitom diskuse za využití argumentační syntézy, ve které reaguji na odhalené výzvy a překážky pro uplatnění povinností při porušení zabezpečení osobních údajů dle Obecného nařízení skrze zhodnocení možných řešení a postupů *de lege ferenda*.

2 RIZIKO A DŮSLEDKY NEOPRÁVNĚNÉHO PŘÍSTUPU K OSOBNÍM ÚDAJŮM V DIGITALIZOVANÉ SPOLEČNOSTI

Život v moderní společnosti je založen na shromažďování, zpracování a sdílení informací. Nosičem jsou v převážné míře elektronické záznamy, data, která jsou všudypřítomným hybatelem informačních a komunikačních technologií.[43] Nelze však pomíjet, že negativním vedlejším důsledkem zvyšující se závislosti moderní společnosti na digitalizované komunikaci a zpracování dat je rostoucí náchylnost k úmyslnému či náhodnému porušení bezpečnosti zpracovávaných údajů. To je zvláště platné pro data, která nesou informace o identifikované či identifikovatelné fyzické osobě, tedy pro osobní údaje.[44]

2.1 Porušení bezpečnosti osobních údajů jako bezpečnostní incident

S přechodem na digitální vedení záznamů a počátkem propojení světa skrze globální internetovou síť významně vzrostlo riziko neoprávněného zpřístupnění těchto záznamů a jejich následného zkopírování, smazání, změny či jiného zneužití. První veřejně ohlášené případy porušení bezpečnosti zpracovávaných údajů lze zaznamenat ve Spojených státech již v 80. letech 20. století.[45]

Za zvláštní zmínku pak stojí incident z roku 1984, týkající se porušení bezpečnosti 90 milionů záznamů v databázích společnosti *TRW* podnikající s informacemi o úvěrech. Tento tehdy značně mediálně sledovaný případ vedl ve Spojených státech k legislativní odezvě, kterou bylo neoprávněné vniknutí do databází zařazeno mezi federální trestné činy.[46]

43 Šíře uplatnění a závislosti nejrůznějších činností na využití těchto nástrojů a s nimi spojených datových toků byla nedávno zdůrazněna v průběhu karanténních opatření při pandemii COVID-19. Přínosy, které má tato vysoká míra virtuální propojenosti společnosti skrze kyberprostor, byly v této mimořádné celosvětové situaci více než zjevné.

44 Pojem vymezuje článek 4 bod 1 Obecného nařízení a bude o něm podrobněji pojednáno v oddílu 3.2.2.

45 Srov. HAYDEN, Ernie. Data breach protection requires new barriers. *SearchSecurity* [online]. 2013 [cit. 12. 7. 2021]. Dostupné z: https://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers

46 Stalo se tak skrze The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (H.R. 5616). Blíže viz BETTS, Mitch. DP crime bill toughened. *Computerworld*, 1984, roč. 18, č. 27.

Od té doby s rostoucí rolí informačních a komunikačních technologií narůstala i frekvence a dopad incidentů týkajících se přístupu k digitálním záznamům. Od počátku milénia pak došlo k desítkám rozsáhlých bezpečnostních incidentů, které se dotkly miliard digitalizovaných záznamů nejrůznější důvěrnosti a citlivosti pro dané jednotlivce.[47]

Již zde lze zmínit bezpečnostní incident, ke kterému se vrátíme podrobněji v oddílu 3.3.3. Odehrál se z počátku roku 2002 v kalifornském *Stephen P. Teale Data Center* a vedl k neoprávněnému zpřístupnění záznamů o 265 000 státních zaměstnancích.[48] Ačkoliv dopady tohoto porušení bezpečnosti pro dotčené jednotlivce nebyly v porovnání s jinými nijak závažné, byl to právě tento incident, který stál u zrodu první specifické právní úpravy notifikačních povinností.[49]

Tento případ porušení bezpečnosti je každoročně zastíněn mnohem rozsáhlejšími bezpečnostními incidenty. Pro ilustraci rozsahu, kterého mohou tyto případy dosahovat, lze zmínit následující: (i) bezpečnostní incident společnosti *Yahoo* během let 2013–2014, který se dotkl záznamů na třech miliardách uživatelských účtů; (ii) bezpečnostní incident společnosti *Mariott International* během let 2014–2018 dotýkající se záznamů půl miliardy návštěvníků těchto hotelů; (iii) bezpečnostní incident společnosti *Equifax*, spravující registr dlužníků ve Spojených státech, v roce 2017, který vedl ke zpřístupnění citlivých záznamů 148 milionů amerických občanů; či (iv) bezpečnostní incident společnosti *My Fitness Pal* z února 2018, dotýkající se záznamů 150 milionů uživatelů.[50]

47 Více digitálních záznamů se může vztahovat k jedné osobě (např. uživatelské jméno, datum narození, jméno a příjmení), případně může jít při více porušením bezpečnosti o opakovaný únik záznamu se stejnou informační hodnotou (např. právě datum narození či jméno a příjmení). Pro výstižný přehled viz GROOT, Juliana de. The History of Data Breaches. *Digital Guardian* [online]. 12. 11. 2018 [cit. 12. 7. 2021]. Dostupné z: https://digitalguardian.com/blog/history-data-breaches; INFORMATION IS BEAUTIFUL. World's Biggest Data Breaches & Hacks. *Information is Beautiful* [online]. 1. 2. 2019 [cit. 19. 2. 2021]. Dostupné z: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

48 Srov. LUCAS, Greg. Hackers accessed state computer but took no data / Payroll information was at risk. *SFGate* [online]. 7. 6. 2002 [cit. 12. 7. 2021]. Dostupné z: https://www.sfgate.com/bayarea/article/Hackers-accessed-state-computer-but-took-no-data-2830442.php

49 Viz SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC. *Security Breach Notification Laws: Views from Chief Security Officers* [online]. Berkeley: University of California-Berkeley School of Law, 2007, s. 8 [cit. 12. 7. 2021].

50 Blíže viz SWINHOE, Dan. The 15 biggest data breaches of the 21st century. *CSO Online* [online]. 17. 4. 2020 [cit. 12. 7. 2021]. Dostupné z: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Významné bezpečnostní incidenty se přitom nevyhýbají ani České republice, zvláště pak v nedávné době. Lze zmínit napadení informačních systémů nemocnic v Brně[51] a v Benešově[52] či těžební společnosti OKD.[53]

Ačkoliv uznávám, že poskytnutý přehled byl notně zkrácený a značně selektivní, jeho účelem bylo především zdůraznění rozsahu problematiky, která je touto prací postihována. Porušení bezpečnosti u subjektů spravujících rozsáhlé databáze záznamů o fyzických osobách mohou, jak výše uvedeno, postihovat stamilióny osob. V současné době přitom subjektů, které disponují a běžně operují s takto rozsáhlými soubory osobních údajů neustále přibývá,[54] což je mimo jiné způsobeno i rozvojem internetu věcí, jak bude přiblíženo v rámci čtvrté kapitoly. S tím je v posledních letech spojováno několik rozsáhlých bezpečnostních incidentů, které byly specifické především globálním dopadem a postižením širokého spektra různých subjektů. Jde především o *malware* vytvářející *botnety*, tedy sítě ovládaných zařízení, která mohou být využita k zesílení útoku na konkrétní cíl. To byl případ široce rozšířeného *malware* s označením *Mirai* v roce 2016,[55] či značně zničujícího *malware* s označením *NotPetya*.[56]

51 Viz PRCHAL, Lukáš. Brněnská nemocnice po kyberútoku ruší operace, testování koronaviru ohrožené není. *Deník N* [online]. 2020 [cit. 14. 9. 2021].

52 Viz ČTK. Provoz benešovské nemocnice ochromil počítačový virus. *ČTK České noviny* [online]. 11. 12. 2019 [cit. 13. 7. 2021]. Dostupné z: https://www.ceskenoviny.cz/zpravy/provoz-benesovske-nemocnice-ochromil-pocitacovy-virus/1831202

53 Srov. CENTRUM KYBERNETICKÉ BEZPEČNOSTI. Kybernetické útoky míří na strategická odvětví, aktuálně na těžební společnost OKD. *Centrum kybernetické bezpečnosti* [online]. 24. 12. 2019 [cit. 13. 7. 2021]. Dostupné z: https://centrumkyberbezpecnosti.cz/kyberneticke-utoky-miri-na-strategicka-odvetvi-aktualne-na-tezebni-spolecnost-okd/

54 Viz např. RESEARCH AND MARKETS. Big Data Analytics Industry Report 2020. *GlobeNewswire News Room* [online]. 3. 2. 2020 [cit. 14. 9. 2021]. Dostupné z: http://www.globenewswire.com/news-release/2020/03/02/1993369/0/en/Big-Data-Analytics-Industry-Report-2020-Rapidly-Increasing-Volume-Complexity-of-Data-Cloud-Computing-Traffic-and-Adoption-of-IoT-AI-are-Driving-Growth.html

55 Blíže viz CLOUDFLARE. What is the Mirai Botnet? *Cloudflare* [online]. 2020 [cit. 22. 5. 2021]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/; FRUHLINGER, Josh. The Mirai botnet explained: How IoT devices almost brought down the internet. *CSO Online* [online]. 9. 3. 2018 [cit. 22. 5. 2021]. Dostupné z: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html; KREBS, Brian. New Mirai Worm Knocks 900K Germans Offline. *Krebs on Security* [online]. 30. 11. 2016 [cit. 20. 3. 2021]. Dostupné z: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

56 Blíže viz GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired* [online]. 2018 [cit. 22. 5. 2021].

Tyto hrozby přitom nesměřují pouze na významné podniky, věnující zpravidla značné úsilí na zabezpečení svých sítí a databází, ale v určité míře v podstatě na všechny subjekty zpracovávající elektronické záznamy. Jak bude dále diskutováno především v oddílu 4.4.3, může však právě u menších podnikatelských subjektů opomíjení rizik spojených s porušením bezpečnosti osobních údajů vést k závažným újmám dotčených fyzických osob, zvláště pokud tato porušení zůstávají dlouhodobě neodhalena v důsledku nedostatečných opatření zavedených těmito subjekty.

2.2 Podoby, rozsah a trend

Porušení bezpečnosti je buďto výsledkem chybného jednání nebo úmyslné snahy o neoprávněný přístup k danému souboru dat. Dané záznamy mohou být změněny, zveřejněny, smazány, zkopírovány či zneužity jiným způsobem. Přestože z hlediska právního vymezení pojmu porušení bezpečnosti osobních údajů není tento jev limitován na elektronické záznamy, jsou pro jejich rozšířenost napříč činnostmi v dnešní společnosti, jakožto i specifické vlastnosti digitálního záznamu,[57] převažující formou bezpečnostní incidenty. S ohledem na zaměření této monografie na nové formy informačních a komunikačních technologií je tak pozornost soustředěna právě na tuto převažující podobu, ač je respektováno, že porušení bezpečnosti se v závislosti na vymezení v dané právní úpravě (jako je tomu v Obecném nařízení) může dotýkat i fyzických či analogových záznamů osobních údajů.

Bezpečnostní incidenty jsou vzhledem ke svému významu v oblasti kyberbezpečnosti dobře popsaným a kategorizovaným jevem. Nicméně sjednocení těchto klasifikací je náročný úkol, jak naznačuje práce na referenční taxonomii klasifikace bezpečnostních incidentů agentury ENISA.[58] Referenční taxonomie vychází z taxonomie ecsirt.net, která mapuje bezpečnostní incidenty do deseti kategorií, každá s popisem a několika příklady. Jedná se o: zneužitelný obsah (spam, nenávistné projevy, sexuální obsah …); škodlivý kód (viry, červy *(worms)*, trojské koně …); shromažďování informací (skenování, *sniffing* …); pokusy

57 Zde je myšleno především jeho snadné rozmnožení, sdílení, úprava, a naopak nesnadné dohledání všech uniklých záznamů, kontrola šíření či zjištění pozměnění.

58 Viz Reference Incident Classification Taxonomy. *ENISA* [online]. Heraklion: ENISA 2018 [cit. 21. 10. 2021]. Dostupné z https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

o vniknutí (zneužití zranitelnosti, pokus o přihlášení …); vniknutí (neoprávněný přístup k účtu, zapojení do botnetu …); útoky na dostupnost (DDoS, sabotáž …); porušení zabezpečení informačního obsahu (neoprávněný přístup k údajům nebo jejich modifikace); podvody *(phishing, spear-phishing …)*; vytvoření zranitelnosti (*backdoor* přístupy, zveřejnění zranitelnosti …); a kategorie pro ostatní incidenty.[59] Jak ověřeno ENISA, tato taxonomie se poměrně dobře překrývá s jinými taxonomiemi (např. se společnou taxonomií pro orgány činné v trestním řízení a CSIRTy[60]), ale struktura a prvky mohou být mapovány jinak.

Příkladem je kvalifikace užívaná společností *Verizon* v pravidelných zprávách o bezpečnostní situaci v kyberprostoru od roku 2014.[61] Za běžné podoby porušení bezpečnosti záznamů lze tak označit využití zranitelností na úrovni kódu; překonání autentizačních mechanismů; dálkové narušení terminálu v místě prodeje; neoprávněné a škodlivé jednání zaměstnanců či partnerů s přístupovými právy; aktivity státem financovaných aktérů; neoprávněný sběr dat o platebních kartách *(skimming)*; útoky přerušením služby *(denial of service attack)*; neúmyslné jednání jako například zaslání informací špatnému příjemci či nevhodné nastavení online databáze; a především pak všechny formy škodlivého software *(malware)*, užívané zpravidla oportunisticky s úmyslem finančního zisku, jak názorně typizuje široké uplatnění tzv. *ransomware*.[62] Značný význam mají také neoprávněné přístupy k uchovávaným záznamům a osobním údajům skrze techniky sociálního inženýrství *(social engineering)*, kterými je dosahováno porušení bezpečnosti skrze oklamání či manipulaci uživatele s přístupovým oprávněním či přístupem k údajům (např. zaměstnance technické podpory), namísto vlastního překonání technických bezpečnostních opatření.[63]

Taxonomie umožňuje klasifikaci jevu, ale neposkytuje vhled do toho, jak je rozšířený a jaký trend sleduje. Zmapování současného stavu prostředí kybernetických bezpečnostních hrozeb je obtížné, což je problém, který ještě

59 Ibid., s. 10.

60 Ibid., s. 13.

61 Viz 2019 Data Breach Investigations Report: Executive Summary. *VERIZON* [online]. New York: Verizon, 2019, s. 7 [cit. 24. 5. 2021].

62 Srov. 2019 Data Breach Investigations Report. *VERIZON* [online]. New York: Verizon, 2019, s. 23 [cit. 24. 5. 2021].

63 Blíže viz HADNAGY, Christopher. *Social engineering The Art of Human Hacking.* Indianapolis: Wiley Publishing, 2011, s. 3.; MOUTON, Francois, Louise LEENEN a Hein S. VENTER. Social engineering attack examples, templates and scenarios. *Computers & Security* [online]. 2016, roč. 59, s. 187 a násl.

zhoršuje skutečnost, že většina dostupných údajů poskytuje pouze extrapolaci na základě souboru dat představujícího nereprezentativní fragment prostředí. S vědomím těchto omezení jsou však dostupné odhady frekvence a dopadů odhalených bezpečnostních incidentů ohromující. Zpráva společnosti *IBM* z roku 2020 došla k množství 8,5 miliardy neoprávněně zpřístupněných záznamů pouze za rok 2019.[64] Pro vyjádření tohoto objemu z jiné perspektivy pak poslouží zpráva společnosti *Thales* z roku 2020, ze které vyplývá, že 26 % jejích respondentů (tzn. zřejmě především komerčních subjektů) u sebe zaznamenalo v předchozím roce bezpečnostní incident.[65] Tato ilustrace rozšířenosti bezpečnostních incidentů v dnešní době na základě každoročních zpráv těchto společností představujících významné hráče v odvětví kyberbezpečnosti přitom stále zřejmě nepostihuje skutečný rozsah problému.

Je totiž značně pravděpodobné, že velké množství incidentů není odhaleno či přiznáno.[66] Tento předpoklad formulují také *Naghizadeh* a *Liu*, byť přiznávají, že podklady pro tyto domněnky jsou z pochopitelných důvodů nesnadno získatelné a statisticky v zásadě neprůkazné.[67] Posiluje jej však také poznatek, že i v případě sdílení informací o bezpečnostním incidentu je zpravidla zájmem dotčené entity zveřejnit co nejméně detailů,[68] tedy například nešířit údaj o celkovém množství zpřístupněných či ohrožených záznamů.[69] Proto vychází výše uvedené zprávy často z odhadů, což činí skutečnou četnost bezpečnostních incidentů o to méně uchopitelnou.[70]

64 Viz IBM X-FORCE INCIDENT RESPONSE AND INTELLIGENCE SERVICES. *X-Force Threat Intelligence Index 2020* [online]. Armonk, NY: IBM, 2020, s. 8 [cit. 3. 3. 2021].

65 Viz IDC. *The Changing Face of Data Security 2020 Thales Data Threat Report Global Edition* [online]. Paris: Thales, 2020, s. 7 [cit. 3. 3. 2021].

66 Srov. BISOGNI, Fabio, Hadi ASGHARI a Michel J. G. VAN EETEN. Estimating the size of the iceberg from its tip. In: *16th Annual Workshop on the Economics of Information Security*: *WEIS 2017* [online]. San Diego: University of California, 2017 [cit. 12. 7. 2021].

67 Srov. např. dotazník mezi účastníky konference RSA z roku 2007, ze kterého vyplynulo, že 89 % bezpečnostních incidentů v daném roce zůstalo neohlášeno. Podobně dotazník na americké podnikové bezpečnostní specialisty z roku 2013 ukázal, že 6 z 10 odhalených bezpečnostních incidentů nebylo ohlášeno či jinak sděleno. Blíže viz NAGHIZADEH, Parinaz a Mingyan LIU. Inter-Temporal Incentives in Security Information Sharing Agreements. In: *AAAI workshop on Artificial Intelligence for Cyber Security (AICS)* [online]. Phoenix: AAAI, 2016, s. 1 [cit. 12. 7. 2021].

68 Motivacím podniků ve vztahu ke sdílení informací o porušení bezpečnosti se podrobně věnuji v páté kapitole.

69 Srov. RISK BASED SECURITY. *Data Breach QuickView Report 2019 Q3 Trends* [online]. Richmond, VA: Risk Based Security, 2019, s. 10 [cit. 6. 4. 2021].

70 Ibid.

Snaha o adekvátní vykreslení rozsahu řešené problematiky je o to složitější, pokud bychom chtěli hovořit nikoliv o bezpečnostních incidentech obecně, ale pouze o případech porušení bezpečnosti zpracovávaných údajů. Narážíme zde totiž hned na dvě klíčové překážky. První překážkou je různé vnímání obsahu tohoto pojmu s ohledem na různý rozsah pojetí údajů vztahujících se k jednotlivci, jak bylo nastíněno v podkapitole 1.2. Pojem osobní údaj zakotvený v rámci unijního přístupu k ochraně osobních údajů se totiž pouze částečně překrývá se srovnatelnými pojmy v jiných právních úpravách, především pak těch ve Spojených státech amerických.[71] Ohlášené případy v různých jurisdikcích tak nevytvářejí zcela homogenní soubor, a takto shromažďovaná globální data lze tedy použít pouze pro „hrubou" představu o situaci, tak jak bylo nastíněno výše. Tento problém je možné překonat zúžením pozornosti na oblast s jednotnou úpravou, pro naše účely tedy na situaci v rámci Evropské unie.

Zde však narážíme na druhou překážku, kterou je absence dostatečné historické řady statistických údajů pro dovozování smysluplných závěrů ohledně trendů. Ačkoliv byla s použitelností Obecného nařízení v květnu 2018 zavedena plošná povinnost ohlašování případů porušení zabezpečení osobních údajů dozorovým úřadům, tak jak bude podrobně představeno v podkapitole 3.2, jsou v současné době dostupné pouze neoficiální statistiky o plnění této povinnosti. Dle těchto statistik shromážděných advokátní kanceláří *DLA Piper* bylo za období od 25. května 2018 do 27. ledna 2021 ohlášeno příslušným dozorovým úřadům v rámci EU celkem 281 000 porušení zabezpečení.[72] Jelikož daná statistika pokrývá zatím pouze tři časová období, tedy 8 měsíců od května 2018 do ledna 2019, 12 měsíců od ledna 2019 do ledna 2020 a 12 měsíců od ledna 2020 do ledna 2021, nemají trendy v těchto datech přílišnou vypovídací hodnotu. Je sice zjevný nárůst v množství ohlašovaných případů porušení zabezpečení (v prvních 8 měsících bylo ohlášeno průměrně 7 400 případů za měsíc, v následujícím roce to bylo již přes 8 300 případů za měsíc, v posledním sledovaném období pak je frekvence již téměř 10 000 případů za měsíc), ten může být však způsoben například postupným

71 Blíže se tomuto aspektu problematiky věnuji ve třetí kapitole.

72 Viz DLA PIPER'S CYBERSECURITY AND DATA PROTECTION TEAM. *DLA Piper GDPR data breach survey: January 2021* [online]. Londýn: DLA Piper, 2021, s. 11 [cit. 20. 10. 2021].

zaváděním potřebných opatření u povinných subjektů či zvyšujícím se tlakem dozorových úřadů na vymáhání dodržování ohlašovací povinnosti. Nemusí tak vypovídat o změně v intenzitě těchto jevů jako takových. O situaci v EU před rokem 2018 sice existují určitá oficiální statistická data, ta však neoperují s případy porušení zabezpečení osobních údajů, ale s počty bezpečnostních incidentů[73] a nelze je tudíž provázat s výše uvedenými daty o nic lépe než údaje ze zpráv společností působících v odvětví kyberbezpečnosti, se kterými bylo pracováno výše.

Přesto však z dostupných informací vyplývá, že obecný trend digitalizace společnosti s sebou přináší nová kyberbezpečnostní rizika, mezi které lze řadit především častější případy porušení bezpečnosti zpracovávaných údajů a zvyšující se závažnost a rozsah tohoto druhu bezpečnostních incidentů.[74] Tomuto budeme podrobněji věnovat pozornost v příslušných částech čtvrté kapitoly po představení kontextu internetu věcí, pro účely diskuse jeho dopadů na plnění povinností souvisejících s porušením bezpečnosti osobních údajů.

2.3 Újma hrozící v důsledku porušení bezpečnosti osobních údajů

Výše poskytnuté stručné nastínění prostředí bezpečnostních incidentů dotýkajících se osobních údajů by mělo čtenáři poskytnout základní představu o situacích, ve kterých uchovávané či zpracovávané osobní údaje unikají z kontroly správce či zpracovatele a mohou být zneužity třetí stranou k újmě dotčeného jednotlivce. Nyní zaměřme pozornost na podoby, kterých tato újma může nabývat, jelikož je zřejmé, že v závislosti na konkrétním případě může nabývat různé míry závažnosti.

---

73 Srov. např. POLICY DEPARTMENT A ECONOMIC AND SCIENTIFIC POLICY. *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts* [online]. IP/A/ITRE/NT/2013-5 PE 507.476. Brussels: Directorate-General for Internal Policies. 2013 [cit. 12. 7. 2021]; Relevantní jsou v tomto směru také statistiky ENISA, viz ENISA. Incident Reporting. *European Union Agency for Cybersecurity* [online]. 2020 [cit. 13. 7. 2021]. Dostupné z: https://www.enisa.europa.eu/topics/incident-reporting

74 Srov. X-Force Threat Intelligence Index 2020. *IBM X-Force Incident Response and Intelligence Services*. [online]. Armonk, NY: IBM, 2020, s. 5 [cit. 3. 3. 2021]; The Changing Face of Data Security 2020 Thales Data Threat Report Global Edition. *IDC* [online]. Paris: Thales, 2020, s. 23 [cit. 3. 3. 2021].

V nejzákladnější rovině dochází neoprávněným zpřístupněním a případně šířením osobních údajů, které mohou být citlivé či intimní povahy, k narušení soukromí a práva na ochranu osobních údajů ve smyslu práva na informační sebeurčení.[75] Nekontrolovatelná dostupnost jinak privilegovaných informací o osobním životě, charakteristikách, preferencích, názorech, volbách či jednání jednotlivce může mít negativní dopad na jeho společenské, pracovní či osobní postavení.[76] S ohledem na postavení a společenskou roli dané fyzické osoby může tento zásah do osobnostního práva nabývat i formy zásahu do dobré pověsti.[77]

Od dostupnosti těchto jinak neveřejných informací o jednotlivci se následně odvíjejí další možná zneužití.[78] Informace o návycích, zájmech či slabostech jedince mohou být uplatněny při profilování vhodných cílů náchylných pro sociální inženýrství či jiné nelegální praktiky a následnému zvýšenému ohrožení aktiv této osoby či třetích osob, k nimž umožní její manipulace či oklamání přístup (např. zaměstnavatele).

Zde lze zmínit nedávný případ porušení bezpečnosti mobilní aplikace pro izraelské voliče, kterým došlo k neoprávněnému zpřístupnění identifikačních údajů 6,5 milionu voličů (celá jména, adresy, čísla průkazů totožnosti) několik týdnů před celostátními volbami.[79] Lze například zvažovat využití takto zpřístupněných informací pro zohlednění nerelevantních aspektů osobnosti dotčené osoby v rámci rozhodovacích či hodnotících procesů, a tedy za účelem diskriminace.

Jelikož je však významná část nelegálních aktivit, které vedou k porušení bezpečnosti motivována finančním ziskem, pojí se se zpřístupněním citlivých osobních údajů zpravidla rizika vydírání nebo krádeže identity. Vydírání je v tomto směru jen dalším nástrojem z arzenálu sociálního inženýrství, kdy

75 Těmto aspektům problematiky jsem se blíže věnoval v KASL, František. 9 Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 424–427.

76 Např. veřejná dostupnost nelichotivých informací o soukromém životě či jinak v soukromí sdílených názorů může mít vliv na atraktivitu jedince při pracovním pohovoru.

77 Např. zveřejnění soukromé korespondence veřejně známé osoby může mít negativní dopad na její popularitu.

78 Srov. KASL, František. 9 Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 434.

79 Viz VICTOR, Daniel, Sheera FRENKEL a Isabel KERSHNER. Personal Data of All 6.5 Million Israeli Voters Is Exposed. *The New York Times* [online]. 2020 [cit. 13. 7. 2021].

může být využita hrozba zpřístupnění kompromitujících či dehonestujících informací osobám blízkým, osobám v nadřízeném postavení, či jejich prosté zveřejnění jako nástroj k vynucenému zneužití funkce či oprávnění dané osoby.

Zde je vhodným příkladem porušení bezpečnosti služby *Ashley Madison* z července 2015.[80] Šlo o únik údajů (jmen, adres, přístupových údajů, platebních údajů, historie vyhledávání, seznamu preferencí) vztahujících se k uživatelům této komerční seznamovací platformy pro manželskou nevěru. Již vlastní veřejná dostupnost těchto citlivých údajů představuje zásah do soukromí a dobré pověsti identifikovatelných jednotlivců a měla pravděpodobný negativní dopad na jejich manželské, společenské či pracovní vztahy. Tyto informace mohly být dále zneužity k manipulaci těchto osob, či jejich vydírání. K vydírání docházelo zvláště u osob s e-mailovými adresami s koncovkou .sa (cizoložství je totiž v Saudské Arábii trestným činem), .mil (členové vojenských sil Spojených států), či .gov (vládní zaměstnanci institucí Spojených států).[81] V jiných případech může hrozba namísto zveřejnění směřovat k trvalé ztrátě přístupu k daným údajům, typicky skrze *ransomware*.[82]

Oproti konfrontačnímu zneužití osobních údajů skrze vydírání je pak krádež identity o to záludnější, jelikož na ni nemusí být dotčená osoba vůbec upozorněna. Rizika s ní spojená jsou však o to vyšší, o co významnější daná virtuální identita a související účet pro jednotlivce je. Naše závislost na různých účtech k online službám (např. e-mail, internetové bankovnictví, účty na obchodních portálech, účty mediálních služeb, účty na sociálních sítích či přístupové oprávnění do sítě zaměstnavatele) se přitom zvýraznila při snaze každého z nás o běžné fungování v režimu vynuceného omezení sociálního kontaktu a přesunu většiny mezilidské interakce do kyberprostoru.

80 Viz MANSFIELD-DEVINE, Steve. The Ashley Madison affair. *Network Security* [online]. 2015, roč. 2015, č. 9, s. 8.

81 Srov. FRANCE 24. The global fallout of the Ashley Madison hack. *France 24* [online]. 2015 [cit. 24. 5. 2021].

82 Jedná se o *malware*, který zašifruje bezpečnostním klíčem data v zařízení oběti a vydírá ji k platbě či aktivitě, za kterou je jí slibován bezpečnostní klíč, a tudíž opětovný přístup k datům. Blíže k tomuto pojmu viz KHARRAZ, Amin et al. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: ALMGREN, Magnus, Vincenzo GULISANO a Federico MAGGI (eds.). *Detection of Intrusions and Malware, and Vulnerability Assessment* [online]. Cham: Springer International Publishing, 2015, Lecture Notes in Computer Science.

Útočník při krádeži identity překoná bezpečnostní opatření daného účtu zpravidla skrze znalost přístupového jména a hesla, případně skrze změnu těchto parametrů či nastavení zabezpečení díky kontrole a přístupu k jinému účtu (např. kontaktnímu e-mailu). Následně může v zásadě bez omezení operovat s daným účtem. Hrozbu pro aktiva, kontakty či soukromí dotčené osoby bezpochyby představuje aktivita útočníka v podobě převzetí kontroly nad daným účtem (např. bankovní účet), jeho smazání (např. účet na online tržištích a související ztráta benefitů) či pozměnění záznamů (např. šíření problematického obsahu přes účet na sociální síti). Výsledkem je tak neoprávněné jednání útočníka cizím jménem a na cizí účet, přičemž vzhledem k nabytí identity oběti je nesnadné odlišit jednání oběti a jednání útočníka, čímž vyvstává problém s přičitatelností následků a nákladů tohoto často škodlivého jednání. Nepominutelné riziko je však spojeno již se samotným volným a skrytým přístupem útočníka do daného účtu, který jej může užívat pouze pasivně pro sledování aktivit dané osoby (např. čtení pošty na e-mailovém účtu) a minimalizovat tak možnost dotčené osoby zjistit, že k jejímu účtu má neoprávněný přístup třetí osoba. Krádež identity tak představuje riziko zásadního narušení osobního a sociálního postavení jedince, jeho ztrátu kontroly nad vlastní identitou v době, kdy virtuální identity jsou stále významnější složkou naší osobnosti a sociální role. Následky spojené s řešením odhalené krádeže identity pak často pro oběť přinášejí vysoké finanční či časové náklady, narušení běžného života či vztahů, psychické a emoční zatížení, zvláště pokud je řešení obtížné a zdlouhavé.[83]

Vedle dopadu na dotčené jednotlivce způsobují porušení bezpečnosti zpracovávaných údajů také přímé a nepřímé náklady dotčené entitě, tedy správci či zpracovateli osobních údajů. Zveřejnění informace o významném porušení bezpečnosti a související ohrožení údajů zpracovávaných danou entitou může zasáhnout její dobrou pověst, přinést negativní pozornost médií, vést ke ztrátě důvěry ze strany obchodních partnerů a uživatelů, či zvýšit náklady pojistného či operativního financování.[84] Potenciálně vysoké náklady se také

83 Blíže viz LAI, Fujun, Dahui LI a Chang-Tseh HSIEH. Fighting identity theft: The coping perspective. *Decision Support Systems* [online]. 2012, roč. 52, č. 2.

84 Srov. BOASIAKO, Kwabena Antwi a Michael O'CONNOR KEEFE. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. *SSRN Electronic Journal* [online]. 2018, s. 2 [cit. 5. 9. 2021].

pojí s uložením regulatorní sankce za nedostatečná bezpečnostní opatření či se soudními spory s poškozenými jednotlivci o náhradu způsobené újmy.[85] Tyto náklady přitom rozhodně nelze považovat za zanedbatelné. Každoroční zpráva *Ponemon Institute* o nákladech bezpečnostních incidentů uvádí průměrné celkové náklady na takovýto incident za rok 2019 v blízkosti čtyřech milionů USD[86] při průměrném nákladu 150 USD na dotčený záznam[87] a při disproporčně vyšších relativních nákladech u menších podniků.[88] I z tohoto důvodu bude rostoucím výzvám spojeným se zabezpečením sítí a systémů mikropodniků s rozvojem nových technologií věnována zvláštní pozornost v příslušené kapitole 4.4.3 této monografie.

2.4 Shrnutí kapitoly

V rámci této kapitoly jsem čtenáři poskytl úvodní vhled do současné globální situace a trendů v oblasti bezpečnostních incidentů a porušení bezpečnosti zpracovávaných údajů. Na oba tyto pojmy jsem přitom nahlížel primárně z kyberbezpečnostní perspektivy, tedy jako na realizaci hrozeb pro chráněná aktiva, bez specifického zohledňování souvisejícího právního rámce (tomu věnuji následující kapitolu).

Předně zde poukazuji na skutečnost, že se jedná o hrozbu inherentně spojenou s užíváním informačních a komunikačních technologií ke společenské interakci. Nárůst četnosti, jakož i intenzita a škodlivý dopad bezpečnostních incidentů se tudíž zásadně stupňuje s rozvojem digitalizace společnosti, nárůstem konektivity a přibývajícím množstvím zpracovávaných údajů. Tento obecný trend, podložený nejen příklady významných bezpečnostních incidentů, ale též dostupnými statistikami, nám poskytuje výchozí bod pro analýzu proměny, kterou přináší internet věcí, obsaženou ve čtvrté kapitole, především pak při nalézání odpovědí na dílčí otázky (3)[89] a (4)[90].

85 Viz KAMIYA, Shinichi et al. What is the Impact of Successful Cyberattacks on Target Firms? *National Bureau of Economic Research: Working Papers* [online]. 2018, roč. 2018, č. 24409 [cit. 25. 5. 2021].

86 Viz PONEMON INSTITUTE. *Cost of a Data Breach Report 2019* [online]. Traverse City: IBM Security, 2019, s. 18 [cit. 22. 5. 2021].

87 Ibid., s. 19.

88 Ibid., s. 20.

89 Dochází v tomto prostředí k navýšení četnosti a rozsahu porušení bezpečnosti?

90 Narůstá zde též intenzita a škodlivý dopad případů porušení bezpečnosti?

Z představených informací o aktuální situaci dále vyplývá, že problematika porušení bezpečnosti nabývá značného a stále rostoucího rozsahu, což značí, že se jedná o významné téma s nepominutelným společenským dopadem. V konkrétních případech přitom může být situace velmi různorodá, jak jsem se v rámci kapitoly snažil poodhalit. Je možné identifikovat velmi rozsáhlé případy porušení bezpečnosti zpracovávaných údajů, které přivodili značnou újmu milionům dotčených osob. Daleko častěji však dochází k převážně přehlíženým či dokonce neodhaleným případům porušení bezpečnosti menšího rozsahu či u méně exponovaných subjektů, které však jsou i tak s to přivodit zásadní újmu jednotlivým fyzickým osobám. Za nejvážnější formu újmy pro jednotlivce jsem identifikoval krádež identity, tedy zjevnou či skrytou ztrátu (výlučné) kontroly nad částí svých uživatelských účtů či nad jinými projevy své virtuální identity. Současně jsem věnoval pozornost negativním dopadům, které případ porušení bezpečnosti má na postiženou entitu. Ty lze přitom dělit na takové, které vyplývají z incidentu samotného a ty, které jsou dodatečným následkem sdílení informací o této události a jejích parametrech. Právě existence druhé kategorie nákladů pro postiženou entitu, kterých se lze do značné míry vyvarovat při utajení a interním vyřešení daného incidentu, bude vystupovat do popředí jako prvek morálního hazardu v rámci zkoumání motivace povinných podniků pro neplnění notifikačních povinností v kapitole páté.

Předtím, než přistoupím k této perspektivě je však na místě soustředit pozornost na vývoj, systematiku a prvky unijní a americké právní úpravy. Ty přitom reflektují rozsah a závažnost hrozeb pojících se s těmito jevy. Směřují tudíž především ke zvýšení transparentnosti ohledně činností a opatření povinných subjektů jak ve vztahu k předcházení porušení bezpečnosti zpracovávaných údajů, tak ve snaze přispět ke snížení následné újmy skrze efektivnější komunikaci a spolupráci mezi postiženou entitou, dotčenými jednotlivci a regulatorními orgány.

3 PRÁVNÍ ÚPRAVA POVINNOSTÍ SPOJENÝCH S PORUŠENÍM BEZPEČNOSTI

Reforma unijního práva na ochranu osobních údajů představovaná především přijetím a následnou přímou použitelností Obecného nařízení dne 25. května 2018 přinesla mnoho nových prvků. S nimi souvisí i řada výzev pro povinné subjekty v postavení správců a zpracovatelů osobních údajů v souvislosti s činnostmi v rámci Evropské unie. Mezi nimi, v podobě ustanovení článků 33 a 34 Obecného nařízení byla zásadně rozšířena aplikovatelnost, do té doby značně opomíjených, právních povinností ohlašování a oznamování případů porušení zabezpečení osobních údajů. Ty byly dříve relevantní pouze pro malý okruh podniků v roli poskytovatelů veřejně dostupných služeb elektronických komunikací.[91]

Pro relativně nízkou pozornost, kterou tato část novinek v rámci Obecného nařízení vzbudila v akademickém diskurzu, je mým cílem napříč touto kapitolou poukázat na významnost role, kterou tento prvek transparentnosti a odpovědnosti ve struktuře ochrany osobních údajů dle mého názoru zaujímá. K tomu bude přistoupeno historickou a systematickou analýzou těchto povinností, a to nejen z hlediska zrodu příslušných norem v Obecném nařízení, ale následně také s přihlédnutím ke srovnatelné úpravě v právu Spojených států amerických. Ta na jedné straně sloužila jako inspirace unijnímu normotvůrci, a na druhé straně nabízí s ohledem na délku, rozsah a různorodost zdejší úpravy přínosné akademické i praktické vstupy do prozatím značně omezeného evropského diskurzu týkajícího se této problematiky.

Závažnost časté informační asymetrie mezi entitou, u které došlo k porušení bezpečnosti na straně jedné a regulatorním orgánem či dotčenými fyzickými osobami na straně druhé byla totiž předmětem pozornosti amerických zákonodárců již na počátku milénia. Průkopnickým právním předpisem byl v tomto směru statutární předpis *California Senate Bill 1386* z roku 2002,[92]

91 Této úpravě je věnován oddíl 3.1.1.

92 Srov. An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. *California legislative information* [online]. 26. 9. 2002 [cit. 13. 7. 2020]. Blíže je předpis představen na úvod oddílu 3.3.3.

který zahájil trend směřující k vynucování vyšší transparentnosti na základě povinnosti postižených entit urychleně sdílet informace o tomto porušení bezpečnosti s dotčenými fyzickými osobami, a případně též regulatorními orgány. Přestože doposud nedošlo k přijetí jednotící federální úpravy, existuje dnes ve Spojených státech rozsáhlý soubor státních předpisů a regulatorních rámců pro vybraná odvětví, který je v řadě ohledů komplexnější než v EU použitelná úprava dle Obecného nařízení.

Ta přitom i tak představuje nesnadnou výzvu pro řadu správců osobních údajů v EU, kteří museli přizpůsobit vnitřní procesy dokumentační, ohlašovací a oznamovací povinnosti, avšak postrádali příslušné zkušenosti nebo oborově specifikovaná doporučení, jak k tomu přistoupit. Situace se sice v tomto směru od data použitelnosti nařízení do určité míry zlepšila, ovšem, jak bude poukázáno v rámci následující čtvrté kapitoly, v mezičase technologický pokrok přináší nové výzvy, se kterými se musejí povinné subjekty stále častěji vypořádat. Napříč publikací jsou tak předkládány argumenty pro tezi, že bez adekvátních podpůrných opatření a uzpůsobení těchto povinností na novou realitu internetu věcí bude jejich uplatnění značně ztíženo, což bude mít negativní dopad (nejen) na úroveň ochrany práv a zájmů subjektů údajů.

3.1 Povinnosti před použitelností Obecného nařízení

Unijní právní rámec ochrany osobních údajů byl po dlouhou dobu primárně formován harmonizačními snahami na základě směrnice 95/46/ES o ochraně osobních údajů.[93] Problematika případů porušení bezpečnosti osobních údajů zde přitom nebyla přímo zohledněna, což může souviset s poměrně nerozvinutým prostředím Internetu a relativně nevýznamným hrozbám bezpečnostních incidentů v evropském prostředí na počátku 90. let. Ostatně i v americkém prostředí, které lze (nejen) v té době vnímat na popředí technologického rozvoje na poli ICT, byly sice zaznamenány některé významné případy porušení bezpečnosti zpracovávaných údajů (jako případ společnosti *TRW* představený v rámci podkapitoly 2.1), ale přesto v něm nedošlo v tomto období k prosazení konceptu notifikačních povinností.[94]

93 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

94 Blíže viz podkapitola 3.3.

3.1.1 Poskytovatelé veřejně dostupných služeb elektronických komunikací

První relevantní unijní úpravu povinností spojených s porušením bezpečnosti osobních údajů obsahovala teprve směrnice 2009/136/ES,[95] kterou byla upravena směrnice 2002/58/ES, o soukromí a elektronických komunikacích.[96] Aplikace se přitom omezovala na poskytovatele veřejně dostupných služeb elektronických komunikací, obsahovala však již v zásadě definice, strukturu a prvky, které se staly základem úpravy v článcích 33 a 34 Obecného nařízení.

Tímto unijním předpisem byla zavedena definice narušení bezpečnosti osobních údajů[97] *(personal data breach; Verletzung des Schutzes personen bezogener Daten; violation de données à caractère personnel)*, v podobě *„narušení bezpečnosti, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně či neoprávněnému vyzrazení nebo zpřístupnění osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných v souvislosti s poskytováním veřejně dostupné služby elektronických komunikací ve Společenství."*[98] Tato definice byla pak následně bez obsahových změn přenesena do návrhu Obecného nařízení.[99] Transpozice do českého práva zákonem č. 127/2005 Sb., o elektronických komunikacích, přitom operuje s pojmem *porušení ochrany osobních údajů*.[100]

95 Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.

96 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

97 České znění směrnice sice používá poněkud odlišné termíny, než transponující národní předpisy či Obecné nařízení, vzhledem k jednotnosti terminologie v jiných jazycích členských států se však dle mého názoru jedná o nedostatek českého znění, nikoliv o normativně relevantní terminologický vývoj. Podrobně jsem se této nejednotnosti věnoval v KASL, František. K pojmové nejednotnosti porušení zabezpečení/bezpečnosti osobních údajů v českém právu. *AUC IURIDICA* [online]. 2019, roč. 2019, č. 3.

98 Srov. čl. 2 písm. i) konsolidovaného znění směrnice 2002/58/ES.

99 Viz Návrh 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). *Evropská komise* [online]. COM(2012) 11 final 2012/0011 (COD). Brusel: Evropská komise, 2012, s. 7 [cit. 29. 4. 2021].

100 Viz § 2 písm. y) zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů. In: ASPI.

Poskytovateli byla ustanovením článku 4 odst. 3 a 4 konsolidovaného znění směrnice 2002/58/ES ve vztahu k těmto situacím uložena trojí povinnost. Tato struktura notifikačních povinností zůstala zachována i v Obecném nařízení, kde se jedná o povinnost ohlašování, povinnost oznamování a povinnost dokumentace, jak bude podrobně rozebráno dále v této kapitole.

Ohlašovací povinnost:[101] První povinnost, nepodmíněná, oznámit všechna narušení bezpečnosti osobních údajů bez zbytečného prodlení příslušnému vnitrostátnímu orgánu. Tím byl v českém prostředí na základě § 88 odst. 4 zákona č. 127/2005 Sb. stanoven Úřad pro ochranu osobních údajů (dále jen „Úřad").

Oznamovací povinnost: Druhá je pak podmíněna tím, že *„je pravděpodobné, že narušení bezpečnosti osobních údajů nepříznivě ovlivní osobní údaje nebo soukromí účastníka nebo jednotlivce"*.[102] Transpozice v české úpravě přitom tuto podmínku formuluje jinak, když ji váže na způsobilost porušení ochrany osobních údajů *„ovlivnit zvláště závažným způsobem soukromí fyzické osoby"*.[103] Tyto dvě množiny přitom mohou zahrnovat odlišné situace a staví poskytovatele před výkladovou nejistotu.[104] Pokud poskytovatel vyhodnotí, že je podmínka naplněna, je povinen dané narušení bez zbytečného prodlení oznámit rovněž dotčené fyzické osobě. I za splnění této podmínky však nemusí poskytovatel k informování přistoupit, pokud ke spokojenosti Úřadu prokázal, že zavedl náležitá technická ochranná opatření ve vztahu k dotčeným údajům.[105] Úřad pak může naopak na základě svého zhodnocení situace uložit povinnost

101 Za účelem zvýšení přehlednosti textu a usnadnění orientace čtenáře je napříč prací doplněno označení dílčího tématu či problematiky, které je daný odstavec či několik odstavců věnováno. V souladu s podkapitolou 1.2 zde užívám pojmu ohlášení, jelikož jde o sdělení informací dozorovému úřadu, ačkoliv česká právní úprava používá pojmu oznámení.

102 Srov. čl. 4 odst. 3 konsolidovaného znění směrnice 2002/58/ES.

103 Srov. § 88 odst. 5 zákona č. 127/2005 Sb.

104 Množina situací, kdy je na místě oznámit incident dle unijní úpravy je zjevně širší, jelikož nepříznivé ovlivnění je širší pojem než ovlivnění zvláště závažným způsobem a osobní údaje se neomezují pouze na soukromí jednotlivce. Je přitom na místě respektovat eurokonformní výklad předmětných ustanovení národního předpisu. Tyto úvahy jsou relevantní i za použitelnosti Obecného nařízení, jelikož jím nebyla příslušná úprava zrušena a uplatňuje se tedy u příslušných povinných subjektů paralelně s povinnostmi dle čl. 33 a 34 Obecného nařízení.

105 Tato opatření mají učinit případné neoprávněně zpřístupněné údaje nesrozumitelné a zabránit tak možnému dalšímu zpracování. Lze tedy uvažovat především o šifrování a pseudonymizaci.

informovat dotčené uživatele a jednotlivce, i pokud z pohledu poskytovatele není výše uvedená podmínka naplněna.[106]

Oznámení má obsahovat alespoň informace:

1. o povaze narušení bezpečnosti;
2. o kontaktním místu, kde je možné získat více informací; a
3. o doporučených opatřeních ke zmírnění možných nepříznivých důsledků ze strany dotčených osob.

Ohlášení příslušnému orgánu dozoru nadto zahrnuje také:

4. popis důsledků narušení bezpečnosti; a
5. popis již přijatých či navrhovaných opatření ze strany poskytovatele.[107]

Dokumentační povinnost: Třetí povinností poskytovatele je pak vést přehled narušení bezpečnosti osobních údajů zahrnující okolnosti porušení, jeho následky a opatření přijatá pro jeho nápravu, a to především pro potřeby případného přezkumu ze strany Úřadu.

V návaznosti na zhodnocení transpozice těchto povinností do národních předpisů členských států využila Evropská komise (dále jen „Komise“) zmocnění dle čl. 4 odst. 5 konsolidovaného znění směrnice 2002/58/ES k vydání nařízení Komise 611/2013,[108] upravujícího a sjednocujícího okolnosti, formát a postupy při oznamování případů narušení bezpečnosti. Toto nařízení Komise 611/2013 pak přináší řadu dílčích specifikací povinností, které taktéž našly svou cestu do úpravy obsažené v článcích 33 a 34 Obecného nařízení, jak bude přiblíženo dále. To je dáno skutečností, že předmětné nařízení Komise 611/2013 bylo již připravováno paralelně s legislativními pracemi na návrhu Obecného nařízení.[109]

Nařízení Komise 611/2013 předně stanovilo konkrétní lhůty pro oznámení narušení bezpečnosti příslušnému orgánu, konkrétně 24 hodin po zjištění pro oznámení alespoň prvotních informací a 72 hodin od tohoto prvního oznámení pro zbývající informace. Případnou nemožnost dodržení lhůt musí

106 To se může týkat především výše zmíněné výkladové nejistoty a aplikace eurokonformního výkladu Úřadem na situaci, kdy se daný poskytovatel držel úzkého výkladu národního předpisu.

107 Srov. čl. 4 odst. 3 konsolidovaného znění směrnice 2002/58/ES.

108 Nařízení Komise (EU) 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.

109 Srov. bod odůvodnění 19 nařízení Komise 611/2013.

poskytovatel odůvodnit.[110] Dále je upravena spolupráce mezi dozorovými orgány při narušení bezpečnosti dotýkající se údajů osob z více členských států.[111] Jsou také specifikovány parametry relevantní pro posouzení, zda je splněna podmínka pro oznámení dotčeným jednotlivcům. Dle čl. 3 odst. 2 nařízení Komise 611/2013 je na místě přihlížet především k:

1. povaze a obsahu dotčených osobních údajů;[112]
2. pravděpodobným důsledkům pro dotčeného jednotlivce;[113] a
3. okolnostem narušení bezpečnosti osobních údajů.[114]

Dále je specifikováno, že oznámení dotčeným jednotlivcům je (časově) nezávislé na ohlášení dozorovému orgánu. Mělo by proběhnout, jakmile má poskytovatel k dispozici příslušné informace. Lze jej přitom oddálit jen ve výjimečných případech, např. v zájmu trestního vyšetřování.[115] Pokud poskytovatel přes vynaložené úsilí není schopen ve lhůtě identifikovat všechny dotčené osoby, může přistoupit k oznámení informací pomocí hlavních celostátních nebo regionálních médiích, přesto má však pokračovat v úsilí o přímé kontaktování všech dotčených jednotlivců.[116]

V nařízení Komise 611/2013 byla také vymezena vhodná technická opatření, která umožňují uplatnění výjimky z oznamovací povinnosti vůči jednotlivcům. Jedná se o účinnou ochranu obsahu údajů za pomoci šifrování, kódování či hashování.[117] Tato opatření sama o sobě však nelze považovat za dostatečná. Poskytovatelé by měli také provádět vhodná organizační a technická opatření na prevenci, odhalování a zamezení narušení bezpečnosti osobních údajů.[118]

110 Viz čl. 2 odst. 3 nařízení Komise 611/2013.
111 Viz čl. 2 odst. 5 nařízení Komise 611/2013.
112 Za významné jsou považovány především finanční informace, zvláště citlivé kategorie údajů, lokalizační údaje, internetové soubory protokolů, historie navštívených webových stránek, údaje týkající se elektronické pošty či údaje o uskutečněných voláních.
113 Zejména jde o riziko, že by porušení mohlo vést ke krádeži nebo zneužití, fyzické újmě, psychickému strádání, ponížení nebo poškození pověsti dané osoby.
114 Zejména zda je poskytovateli známo, že údaje byly odcizeny a jsou v držení neoprávněné osoby.
115 Srov. čl. 3 odst. 3 a 5 a také bod odůvodnění 13 nařízení Komise 611/2013.
116 Srov. čl. 3 odst. 7 a také bod odůvodnění 14 nařízení Komise 611/2013.
117 Srov. čl. 4 odst. 2 nařízení Komise 611/2013. Šifrování je zabezpečení záznamu za pomoci normalizovaného algoritmu, kódování znamená převedení záznamu do pevně stanoveného kódu či znakové sady a hashování představuje užití hash funkce, což je specifická široce užívaná forma kódování.
118 Srov. bod odůvodnění 17 nařízení Komise 611/2013.

Zkušenosti s plněním představených povinností poskytovatelů veřejně dostupných služeb elektronických komunikací, za jejichž porušení jim dle české právní úpravy hrozí sankce za přestupek do výše 20 000 000 Kč,[119] jsou nejen ze strany Úřadu 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.“*[120]

Nastíněný problém motivace povinných subjektů ke sdílení informací s dozorovým úřadem či dotčenými fyzickými osobami ohledně situace, která pro ně představuje riziko sankcí či jiných negativních nákladů je vlastní problematice ohlašování porušení bezpečnosti zpracovávaných údajů (tedy i dále představené úpravě dle Obecného nařízení či úpravám z amerického prostředí) a bude mu proto věnována zvláštní pozornost především v páté a šesté kapitole.

3.1.2 Národní úpravy povinností ve spojitosti s porušením bezpečnosti

Nejen na základě transpozice výše zmíněné směrnice se povinnosti související s porušením bezpečnosti osobních údajů dostaly do národních právních řádů členských států. Například ve Španělsku byla určitá omezená forma ohlašovací povinnosti a registru ohlášených případů porušení zavedena již královským dekretem o ochraně osobních údajů *(Real Decreto de protección de datos de carácter personal)* z roku 2007 skrze článek 90.[121] Také v Německu byly tyto povinnosti v omezené míře upraveny již od července 2009[122] i nad rámec výše představené směrnice, a to na základě dnes již neúčinného § 42a federálního

119 Srov. § 88 a 118 odst. 12 písm. a) a odst. 22 písm. c) zákona č. 127/2005 Sb.

120 Srov. BURIAN, David a Zuzana RADIČOVÁ. K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR). *Právní prostor* [online]. 25. 2. 2016 [cit. 13. 7. 2021]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr

121 Viz MINISTERIO DE JUSTICIA. *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* [online]. 19. 4. 2008 [cit. 12. 7. 2021].

122 Srov. EHMANN, Eugen. *Lexikon für das IT-Recht 2017/2018. Spezialausgabe für Behörden*. 5. vyd. Heidelberg: Jehle, 2017, s. 74.

zákona na ochranu osobních údajů *(Bundesdatenschutzgesetz)*.[123] V Nizozemí pak nabyl k 1. lednu 2016 účinnosti zvláštní národní právní předpis, který zavedl úpravu ohlašování a oznamování případů porušení bezpečnosti osobních údajů i pro mezidobí před přímou použitelností Obecného nařízení.[124]

3.2 Ohlašování, oznamování a dokumentace porušení zabezpečení dle Obecného nařízení

Byla to však až použitelnost Obecného nařízení, která s sebou přinesla skutečně významný posun v evropském vnímání adekvátní normativní reakce na rostoucí všudypřítomnost bezpečnostních rizik při zpracování osobních údajů. Tato úprava je s ohledem na její současnou použitelnost zvláště významná pro řešenou problematiku, bude tudíž přistoupeno k jejímu funkčnímu výkladu.[125] Nejprve bude rozebrán historický legislativní vývoj příslušných ustanovení Obecného nařízení a poté bude představena struktura a hlavní prvky platného a použitelného znění. V rámci navazující diskuse bude nejprve sledována vazba těchto ustanovení na nařízení jako celek, pak bude identifikován soubor objektivních, racionálních a dostatečně konkrétních účelů[126] těchto norem a na závěr budou nastíněny současné výzvy spojené s řádným plněním uložených povinností, na což bude navázáno v šesté kapitole při nalézání řešení pro jejich překonání.

3.2.1 Legislativní vývoj relevantních ustanovení Obecného nařízení

Již během přijímání výše zmíněné změnové směrnice 2009/136/ES v roce 2009 formuloval Evropský parlament výzvu k vytvoření podobné úpravy ohlašovací, oznamovací a dokumentační povinnosti porušení bezpečnosti aplikovatelné bez takto úzkého sektorového vymezení. V argumentaci

123 Srov. § 42a Bundesdatenschutzgesetz, BGBl. I S. 66, alte Fassung.

124 Viz BRUYNE, M. F. de. *Data breach notification and the risk of over-notification under the GDPR. A comparative analysis of US and EU experiences in practice*]. Master's Thesis. Tilburg, Tilburg University, 2016, s. 51.

125 K podrobnějšímu vyložení postupu viz výše podkapitola 1.4 osvětlující zvolenou metodologii této monografie. K pojmu funkčního výkladu pak blíže SEHNÁLEK, David. *Specifika výkladu práva Evropské unie a jeho vnitrostátní důsledky*. Praha: C. H. Beck, 2019, s. 110 a násl.

126 Právě jeho vymezení je Sehnálkem vnímáno za nezbytný krok v procesu výkladu unijního předpisu. Srov. SEHNÁLEK, David. *Specifika výkladu práva Evropské unie a jeho vnitrostátní důsledky*. Praha: C. H. Beck, 2019, s. 117.

přitom stálo, že *„zájem uživatelů být informován zřetelně není omezen na sektor elektronických komunikací, a tudíž by měl být v režimu priority zaveden na úrovni Společenství výslovný mandatorní požadavek notifikace použitelný na všechny sektory."*[127]

Tento záměr byl převzat Komisí a soubor předmětných povinností aplikovatelný bez sektorového omezení měl své místo již v úvodní zmínce o reformě ochrany osobních údajů v roce 2010.[128] Podporu tomuto kroku vyjádřil v roce 2011 také Evropský inspektor ochrany údajů v příslušném stanovisku k prohlášení Evropské komise.[129]

Znění navržené Komisí: Formulace článků 31 a 32 návrhu Komise na budoucí znění Obecného nařízení (pozdější články 33 a 34 Obecného nařízení) přímo navazovala na strukturu povinností založených směrnicí 2009/136/ES.[130] Navrhovaný článek 31(33) zaváděl přísnou lhůtu pro ohlášení dozorovému úřadu během 24 hodin po odhalení porušení zabezpečení osobních údajů.[131] Povinnost oznámení dotčeným subjektům údajů podle článku 32(34) byla dána, pokud je *„… pravděpodobné, že narušení bezpečnosti osobních údajů se nepříznivě dotkne ochrany osobních údajů nebo soukromí subjektu údajů …"*[132] Výjimkou z této povinnosti by bylo dle odstavce 3 dostatečné prokázání přítomnosti přiměřených technických ochranných opatření, která činí příslušné údaje nesrozumitelné pro neoprávněné zpracování.[133] Navázání na koncept založený směrnicí 2009/136/EC je zde více než zřejmé.

Článek 31(33) také obsahoval později vypuštěný odstavec 5, který zakládal zvláštní zmocnění Komise, aby přijala prováděcí předpis specifikující kritéria

127 *„… [t]he interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority …"* Srov. EUROPEAN PARLIAMENT. *Position of the European Parliament* [online]. EP-PE_TC2-COD(2007)0248. Strasbourg: European Parliament, 2009, s. 21 [cit. 24. 5. 2021].

128 Viz EUROPEAN COMMISSION. *Communication from the Commission* [online]. COM/2010/0609 final. Brussels: European Commission, 2010 [cit. 24. 5. 2021].

129 Srov. HUSTINX, Peter. *Opinion of the European Data Protection Supervisor on the Communication from the Commission* [online]. Brussels: European Data Protection Supervisor, 2011, s. 17 [cit. 24. 5. 2021].

130 Srov. Návrh 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). *Evropská komise* [online]. COM(2012) 11 final 2012/0011 (COD). Brusel: Evropská komise, 2012, s. 10 [cit. 29. 4. 2021].

131 Ibid., s. 58.

132 Ibid., s. 59.

133 Ibid.

porušení zabezpečení osobních údajů a vymezující konkrétní podmínky, za kterých je správce a zpracovatel povinen ohlašovat tyto případy.[134] Tento přístup byl také převzat ze směrnice 2009/136/ES, jak bylo nastíněno výše při představení nařízení Komise 611/2013. Článek 32(34) obsahoval podobný odstavec 5 vztahující se ke specifikaci okolností, za nichž je případ porušení zabezpečení osobních údajů pravděpodobně způsobilý mít negativní dopad na dotčené osobní údaje.[135] Ani tento text nepřetrval do finálního znění.

Znění přijaté v prvním čtení Evropským parlamentem: Text, který byl přijat Evropským parlamentem v březnu 2014 na základě 621 z 653 možných hlasů,[136] přinesl významné změny do obsahu zde sledovaných ustanovení.[137] Lhůta 24 hodin v článku 31(33) byla nahrazena obecnou formulací ohlášení bez zbytečného odkladu.[138] Nový odstavec přinesl ustanovení, že dozorový úřad bude vést veřejný registr o typech ohlášených případů porušení zabezpečení osobních údajů.[139] Předpoklady pro oznámení subjektu údajů dle článku 32(34) byly rozšířeny tak, že se povinnost měla vztahovat i na situace, kdy se hrozba vztahovala na jiná práva či legitimní zájmy dotčeného jednotlivce než jen jeho soukromí.[140] Předepsaný obsah těchto oznámení a jejich forma byly posíleny a rozšířeny.[141] Zmocnění k prováděcím předpisům dle odstavců 5 obou článků bylo přeneseno z Komise na nově tímto předpisem zřizovaný Evropský sbor pro ochranu osobních údajů (dále jen „Sbor“).[142]

134 Ibid.

135 Ibid., s. 60.

136 EUROPEAN DATA PROTECTION SUPERVISOR. The History of the General Data Protection Regulation. Timeline. *European Data Protection Supervisor* [online]. 8. prosinec 2016 [cit. 24. 5. 2021]. Dostupné z: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

137 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). *Evropský parlament* [online]. COM(2012)0011-C7-0025/2012-2012/0011(COD). Štrasburk: Evropský parlament, 2014, s. 176–181 [cit. 29. 4. 2021].

138 Ibid., s. 176.

139 Ibid., s. 178.

140 Ibid., s. 179.

141 Ibid., s. 180.

142 Sbor představuje na základě článku 68 Obecného nařízení nezávislý společný orgán dozorových úřadů členských států s vlastní právní subjektivitou. Ve svých úkolech zachycených v článku 70 Obecného nařízení navazuje na činnost Pracovní skupiny zřízené dle článku 29 směrnice 95/46/ES, která plnila srovnatelnou funkci, avšak bez právní subjektivity.

Ten byl dále pověřen vytvářením vodítek, doporučení a příkladů nejlepší praxe pro specifické předpoklady založení povinnosti, jakožto i pro vymezení jednání bez zbytečného odkladu. Dříve obsažené zmocnění Komise v odstavci 6 ohledně formulace standardního formátu ohlášení a souvisejících procesů bylo opuštěno.

Znění přijaté v prvním čtení Radou EU: Rada EU přijala v červnu 2015 znění kompromisního textu upravujícího úvodní návrh Komise.[143] Tato verze nabízela třetí a poněkud zjednodušenou formulaci zde představovaných ustanovení.

Jak ohlašovací, tak oznamovací povinnost měly vzniknout pouze v případě, *„[d]ojde-li k porušení ochrany osobních údajů, u nějž je pravděpodobné, že bude představovat vysoké riziko pro práva a svobody fyzických osob, jako je diskriminace, krádež či zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, ztráta důvěrnosti údajů chráněných služebním tajemstvím nebo jakékoli jiné významné hospodářské či společenské znevýhodnění …“*[144] Přípustná lhůta pro ohlášení dozorovému úřadu byla navýšena na 72 hodin od odhalení případu porušení zabezpečení.[145]

Výjimky z ohlašovací i oznamovací povinnosti byly rozšířeny a doplněny. To se týká především zašifrovaných údajů a přítomnosti účinných reakčních opatření.[146] Obsah ohlášení byl stanoven flexibilněji.[147] Všechny zmínky o zmocnění k prováděcím předpisům, vodítkům či jiným standardizačním opatřením byly v tomto znění návrhu z příslušných článků odstraněny, bez navržení nahrazujících ustanovení do článku 66(70) upravujícího činnosti Sboru či jinde v textu.[148]

Znění doporučené Evropským inspektorem ochrany údajů: Evropský inspektor ochrany údajů následně zpracoval porovnávací tabulku výše představených znění Obecného nařízení Komise, Evropského parlamentu

143 Srov. 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) – příprava obecného přístupu. *Rada EU* [online]. 2012/0011 (COD). Brusel: Rada EU, 2015 [cit. 24. 5. 2021].

144 Ibid., s. 119–120.

145 Ibid., s. 119.

146 Ibid., s. 119 a 121.

147 Ibid., s. 119.

148 Ibid., s. 120–121.

a Rady EU a obohatil tento přehled také o vlastní návrh znění příslušných ustanovení.[149] Tato verze přihlížela k jádru jednotlivých návrhů, které byly nejpravděpodobněji přijatelné v rámci kompromisu a představovala tudíž zásadně minimalistickou podobu textace příslušných ustanovení. Výsledný text Obecného nařízení se v mnohém podobá právě tomuto znění.

V této variantě byla ohlašovací povinnost vázána na pravděpodobné riziko pro práva a svobody jednotlivce a spojena s lhůtou 72 hodin.[150] Bylo včleněno poměrně vágní zmocnění pro tvorbu vodítek Sborem, zvláště pro posouzení rizika.[151] To si pak skutečně našlo cestu do článku 70 finálního znění Obecného nařízení upravujícího úkoly a činnosti Sboru, konkrétně do odst. 1 písm. g). Naopak doporučené založení oznamovací povinnosti vůči subjektům údajů při naplnění široké podmínky vycházející z návrhu Komise bylo ve výsledném znění nahrazeno užším okruhem situací vymezeným ve znění přijatém Radou EU.[152] Podobně bylo doporučeno zachování formulace výjimek z této povinnosti podle původního návrhu, ale finální znění zahrnovalo též rozšíření sjednané v rámci Rady EU.[153]

Třístranná jednání a přijetí Obecného nařízení: Poté, co se Rada EU shodla na přijatelné podobě znění předpisu, bylo 24. června 2015 zahájeno první třístranné jednání mezi Komisí, Evropským parlamentem a Radou EU.[154] Třístranné jednání *(trialog)* je neformální, avšak pravidelnou částí legislativního procesu, vedoucí ke sjednocení postoje zákonodárných institucí EU, který byl zaveden v roce 1999 Amsterdamskou smlouvou.[155] Možnost třístranného jednání je v primárním právu dovozována na základě článku 295 Smlouvy

149 Srov. Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations. *European Data Protection Supervisor* [online]. Brussels: European Data Protection Supervisor. 2015 [cit. 24. 5. 2021]; Opinion 3/2015 (with addendum) Europe's big opportunity. *European Data Protection Supervisor* [online]. Brussels: European Data Protection Supervisor. 2015 [cit. 24. 5. 2021].

150 Ibid., s. 169.

151 Ibid., s. 173.

152 Ibid., s. 174.

153 Ibid., s. 175–177.

154 Srov. EUROPEAN COMMISSION. Press release. Commission proposal on new data protection rules to boost EU Digital Single Market supported by Justice Ministers. *European Commission* [online]. 15. 6. 2015 [cit. 13. 7. 2021]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5176

155 Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts.

o fungování Evropské unie, který stanoví: *„Evropský parlament, Rada a Komise se navzájem konzultují a vzájemnou dohodou upravují způsoby své spolupráce. Za tímto účelem mohou v souladu se Smlouvami uzavírat interinstitucionální dohody, které mohou mít závaznou povahu.“*[156] Jde o možnost zefektivnění a urychlení řádného legislativního procesu, který dle Lisabonské smlouvy postupuje z prvního čtení do druhého čtení a následně k dohodovacímu řízení.[157] Konkrétní procedurální pravidla pro průběh trialogu shrnuje Společné prohlášení o praktických opatřeních pro postup spolurozhodování[158] v upravené verzi z června 2007.

K jednáním mezi orgány v souvislosti se zněním Obecného nařízení docházelo již od přijímání znění Evropským parlamentem, avšak „oficiální“ třístranné jednání bylo zahájeno až po přijetí verze Radou EU v červnu 2015.[159] Mimo zúčastněných institucí EU lze za významné aktéry v navazujících jednáních označit kromě výše zmíněného Evropského inspektora ochrany údajů též Pracovní skupinu dle článku 29 směrnice 95/46/ES, tedy budoucí Sbor. Ta volala nejen po jednoduchosti a srozumitelnosti výsledných ustanovení předpisu, ale i po co nejširším přenesení specifikací do vodítek dozorových úřadů a Sboru, jakož i po zachování flexibility pravidel, která nepovede k omezování inovací.[160] Ke klíčovému posunu v jednáních a sjednocení vize finálního znění došlo v prosinci 2015.[161] Rada EU formálně přijala výsledek třístranné dohody v dubnu 2016. Obecné nařízení bylo podepsáno

156 Srov. čl. 295 Smlouvy o fungování Evropské unie.

157 Srov. čl. 251 Lisabonské smlouvy pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství, podepsané v Lisabonu dne 13. prosince 2007.

158 Viz Společné prohlášení o praktických opatřeních pro postup spolurozhodování (článek 251 smlouvy o ES). Dle obecných zásad č. 7 a 8 *„[s]polupráce mezi orgány v rámci spolurozhodování má často podobu třístranných jednání. Užitečnost a flexibilita těchto třístranných jednání se odráží ve skutečnosti, že se významně zvýšil počet dohod dosažených v prvním nebo druhém čtení a že rovněž přispěly k přípravě schůzí dohodovacího výboru. Tato třístranná jednání mají většinou neformální podobu. Mohou se konat kdykoli během spolurozhodování a mohou se jich účastnit zástupci na různých úrovních, a to podle povahy očekávané diskuze.“*

159 Viz PROUST, Olivier. Unravelling the mysteries of the GDPR trilogues. *Fieldfisher* [online]. 16. 7. 2015 [cit. 13. 7. 2021]. Dostupné z: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/unravelling-the-mysteries-of-the-gdpr-trilogues

160 Viz BRACY, Jedidiah a Sam PFEIFLE. WP29 Weighs In on the GDPR Trilogue Process. *IAPP* [online]. 18. 6. 2015 [cit. 13. 7. 2021]. Dostupné z: https://iapp.org/news/a/wp29-weighs-in-on-the-gdpr-trilogue-process-2/

161 Viz WILHELM, Ernst-Olivier. A brief history of the General Data Protection Regulation. *IAPP* [online]. 2016 [cit. 13. 7. 2021]. Dostupné z: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

prezidenty Evropského parlamentu a Rady EU dne 27. dubna 2016 a vyhlášeno v Úředním věstníku Evropské unie dne 4. května 2016. Obecné nařízení vstoupilo v platnost dvacátým dnem po vyhlášení, čímž byla započata v souladu s článkem 99 Obecného nařízení dvouletá legisvakanční lhůta do přímé použitelnosti předpisu ke dni 25. května 2018.

Dílčí transpozice do národních právních řádů na základě směrnice 2016/680: Přestože přímo použitelná ustanovení článků 33 a 34 Obecného nařízení představují ústřední normativní prvek úpravy povinností souvisejících s porušením zabezpečení osobních údajů v právních řádech členských států EU, je nutné na tomto místě doplnit, že paralelně s Obecným nařízením byly v reformním balíčku pro oblast ochrany osobních údajů přijaty též směrnice 2016/680[162] a 2016/681.[163] Přitom směrnice 2016/680 skrze články 30 a 31 poskytuje srovnatelné znění ohlašovací, oznamovací a dokumentační povinnosti k úpravě v Obecném nařízení, zde však aplikovatelné na zpracování osobních údajů veřejnoprávními orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů. Jelikož bylo nutné znění těchto ustanovení oproti přímo použitelné úpravě dle Obecného nařízení transponovat do národních právních řádů členských států, byl umožněn dílčí odklon národního zákonodárce od vymezení a podmínek těchto povinností v daném okruhu zpracování osobních údajů. Stejně tak je na místě přihlížet k dalším omezením věcné působnosti Obecného nařízení, jak stanoví článek 2.[164] Také pro tyto oblasti je možná fragmentace úpravy na národní úrovni na základě uvážení zákonodárce členského státu.

V kontextu problematiky diskutované v rámci představované monografie však nepokládám za významné přihlížet k případným dílčím specifikům těchto oblastí v národních úpravách, jelikož v nich nedochází k podstatnému

162 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

163 Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

164 Jde především o činnosti, které nespadají do působnosti práva Unie, jako jsou činnosti týkající se národní bezpečnosti a dále pak činností v rámci společné zahraniční a bezpečnostní politiky Unie. Srov. bod odůvodnění 16 Obecného nařízení.

či zásadně specifickému rozšiřování internetu věcí. V českém právním řádu jsou pak tyto oblasti upraveny § 12 a 19 odst. 4, 41 a 42 zákona č. 110/2019 Sb. o zpracování osobních údajů. Přes jisté dílčí legislativně technické odlišnosti či výjimky zakotvené v těchto ustanoveních českého národního předpisu považuji dále představované argumenty založené na právní úpravě Obecného nařízení za přenositelné, a tudíž nevyžadující věnování zvláštní pozornosti specifikům této roviny úpravy.

3.2.2 Struktura normativní úpravy a její složky

Výsledné dnes použitelné znění příslušných článků 33 a 34 Obecného nařízení je kompromisem mezi zněními Komise, Evropského parlamentu a Rady EU. Před podrobným představením použitelné úpravy je však na místě opětovně upozornit na terminologický odklon ve finálním českém znění předpisu, který nemá zřejmé obsahové zdůvodnění a vedl mě k užití pluralitní terminologie napříč touto monografií, jak popsáno výše v podkapitole 1.2.

Terminologická nejednotnost: Pozorný čtenář si totiž jistě všiml, že v předchozí podkapitole citovaný text z přípravných znění Obecného nařízení neobsahoval formulaci porušení zabezpečení, ale narušení bezpečnosti. Je tomu totiž tak, že zatímco v českém znění návrhu předloženého Komisí v roce 2012 i ve znění schváleného Evropským parlamentem v roce 2014 je v souladu s ustanoveními novelizované směrnice 2002/58/ES, na kterou (jak bylo výše popsáno) úprava výslovně navazuje a je s ní tudíž terminologicky provázána, užíváno pojmu narušení bezpečnosti osobních údajů, v pozdějších verzích textů již české znění používá jiné pojmy, ačkoliv jiná jazyková znění dodržují kontinuitu pojmu. Shodně se směrnicí 2002/58/ES je užito *personal data breach; Verletzung des Schutzes personen bezogener Daten; violation de données à caractère personnel*. Zmíněny jsou pojmy z anglického, německého a francouzského znění, jelikož tyto jazyky jsou „procesními" jazyky pro vnitřní záležitosti Komise[165] a doznávají tudíž dle mého názoru relativně vyšší přesnosti v ohledu terminologie a zachycení významu právního textu než ostatní oficiální jazyky EU. České znění textu přijaté Radou EU v roce 2015 pak pro změnu užívá v článku 31(33) pojmu porušení ochrany osobních údajů.

165 Srov. EUROPEAN COMMISSION. Frequently asked questions on languages in Europe. *European Commission* [online]. 26. 9. 2013 [cit. 13. 7. 2021]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_825

Výsledné články 33 a 34 Obecného nařízení v českém znění upravují ohlašování a oznamování případů porušení zabezpečení osobních údajů (v ostatních verzích však stále *personal data breach; Verletzung des Schutzes personen bezogener Daten; violation de données à caractère personnel*).

V článku 4 bodu 12) Obecného nařízení je porušení zabezpečení osobních údajů definováno jako *„porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.“*

Struktura povinností souvisejících s porušením zabezpečení: Po vzoru novelizované směrnice 2002/58/ES lze v Obecném nařízení identifikovat trojici specifických povinností správce, které se váží k případu porušení zabezpečení osobních údajů. Jejich vznik je přitom odstupňován a závisí na závažnosti odhaleného porušení zabezpečení pro práva a zájmy dotčených subjektů údajů.

Bez ohledu na rizika spojená s daným případem porušení zabezpečení správce dle článku 33 odst. 5 Obecného nařízení *„dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.“*[166]

Přitom ta porušení zabezpečení, u kterých je pravděpodobné, že by měla za následek riziko pro práva a svobody fyzických osob, je správce dle článku 33 odst. 1 Obecného nařízení povinen ohlásit příslušnému dozorovému úřadu, a to, pokud možno, do 72 hodin od okamžiku odhalení. Případné zpoždění musí být odůvodněno.

Nad rámec těchto povinností pak na základě článku 34 odst. 1 Obecného nařízení v případě, kdy *„je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.“* V souladu s odst. 4 pak může dozorový úřad po vlastním posouzení pravděpodobnosti vysokého rizika pro subjekty údajů rozhodnout, zda byla tato podmínka splněna, a tudíž že má správce oznámení provést, či naopak, že jej provádět nemusí.

Mimo tyto výslovně formulované povinnosti se s porušením zabezpečení pojí i specifická část obecné povinnosti správce i zpracovatele na zajištění

166 Viz čl. 33 odst. 5 Obecného nařízení.

přiměřené úrovně zabezpečení zpracovávaných osobních údajů dle článku 32 odst. 1 Obecného nařízení. Ta představuje nejen provedení vhodných a přiměřených opatření, která směřují k zabránění vzniku porušení zabezpečení, ale především jde o využívání nástrojů a postupů pro jejich včasné a účinné odhalování.[167] Pracovní skupina dle článku 29 (nyní Sbor) ve svém vodítku k povinnostem spojeným s porušením zabezpečení dle Obecného nařízení výslovně uvádí: *„Článek 32 objasňuje, že správce a zpracovatel údajů by měli mít zavedena vhodná technická a organizační opatření k zajištění odpovídající úrovně zabezpečení osobních údajů: za základní prvky těchto opatření je nutno považovat schopnost porušení včas odhalit, reagovat na něj a ohlásit ho.“*[168]

Dokumentační povinnost dle článku 33 odst. 5 Obecného nařízení: Na prvním místě je vhodné přiblížit povinnost, která se váže na veškeré případy porušení zabezpečení. Ta je výslovně uložena pouze správci (tedy subjektu, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů)[169], na zpracovatele (tedy subjekt, který zpracovává osobní údaje pro správce)[170] se přímo nevztahuje. Ten je především povinen při zjištění případu porušení bez zbytečného odkladu tuto skutečnost ohlásit správci,[171] přičemž není primárně na něm, aby posoudil závažnost daného případu porušení zabezpečení či dokumentoval jeho výskyt.

Tento výklad je však zjednodušující a vzhledem k praktickým aspektům vztahu řady správců a zpracovatelů ve své podstatě zavádějící. Zpracovatel je totiž ve vztahu se správcem na základě smlouvy nebo právního aktu, který dle článku 28 odst. 3 písm. f) Obecného nařízení musí mimo jiné stanovit, že zpracovatel *„je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici.“* Je tedy nutné přihlížet ke specifickým parametrům vztahu zpracovatele a správce při daném zpracování.

Například jde-li o vztah mikropodniku s OSVČ zajišťující komplexní správu IT systémů a sítí včetně zabezpečení, zálohování a archivace, lze

167 Srov. bod odůvodnění 87 Obecného nařízení.

168 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 13 [cit. 28. 2. 2021].

169 Srov. čl. 4 bod 7) Obecného nařízení.

170 Srov. čl. 4 bod 8) Obecného nařízení.

171 Viz čl. 33 odst. 2 Obecného nařízení.

považovat za vhodné, aby daný správce sítě v rámci povinností vyplývajících mu z daného smluvního vztahu též zajišťoval dokumentaci a případně též ohlašování či oznamování případů porušení zabezpečení pro daný podnik, byť lze předpokládat, že vystupuje zásadně v postavení zpracovatele. Při vědomí tohoto praktického řešení příslušných povinností, které se ve své podstatě nijak neodlišuje od jiných forem outsourcingu specifických povinností specializovanému subjektu (uvažujte např. daňové účetnictví) je však nutné vnímat sled tímto založených právních závazků. Ve vztahu k povinnostem založeným články 33 a 34 Obecného nařízení stojí jako primárně odpovědný subjekt vždy správce, byť může skrze sekundární právní vztah přenést realizaci těchto povinností na zpracovatele.[172] Případné nedodržení těchto povinností ze strany zpracovatele je tudíž v prvé řadě odpovědností správce, který musí čelit příslušné sankci či náhradě újmy, byť se může případně zhojit na zpracovateli skrze příslušná ujednání o smluvní sankci.

Výklad pojmu porušení zabezpečení osobních údajů: Pokud se vrátíme k dokumentační povinnosti správce, je při jejím výkladu a aplikaci nutno předně přihlížet k vymezení klíčového pojmu řešené problematiky, a to porušení zabezpečení osobních údajů. Povinnost se totiž vztahuje na veškeré tyto případy a pro adekvátní stanovení množiny jevů, které jsou jí postihovány, je tudíž pro správce potřebné být schopen důsledně vyložit tento pojem. Jeho výklad je pak pochopitelně přenositelně aplikovatelný i na dále diskutovanou ohlašovací a oznamovací povinnost.

Dle článku 4 bodu 12) Obecného nařízení je *„ ‚porušením zabezpečení osobních údajů' porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů."* K tomu může dojít jak ve vztahu k fyzicky zachyceným osobním údajům (např. ztráta vytištěných dokumentů) tak na elektronický uchovávaných záznamech. Pracovní skupina dle článku 29 (nyní Sbor) přitom rozlišuje tři formy porušení zabezpečení:

1. porušení důvěrnosti, kdy došlo k neoprávněnému či náhodnému zpřístupnění či zveřejnění osobních údajů;

172 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 14 [cit. 28. 2. 2021].

2. porušení integrity, kdy došlo k neoprávněnému či náhodnému pozměnění osobních údajů; a
3. porušení dostupnosti, kdy došlo k neoprávněné či náhodné ztrátě přístupu či smazání osobních údajů.[173]

K tomuto dělení přitom bylo přistupováno již s ohledem na výklad povinností dle novelizované směrnice 2002/58/ES.[174] Není vyloučeno, aby došlo k porušení zabezpečení, které kombinuje kvality více forem či dokonce všech tří forem zároveň.[175]

Jak bylo podrobně představeno v podkapitole 2.1, pokládám porušení zabezpečení u elektronických záznamů v podobě bezpečnostního incidentu za mnohem významnější, škodlivější a častější než incidenty u fyzických nosičů. Současně je fyzická forma v zásadě irelevantní v kontextu dále řešené problematiky osobních údajů zpracovávaných zařízeními internetu věcí, proto jí nebude věnována zvláštní pozornost.

Výklad pojmu osobní údaj: Pro další rozbor je vhodné se alespoň ve stručnosti zmínit o pojetí dvou stěžejních pojmů, které jsou prvky výše uvedené definice. V prvé řadě je nutné brát ohled na rozsah pojmu osobní údaj. Ten je v článku 4 bodě 1) Obecného nařízení přiblížen jako *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen ‚subjekt údajů'); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby"*.[176] Přes, dle mého názoru, poměrně snadnou a obecně shodnou intuitivní představu každého z nás o rozsahu pojmu osobní údaj na základě výše uvedené definice jde o jeden z nejsložitějších výkladových problémů na poli ochrany osobních údajů v dílčích otázkách a konkrétních

173 Ibid., s. 7.

174 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 03/2014 k oznámení o narušení bezpečnosti osobních údajů* [online]. 693/14/CS WP 213. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2014, s. 5 [cit. 12. 7. 2021].

175 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 8 [cit. 28. 2. 2021].

176 Srov. čl. 4 bod 1) Obecného nařízení.

aplikacích.[177] V důsledku pokroku v informačních a komunikačních technologiích stojí na datech fungování současného světa a naše individuální existence dnes zanechává trvalou, podrobnou a neustále se rozšiřující digitální stopu. Je tak velmi nesnadné přesně vymezit hranici, která z těchto dat mají v konkrétní situaci ještě informační hodnotu osobního údaje (tzn. je s jejich pomocí možné nepřímo identifikovat fyzickou osobu) a která již nikoliv.

Při posuzování identifikovatelnosti je na místě brát v potaz objektivní faktory, jakými jsou volná dostupnost referenčních údajů, stav techniky, náklady na identifikaci či časová a systematická náročnost této operace.[178] Zrádnost definice pak spočívá v zahrnutí nepřímých identifikátorů, které mohou vycházet z kombinace informační hodnoty několika společně pojímaných záznamů, které ve výsledku umožňují identifikaci fyzické osoby.[179] Jelikož současné převažující výkladové tendence SDEU směřují spíše k objektivnímu pojetí osobních údajů,[180] je nutné informační potenciál daného údaje zohledňovat v kombinaci s celkovým myslitelným souborem dostupných údajů.[181] Kombinace věku, pohlaví, váhy a vzdělání tak může vést k určení konkrétní osoby v rámci zkoumané skupiny, ačkoliv žádný z těchto údajů k tomu samostatně způsobilý není. *Poullet* upozorňuje na potřebu zohlednění stále širšího spektra takovýchto jednoduchých dat, která vedou k profilování jednotlivce. Zvláště zdůrazňuje roli „souhlasných identifikátorů" *(matching identifiers)*, které v online prostředí slouží jako metadatová struktura k propojení záznamů o určité osobě z různých databází.[182] Těmito identifikátory mohou být např. uživatelské jméno, IP adresa či cookies.

177 Blíže viz BYGRAVE, Lee A. a Luca TOSONI. Article 4(1). In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 110–111.

178 Viz PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017. Beck'sche Kompakt-Kommentare. Art. 4 Rn 10.

179 Viz NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. 1. vyd. Praha: Wolters Kluwer, 2014, s. 88.

180 Srov. např. rozhodnutí SDEU ze dne 19. 10. 2016, ve věci *Breyer,* C-582/14..

181 Při důsledné aplikaci této šíře pojmu lze však narážet na limity koncepční přípustnosti. Blíže viz např. MÍŠEK, Jakub. Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing). In: SVANTESSON, Dan a Dariusz KLOZA (eds.). *Trans-atlantic Data Privacy Relations as a Challenge for Democracy*. Cambridge: Intersentia, 2017, European Integration and Democracy Series.

182 Srov. POULLET, Yves. About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Data Protection in a Profiled World* [online]. Dordrecht: Springer Netherlands, 2010, s. 11–12, [cit. 13. 7. 2021].

Pro posouzení pojmu porušení zabezpečení osobních údajů z výše nastíněného výkladu vyplývá, že je k němu na místě přistupovat extenzivně. Až na výjimky údajů, které zcela zřetelně nemají vypovídací schopnost o fyzické osobě bez ohledu na kombinaci s jinými údaji[183] je nutné vycházet s ohledem na objektivní přístup z předpokladu, že mezi daty ohroženými předmětným porušením zabezpečení mohou být i osobní údaje.

Výklad pojmu zpracování: Druhým pojmem, který umožňuje určité omezení výše nastíněné množiny relevantních jevů je chápání činnosti „zpracování" v kontextu ochrany osobních údajů. Dle článku 4 bodu 2) Obecného nařízení je *„zpracováním jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení."*[184] Byť tato definice sama o sobě příliš prostoru k omezení aplikace povinností nenabízí, je nutné zohlednit užití tohoto pojmu v rámci článku 2 Obecného nařízení, kterým je omezena věcná působnost předpisu. Dle odst. 1 tohoto článku se Obecné nařízení nevztahuje na zpracování osobních údajů, které probíhá neautomatizovaně a údaje nejsou obsaženy v evidenci nebo do ní nejsou zařazovány. Evidencí je přitom v souladu s článkem 4 bodem 6) Obecného nařízení *„jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska."*[185] Vzhledem k povaze elektronických záznamů lze předjímat, že toto omezení není příliš relevantní, jelikož se vztahuje spíše na dílčí nesystematické poznámky či sdílení osobních údajů v rámci konverzace.[186]

Podstatnější je vyloučení působnosti Obecného nařízení z oblastí uvedených v odst. 2, konkrétně zpracování *„(a) při výkonu činností, které nespadají do oblasti působnosti práva Unie* [rozumějte např. zajištění bezpečnosti státu a činnosti

183 Např. technické údaje o fungování strojů či datové komunikaci mezi zařízeními, údaje o počasí či znečištění ovzduší, agregované finanční záznamy právnické osoby.

184 Srov. čl. 4 bod 2) Obecného nařízení.

185 Srov. čl. 4 bod 6) Obecného nařízení.

186 Srov. TOSONI, Luca. Article 4(6). In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 142–143.

armády[187]*; (b) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU* [rozumějte společná zahraniční a bezpečnostní politika[188]]*; (c) fyzickou osobou v průběhu výlučně osobních či domácích činností* [rozumějte např. soukromá korespondence]*; (d) příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení* [rozumějte výše zmíněná paralelní úprava směrnicí 2016/680, která však obsahuje srovnatelnou normativní úpravu povinností ve spojení s případy porušení zabezpečení osobních údajů jako Obecné nařízení]." Obecné nařízení také přímo nedopadá na zpracování osobních údajů orgány, institucemi a jinými subjekty Unie, kde se uplatní speciální úprava na základě nařízení 2018/1725.[189] To pak z podstaty věci neobsahuje srovnatelnou úpravu povinností v souvislosti s porušením zabezpečení osobních údajů.

Obsah dokumentační povinnosti: K takto vymezené množině situací, které představují případy porušení zabezpečení osobních údajů ve smyslu Obecného nařízení, je správce povinen vést dokumentaci (samozřejmě za předpokladu, že dané porušení zabezpečení odhalí, ovšem jeho neodhalení značí pochybení v obecné povinnosti dle článku 32 Obecného nařízení, jak popsáno výše). Tato dokumentace má obsahovat informace o

1. skutečnostech, které se týkají daného porušení,
2. jeho účincích a
3. přijatých nápravných opatřeních.[190]

Při výkladu těchto požadavků je pak na místě přihlížet k účelu této dokumentace, tedy umožnit dozorovému úřadu ověření souladu, především s ohlašovací povinností popsanou dále. Je přitom příhodné požadavky na tuto dokumentační povinnost vykládat analogicky k požadavkům na povinnost vést záznamy o činnostech zpracování dle článku 30 Obecného nařízení, tedy že dokumentace má být sice písemná, ale konkrétní forma, tedy např. zda

187 Srov. bod odůvodnění 16 Obecného nařízení.
188 Ibid.
189 Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES.
190 Viz čl. 33 odst. 5 Obecného nařízení.

jsou záznamy v elektronické či tištěné podobě, je na uvážení správce.[191] I zde je však nutné zohledňovat, že účelem dokumentace je poskytnout na vyžádání podklady dozorovému úřadu a lze tak předpokládat, že zachovávat systematičnost a jednotnou formu dokumentace je v zájmu daného správce.

Ohlašovací povinnost dle článku 33 Obecného nařízení: Ohlašovací povinnost vůči dozorovému úřadu upravenou článkem 33 odst. 1, 3 a 4 Obecného nařízení považuji za ústřední komponentu postihující tuto problematiku. Toto usuzuji především z nastavení podmínek pro založení povinnosti v poměru k oznamovací povinnosti vůči dotčeným subjektům údajů. Požadavky na vznik ohlašovací povinnosti jsou na jedné straně nižší, naopak je přísněji stanovena lhůta pro splnění této povinnosti a šířeji vymezen rozsah informací, které je správce povinen dozorovému úřadu sdělit. Jak bude blíže představeno dále v oddílu 3.3.3, v tomto směru vnímám odlišnost konceptu unijní a americké úpravy, která klade primární důraz na oznamování dotčeným subjektům údajů a omezuje povinnost ohlašování regulatorním orgánům pouze na významnější případy porušení bezpečnosti zpracovávaných údajů.

O pojmu porušení zabezpečení, a tudíž základní množině relevantních situací, bylo pojednáno výše u dokumentační povinnosti. Ohlašovací povinnost však nevzniká, je-li *„nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.“*[192] Vstupují zde tudíž při výkladu povinným subjektem do hry dodatečné neurčité právní pojmy, které je na místě přiblížit. Jde předně o to,

1. co je považováno za *nepravděpodobné riziko* a
2. která *práva a svobody fyzických osob* je nezbytné v tomto směru zohledňovat.

Výklad pojmu nepravděpodobné riziko: Při výkladu, jaká rizika jsou či nejsou v tomto kontextu pravděpodobná, je předně podstatné, aby dosud nenastala subjektům údajů žádná újma na právech a svobodách v důsledku daného porušení zabezpečení.[193] Správce musí tudíž při posuzování vzniku povinnosti zvažovat možné budoucí újmy a jejich pravděpodobnost. Tato prognóza by měla optimálně být založena na metodologicky podložené

191 Viz PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017. Beck'sche Kompakt-Kommentare. Art. 30 Rn 24.
192 Srov. čl. 33 odst. 1 Obecného nařízení.
193 Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017. Beck'sche Kompakt-Kommentare. Art. 33 Rn 25.

analýze dostupných informací v okamžiku posuzování.[194] Jelikož se vznik ohlašovací povinnosti váže na povědomí správce o porušení zabezpečení, je při posuzování rozhodování správce směrodatné, zda byly učiněné závěry podložené při zohlednění okruhu znalostí správce v okamžiku rozhodování a při použití vhodných odborných metod pro posouzení rizikovosti.[195]

Tím přecházíme k dalšímu významnému pojmu v rámci představované problematiky a tím je riziko a jeho hodnocení. Jelikož řádné vymezení tohoto pojmu nezahrnuje pouze čistě právní analýzu, věnuji mu více pozornosti z pohledu neprávní kvalifikace později v rámci podkapitoly 5.1. Pro právní výklad v daném kontextu je podstatné, že hodnocení rizik představuje jeden z klíčových prvků regulace na základě Obecného nařízení.[196] Pro vyhodnocení založení povinnosti je nezbytné vnímat záměr tvůrců nařízení, který směřoval k výjimce za předpokladu nepatrného rizika (jelikož skutečná bezrizikovost není v praxi dosažitelná). Jde tedy o kombinaci pravděpodobnosti vzniku a rozsahu újmy, které při rozumném zvážení všech relevantních okolností nečiní ohlášení potřebným.[197] Na rozdíl od jiných režimů posuzování rizik v rámci Obecného nařízení se zde řeší konkrétní důsledky reálně nastalého porušení zabezpečení, přičemž v rámci příslušného ustanovení nejsou k dispozici kritéria, která má správce zohlednit, jako např. u přiměřenosti opatření dle článku 32 Obecného nařízení.[198]

Je však možné vycházet z pokynů Pracovní skupiny dle článku 29 (nyní Sboru), které uvádí, že pro určení míry rizika hrají roli kritéria zahrnující především:

1. formu porušení;
2. povahu, citlivost a množství dotčených osobních údajů;
3. identifikovatelnost jednotlivce z dotčených údajů;
4. předpokládanou závažnost dopadů na jednotlivce;
5. možný dopad na děti či jiné zvlášť zranitelné kategorie subjektů údajů;

194 Ibid., Art. 33 Rn 26.

195 Ibid.

196 Srov. MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. 1. vyd. Brno: Masarykova univerzita, 2020, s. 169.

197 Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017, Beck'sche Kompakt-Kommentare, Art. 33 Rn 22.

198 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 24 [cit. 28. 2. 2021].

6. odhadované množství dotčených osob; či
7. případné specifické postavení správce.[199]

Jelikož jde o riziko související s porušením zabezpečení, lze předpokládat, že důraz by měl být kladen především na rozsah možné újmy, kterou lze vymezit s ohledem na množství a kategorie zpřístupněných osobních údajů a poznatelné cíle a schopnosti třetí strany, která hrozí neoprávněným přístupem k těmto údajům.[200] Za situaci s nepravděpodobným rizikem pro práva a svobody fyzických osob lze tak například uvažovat takovou, kdy všechny uniklé osobní údaje byly již před incidentem veřejně dostupné či pokud byly dotčeny pouze kvalitně zašifrované údaje, což účinně brání jejich neoprávněnému zpracování a správce má zároveň k dispozici jejich záložní kopie (tedy nedošlo ani k porušení jejich dostupnosti). Přesto i zde platí, že riziko je nutno posuzovat s plynutím času a případně, např. byl-li zveřejněn postup pro účinné prolomení užité metody šifrování, dodatečně provést ohlášení porušení zabezpečení.[201] Podrobnější návod poskytují dostupné metodologie,[202] je však nutno vycházet z principu, že pokud si správce není jistý, zda má ohlašovací povinnost, je na místě jednat v zájmu ochrany subjektů údajů a kontaktovat dozorový úřad.[203]

Výklad pojmů práva a svobody fyzických osob: Chráněnými hodnotami, ke kterým se váže zhodnocení pravděpodobné újmy, jsou práva a svobody fyzických osob. Výkladu tohoto sousloví přitom napomáhá bod odůvodnění 75 Obecného nařízení, který uvádí, že *„[r]ůzně pravděpodobná a závažná rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy*

199 Ibid., s. 24–26.

200 Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017, Beck'sche Kompakt-Kommentare, Art. 33 Rn 23.

201 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 20 [cit. 28. 2. 2021].

202 Blíže viz ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches [online]. 20. prosinec 2013 [cit. 7. 2. 2021]. Dostupné z: https://www.enisa.europa.eu/publications/dbn-severity

203 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 27 [cit. 28. 2. 2021].

by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatření, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu a pohybu, kdy jsou zpracovávány osobní údaje zranitelných osob, především dětí, nebo kdy je zpracováván velký objem osobních údajů a zpracování se dotýká velkého počtu subjektů údajů."[204] Tím je komplexně pojata množina hrozeb, které byly v této souvislosti přiblíženy již v podkapitole 2.3.

Obsah ohlašovací povinnosti: Správce má za splnění výše rozebrané podmínky pravděpodobného rizika pro práva a svobody fyzických osob povinnost ohlásit porušení zabezpečení příslušnému dozorovému úřadu, tedy v českém kontextu Úřadu, zásadně bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl.[205] Za tento okamžik je na místě považovat moment, kdy s rozumnou mírou jistoty dospěl k závěru, že došlo k porušení zabezpečení, které se dotýká osobních údajů.[206] Pokud porušení zabezpečení zjistí zpracovatel, je povinen o něm bez zbytečného odkladu informovat správce,[207] na toho se pak vztahuje domněnka, že se o porušení zabezpečení dozvěděl ve chvíli, kdy se o něm věděl zpracovatel.[208] Správce může zmocnit

204 Srov. bod odůvodnění 75 Obecného nařízení.

205 Srov. čl. 33 odst. 1 Obecného nařízení.

206 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 11 [cit. 28. 2. 2021].

207 Srov. čl. 33 odst. 2 Obecného nařízení.

208 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 12 [cit. 28. 2. 2021].

zpracovatele k ohlašování porušení zabezpečení přímo dozorovému úřadu, tím však není zbaven primární odpovědnosti za včasnost a řádnost tohoto ohlášení.[209] Dále je na místě uvést, že ohlašovací povinnost dle článku 33 Obecného nařízení je nezávislá na dalších srovnatelných povinnostech na základě jiných právních předpisů,[210] a uplatní se tedy případně paralelně.

Za významnou rovinu této povinnosti dále považuji její informační kvalitu. Jedná se, dle mého názoru, o prvek tzv. chytré regulace, což bude podrobněji rozebráno v rámci diskuse v následující podkapitole. Je tudíž zásadní, aby jejím splněním byly poskytnuty regulatornímu orgánu užitečné a aktuální informace. Ty mají posloužit nejen pro zacílení jeho dozorové činnosti, ale především vypomoci s reakcí na vzniklou rizikovou situaci. K tomu může dojít odborným vedením při řešení situace ohlašujícího správce či preventivní komunikací vůči dalším správcům, kteří na základě zhodnocení dozorového úřadu mohou být ohroženi následky daného porušení zabezpečení či jeho další iterací.

Je proto stanoveno článkem 33 odst. 3 Obecného nařízení, že ohlášení musí obsahovat přinejmenším:

> *„(a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;*
>
> *(b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;*
>
> *(c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;*
>
> *(d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.“*[211]

V případě složitějších porušení zabezpečení je předpokládána možnost ohlašování po částech.[212] Porušení zabezpečení, které se dotýká fyzických osob

209 Ibid., s. 14.

210 Jde zde především o notifikační povinnosti na základě ZoKB nebo zákona č. 127/2005 Sb.

211 Srov. čl. 33 odst. 3 Obecného nařízení.

212 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 16 [cit. 28. 2. 2021].

z více členských států, ohlašuje správce vedoucímu dozorovému úřadu, tedy úřadu příslušnému dle hlavní provozovny správce.[213]

Oznamovací povinnost dle článku 34 Obecného nařízení: K třetí zde diskutované povinnosti správce se váže nejvíce podmínek. Oznamovací povinnost vůči dotčeným subjektům údajů dle článku 34 Obecného nařízení vzniká, *„[p]okud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob."*[214] V takovém případě je správce povinen přistoupit k oznámení bez zbytečného odkladu.

Pro výklad povinnosti jako takové je nad rámec již rozebraných pojmů potřeba odlišit, kdy se riziko pro práva a svobody fyzických osob stává rizikem vysokým. Lze vycházet z toho, že záměrem tvůrců předpisu bylo omezit povinnost na situace, kdy ohrožení zájmů subjektů údajů vyžaduje jejich informovanost, aby mohli případně sami zakročit a aktivně chránit své zájmy. *Paal* a *Pauly* tak považují za nezbytné, aby pro založení oznamovací povinnosti byla v dané situaci doložitelná významná a specifická hrozba újmy[215] či újma se značnou pravděpodobností[216].[217] Z toho implicitně vyplývá, že pokud k újmě v důsledku porušení zabezpečení již prokazatelně došlo, je založena oznamovací povinnost.[218]

Výklad pojmu vysoké riziko: Při výkladu pojmu vysoké riziko je dále možné analogicky vycházet z kritérií relevantních pro *ex ante* hodnocení vysokého rizika v souvislosti s povinností posouzení vlivu na ochranu osobních údajů dle článku 35 Obecného nařízení.[219] V tomto kontextu je vysoké riziko shledáváno především v případech, které zahrnují:

> *„(a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování,*

213 Ibid., s. 18.

214 Srov. čl. 34 odst. 1 Obecného nařízení.

215 Přičemž usuzují, že se zvyšujícím se rozsahem hrozící újmy postačí i její nižší pravděpodobnost.

216 Zde naopak s rostoucí pravděpodobností postačí i menší rozsah očekávané újmy na právech a svobodách.

217 Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017. Beck'sche Kompakt-Kommentare. Art. 34, Rn 29-30.

218 Je-li totiž riziko vnímáno jako následek s určitou pravděpodobností, není na místě označovat rizikem újmu, jejíž realizace je jistá, jelikož pravděpodobnost se ze své podstaty vztahuje k budoucí nejistotě.

219 Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017. Beck'sche Kompakt-Kommentare. Art. 34 Rn 30a.

a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

(b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v článku 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo

(c) rozsáhlé systematické monitorování veřejně přístupných prostorů."[220]

Další specifikaci vysokého rizika lze nalézt v příslušných pokynech Pracovní skupiny dle článku 29 (nyní Sboru).[221] Zde je uváděno celkem devět kritérií, přičemž při naplnění i jediného z nich lze zpracování pokládat za nesoucí vysoké riziko pro práva a svobody fyzických osob.[222] Mezi tato kritéria se řadí:

1. zpracování zahrnuje hodnocení či bodování, včetně profilování;[223]
2. zpracováním dochází k automatizovanému rozhodování, které má právní nebo podobně závažný dopad, např. vyloučení jednotlivce ze skupiny;
3. systematické monitorování, ať již prostřednictvím sítí či na veřejně přístupném prostoru;
4. zpracování zahrnuje citlivé údaje či údaje vysoce osobní povahy;[224]
5. zpracování osobních údajů v rozsáhlém měřítku;[225]
6. zpracováním dochází k přiřazování či slučování datových souborů;[226]

220 Srov. čl. 35 odst. 3 Obecného nařízení.

221 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679* [online]. wp248rev.01_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2017, s. 679 [cit. 29. 5. 2021].

222 Tamtéž, s. 12.

223 Podstatou profilování v pojení Obecného nařízení je *„jakákoliv forma automatizovaného zpracování osobních údajů hodnotící osobní aspekty vztahující se k fyzické osobě, zejména za účelem analýzy či předvídání aspektů souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním, místem pobytu či pohybu, pokud má pro něj právní účinky nebo se jí podobným způsobem významně dotýká."* Srov. bod odůvodnění 71 Obecného nařízení.

224 Např. zdravotní dokumentace, rozsudky v trestních věcech, ale též lokalizační údaje, finanční údaje či osobní dokumenty.

225 Rozsah závisí na počtu dotčených subjektů údajů, množství kompromitovaných osobních údajů, délce trvání i zeměpisném rozsahu činnosti. Směrodatné hodnoty však nejsou Pracovní skupinou dle článku 29 poskytnuty, za rozsáhlé lze však bezesporu považovat např. významné případy porušení bezpečnosti zmiňované v druhé kapitole.

226 Typickým příkladem je kombinování údajů v rámci vytěžování velkých databází *(big data mining)*. Blíže viz např. WU, Xindong et al. Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering* [online]. 2014, roč. 26, č. 1.

7. údaje se týkají zranitelných subjektů, např. dětí, starších osob, zaměstnanců, pacientů, duševně nemocných či žadatelů o azyl;[227]
8. ke zpracování dochází za využití nových technologií nebo organizačních řešení;[228]
9. zpracování *„brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy“*[229] (např. jde o proces posuzování úvěrové bonity).[230]

Z výše uvedeného lze ve stručnosti zdůraznit, že hlavní vliv na určení, že porušení zabezpečení přináší vysoké riziko pro práva a svobody fyzických osob budou mít skutečnosti, zda došlo k postižení zvláštních kategorií osobních údajů (ve smyslu článků 9 a 10 Obecného nařízení); údajů, které vznikly v rámci profilování, systematického monitorování či automatizovaného zpracování; či zda se s ním pojí pro dotčené fyzické osoby očekávatelné budoucí porušení zabezpečení.[231]

Jelikož je však častější povinností správce ohlašovat případy porušení dozorovému úřadu, lze předpokládat, že posouzení o nutnosti oznámení dotčeným osobám je činěno ve spolupráci s tímto úřadem. Dotčené subjekty údajů není nutné informovat o povaze incidentu či jeho rozsahu, je však nutné jim sdělit možné následky, přijatá opatření a kontakt, kde mohou získat bližší informace (tím by měl být především pověřenec pro ochranu osobních údajů).[232] Pro komunikaci těchto informací by měl správce nejlépe užít zvláštní komunikační kanál (např. zvláštní e-mailovou adresu správce) a měl by se vyhnout

227 Blíže k vymezení zranitelných subjektů údajů viz bod odůvodnění 75 Obecného nařízení.

228 V této souvislosti je výslovně zmíněn jako významný příklad právě v této monografii podrobně diskutovaný kontext internetu věcí.

229 Srov. bod odůvodnění 91 Obecného nařízení.

230 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679* [online]. wp248rev.01_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2017, s. 10–12 [cit. 29. 5. 2021].

231 Očekávatelné budoucí porušení bezpečnosti lze spojovat např. s únikem přístupových údajů k e-mailovému účtu, pokud byl tento účet užit pro registraci a validaci uživatele na jiných platformách a lze s jeho pomocí tudíž změnit přístupové údaje a ukrást identitu dotčené fyzické osoby. Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017, Beck'sche Kompakt-Kommentare, Art. 34 Rn 30b.

232 Srov. čl. 34 odst. 2 Obecného nařízení.

sdělování na kontaktní údaje, které byly zřejmě kompromitovány oznamovaným porušením zabezpečení.[233]

Oznámení i při splnění podmínky vysokého rizika není nutné, pokud byly údaje subjektů zajištěny opatřením, které je činí nesrozumitelnými při neoprávněném přístupu (např. šifrování v souladu se stavem techniky) nebo pokud vzápětí po události přijal správce opatření, která zásadně omezila pravděpodobnost vysokého rizika pro práva a svobody dotčených subjektů údajů.[234] Je-li kontaktování všech dotčených osob nepřiměřeně obtížné, může správce zvolit formu veřejného oznámení, zajištění informační linky na vyžádání nebo obdobné opatření.[235]

3.2.3 Diskuse právní úpravy povinností dle článků 33 a 34 Obecného nařízení

V této části kapitoly nahlédneme za vlastní znění normativní úpravy povinností spojených s případy porušení zabezpečení osobních údajů a nabídneme systematický a teleologický pohled na jejich účel a význam v kontextu právního rámce ochrany osobních údajů. Současně přistoupíme k identifikaci výzev, které se v dnešní situaci pojí s aplikací a výkladem těchto povinností v praxi.

Systematická provázanost s jinými prvky úpravy: Ochrana osobních údajů před neoprávněným zpracováním je ústředním motivem zde diskutovaného právního rámce.[236] Její klíčová úloha je dále zdůrazňována skrze řadu specifikujících ustanovení, v návaznosti na požadavky minimalizace zpracování osobních údajů a bezpečnosti, integrity a důvěrnosti oprávněných

233 Srov. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 22 [cit. 28. 2. 2021].

234 Viz čl. 34 odst. 3 písm. a) a b) Obecného nařízení. Za taková opatření lze považovat např. okamžitou změnu přístupových údajů a revokaci oprávnění spojených s účty dotčených fyzických osob pod podmínkou nové autentizace, čímž dojde k zásadnímu znehodnocení uniklých osobních údajů.

235 Srov. čl. 34 odst. 3 písm. c) Obecného nařízení, blíže pak PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 23 [cit. 28. 2. 2021].

236 Viz DE TERWANGNE, Cécile. Article 5. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 318.

zpracování v souladu se základními principy této právní úpravy.[237] Přes zdánlivou jednoznačnost základních zásad a zákonných požadavků na zpracování osobních údajů je často nesnadné vymezit pro specifické situace konkrétní podobu přiměřených opatření.[238]

Přitom jedním z nejzjevnějších signálů o nedostatečnosti zavedených opatření je odhalení porušení zabezpečení osobních údajů. To může poukázat nejen na specifickou zranitelnost zvolených opatření, která může přetrvávat v operacích daného správce, ale především může být mnohem rozšířenější a představovat tak snadno zneužitelnou zranitelnost širšího okruhu správců. V tomto ohledu je tudíž významné vnímat potřebu dozorového úřadu být včas a řádně informován o případech porušení zabezpečení napříč skupinami podobně fungujících regulovaných subjektů.

Výkladová nejistota ve vztahu ke konkretizaci povinností uložených Obecným nařízením je do značné míry nevyhnutelná i vzhledem k vlastní šíři spektra situací, na které právní úprava ochrany osobních údajů dopadá. Tomu odpovídá různorodost přiměřených scénářů opatření, která je vhodné na konkrétní okolnosti zpracování aplikovat. V právním rámci Obecného nařízení se toto odráží skrze ústřední roli hodnocení rizikovosti činností s osobními údaji[239] a dále pak na základě širokého využití performativních pravidel jakožto právního nástroje pro flexibilní, technologicky neutrální a časově rezistentní požadavky na povinné subjekty.[240]

Roli hodnocení rizikovosti zpracování v systematice Obecného nařízení se v českém akademickém diskurzu v nedávné době věnoval *Míšek*.[241] Poukazuje

237 Srov. čl. 5 odst. 1 písm. c) a f) Obecného nařízení.

238 Srov. BURTON, Cédric. Article 32. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 635–636.

239 Srov. čl. 24 odst. 1, čl. 25 odst. 1, či čl. 35 odst. 1 Obecného nařízení.

240 Ta do značné míry nahrazují rigidní režim dozoru na základě oznamovací povinnosti pro zcela nebo částečně automatizovaná (příp. o ohledem na zvolenou formu transpozice též neautomatizovaná) zpracování dle článku 18 směrnice 95/46/ES. Jak uvedeno v bodě odůvodnění 89 Obecného nařízení: *„Tato povinnost přináší administrativní a finanční zátěž, avšak nepřispěla ve všech případech ke zlepšení ochrany osobních údajů. Proto by měla být tato nerozlišená obecná ohlašovací povinnost zrušena a nahrazena účinnými postupy a mechanismy, které by se místo toho zaměřily na takové typy operací zpracování, jež mohou s ohledem na svou povahu, rozsah, kontext a účely představovat vysoké riziko pro práva a svobody fyzických osob."*

241 Viz MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. 1. vyd. Brno: Masarykova univerzita, 2020. s. 169–177.

přitom na to, že Obecné nařízení je příkladem regulace rizik *(risk regulation)*, tedy normativním nástrojem zákonodárce omezit na přijatelnou míru soubor rizik hrozící osobám či statkům.[242] Současně se ale jedná i o regulaci postavenou na riziku *(risk based regulation)*, tedy na regulatorní metodě, kde je hodnocení rizika součástí postupů pro zajištění efektivního plnění povinností, což se v Obecném nařízení odráží v zásadě odpovědnosti správce *(accountability)*.[243]

Performativní pravidla: Oblast technologií přináší s ohledem na svůj vysoce dynamický rozvoj zásadní překážku pro včasné a adekvátní utváření regulatorního rámce, který by plně postihoval i nejnovější postupy, procesy a možnosti. To nevyhnutelně vede k mezeře mezi technologickým kontextem, na který je optimalizována právní úprava při legislativním procesu a technologickou realitou, na kterou je následně aplikována. S ohledem na rostoucí rychlost pokroku zvláště na poli ICT se přitom tato disproporce mezi normativním rámcem a upravovaným prostředím dále prohlubuje, což vede k jevu, který *Marchant, Allenby* a *Herkert* označují jako problém tempa *(pacing problem)*.[244] Jednou z možných reakcí práva na tuto výzvu jsou performativní pravidla *(performance-based rules)*.[245] Těm se v zahraničním diskurzu podrobně věnoval především *Coglianese*.[246] Výstižné vymezení tohoto pojmu poskytuje *Míšek,* když uvádí, že *„[p]rincip performativní regulace* […] *spočívá v tom, že zákonodárce nestanoví konkrétní cestu, jejíž splnění vede k dosažení regulací sledovaného cíle, ale naopak určí cílový stav a nechá regulované subjekty, aby si samy určily, jak takového zákonem stanoveného cíle dosáhnou.“*[247]

242 Ibid., s. 170.

243 Ibid., s. 171, s odkazem na QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, roč. 9, č. 3, s. 510–511.

244 Srov. MARCHANT, Gary E., Braden R. ALLENBY a Joseph R. HERKERT (eds.). *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*. Dordrecht: Springer, 2011, s. 19 a násl., The International Library of Ethics, Law and Technology, 7.

245 Za vhodnější, avšak těžkopádnější český překlad pojmu lze vnímat spojení „pravidla založená na výkonu a projevech“. Srov. HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti*. Disertační práce. Brno: Masarykova univerzita, Právnická fakulta, 2018, s. 53.

246 Viz COGLIANESE, Cary. Performance-based regulation: concepts and challenges. In: BIGNAMI, Francesca a David ZARING (eds.). *Comparative Law and Regulation. Understanding the Global Regulatory Process*. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2016, s. 403 a násl., Comparative Law and Regulation.

247 Srov. MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. 1. vyd. Brno: Masarykova univerzita, 2020. s. 149.

Z prostředí české právní vědy je pak také na místě zmínit pojetí *Polčáka*, který akcentuje postavení subjektu, kterému je performativní pravidlo určeno, jako definiční autority (Tzn. subjektu vykonávajícího skutečnou kontrolu nad určitou oblastí kyberprostoru,[248] zpravidla technické infrastruktury, a proto je schopen nejefektivněji přizpůsobit parametry regulace danému prostředí pro dosažení stanoveného účelu.[249]). *„Performativní pravidlo tak má charakter obecně (až teleologicky) definované povinnosti ukládající definiční autoritě vytvoření a technickou implementaci konkrétních pravidel, přičemž jejich obsah je ponechán úvaze definiční autority v návaznosti na parametry příslušného systému nebo sítě. Různé definiční autority mohou na své fyzické nebo logické infrastruktuře dle svého uvážení implementovat obsahově zcela různá pravidla, jejichž fungování však vede k témuž cíli."*[250]

Performativní pravidla jsou tedy faktickým přenesením části specifikace či výkladu normativní povinnosti na povinný subjekt, což v obecné rovině snižuje zátěž spojenou s výkladem rigidní úpravy neodpovídající regulované realitě a umožňuje vyšší míru inovace.[251] V tom lze shledávat odraz pragmatické metody v právu. Jak přibližuje *Polčák*, stojí za ním přihlédnutí k relevantním empirickým faktorům, z nichž pro kontext ochrany osobních údajů za zřejmě nejvýznamnější lze vnímat právě dynamický technologický vývoj. V takovém regulovaném kontextu se pak pragmatická metoda jeví nejen navýsost vhodnou, ale v podstatě jedinou umožňující pružně reagovat na proměnlivý stav techniky.[252]

Současně je však rozsáhlým využitím performativních pravidel zvyšována nejistota ohledně vhodného přístupu k hodnocení situace a výkladu parametrů regulatorního rámce u povinných subjektů. To může být problematické zvláště u komplexní a výkladově složité úpravy, jakou Obecné nařízení bezesporu je. *The Economist* jej dokonce označil za *„zřejmě nejsložitější regulatorní*

248 Srov. POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 137.

249 Viz POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 89.

250 Srov. POLČÁK, Radim. 1 Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 14.

251 Viz MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*, 2003, roč. 25, č. 4, s. 387.

252 Srov. POLČÁK, Radim. 1 Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 5.

dílo, který kdy EU vytvořila."[253] Toto ve spojení s různorodostí subjektů, které stojí v pozici správců a zpracovatelů (od nadnárodních technologických gigantů typu *Facebook* po miliony mikropodniků s jen několika zaměstnanci)[254] staví do klíčové pozice „převodní články" pro konkretizaci výkladu regulatorního rámce, tedy doporučení, metodiky a příklady dobré praxe.[255] Ta by měla být zajišťována předně skrze pokyny, stanoviska a potažmo rozhodovací praxi národních dozorových úřadů a Sboru (plynule navazujícího na činnost Pracovní skupiny dle článku 29). Současně by mělo k větší sektorové specifikaci přispět utváření kodexů chování v souladu s články 40 a 41 Obecného nařízení. Dalším nástrojem, který je zde možné zvažovat jsou osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu, tak jak upravují články 42 a 43 Obecného nařízení. Těmto nástrojům a souvisejícímu vývoji na poli kyberbezpečnosti budou věnovány podkapitoly 6.1 a 6.2.

Potřeba výkladu přiměřenosti opatření či podmínek pro založení povinnosti přenáší část zátěže při překonávání výkladové nejistoty zpět na dozorové úřady. Současně je nezbytné při zachování stejnocenné aplikace právní úpravy Obecného nařízení klást zvláštní důraz na koordinaci a spolupráci mezi dozorovými úřady, tak aby byl zajištěn vyvážený výklad i rozhodovací praxe. Nedávná analýza činnosti dozorových úřadů po dvou letech použitelnosti Obecného nařízení však upozorňuje na značné přetrvávající nedostatky ve spolupráci a jednotnosti mezi dozorovými úřady.[256] Pro ty je přitom rozsáhlé užití performativních pravidel také značně zatěžující při dozorové činnosti, jelikož musejí v dílčích situacích důsledně porovnat vhodný

253 *„Arguably the most complex piece of regulation the European Union (EU) has ever produced."* Viz THE ECONOMIST. The joys of data hygiene – Europe's tough new data-protection law. *The Economist* [online]. 5. 4. 2018 [cit. 13. 7. 2021].

254 Dle dostupných statistik bylo v roce 2018 v EU přes 23 milionů mikropodniků, tedy podniků s maximálně 9 zaměstnanci. Srov. EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES (EASME). *Annual Report on European SMEs 2018/2019, Research & Development and Innovation by SMEs* [online]. EASME/COSME/2017/031. Brusel: Evropská komise, 2019, s. 17 [cit. 21. 5. 2021]. Jejich perspektiva bude blíže zohledněna v rámci oddílu 4.4.3.

255 Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017. Beck'sche Kompakt-Kommentare. Art. 33 Rn 6.

256 Srov. MASSÉ, Estelle. *Two Years under the EU GDPR. An Implementation Progress Report. State of Play, Analysis and Recommendations* [online]. New York: Access Now, 2020, s. 12–14 [cit. 12. 7. 2021].

a přiměřený přístup s přístupem zvoleným povinným subjektem, tak aby bylo možné adekvátně podložit případné závěry o jeho nedostatečnosti v rámci auditu.

Performativní pravidla ve spojitosti s porušením zabezpečení: Za zřejmé uplatnění performativních pravidel v tomto kontextu platí především volba a rozsah přiměřených ochranných a detekčních opatření na základě článku 32 Obecného nařízení. Jak lze vysledovat z pojetí ohlašovací a oznamovací povinnosti, představených v oddílu 3.2.2, i zde se uplatňují dílčí prvky performativního pravidla. Správce je totiž konfrontován s neurčitými právními pojmy a zobecněnými kritérii k volbě metody zhodnocení rizika spojeného s odhaleným případem porušení zabezpečení a vyvození pro sebe právních důsledků v podobě rozsahu případných notifikačních povinností.

Toto přenesení výkladové nejistoty na správce je pochopitelné s ohledem na skutečnost, že právě správce je zpravidla v postavení prvního subjektu způsobilého a oprávněného urychleně a celostně zhodnotit odhalený případ porušení zabezpečení.[257] Dané povinnosti přitom nepředstavují typický příklad performativních pravidel, jelikož jejich ústřední složkou je transparentnost a povinnost sdílení informací. To je v pojetí teoretického zakotvení, které performativním pravidlům poskytuje *Coglianese* sice související, ale poněkud odlišný koncept regulatorního nástroje.[258] Jelikož je však tato informační povinnost podmíněna aktivitou a výkladem povinného subjektu, považuji provázanost s performativními pravidly za značnou.

Volnost spojená s přenesením významnější role při výkladu prvků na povinný subjekt, které mu zakládají notifikační povinnost, může být dvousečná. Pro performativní pravidla obecně platí, že přes jejich značnou oblíbenost ze strany regulátorů a zákonodárců absentuje významnější empirický výzkum, který by doložil, že tento přístup k regulaci je pro zvolené situace skutečně funkční (resp. funkčnější než rigidnější regulatorní metody).[259] Naopak lze

257 Je zde na místě zohledňovat jeho specifickou komplexní znalost jak dotčených databází, systémů a sítí, tak procesů a rozsahu zpracování osobních údajů v rámci všech souvisejících činností.

258 Viz COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michingan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 534 a 536.

259 Srov. COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-based regulation: Prospects and limitations in health, safety and environmental protection. *Administrative Law Review*, 2003, roč. 55, č. 4, s. 708.

nalézt významné případy, kdy regulace na základě performativních pravidel nevynutila u povinných subjektů řádné dodržování požadavků stanovených právní úpravu aniž by to byl regulátor s to po dlouho dobu odhalit (uvažujte např. rozsáhlý globální skandál s přípustným množstvím emisí z dieselových motorů, který notně otřásl důvěrou v adekvátnost regulatorního rámce pro automobilový průmysl).[260] V tomto směru vnímám za klíčové, aby pro regulatorní přístup, který po povinném subjektu vyžaduje sdílení (pro něj potenciálně poškozujících) informací a dává mu prostor pro výklad splnění podmínek pro vznik této povinnosti, existovala jedna ze dvou situací, která zakládá předpoklad dostatečné motivace povinného subjektu k řádnému dodržování dané povinnosti.

Předpoklady adekvátnosti uložení povinnosti sdílet informace: První je situace, kdy jsou zájmy povinného subjektu (správce) a příjemců informace (dozorového úřadu, resp. subjektů údajů) souladné, či alespoň kompatibilní. Pokud je se sdílením informací spojen zjevný benefit jak pro příjemce, tak pro povinný subjekt, lze očekávat jeho zvýšenou tendenci k řádnému ohlašování. Příkladem uvádím informační povinnosti na podporu zlepšení služeb přeshraničního dodávání balíků dle článku 4 nařízení 2018/644 o službách přeshraničního dodávání balíků,[261] kde vnímám přínos sdílení informací pro normalizaci tržního prostředí. To považuji za zřetelný benefit nejen pro uživatele, ale i pro povinné subjekty působící na tomto trhu.

Souladnost zájmů však může být narušena, pokud je předvídatelné, že skrze informační povinnost bude též doloženo porušení jiné povinnosti ohlašujícím subjektem (uvažujte např. v českém kontextu rozsáhle diskutovanou evidenční povinnost na základě § 18 a násl. zákona č. 112/2016 Sb. o evidenci tržeb), který se tak vystavuje hrozbě sankčního postihu. V takové situaci nastává konflikt zájmů a povinný subjekt může být na základě racionálního rozhodování odrazován od řádného sdílení informací v právní úpravou předjímaných situacích.[262]

260 Viz COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michingan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 530–531.

261 Nařízení Evropského parlamentu a Rady (EU) 2018/644 ze dne 18. dubna 2018 o službách přeshraničního dodávání balíků.

262 Hlouběji bude racionální rozhodování povinného subjektu o sdílení informací rozebíráno v páté kapitole.

Tento konflikt na straně povinného subjektu může být překonán v druhé situaci, kdy regulátor disponuje přiměřenými možnostmi kontroly a postihování porušování uložené povinnosti. Přestože je tedy s ohlášením informací pro subjekt spojeno riziko postihu, riziko postihu za vlastní neohlášení je významnější. *Coglianese* shledává tuto kapacitu regulátora za klíčový prvek, ale současně též za složku, které je často složité či dokonce nemožné dostát, případně pouze za společenských nákladů, které převyšují společenské přínosy daného regulatorního přístupu.[263] Pro posouzení souladu zájmů regulátora a regulovaného subjektu je přitom zásadní identifikovat účel dané normy.

Účel normy: Na základě v úvodu podkapitoly 3.2 nastíněného směřování k funkčnímu výkladu příslušných ustanovení Obecného nařízení je účel normativních povinností dle článků 33 a 34 Obecného nařízení zkoumán ve třech rovinách. Prvně je zohledněno samotné textové zachycení právní úpravy v příslušných článcích, jakožto východisko pro účelový výklad.[264] Následně je vzhledem ke specifické povinné existenci odůvodnění u předpisů sekundárního unijního práva zkoumána tato složka právní úpravy ve snaze o případné odhalení úmyslu zákonodárce ohledně účelu předmětných povinností. Třetí rovinou je výklad teleologický, ve snaze o nalezení účelu z objektivního hlediska.[265]

Účel vyjádřený v textu: Ve vztahu k dokumentační povinnosti dle článku 33 odst. 5 Obecného nařízení je účel této povinnosti zakotven v druhé větě ustanovení, která uvádí: *„Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem."*[266] Je tudíž zřejmé, že účelem dané povinnosti je usnadnění, resp. umožnění posouzení souladu správce s ohlašovací povinností založenou týmž článkem, v souladu se zásadou odpovědnosti *(accountability)* dle článku 5 odst. 2 Obecného nařízení. Ta zahrnuje i schopnost správce doložit dodržení souladu s povinnostmi dle tohoto nařízení. Pro povinnost ohlášení i oznámení pak z vlastního textu ustanovení vyplývá pouze, že je podmíněna pravděpodobným rizikem, resp. vysokým rizikem pro práva

263 Srov. COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michingan Journal of Law Reform*, 2017, roč. 50, č. 3, s. 562–563.

264 Viz SEHNÁLEK, David. *Specifika výkladu práva Evropské unie a jeho vnitrostátní důsledky*. Praha: C. H. Beck, 2019, s. 111.

265 Ibid., s. 110 a 116–117.

266 Srov. čl. 33 odst. 5 Obecného nařízení.

a svobody fyzických osob. Je zde tudíž zřejmé navázání na obecný cíl této právní úpravy, vyjádřený v článku 1 odst. 2 Obecného nařízení: *„Toto nařízení chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů."*[267] Konkrétnější účel povinností dle článků 33 a 34 lze pak usuzovat z jejich povahy a stanoveného rozsahu sdílených informací.[268] Jde o informační povinnosti, cílem je tedy včasně sdílet informace o určitém jevu[269] se subjekty, které tyto informace nemají (ale je pro ně příhodné, aby je měli). Vlastní účel tohoto sdílení však z textového zachycení daných povinností nelze bez dalšího vyčíst.

Účel zachycený v bodech odůvodnění: Nápomocné v tomto směru však mohou být související body odůvodnění, vystihující úmysl či úvahy tvůrců Obecného nařízení v kontextu jednotlivých institutů a povinností. Především bod odůvodnění 85 Obecného nařízení v tomto směru osvětluje, že *„[n]ení-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým osobám způsobit fyzickou, hmotnou či nehmotnou újmu …"*[270] Z toho vyplývá, že účelem dané povinnosti je předcházet újmě fyzických osob skrze přispění k náležitému a včasnému řešení porušení zabezpečení.

Role sdílení informací s dotčeným subjektem údajů na základě oznamovací povinnosti je zřejmá a přímá, jelikož vědomí o hrozící újmě a okolnostech jejího vzniku je nezbytným předpokladem pro subjekt údajů, aby mohl jednat a učinit přiměřená opatření k jejímu odvrácení.[271] V tomto směru lze oznamovací povinnost dle článku 34 Obecného nařízení označit za specifikaci obecné prevenční povinnosti v rámci škodního práva pro oblast ochrany osobních údajů.

Ta je v českém právu zakotvena v zákoně č. 89/2012 Sb., občanský zákoník v § 2900–2901. Konkrétně § 2900 zakládá *„počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného."*[272]

---

267 Srov. čl. 1 odst. 2 Obecného nařízení.

268 Viz čl. 33 odst. 3, resp. čl. 34 odst. 2 Obecného nařízení.

269 Zde o případu porušení zabezpečení osobních údajů odhaleném daným správcem, resp. jemu přidruženým zpracovatelem.

270 Srov. bod odůvodnění 85 Obecného nařízení.

271 Např. znehodnocením ohrožených osobních údajů, informováním subjektů, u kterých hrozí zneužití takto neoprávněně zpracovávaných osobních údajů či obnovení přístupových údajů pro zabránění šíření újmy napříč účty virtuálních identit jedince.

272 Viz § 2900 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

To v kontextu ochrany osobních údajů odpovídá obecným povinnostem přiměřeného zabezpečení osobních údajů dle článku 32 Obecného nařízení. § 2901 pak ukládá, že musí *„zakročit na ochranu jiného každý, kdo vytvořil nebezpečnou situaci nebo kdo nad ní má kontrolu, anebo odůvodňuje-li to povaha poměru mezi osobami."*[273] Poměr mezi subjektem údajů a správcem zde zjevně má povahu, která takovou aktivitu zakládá. Ta přitom spočívá především ve včasném odhalení případu porušení zabezpečení a následně reaktivních opatřeních správce, která zabrání či omezí újmu hrozící v jeho důsledku subjektu údajů. Oznamovací povinnost je pak jednoznačnou konkretizací či rozšířením obecné oznamovací povinnosti na základě § 2902, dle kterého *„[k]do porušil právní povinnost, nebo kdo může a má vědět, že ji poruší, oznámí to bez zbytečného odkladu osobě, které z toho může újma vzniknout, a upozorní ji na možné následky."*[274]

Ohlašovací povinnost a chytrá regulace: Stejně snadné však není přijetí výše dovozeného účelu oznamovací povinnosti pro ohlašovací povinnost vůči dozorovému úřadu. Zde se totiž nejedná o přímý krok prevence hrozící újmy, dozorový úřad není poškozený ani nemá přímé nástroje, kterými by mohl zakročit na ochranu subjektu údajů. Může však vrchnostensky jednat vůči danému správci a vést jej k zavedení reaktivních opatření, která sníží následky ohlášeného porušení zabezpečení a zabrání tak hrozící újmě subjektů údajů. Účel této povinnost proto vnímám především jako prvek chytré regulace. Podle *Polčáka*, *„[j]de o regulatorní techniku obsahující mechanismy flexibilně reagující na kvalitu regulovaného prostředí. K tomu, aby tato technika v praxi fungovala, je třeba samozřejmě disponovat daty, která regulované prostředí adekvátně popíšou."*[275] Na rozdíl od performativních pravidel tak jde o metodu zvýšení informovanosti regulátora, která mu umožňuje aktivně a cíleně stanovovat konkrétní povinnosti či ukládat zavedení opatření. Jak dále uvádí *Polčák*, *„[r]egulované subjekty tedy v tomto případě nejsou nuceny ke konkretizaci obecných pravidel ve formě autonomní normotvorby, ale pouze k tomu, aby vrchnosti poskytovaly v reálném čase informační servis o fungování příslušného systému nebo služby."*[276]

273 Viz § 2901 zákona č. 89/2012 Sb.
274 Viz § 2902 zákona č. 89/2012 Sb.
275 Srov. POLČÁK, Radim. 1 Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 17.
276 Viz POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 90.

Jak vyplývá z výkladu Pracovní skupinou dle článku 29 (nyní Sbor), účelem ohlašovací povinnosti je podnítit správce k včasné reakci na porušení zabezpečení, omezení jeho následků, a pokud možno také obnovení narušených osobních údajů.[277] V tomto směru jim přitom dozorový úřad může nabídnout podporu a doporučení, současně však platí, že toto sdílení informací s dozorovým úřadem může vést k jeho zásahu v souladu s úkoly a pravomocemi dle Obecného nařízení.[278] Za významný pak vnímám především úkol monitorovat a vymáhat uplatňování tohoto nařízení dle článku 57 odst. 1 písm. a) Obecného nařízení. Význam ohlašovací povinnosti v boji proti bezpečnostním mezerám je přitom zásadní, jelikož včasné uvědomění regulátora ohledně incidentů a souvisejících rizik je nezbytným předpokladem pro umožnění jeho reakce.[279]

Za srovnatelný prvek chytré regulace lze přitom považovat také povinnost hlášení kybernetických bezpečnostních incidentů na základě ZoKB. Vzájemný vztah těchto povinností sdílet informace bude podrobněji zkoumán v podkapitole 6.5.

Účel z objektivního hlediska: Přijmeme-li ohlašovací povinnost dle článku 33 Obecného nařízení jako prvek chytré regulace, pokusme se nyní identifikovat účel, ke kterému tato regulace směřuje. Vhodným výchozím bodem bude stručná charakteristika postavení jednotlivých aktérů, tedy správce, subjektu údajů a dozorového úřadu.

Správce disponuje osobními údaji fyzických osob, za jejichž ochranu nese odpovědnost. Současně získává v případě řádného provedení detekčních opatření záhy poté, co dojde k porušení zabezpečení, informaci o této skutečnosti. Nelze sice pomíjet, že správci tímto vzniká újma na jeho aktivech,[280] ta však není chráněnou hodnotou z hlediska právního rámce ochrany osobních údajů. V tomto ohledu tak správce disponuje informacemi o skutečnosti, která hrozí významným škodlivým účinkem pro jiný subjekt. Tímto subjektem je fyzická osoba identifikovatelná na základě neoprávněně zpracovávaných

277 Srov. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 16 [cit. 28. 2. 2021].

278 Srov. bod odůvodnění 87 Obecného nařízení.

279 Srov. PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017. Beck'sche Kompakt-Kommentare. Art. 33 Rn 5.

280 V podobě dodatečných nákladů pro nápravu zabezpečení sítí, systémů a zařízení, újmy v důsledku ztráty dat či ušlého zisku v důsledku narušení jeho činnosti.

osobních údajů. Ta se přitom o hrozící újmě včas nedozví, tak aby jí mohla odvrátit či zmírnit, pokud jí o tom správce neinformuje.

Mezi správcem a subjektem údajů tak lze identifikovat jednak problém přenesené újmy a dále pak informační asymetrii.[281] Řešení těchto překážek pro odvrácení újmy v souladu s výše identifikovanou konkretizací preventní povinnosti vnímáme jako účel oznamovací povinnosti dle článku 34 Obecného nařízení určitelný z objektivního hlediska.

Ve vztahu k dozorovému úřadu je situace poněkud odlišná. Správce na jedné straně disponuje informacemi o možném porušení svých povinností ve vztahu k zabezpečení zpracovávaných osobních údajů,[282] za které mu hrozí postih ze strany dozorového úřadu.[283] Dozorový úřad oproti tomu nemá s nejvyšší pravděpodobností k dispozici jiný zdroj informací o daném porušení zabezpečení.[284] Jeho realizace dozorové činnosti ve spojení s porušením zabezpečení je tak do značné míry závislá na „přiznání" daného správce, že k incidentu došlo a informacích o jeho rozsahu a okolnostech. Lze sice v obecně normativní rovině zvažovat, že dozorový úřad by měl být schopen na základě své nahodilé kontrolní činnosti v podobě auditů ochrany údajů dle článku 58 odst. 1 písm. b) Obecného nařízení odhalit významné případy porušení zabezpečení. To je však dle mého názoru iluzorní představa především při zohlednění:

1. rostoucí složitosti a reálné neodhalenosti (v případě aktivit státních aktérů) řady těchto bezpečnostních incidentů, jak bylo nastíněno v rámci druhé kapitoly;

281 To znamená, že situace nastalá u správce (ať již jeho pochybením či nikoliv), o které má (mít) informace, hrozí újmou (především) pro subjekt údajů, který o ní však zásadně nemá (dostatečné a včasné) informace. Blíže se k pojmu vrátím při zohlednění ekonomické perspektivy v páté kapitole. K jeho obsahu viz např. AURONEN, Lauri. Asymmetric Information: Theory and Applications. *Semin. Strategy Int. Business*. 2003.

282 Ty mohou být současně pro dozorový úřad užitečnými informacemi pro prevenci srovnatelných pochybení u jiných správců.

283 Ten mu však může zároveň i pomoci s řešením dané situace a zabránění nárůstu výsledné újmy, ať již v podobě té přímo utrpěné správcem na jeho aktivech nebo té, která na něj bude následně přenášena postiženými subjekty údajů, ať již na základě nároků dle národního škodního práva, či dle čl. 79 Obecného nařízení.

284 O jeho existenci může být potenciálně spraven např. na základě podnětu postiženého subjektu údajů či pověřence pro ochranu osobních údajů daného správce, při jeho důsledném plnění úkolů dle čl. 39 odst. 1 písm. b) a d) Obecného nařízení. Další možné zdroje informací o porušení zabezpečení při absenci spolupráce povinného správce jsou diskutovány v podkapitole 6.5.

2. skutečnosti, že v EU působí přes 25 milionů podniků;[285]
3. významných rozpočtových a personálních limitů dozorových úřadů (a tudíž množství provedených auditů);[286] a především pak
4. potřeby dozorového úřadu v rámci auditů posuzovat plnění řady dalších povinností na základě Obecného nařízení.[287]

K asymetrické informaci zde tak přistupuje konflikt zájmů na straně správce,[288] který zakládá riziko morálního hazardu.[289]

Na základě dosud uvedeného tudíž vyvozuji, že účelem ohlašovací povinnosti jako nástroje chytré regulace je shromažďovat pro regulatorní činnost dozorového úřadu aktuální a komplexní informace o stavu zabezpečení osobních údajů u správců a zpracovatelů. Ty následně mají přispívat k účinným a efektivním regulatorním rozhodnutím dozorového úřadu vedoucím ke zajišťování vysoké úrovně ochrany osobních údajů ve společnosti (skrze monitorování a vymáhání řádného dodržování uložených povinností). Zásadní roli tak hraje včasnost a plošné plnění ohlašovací povinnosti, což činí výše naznačený konflikt zájmů správce možnou významnou překážkou. Zaměříme na něj tudíž pozornost v páté kapitole, při analýze motivace a racionálního rozhodování povinného subjektu.

Jelikož odhalený konflikt zájmů směřuje k jádru konceptu notifikační povinnosti o porušení zabezpečení, nastíněná překážka se neomezuje pouze na úpravu dle Obecného nařízení. Byla o ní ostatně již zmínka výše,

285 Srov. EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES (EASME). *Annual Report on European SMEs 2018/2019, Research & Development and Innovation by SMEs* [online]. EASME/COSME/2017/031. Brusel: Evropská komise, 2019, s. 17 [cit. 21. 5. 2021].

286 Srov. MASSÉ, Estelle. *Two Years under the EU GDPR. An Implementation Progress Report. State of Play, Analysis and Recommendations* [online]. New York: Access Now, 2020, s. 9 [cit. 12. 7. 2021].

287 Domnívám se přitom, že většina ostatních povinností je snadněji kontrolovatelná a ze strany správce při jejich kontrole bude nabízena větší míra součinnosti.

288 V kolizi jsou především zájem na plnění povinností a zájem na minimalizaci újmy skrze opominutí sdílení informace o vlastním pochybení vedoucí k uložení sankce.

289 Jedná se o rozhodnutí správce k jednání, které je z jeho pozice výhodnější (tzn. neohlášení porušení zabezpečení), ale vede k celospolečenské újmě (tzn. snížení přehledu dozorového úřadu o celkové situaci a nezabránění důsledků daného porušení zabezpečení). Jelikož jde o problematiku spadající do ekonomického přístupu k právu či *law and economics*, budeme mu věnovat větší pozornost později v páté kapitole. Blíže pojem morálního hazardu představuje např. BAKER, Tom. On the Genealogy of Moral Hazard. *Texas Law Review*, 1996, roč. 75.

v oddílu 3.1.1, ve vyjádření Úřadu popisujícího zkušenosti s dodržováním notifikačních povinností u poskytovatelů veřejně dostupných služeb elektronických komunikací.

K jejímu řešení pak mohou přispět příspěvky do odborného diskurzu vztahujícího se k americké právní úpravě notifikačních povinností ohledně porušení bezpečnosti zpracovávaných údajů. Významně delší použitelnost ustanovení vztahujících se k této problematice v americkém prostředí totiž zavdala více prostoru analýze a rozboru daného konfliktu zájmů se zahrnutím právní i ekonomické perspektivy. Z těch vnímám za vhodné čerpat i pro účely této monografie, byť je v první řadě nezbytné představit systematiku a strukturu americké úpravy a upozornit na relevantní odlišnosti, které panují mezi oběma systémy práva.

3.3 Povinnosti při porušení bezpečnosti v právu Spojených států amerických

Pro komplexní zachycení diskutované problematiky a ve snaze o potvrzení či vyvrácení teze, že výše určená překážka konfliktu zájmů u povinného subjektu a omezených možností kompenzace informační asymetrie regulátora skrze audit je skutečně koncepční, a nikoliv specifická pro ustanovení Obecného nařízení, nahlížím též na vývoj notifikačních povinností v souvislosti s porušením bezpečnosti v právu Spojených států amerických.

Jsem si přitom plně vědom nejen odlišností příslušných právních systémů ve struktuře norem a přístupu k souvisejícím otázkám (např. ochrana soukromí), ale i překážek a omezení, které se pojí s přístupem srovnávání právních úprav mezi jurisdikcemi.[290] Přesto nelze, dle mého názoru, americké prostředí při důsledné analýze a diskusi předmětné problematiky opomíjet. Předně se jedná o hodnotově blízké prostředí, které nabízí prvotní historický vývoj diskutovaných notifikačních povinností, který byl výslovným podkladem a inspirací vedoucí k dnešní unijní úpravě v Obecném nařízení.[291]

290 Blíže viz ADAMS, Maurice a Jacco BOMHOFF (eds.). *Practice and Theory in Comparative Law* [online]. Cambridge: Cambridge University Press, 2012 [cit. 14. 7. 2021]; BOGDAN, Michael. *Comparative Law*. Stockholm: Springer, 1994.

291 Srov. oddíl 3.1.1 popisující novelizaci směrnice 2002/58/ES skrze směrnici 2009/136/ES na základě inspirace úpravou státu Kalifornia a dále pak oddíl 3.2.1 popisující vznik úpravy v Obecném nařízení a její zakotvení na úpravě dle směrnice 2009/136/ES.

Zavedenost notifikačních povinností při porušení bezpečnosti zpracovávaných údajů ve srovnání s jejich relativní novostí v unijním právu ochrany osobních údajů dále podtrhuje významně širší okruh pramenů a odborných zdrojů, které se problematice věnují. To se přitom týká nejen omezeně přenositelných právních tezí, ale též zkušeností s limity těchto povinností a studií ekonomického modelování rozhodování povinných subjektů, kterým je věnována pátá kapitola.

Podporu pro začlenění přehledu a diskuse kontextu americké úpravy pak nacházím i ve vyjádření, kterým *Bygrave* nabádá, aby výzkum v oblasti ochrany osobních údajů zahrnoval prvky přesahující jurisdikce. K tomu uvádí, že ačkoliv možnost normativní komparace je metodologicky nesnadná, *„přesto by právní věda měla přinejmenším zjišťovat základní podobnosti a rozdíly mezi různými národními a mezinárodními regulatorními rámci se záměrem zdůraznění možných střetů, problémů a strategií. A také by měla přinejmenším usilovat o nalezení měřitel pro posouzení relativní účinnosti jednotlivých rámců."*[292]

Je tedy na místě zdůraznit, že záměrem této představované části monografie není komparace americké a evropské právní úpravy, jakožto ani vyčerpávající představení a analýza americké úpravy jako takové. V tomto směru je ostatně již dnes dostupná řada odborných pramenů.[293] Záměrem je toliko představení nosných prvků a případných specifik americké úpravy, na které je možné referovat při následné diskusi překážek notifikačních povinností, jako je konflikt zájmů povinného subjektu. Z pramenů založených na zde představené úpravě je pak čerpáno při úvahách možných řešení pro současnou unijní úpravu v kontextu internetu věcí v šesté kapitole.

---

292 *„Nonetheless, legal research ought at the very least to ascertain basic similarities and differences between various national and international regulatory frameworks with a view to highlighting possible conflicts, issues and strategies. And it ought, at the very least, to seek to find benchmarks for assessing the relative effectiveness of the respective frameworks."* Srov. BYGRAVE, Lee A. Legal Scholarship on Data Protection: Future Challenges and Directions. In: *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde Liber Amicorum Yves Poullet*. 1. vyd. Brussels: Larcier, 2018, s. 499.

293 Viz např. DAVIS WRIGHT TREMAINE LLP. Summary of U.S. State Data Breach Notification Statutes [online]. 2019 [cit. 4. 6. 2021]. Dostupné z: https://www.dwt.com/gcp/state-data-breach-statutes; Comparison of US State and Federal Security Breach Notification Laws. *STEPTOE & JOHNSON LLP.* [online]. 2016 [cit. 30. 5. 2021]. Dostupné z: https://www.steptoe.com/images/content/6/5/v1/6571/SteptoeDataBreachNotificationChart.pdf

3.3.1 Terminologie problematiky v kontextu práva Spojených států amerických

Jak bylo již nastíněno na úvod v podkapitole 1.2, je na místě odlišovat pojmy amerického práva na ochranu soukromí a údajů o jednotlivci od tradičně užívané terminologie unijního práva ochrany osobních údajů. V americkém právu je pak dále např. pro termín porušení bezpečnosti převážně užíván termín *„security breach"*, namísto v unijním právu zakotveného anglického termínu *„personal data breach"*.[294]

Tato odlišnost odráží hlubší rozdílnost mezi americkým a evropským přístupem k ochraně údajů o jednotlivci, která je stručně nastíněna v následujícím oddílu. V americkém právu není zakotven srovnatelný pojem pro „osobní údaj" v pojetí Obecného nařízení. Za obsahově nejbližší termíny hojně užívané relevantními předpisy pro zde řešenou problematiku platí *„personal information"* a *„personally identifiable information"*, které by však při důsledném překladu vedly k doktrinálně zavádějícímu užití pojmu „informace", které v tomto kontextu pokládám za nevhodné.[295] Budu tudíž používat pojem „údaje o jednotlivci",[296] který případně doplním o specifikaci obsahového významu v kontextu konkrétního předpisu amerického práva.

3.3.2 Relevantní specifika americké právní úpravy

Přes historicky převažující roli soudcovské tvorby práva jako základní komponenty v americkém prostředí je dnešní systém spíše smíšený. Skrze rostoucí význam právních předpisů a kodifikací se americké právo přibližuje

294 Srov. BRUYNE, M. F. de. *Data breach notification and the risk of over-notification under the GDPR. A comparative analysis of US and EU experiences in practice* [online]. Tilburg, 2016, s. 9 [cit. 19. 3. 2021]. Master's Thesis. Tilburg University.

295 Pojem informace vnímám jako hodnotovou kvalitu spojenou s pozitivně organizujícím efektem (tedy potlačováním entropie). Pojem data naopak zachycuje záznam údaje, který může mít informační kvalitu. Jelikož jsme však schopni vykonávat kontrolu toliko nad daty, nikoliv nad jejich informační hodnotou per se, je užití pojmu informace pro sekundární objekty práva nevhodný, byť poměrně rozšířený i v českém prostředí. Blíže viz POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*, 2016, roč. 7, č. 13, s. 67 a násl.

296 Vzhledem ke značné fragmentaci americké úpravy nejsou notifikační povinnosti vázány na jednotný okruh relevantních údajů, které jsou s to identifikovat jednotlivce, nelze zde tudíž hovořit ani o srovnatelném jednotícím konceptu, jakým jsou osobní údaje pro unijní právní úpravu.

kontinentálním právním řádům, kde přitom naopak roste význam rozhodovací činnosti soudů.[297]

Právní předpisy se dělí na federální právo a právní řády jednotlivých států (státní právo), přičemž státní právo není sjednocené. Jednotlivé státy federace mají nezávislé právní systémy s oddělenými soudními soustavami, kde v tomto směru není (na rozdíl od federálního práva) jednotící role Nejvyššího soudu Spojených států (*Supreme Court of the United States*, SC USA).[298]

Rozsáhlejší význam než v evropské kontinentální právní tradici náleží při interpretaci amerického práva soudním precedentům na základě doktríny *stare decisis*. K výkladu státního práva přitom dochází zásadně nezávisle na sobě jednotlivými soudními soustavami s nejvyšším soudem státu.[299]

Americké soukromoprávní procesní právo má obecně řadu specifik, jejichž rozbor sahá nad rámec zaměření této publikace a jejichž bližší představení není, dle mého názoru, nezbytné pro diskusi zde řešené problematiky. Zmínku si však zaslouží možnost uložení náhrady újmy nad rámec doložené způsobené újmy jako forma sankce *(punitive damages)*[300] a široké užití procesního nástroje skupinových žalob *(class action)*,[301] o kterých bude zmínka dále v textu.

Za významné platí, že ve Spojených státech nenacházíme sjednocený a celistvý právní rámec na ochranu soukromí nebo bezpečnosti dat, natož pak pro ochranu osobních údajů v duchu Obecného nařízení či alespoň v duchu předchozí směrnice 95/45/ES.[302] Jak představují podrobně ve svém příspěvku *Schwartz* a *Peifer*,[303] teoretický koncept soukromí v americkém právu

297 Srov. HAY, Peter. *Law of the United States*. 2. München: C. H. Beck, 2005, s. 7.

298 Ibid., s. 8–9.

299 Ibid., s. 9; Orientace v prostředí amerických státních soudních rozhodnutí z pozice vně Spojených států je možná především díky jejich dostupnosti v databázi *Google Scholar*. Srov. STANLEY, Tim. Free US Case Law from Google! – US Federal + 50 State Case Law. *Justia Law Blog* [online]. 17. 11. 2009 [cit. 3. 3. 2021]. Dostupné z: https://lawblog.justia.com/2009/11/17/free-us-case-law-from-google-us-federal-50-state-case-law/

300 Jedná se o náhradu újmy s účelem potrestat žalovaného a odradit ostatní od postihovaného jednání. Oproti běžně pojímané náhradě újmy je zde výše stanovena v návaznosti na finanční sílu žalovaného, nikoliv způsobenou újmu. Srov. HAY, Peter. *Law of the United States*. 2. München: C. H. Beck, 2005, s. 69 a 174–175.

301 Ibid., s. 78–79.

302 Srov. RAUL, Charles Alan a Sidley AUSTIN (eds.). *Chambers Global Practice Guide: Data Protection & Cyber Security 2019*. Glasgow: Chambers & Partners, 2018, s. 359.

303 Viz SCHWARTZ, Paul M. a Karl-Nikolaus PEIFER. Transatlantic Data Privacy Law. *The Georgetown Law Journal*, 2017, č. 106, s. 116.

se ve významných aspektech odlišuje od jeho pojetí v evropském kontextu. Z pohledu amerického práva lze soukromí přiblížit k aktivu, které je jednotlivcem vnímáno z pozice spotřebitele v prostředí svobodného a otevřeného trhu[304] a ochrana soukromí tak primárně směřuje ke spravedlivým podmínkám pro jeho volbu v tomto pojetí.[305] Tato hluboce zakořeněná perspektiva ochrany spotřebitele a svobodného tržního rozhodování je pak v kontrastu s pojetím soukromí jako přirozené lidské hodnoty a základního práva na informační sebeurčení.[306]

V návaznosti na tento rozdíl v přiřazení hodnoty se dostupné právní nástroje ochrany údajů o jednotlivci ve Spojených státech úzce váží na jeho ochranu jako spotřebitele. Jejich jádrem je ochrana proti nekalým tržním praktikám *(unfair trade law)* a dozorová činnost Federální obchodní komise (*Federal Trade Commission*, FTC) při výkladu a postihování zakázaných nekalých a klamných jednání nebo praktik (*unfair and deceptive acts or practices,* UDAP).[307] Přes nepřímou vazbu extenzivního výkladu této pravomoci vystupuje FTC jako *de facto* regulátor problematiky ochrany soukromí a bezpečnosti dat,[308] což zahrnuje i (pro tuto monografii relevantní) oznamovací a ohlašovací povinnosti ohledně případů porušení bezpečnosti zpracovávaných údajů. K ranému zakotvení pravidel pro oznamování případů porušení bezpečnosti v americkém právu zřejmě dopomohla právě představená úzká vazba na ochranu spotřebitele.

Užití informací na základě těchto oznámení je tudíž bráno mnohem individuálněji, jak bude představeno v následujícím rozboru příslušných úprav, kdy notifikace primárně směřují k dotčeným jednotlivcům, spíše než k dozorovému úřadu. I zde lze vnímat kontrast k pojetí v EU, které je silněji zaměřeno na celkové vytvoření prostředí s vysokou úrovní ochrany osobních údajů založeného na zásadách a nalézání proporcionality, které je včleněno

304 Zde je nutno upozornit, že autoři užívají pojmu spotřebitel s akcentem na volnější americké užití tohoto pojmu, nikoliv poměrně jasně vymezené pojetí na základě harmonizované unijní úpravy. Tu však v příspěvku berou na vědomí a poukazují na přesahy amerického vnímání, které umožňují konstruovat ochranu soukromí jako jednu z rovin ochrany spotřebitele.

305 Ibid., s. 121.

306 Ibid., s. 123.

307 Srov. HAY, Peter. *Law of the United States*. 2. München: C. H. Beck, 2005, s. 278.

308 Viz RAUL, Charles Alan a Sidley AUSTIN (eds.). *Chambers Global Practice Guide: Data Protection & Cyber Security 2019*. Glasgow: Chambers & Partners, 2018, s. 359.

do rozhodovací praxe podniků formou zohledňování zájmů a perspektivy subjektů údajů při všech podnikatelských činnostech.[309]

I při přijetí těchto širších odlišností však zůstává značný koncepční překryv mezi účely, zaměřením a nástroji ochrany údajů o jednotlivci v právu Spojených států a unijním rámcem ochrany osobních údajů; a to dle mého názoru zvláště z hlediska povinností spojených s případy porušení bezpečnosti.

3.3.3 Struktura úpravy v právu států Spojených států amerických

Rámec povinností spojených s porušením bezpečnosti v právu Spojených států lze označit jako kombinaci obecně aplikovatelných předpisů na státní úrovni a specificky zaměřené federální úpravy pro rizikové kontexty finančního a zdravotního sektoru s charakteristickým zpracováním rozsáhlých databází citlivých údajů.

Bylo to původně ve finančním sektoru, kde skrze autorizaci dozorového orgánu k širším pravomocem ve vztahu k dodržování ochrany údajů o jednotlivcích na základě *Gramm-Leach-Bliley Act* z roku 1999[310] vznikl koncept oznamovací povinnosti vůči dotčeným osobám v případě porušení bezpečnosti zpracovávaných údajů za účelem snížení vzniklé či hrozící újmy.

Avšak první výslovnou právní úpravou obsahující oznamovací a ohlašovací povinnost pro případy porušení bezpečnosti obsahoval až kalifornský státní předpis *California Senate Bill 1386* z roku 2002.[311] Tato právní úprava byla reakcí na stále citelnější dopady porušení bezpečnosti zpracovávaných údajů a rostoucí potřebu poskytnout dotčeným jednotlivcům přiměřené mechanismy včasného varování, které by snížily riziko krádeže identity a dalších negativních důsledků.

---

309 Srov. EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock* [online]. COM(2019) 374 final. Brussels: EU, 2019, s. 1 [cit. 3. 3. 2021].

310 Zde užitý pojem *„nonpublic personal information"* je vymezen jako finanční informace o klientovi, které jím byly poskytnuty, vznikly v důsledku transakce či poskytnutí služby či byly jinak získány finanční institucí. Srov. Gramm–Leach–Bliley Act of 1999, Public Law 106–102, 113 Stat. 1338, section 509(4)(A).

311 Srov. An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. *California legislative information* [online]. 26. 9. 2002 [cit. 13. 7. 2020].

Od přijetí státního předpisu v Kalifornii přijalo i zbývajících 49 států srovnatelnou státní úpravu.[312] Ačkoliv se tato úprava projevila natolik potřebnou, že ji nyní nalezneme ve všech státech federace, doposud nebyla úspěšně přijata jednotná federální úprava. Došlo přitom ke značnému počtu návrhů takové úpravy, jak bude popsáno v oddílu 3.3.5. Jedná se tak o systém povinností, který má podobný, ale nesjednocený obsah na úrovni mezi státy, což vede ke značnému zatížení povinných subjektů působících napříč Spojenými státy.

Definice pojmu porušení bezpečnosti zpracovávaných údajů: Ve Spojených státech je absence jednotné definice pojmu zjevným důsledkem fragmentovaného zakotvení povinností na úrovni jednotlivých států federace.[313] *Murray* poukazuje na rozdílnost v definici pojmu napříč státními jurisdikcemi na příkladu srovnání úpravy v právních předpisech státu Michigan a státu Ohio. V obou případech je jádrem definice neoprávněný přístup a získání údajů o jednotlivci v důsledku porušení jejich bezpečnosti a důvěrnosti. Avšak v zákonné úpravě státu Ohio je dále vyžadováno pro vznik povinnosti rozumné očekávání, že tento přístup k údajům způsobil, či způsobí majetkovou újmu *(material risk of harm)*.[314]

Za nejvíce směrodatné vymezení pojmu pro americké prostředí považuji to obsažené ve výše zmíněném kalifornském předpise *California Senate Bill 1386*, který posloužil jako vzor pro řadu později přijatých státních předpisů. To zní: *„Porušení bezpečnosti systému představuje neoprávněné získání počítačových dat, které narušuje bezpečnost, důvěrnost nebo integritu osobních informací uchovávaných příslušnou osobou nebo podnikem."*[315] Výjimka z vymezeného okruhu jevů je následně dána pro *„získání osobních informací zaměstnancem nebo zástupcem osoby nebo podniku za účelem stanoveným touto osobou nebo podnikem* […]*, pokud osobní informace nebudou užity k nebo vystaveny dalšímu neoprávněnému šíření"*.[316] Předpis

312 Viz BOASIAKO, Kwabena Antwi a Michael O'CONNOR KEEFE. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. *SSRN Electronic Journal* [online]. 2018, s. 1–2 [cit. 5. 9. 2021].

313 Srov. MURRAY, Tanya. How to Slay the Hydra: Adopting Charles Ann Wright's the Law of Remedies as a Social Institution as a Framework for Preventing Data Breaches. *University of Detroit Mercyla Review*, 2017, č. 94, s. 136.

314 Ibid., s. 130.

315 *„A ‚breach of the security of the system' is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."* Srov. California Civil Code, 2017, section 1798.82 (g).

316 *„Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business* […]*, provided that the personal information is not used or subject to further unauthorized disclosure."* Srov. California Civil Code, 2017, section 1798.82 (g).

státu Kalifornie neobsahuje pro vznik povinnosti podmínku rozumně očekávatelné újmy (*risk of harm*), tak jako ve výše zmíněné úpravě státu Ohio či části dalších států.[317] Dalším častým omezením relevantních jevů je vztažení pojmu pouze na neoprávněné získání nezašifrovaných počítačových záznamů, či zašifrovaných se současným zpřístupněním šifrovacího klíče.[318]

V průběhu uplynulého desetiletí byl negativní dopad fragmentace úpravy povinností souvisejících s porušením bezpečnosti na úrovni státních předpisů vnímán i federálním normotvůrcem, což vedlo k několika snahám o jednotnou federální úpravu s významnou veřejnou podporou. Za nejvýznamnější pokus lze považovat vládní návrh prezidenta *Obamy* na jednotný americký standard pro notifikační povinnosti při porušení bezpečnosti v rámci *Personal Data Notification and Protection Act* z roku 2015.[319] Zde byla přitom obsažena definice porušení bezpečnosti založená na kalifornském státním předpise.[320] Doposud však snahy o jednotnou úpravu na federální úrovni nebyly úspěšné, což zanechává vymezení pojmu v americkém právu roztříštěné.

Kalifornský státní předpis: *California Senate Bill 1386* byl navržen *Simitianem* (členem *California State Assembly*) a *Peacem* (kalifornským senátorem) dne 12. února 2002.[321] Byla to především reakce na porušení bezpečnosti zpracovávaných údajů ve *Stephen P. Teale Data Center*, které bylo zmíněno

317 Srov. např. Maine Revised Statute Title 10 Chapter 210-B, 2009, section 1348 (1); Louisiana Revised Statute 51, 2011, section 3074 (G); Kansas Statute, 2006, section 50 – 7a02 (a); Iowa Statute Title 16 Chapter 715C, 2017, section 2 (6); Florida Statute Chapter 501, 2014, section 501.171(4)(c).

318 Příkladem viz Kentucky Revised Statute Chapter 365, 2014, section 365.732 (1) (a); Rhode Island General Laws Title 11, 2012, section 49.2-5 (b); Tennessee Code Title 47, 2010, section 2107 (a) (1).

319 Srov. COVINGTON & BURLING LLP. Analysis of White House Data Breach Notification Bill. *The National Law Review* [online]. 15. květen 2015 [cit. 14. 7. 2021]. Dostupné z: https://www.natlawreview.com/article/analysis-white-house-data-breach-notification-bill

320 Příslušná definice měla následující znění: *„Compromise of computerized data that results in or may be reasonably concluded to have resulted in an unauthorized acquisition of sensitive personally identifiable information or access to sensitive personally identifiable information that is for an unauthorized purpose or in excess of authorization."* Srov. LANGEVIN, Jim. Langevin Reintroduces the Personal Data Notification and Protection Act. *Congressman Jim Langevin* [online]. [cit. 24. 5. 2021]. Dostupné z: https://langevin.house.gov/press-release/langevin-reintroduces-personal-data-notification-and-protection-act

321 Srov. An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. *California legislative information* [online]. 26. 9. 2002 [cit. 13. 7. 2020].

již v druhé kapitole. Došlo při něm k ohrožení údajů osobního charakteru 265 000 zaměstnanců státu Kalifornie.[322] Tento právní předpis nabyl účinnosti dne 1. července 2003 jako změna *California Civil Code* ve složkách § 56.06, 1785.11.2, 1798.29 a 1798.82.

Pokroková podoba tohoto předpisu z něj vytvořila model pro řadu dalších obdobných úprav zavádějících oznamovací povinnost pro případy porušení bezpečnosti zpracovávaných údajů v dalších státech Spojených států. Uplatní se na porušení bezpečnosti údajů o jednotlivci s výjimkou takových, které jsou legálně dostupné z veřejných úředních záznamů.[323] Údaje o jednotlivci jsou přitom vymezeny buďto jako nezašifrovaná kombinace jména a uvedených citlivých údajů (jde především o číslo sociálního pojištění,[324] číslo řidičského průkazu, číslo účtu, přístupové heslo k internetovému bankovnictví, zdravotní údaje či údaje o zdravotním pojištění) nebo jako přístupové údaje k online účtu (tedy přístupové jméno a heslo).[325] Tento rozsah je relativně široký i z perspektivy vymezení osobních údajů v EU. Pojem porušení bezpečnosti, který byl zmíněn již výše, je vymezen jako neoprávněné získání počítačových dat, které narušuje bezpečnost, důvěrnost nebo integritu údajů o jednotlivci.[326] Povinné subjekty lze přirovnat k rolím správce a zpracovatele z prostředí unijní úpravy na ochranu osobních údajů. Oznamovací a ohlašovací povinnost[327] se vztahuje na osobu či podnik, který podniká ve státě Kalifornie a vlastní či má licenci ke zpracování počítačových dat *(computerized data)*, která obsahují údaje o jednotlivci.[328] Osoba či podnik spravující tato data pak má povinnost bezodkladně informovat výše uvedenou osobu či podnik o odhaleném porušení bezpečnosti zpracovávaných údajů.[329]

322 Srov. SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC. *Security Breach Notification Laws: Views from Chief Security Officers* [online]. Berkeley: University of California-Berkeley School of Law, 2007, s. 8 [cit. 12. 7. 2021].

323 Srov. California Civil Code, 2017, section 1798.80 (e).

324 Jedná se o devítimístné číslo, které provazuje jednotlivce se systémem sociálního zabezpečení. Blíže viz SOCIAL SECURITY ADMINISTRATION. Social Security Number and Card. *Social Security* [online]. 2020 [cit. 14. 7. 2021]. Dostupné z: https://www.ssa.gov/ssnumber/

325 Srov. California Civil Code, 2017, section 1798.82 (h).

326 Viz California Civil Code, 2017, section 1798.82 (g).

327 Ve smyslu oznamovací povinnosti vůči dotčeným jednotlivcům a ohlašovací povinnosti vůči regulatornímu orgánu.

328 Viz California Civil Code, 2017, section 1798.82 (a).

329 Viz California Civil Code, 2017, section 1798.82 (b).

Výjimka se uplatní na subjekty, na které dopadá specifická federální úprava, tedy především na poskytovatele zdravotních služeb a finanční instituce.[330]

Podmínkou pro vznik povinnosti oznámení porušení bezpečnosti dotčeným obyvatelům státu Kalifornie je rozumné očekávání, že byly nezašifrované údaje o jednotlivci získány neoprávněnou osobou.[331] Případně vzniká též povinnost ohlášení porušení bezpečnosti, pokud se dotýká více než 500 obyvatel státu, přičemž formát by měl odpovídat vzorovému oznámení dotčeným fyzickým osobám.[332] Příjemcem ohlášení je *California Attorney General*, který pro tyto účely zřídil zvláštní oddělení *Privacy Enforcement & Protection Unit*, nahrazující dřívější samostatně stojící *California Office of Privacy Protection*.[333]

Z uvedené struktury podmínek je zjevné, že oproti výše představené úpravy dle Obecného nařízení je prioritou dané úpravy oznámení případu porušení bezpečnosti dotčeným jednotlivcům[334] před sdílením informací s regulátorem.[335] To je bezpochyby odraz již zmíněného odlišného přístupu k ochraně soukromí jednotlivce v americkém prostředí.

Oznámení má být učiněno v nejkratší možné lhůtě *(in the most expedient time)* po odhalení porušení bezpečnosti.[336] Dříve dostupné oficiální doporučení stanovilo, že by tato lhůta neměla překročit 10 pracovních dní.[337] Právní předpis nadto výslovně poskytuje výjimky v případě legitimních důvodů opožděné notifikace na základě požadavků orgánů činných v trestním řízení a nezapočítává do běžící lhůty čas potřebný na nezbytná opatření pro stanovení rozsahu daného incidentu a obnovu přiměřené integrity dotčených systémů a dat.[338] Úprava připouští další výjimky pro podniky, které mají specifické procesy pro oznamování a ohlašování zakotvené v rámci politik informační bezpečnosti

330 Viz California Civil Code, 2017, section 1798.82 (e).
331 Viz California Civil Code, 2017, section 1798.82 (a).
332 Viz California Civil Code, 2017, section 1798.82 (f).
333 Viz OFFICE OF THE ATTORNEY GENERAL. Privacy Enforcement and Protection. *State of California Department of Justice* [online]. 11. říjen 2012 [cit. 24. 5. 2021]. Dostupné z: https://www.oag.ca.gov/privacy
334 Tedy účel úpravy směřující k prevenci vzniku či navýšení hrozící újmy.
335 Tedy zajištění dodržování jiných povinností skrze nástroje chytré regulace za účelem dosahování celkové úrovně ochrany údajů o fyzických osobách.
336 Viz California Civil Code, 2017, section 1798.82 (a).
337 Srov. CALIFORNIA OFFICE OF PRIVACY PROTECTION. *Recommended Practices on Notice of Security Breach Involving Personal Information* [online]. Sacramento, CA: California Office of Privacy Protection. 2012 [cit. 24. 5. 2021].
338 Viz California Civil Code, 2017, section 1798.82 (a).

(customized notification procedures as part of information security policy).[339] Podnikům porušujících příslušné povinnosti hrozí sankce omezením činnosti[340] a vystavují se (hromadným) soukromoprávním žalobám dotčených fyzických osob.[341] Této odpovědnosti se daný subjekt nemůže zřeknout *(waiver)*.[342]

Hlavní společné či odlišující prvky předpisů v dalších státních jurisdikcích: Jak bylo naznačeno výše, rozsah pojmu údaje o jednotlivci se liší napříč právními úpravami. Pro všechny je však přinejmenším společné, že je zahrnuta kombinace jména jednotlivce a nezašifrovaný údaj o čísle sociálního pojištění, čísle řidičského průkazu či čísle státního identifikačního průkazu. Dále se pojem vztahuje na finanční informace jako jsou číslo účtu či číslo kreditní karty společně s příslušným přístupovým kódem či heslem. Nadto řada státních předpisů rozšiřuje okruh relevantních údajů o další citlivé údaje. Například předpis ve státě Wisconsin[343] dopadá i na DNA profil či biometrická data; ve státě Severní Dakota[344] je pak výslovně začleněn elektronický podpis, datum narození a dokonce jméno občanovy matky za svobodna; úprava ve státě Florida[345] se uplatňuje také na uživatelské jméno nebo e-mailovou adresu v kombinaci s heslem či odpovědí na bezpečnostní otázku pro personalizované online účty; předpis ve Wyomingu[346] pak dopadá také na sdílené důvěrné informace *(shared secrets)* a bezpečnostní tokeny užívané pro autentizaci na základě dat.

Většina relevantních státních předpisů dopadá pouze na porušení bezpečnosti údajů zpracovávaných elektronicky. Výjimkou jsou předpisy ve státech Washington,[347] Aljaška,[348] Wisconsin,[349] Iowa,[350] Indiana,[351] Massachusetts,[352] Severní Karolína[353] a Havaj.[354]

339 Viz California Civil Code, 2017, section 1798.82 (k).
340 Viz California Civil Code, 2017, section 1798.84 (e).
341 Viz California Civil Code, 2017, section 1798.84 (b).
342 Viz California Civil Code, 2017, section 1798.84 (a).
343 Viz Wisconsin Statutes Chapter 134, 2007, section 134.98.
344 Viz North Dakota Century Code, 2017, section 51-30-01 a násl.
345 Viz Florida Statute Chapter 501, 2014, section 501.171.
346 Viz Wyoming Statues Title 40 Chapter 12, 2018, section 501-502.
347 Viz Washington Statute Title 19 Chapter 255, 2015, section 010-020.
348 Viz Alaska Statute Title 45 Chapter 48, 2018, section 010.
349 Viz Wisconsin Statutes Chapter 134, 2007, section 98.
350 Viz Iowa Statute Title 16 Chapter 715C, 2017, section 1 and 2.
351 Viz Indiana Code Title 24 Article 4.9, 2017, section 1 a násl.
352 Viz Massachusetts General Law Part I Title XV Chapter 93H, 2019, section 1-6.
353 Viz North Carolina Statute, 2015, section 75-61 and 75-65.
354 Viz Hawaii Revised Statute, 2019, section 487N-1 a násl.

Základní vymezení pojmu porušení bezpečnosti vychází z kalifornské definice. Jádrem je neoprávněné nabytí dat od jiného subjektu, které vede k porušení bezpečnosti, důvěrnosti nebo integrity obsažených údajů o jednotlivci, s výjimkou určitých případů nabytí v dobré víře. Lze nalézt jisté odlišnosti, např. předpis státu Ohio, který nezmiňuje případy narušení integrity,[355] či floridská úprava, která si vystačí se zjednodušenou definicí: *„neoprávněného přístupu k datům v elektronické podobě obsahující osobní informace"*.[356] Hlavní rozdíl vymezení pojmu napříč Spojenými státy se týká podmíněností vzniku oznamovací povinnosti očekávatelnou újmy *(risk of harm)*. Podobně jako v Kalifornii tato podmínka není založena v předpisech Nevady,[357] Texasu,[358] Georgie,[359] New Yorku[360] a několika dalších státních jurisdikcích. Většina ostatních států, např. Ohio, Florida, Wyoming nebo Iowa, oproti tomu vyžadují pro vznik povinností překročení jistého prahu závažnosti, zpravidla v podobě rozumně očekávatelné újmy. Úpravy se nadto mírně liší ve významu (bezpečného) šifrování dat a možnosti výjimky z oznamovací a ohlašovací povinnosti v případě přijetí přiměřených reaktivních opatření, většina však odpovídá koncepci státního předpisu Kalifornie.

Odlišnosti mezi úpravami lze vnímat u stanovení příjemců oznámení. Několik státních předpisů, mezi nimi ty v Idaho,[361] Utahu,[362] či Mississippi,[363] omezují povinnost na oznámení případu dotčeným jednotlivcům. Jinak je však běžné, že je alespoň pro významná porušení bezpečnosti stanovena dodatečná ohlašovací povinnost. Některé nedávné úpravy relevantních předpisů pak tuto povinnost dodatečně zavedly, jako např. ve státě Arizona.[364] Nejčastějším příjemcem ohlášení je státní *Attorney General*, podobně jako je tomu v Kalifornii. Ve státě Puerto Rico mají být případy porušení bezpečnosti ohlašovány jen

355 Viz Ohio Revised Code Title 13 Chapter 1349, 2007, section 1349.19 (A) (1) (a).

356 *„Unauthorized access of data in electronic form containing personal information."* Srov. Florida Statute Chapter 501, 2014, section 501.171 (1) (a).

357 Viz Nevada Revised Statute Chapter 603A, 2017, section 010 a násl.

358 Viz Texas Business and Commerce Code Chapter 521, 2009, section 002, 053 a 151.

359 Viz Code of Georgia Title 10 Chapter 1, 2019, section 910 a násl.

360 Viz The Laws of New York General Business Article 39-F, 2019, section 899-AA.

361 Viz Idaho Statute Title 28 Chapter 51, 2014, section 104 a násl.

362 Viz Utah Code Title 13 Chapter 44, 2010, section 101 a násl.

363 Viz Mississippi Code Title 75 Chapter 24, 2019, section 29.

364 Srov. ARIZONA ATTORNEY GENERAL. New Arizona Law to Protect Data Breach Victims. *Arizona Attorney General Mark Brnovich* [online]. 2019 [cit. 24. 5. 2021]. Dostupné z: https://www.azag.gov/press-release/new-arizona-law-protect-data-breach-victims

místnímu *Department of Consumer Affairs*,[365] zatímco ve státě Arkansas se ohlašovací povinnost vztahuje pouze na některé povinné subjekty, a to jen vůči *Securities Commissioner*, resp. *Insurance Commissioner*.[366] Jinde je povinnost ohlášení vůči státní agentuře zastupující spotřebitele *(state consumer representation agency)*, tak tomu je ve státech Kansas[367] a Pensylvánie[368] při porušení bezpečnosti dotýkajících se více než 1 000 obyvatel státu, nebo ve státech Texas[369] a Georgie,[370] pokud jich je dotčeno více než 10 000. V dosud nezmíněných státech je pak zásadně založena ohlašovací povinnost jak vůči státnímu *Attorney General*, tak státní agentuře zastupující spotřebitele. Příkladem lze zmínit Floridu,[371] Severní Karolínu,[372] Maine,[373] či Montanu.[374]

Lhůta pro oznámení je zásadně stanovena bez zbytečného odkladu, některé státní předpisy pak podobně jako článek 33 Obecného nařízení vymezují maximální lhůtu pro posílení ochrany poskytované dotčeným fyzickým osobám. Zde je však nutné uvést, že jde o významně delší lhůty než v unijním kontextu. Ve státě Delaware je tak oznámení vyžadováno ve lhůtě maximálně 60 dnů od odhalení porušení bezpečnosti,[375] v Ohiu,[376] Washingtonu[377] a Oregonu[378] pak 45 dnů a na Floridě (kde je tato pevná lhůta stanovena nejkratší) stále celých 30 dnů.[379]

Založení soukromoprávních nároků na náhradu způsobené újmy je nosný prvek těchto norem v americkém kontextu, což dále souvisí s notně etablovaným rámcem pro skupinové žaloby. Většina předpisů pak obsahuje možnost dodatečných sankcí vyplývajících z jiných státních předpisů. Ve vlastní úpravě vztahující se k porušení bezpečnosti jsou sankce vymezeny ve státě Havaj,

365 Viz Laws of Puerto Rico Title TEN, 2019, section 4051-4055.
366 Viz Arkansas Code Title 4 Chapter 110, 2019, section 101 a násl.
367 Viz Kansas Statute, 2006, section 50-7a01-04.
368 Viz Pennsylvania Statutes Title 73 Chapter 43, 2006, section 2301-2308 a 2329.
369 Viz Texas Business and Commerce Code Chapter 521, 2009, section 002, 053 a 151.
370 Viz Code of Georgia Title 10 Chapter 1, 2019, section 910 a násl.
371 Viz Florida Statute Chapter 501, 2014, section 171.
372 Viz North Carolina Statute, 2015, section 75-61 a 75-65.
373 Viz Maine Revised Statute Title 10 Chapter 210-B, 2009, section 1346-1350-B.
374 Viz Montana Code Title 30 Chapter 14 Part 17, 2017, section 1704 a 1705.
375 Viz Delaware Code Title 6 Chapter 12B, 2017, section 101 a násl.
376 Viz Ohio Revised Code Title 13 Chapter 1349, 2007, section 19, 191 a 192.
377 Viz Washington Statute Title 19 Chapter 255, 2015, section 010-020.
378 Viz Oregon Revised Statute Chapter 646A, 2018, section 600-604 a 624-626.
379 Viz Florida Statute Chapter 501, 2014, section 171.

kde je zakotvena správní sankce 2 500 USD za porušení,[380] a ve státě Texas, kde povinnému subjektu hrozí správní sankce v rozmezí 2 000 až 50 000 USD za porušení.[381] V floridském státním předpise je pak vymezena správní sankce za dlouhodobější neplnění těchto povinností.[382] Předpis ve státě Washington výslovně stanoví, že nedodržení oznamovací či ohlašovací povinnosti představuje nekalé a klamné jednání *(unfair and deceptive act in trade or commerce or unfair method of competition)* v intencích právní úpravy na ochranu spotřebitele.[383]

3.3.4 Judikatura a činnost státních Attorney General ve vztahu k porušením bezpečnosti

V americké právní tradici je dominantní role při výkladu a aplikaci práva pro společenský kontext přenechána precedentní judikatuře. Porušení bezpečnosti má zpravidla negativní dopad na dotčené jednotlivce a zakládá tak právní nárok na náhradu újmy jako podklad pro žalobu či skupinovou žalobu. Soukromoprávní spory jsou etablovaným prvkem amerického právního systému. Ovšem vzhledem k fragmentované povaze právní úpravy vztahující se k porušení bezpečnosti a ochraně údajů o jednotlivci je možný podklad pro tyto spory značně nejednotný. Právní doložení nároků, na kterých je daný spor založen je tudíž různorodé, sahající od porušení smlouvy, přes porušení péče, poskytnutí nesprávných informací *(misrepresentation)*, porušení dobré víry či porušení záruky po specifické nároky na náhradu újmy vyplývající ze státních či federálních předpisů.[384]

Toto odráží nejen vlastní různorodost případů porušení bezpečnosti nastíněnou v rámci druhé kapitoly, ale též obtížnost zachycení toho jevu v rámci existujícího rámce amerického procesního práva. To je dále podloženo vývojem judikatury ohledně hlavních aspektů předmětných sporů, především požadavků kladených na doložení očekávatelné újmy v důsledku porušení bezpečnosti. Soudy jsou v tomto směru značně nejednotné a donedávna

380 Viz Hawaii Revised Statute, 2019, section 487N-1 a násl.
381 Viz Texas Business and Commerce Code Chapter 521, 2009, section 002, 053 a 151.
382 Viz Florida Statute Chapter 501, 2014, section 171.
383 Viz Washington Statute Title 19 Chapter 255, 2015, section 010-020.
384 Srov. ROMANOSKY, Sasha, David HOFFMAN a Alessandro ACQUISTI. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, 2014, roč. 11, č. 1, s. 25.

upřednostňovaly odmítnutí existence této újmy *(dismissal of harm recognition)* v případech, kdy nebyla doložena skutečná újma *(injury in fact)*.[385] Tato obtížnost doložení újmy porušení bezpečnosti v soukromoprávních sporech má v americkém právu významné důsledky.

Jelikož skupinové žaloby jsou bez ohledu na základ nároku ve státním předpise zpravidla předkládány federálním soudům v souladu s *Class Action Fairness Act,*[386] vede selhání při stanovení újmy *(failure to establish harm)* dle příslušných procesních pravidel ke ztrátě žalobní legitimace *(loss of standing)* a odmítnutí žaloby.[387]

Pokud žalobce v soukromoprávním sporu neprokáže újmu, nemůže soud rozhodnout v jeho prospěch.[388] Rozhodnutí SC USA v roce 2013 ve věci *Clapper proti Amnesty International* vedlo k rozsáhlému odmítání žalob na újmu v důsledku porušení bezpečnosti na základě absence prokazatelné újmy.[389] Porušení bezpečnosti jako takové zpravidla nevede k jednoznačně vyčíslitelné újmě jako důsledku zneužití získaných údajů o jednotlivci. Nemožnost založit žalobní nárok na zvýšeném riziku možné újmy v důsledku porušení bezpečnosti nebo pociťované nejistotě v důsledku zvýšeného rizika pro jejich virtuální aktiva a identity tak efektivně vyřazuje skupinové žaloby z funkčních nástrojů.

Tento vývoj dokumentují empirická data shromážděná ve studii *Romanosky a kol.* z roku 2014,[390] kde bylo sledováno 230 žalob týkajících se porušení bezpečnosti a zjištěno, že ve všech případech vyjma dvou byl spor ukončen před soudním přelíčením, a to buďto na základě odmítnutí soudem nebo mimosoudním smírem *(settlement)*.[391] Význam mimosoudních smírů v rámci kompenzace újmy způsobené rozsáhlými porušeními bezpečnosti lze doložit odkazem na smír v celkovém objemu 50 milionů USD ze strany společnosti

385 Srov. SOLOVE, Daniel J. a Danielle Keats CITRON. Risk and Anxiety: A Theory of Data Breach Harms. *Texas Law Review*, 2016, roč. 2018, č. 96, s. 737.
386 Viz Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) (2012).
387 SOLOVE, Daniel J. a Danielle Keats CITRON. Risk and Anxiety: A Theory of Data Breach Harms. *Texas Law Review*, 2016, roč. 2018, č. 96, s. 750.
388 Ibid., s. 747.
389 Ibid., s. 741; Rozhodnutí SC USA ve věci *Clapper proti Amnesty International*, 568 U.S. 398 (2013).
390 Srov. ROMANOSKY, Sasha, David HOFFMAN a Alessandro ACQUISTI. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, 2014, roč. 11, č. 1.
391 Ibid., s. 92.

Yahoo za porušení bezpečnosti v roce 2014[392] či 115 milionů USD ze strany společnosti *Anthem* za případ z roku 2015.[393]

Rozhodnutím SC USA ve věci *Spokeo, Inc. proti Robins*[394] z roku 2016 přitom vznikl určitý prostor pro úspěch nároků týkajících se porušení bezpečnosti, jelikož bylo připuštěno, že zvýšené riziko nemajetkové újmy zakládá procesně přípustnou podobu újmy *(permissible form of harm)*.[395] Nebylo tím však dáno jednoznačné vodítko pro řešení případů týkajících se nároků z porušení bezpečnosti a judikatura zůstává nejednotná.[396] I proto přetrvávala v roce 2018 žalobní legitimace *(standing)* u federálních soudů jako klíčová výzva pro spory týkající se předmětné oblasti a mimosoudní smír jako častý úkaz.[397]

Ve vztahu k nejzásadnějším případům porušení bezpečnosti tak připadla role pro zajištění kompenzace dotčeným fyzickým osobám především státním *Attorney General*. Tak tomu bylo v případě smíru v objemu 18,5 milionu USD ohledně porušení bezpečnosti společnosti *Target* v roce 2013,[398] v objemu 148 milionů USD ohledně případu společnosti *Uber* z roku 2016, či doposud rekordního smíru v celkovém objemu 600 milionů USD za velmi rozsáhlý a kritický případ porušení bezpečnosti u společnosti *Equifax* v roce 2017.[399]

Tento vývoj naznačuje, že přes upřednostňované oznamování informací o případech porušení bezpečnosti dotčeným jednotlivcům pro podporu jejich nároků v rámci skupinových žalob, se americký systém funkčně přibližuje unijnímu rámci ochrany osobních údajů, kde je prioritní ochrana zajišťována skrze aktivitu dozorových úřadů. Toto přitom platí ještě výrazněji pro následně představené sektorové úpravy na federální úrovni.

392 Yahoo! Inc. Customer Data Security Breach Litigation, No. 16-2752 (N.D. Cal.) 22. 10. 2018.
393 Anthem, Inc. Data Breach Litigation, No. 15-2617 (N.D. Cal.) 16. 8. 2018.
394 Rozhodnutí SC USA ve věci *Spokeo, Inc. proti Robins*, 136 S.Ct. 1540 (2016).
395 Srov. SOLOVE, Daniel J. a Danielle Keats CITRON. Risk and Anxiety: A Theory of Data Breach Harms. *Texas Law Review*, 2016, roč. 2018, č. 96, s. 744.
396 Např. rozhodnutí ve věcech Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018) a Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613 (4th Cir. 2018).
397 Srov. NEUBURGER, Jeffrey D. *Trends in Privacy and Data Security* [online]. Toronto: Thomson Reuters, 2019, s. 29 [cit. 4. 3. 2021].
398 Srov. ABRAMS, Rachel. Target to Pay $18.5 Million to 47 States in Security Breach Settlement. *The New York Times* [online]. 2017 [cit. 4. 3. 2021].
399 Srov. PRESS OFFICE. AG Shapiro Secures $ 600 Million from Equifax in Largest Data Breach Settlement in History. *Pennsylvania Office of Attorney General* [online]. 22. 7. 2019 [cit. 4. 3. 2021]. Dostupné z: https://www.attorneygeneral.gov/taking-action/press-releases/ag-shapiro-secures-600-million-from-equifax-in-largest-data-breach-settlement-in-history/

3.3.5 Federální úprava

Dvě hlavní oblasti, které mají v americkém právu pro tuto oblast specifickou federální úpravu, jsou finanční a zdravotní sektor.

Federální úprava pro finanční sektor: Základ pro ochranu údajů zpracovávaných finančními institucemi je k nalezení v *Gramm-Leach-Bliley Act*.[400] Podle *Section 501(a)* tohoto předpisu příslušná regulatorní autorita stanoví přiměřené standardy pro administrativní, technické a fyzické prvky bezpečnosti záznamů a údajů o zákaznících *(customer records or information)*, tak aby byly chráněny před neoprávněným přístupem nebo zneužitím, které by mohlo vyústit ve významnou újmu či nepohodlí některého ze zákazníků *(substantial harm or incovenience to any customer)*.

Tato úprava se vztahuje jak na banky, tak na nebankovní finanční subjekty. Skupina amerických agentur pro regulaci bankovního sektoru vydala v roce 2001 *Interagency Guidelines Establishing Information Security Standards*,[401] které zavazují americké banky k vytvoření programů informační bezpečnosti *(information security programs)* s přiměřenými reaktivními nástroji. Nezbytnou složkou těchto programů je pak také proces pro ohlášení porušení bezpečnosti primárnímu federálnímu regulátorovi příslušné banky bez zbytečného odkladu po odhalení případu, který dopadá na citlivé údaje o jednotlivcích,[402] jakožto i oznámení dotčeným zákazníkům v odůvodněných případech.[403] Ty jsou dále vymezeny jako situace, kdy banka zhodnotí výskyt nebo rozumnou pravděpodobnost zneužití těchto údajů. Pozdržení notifikace je přípustné na základě písemné žádosti příslušného orgánu činného v trestním řízení pro zabránění narušení probíhajícího vyšetřování.[404]

FTC vydala následně v roce 2002 standardy pro ochranu údajů o jednotlivcích pro nebankovní finanční subjekty.[405] Ty však neukládají těmto subjektům

400 Viz Gramm–Leach–Bliley Act of 1999, Public Law 106–102, 113, Stat. 1338.
401 Srov. CODE OF FEDERAL REGULATIONS. *12 CFR Appendix F to Part 225 – Interagency Guidelines Establishing Information Security Standards* [online]. 2012 [cit. 24. 5. 2021].
402 Ibid., s. 331–332.
403 Ibid., s. 331.
404 Ibid.
405 Srov. FEDERAL TRADE COMMISSION. *16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule* [online]. 2002, s. 36493 [cit. 24. 5. 2021].

výslovnou povinnost ohlašovat či oznamovat porušení bezpečnosti, ale pouze je včas odhalit a reagovat na ně efektivními opatřeními.

Federální úprava pro sektor zdravotních služeb: Zde byly příslušné povinnosti na federální úrovni zakotveny skrze změnu *Health Insurance Portability and Accountability Act* (HIPAA)[406] skrze *Health Information Technology for Economic and Clinical Health Act* (HITECH) v roce 2009, zvláště pak na základě *Section 13402*.[407] Tato úprava byla dále specifikována skrze předpis vydaný *Department of Health and Human Services* (HHS).[408] Zahrnuty jsou nezabezpečené chráněné zdravotní údaje o jednotlivci *(unsecured protected health information)*.[409]

Na pojem porušení bezpečnosti se v tomto předpise dále vztahuje řada výjimek, které zahrnují mimo jiné neúmyslný přístup v omezeném rozsahu či zveřejnění v dobré víře vůči neoprávněné osobě, u které je rozumně předpokládáno, že nebude schopna udržet takto sdělené informace.[410] Za porušení bezpečnosti dále není pokládána situace, kdy je nízká pravděpodobnost zásahu do dotčených chráněných zdravotních údajů o jednotlivci.[411] Oznámení dotčené fyzické osobě má proběhnout bez zbytečného odkladu po odhalení porušení bezpečnosti, nebo poté, co by při řádné péči bylo odhaleno,[412] nejpozději však do 60 dnů.[413] Pokud došlo k dotčení více než 500 obyvatel v daném státě, případ má být oznámen za pomoci významných médií ve srovnatelném časovém horizontu[414] a případ má být dále ohlášen HHS.

Základní údaje o případu porušení bezpečnosti jsou následně zveřejněny skrze *Breach Portal*, což dále přispívá k jejich transparentnosti a šíření příslušné

406 Viz 110 STAT. 1936 Public Law 104-191, Health Insurance Portability and Accountability, Act, 1996.
407 Viz 123 STAT. 226 Public Law 111-5, Health Information Technology for Economic and Clinical Health, Act, 2009.
408 Srov. DEPARTMENT OF HEALTH AND HUMAN SERVICES. *45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule* [online]. 2009, s. 42767 [cit. 24. 5. 2021].
409 Vymezení tohoto pojmu významně zužuje rozsah notifikační povinnosti. Ibid., s. 42768.
410 Příkladem může být pacient s poruchou paměti. Ibid., s. 427687, section 164.402(2).
411 Ibid.
412 Ibid., s. 427688, section 164.404(a).
413 Ibid., section 164.404(b).
414 Ibid., section 164.406.

informace.[415] Méně rozsáhlá porušení bezpečnosti mají být dokumentována a ohlášena pohromadě ke konci kalendářního roku.[416] Pokud je případ porušení bezpečnosti odhalen obchodním partnerem povinného subjektu *(business associate of the covered entity)*, vztahuje se na něj podobná ohlašovací povinnost vůči povinnému subjektu nejpozději do 60 dnů od chvíle, kdy byl při řádné péči daný incident odhalen.[417] Tato odvozená povinnost je srovnatelná úpravě povinností zpracovatele vůči správci v článku 33 Obecného nařízení.

Další specifické povinnosti pro oblast zdravotních služeb pak zakládá *Section 13407 HITECH*.[418] Povinnými subjekty jsou informační brokeři zpracovávající osobní zdravotní záznamy *(vendors of personal health records)* a přidružení poskytovatelé služeb *(third-party service providers)*, kteří nespadají pod působnost HHS. Ke specifikaci této úpravy došlo skrze navazující předpis FTC.[419] Pojetí porušení bezpečnosti je zde odlišné od výše představené úpravy pro subjekty spadající pod HIPAA. Okruh relevantních údajů zahrnuje nezabezpečené elektronické osobní zdravotní záznamy *(unsecured electronic personal health records)* obsahující identifikovatelné zdravotní údaje o jednotlivci *(identifiable health information)*. Dále je okruh dopadu omezen na nabytí těchto údajů bez svolení příslušného jedince.

Kromě těchto odlišností jde o srovnatelnou úpravu s výše představenou v působnosti HHS. Je založena oznamovací povinnost dotčeným osobám, jakož i ohlašovací povinnost vůči FTC, která předává informace o porušení bezpečnosti HHS.[420] Je vymezeno též oznámení rozsáhlejších případů porušení bezpečnosti skrze média srovnatelné s výše popsanou úpravou dle HIPAA. Ohlášení vůči FTC musí v takovém případě být provedeno do 10 pracovních dní.[421]

415 Srov. Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. *Breach Portal* [online]. [cit. 25. 5. 2021]. Dostupné z: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

416 Viz DEPARTMENT OF HEALTH AND HUMAN SERVICES. *45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule* [online]. 2009, s. 427688, section 164.408 [cit. 24. 5. 2021].

417 Ibid., s. 427689, section 164.410.

418 Viz 123 STAT. 226 Public Law 111-5 Health Information Technology for Economic and Clinical Health Act, 2009, s. 226.

419 Srov. FEDERAL TRADE COMMISSION. *16 CFR Part 318 Health Breach Notification Rule; Final Rule* [online]. 2009, s. 42980 [cit. 24. 5. 2021].

420 Ibid., section 318.3(a).

421 Ibid., s. 42981, section 318.5.

Činnost FTC ve vztahu k případům porušení bezpečnosti: Regulatorní role FTC je v kontextu porušení bezpečnosti významná, což je zřejmé již z působnosti nad subjekty zpracovávajícími údaje jednotlivců ve finančním i zdravotním sektoru. Kromě zmíněné přímé působnosti ji zakládá také působnost ve věcech nekalých a klamavých jednání nebo praktik (UDAP).[422] Tento podklad pro dozorovou činnost nad postupy oznamování porušení bezpečnosti byl však opakovaně napadán, jelikož vychází z extenzivního výkladu působnosti nad zásadami ochrany soukromí *(privacy policy)* a postihováním pochybení zavést či řádně provádět takové zásady v souladu s pravidly a standardy FTC.[423] Přesto je aktivita FTC v tomto směru značná, příkladem lze uvést případ porušení bezpečnosti *Wyndham Hotels and Resorts* v roce 2015,[424] případ *AshleyMadison.com* ve stejném roce [425] či případ *LightYear Dealer Technologies* z roku 2016.[426]

Ve výsledku činnost FTC doplňuje koordinované aktivity *Attorney General* a zakládá podklad pro vymáhání náhrad vzniklé újmy pro postižené jednotlivce v rámci ochrany proti porušení bezpečnosti skrze orgán dozoru.

Snahy o jednotnou federální úpravu: Potřeba jednotného přístupu k oznamovací a ohlašovací povinnosti porušení bezpečnosti je ve Spojených státech po dlouhou dobu uznávána a diskutována nejen odborníky na tuto oblast

422 Viz Wheeler-Lea Amendments of the Federal Trade Commission Act (1938), Public Law 75-447, 52 Stat. 1 to the 15 U.S.C. § 45 section 5.

423 Srov. INFORMATION RESELLERS: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace. *United States Government Accountability Office*. [online]. 2013, s. 11 [cit. 23. 4. 2021].

424 Srov. OFFICE OF PUBLIC AFFAIRS. Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk. *Federal Trade Commission* [online]. 9. 12. 2015 [cit. 4. 3. 2021]. Dostupné z: https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment

425 Srov. OFFICE OF PUBLIC AFFAIRS. Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information. *Federal Trade Commission* [online]. 14. 12. 2016 [cit. 4. 3. 2021]. Dostupné z: https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting

426 Srov. OFFICE OF PUBLIC AFFAIRS. FTC Gives Final Approval to Settlement with Auto Dealer Software Company That Allegedly Failed to Protect Consumers' Data. *Federal Trade Commission* [online]. 6. 9. 2019 [cit. 4. 3. 2021]. Dostupné z: https://www.ftc.gov/news-events/press-releases/2019/09/ftc-gives-final-approval-settlement-auto-dealer-software-companyy

práva, ale i v administrativních a politických kruzích.[427] Zvláště silný impuls byl dán rozsáhlým případem porušení bezpečnosti v roce 2013 u maloobchodního řetězce *Target*. V reakci na tuto událost mnoho vlivných hlasů vyzývalo ke sjednocení úpravy na federální úrovni. Mezi nimi byl i *U.S Attorney General*[428] nebo předsedkyně FTC.[429] Podporu pro tuto legislativu projevily i podnikatelské asociace.[430] V roce 2014 byla předložena řada návrhů právních předpisů *(bills)*, které měly přinést harmonizovanou úpravu problematiky.[431] Za nejvýznamnější snahu lze považovat návrh vlády prezidenta *Obamy* z roku 2015, který nesl označení *Personal Data Notification and Protection Act*.[432] Žádný z těchto návrhů však nedošel přijetí jako federální zákon.[433] Další série návrhů[434] přišla v reakci na rozsáhlý případ porušení bezpečnosti u společnosti *Equifax* v roce 2017.[435] Ani z těchto návrhů žádný v legislativním procesu neuspěl. Zatím poslední vlnu zájmu o jednotnou federální

427 Srov. JOERLING, Jill. Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data. *Washington University Journal of Law & Policy*, 2010, č. 32, s. 468–470.

428 Srov. Industry Backs Attorney General's Call for Federal Data-Breach Law. *AdAge* [online]. 25. 2. 2014 [cit. 24. 5. 2021]. Dostupné z: https://adage.com/article/privacy-and-regulation/industry-backs-ag-s-call-federal-data-breach-law/291865

429 Srov. RAMIREZ, Edith. *Prepared Statement of the Federal Trade Commission On Privacy In the Digital Age: Preventing Data Breaches and Combating Cybercrime* [online]. Washington D.C.: United States Senate, 2014 [cit. 24. 5. 2021].

430 Viz SASSO, Brendan. Business groups call for data breach law. *The Hill* [online]. 18. 12. 2013 [cit. 24. 5. 2021]. Dostupné z: https://thehill.com/policy/technology/312163-overnight-tech-business-groups-call-for-data-breach-law

431 Např. Bill for Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. (2014); Bill for Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014); či Bill for Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014).

432 Viz Bill for Personal Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. (2015–2016); SHEAR, Michael D. a Natasha SINGER. Obama to Call for Laws Covering Data Hacking and Student Privacy. *The New York Times* [online]. 2017 [cit. 24. 5. 2021].

433 Viz NEWMAN, Brett V. Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation. *Journal of Law, Technology and Policy*, 2015, roč. 2015.

434 Srov. BAUTISTA, Gregory, Jeremy T. MERKEL a Alex MOH. (Another) Federal Data Breach Notification Law Introduced in Congress. *The National Law Review* [online]. 18. 12. 2017 [cit. 24. 5. 2021]. Dostupné z: https://www.natlawreview.com/article/another-federal-data-breach-notification-law-introduced-congress

435 Viz KREBS, Brian. Equifax breach. *Krebs on Security* [online]. 10. 10. 2017 [cit. 24. 5. 2021]. Dostupné z: https://krebsonsecurity.com/tag/equifax-breach/page/2/

úpravu vyvolal na jaře 2018[436] skandál společnosti *Facebook* ve věci *Cambridge Analytica*.[437] Zájem o toto téma také posilovala diskuse ohledně unijního Obecného nařízení, které mělo dopad na činnost řady mezinárodně působících podnikatelských subjektů ze Spojených států.[438]

Jak vyplývá z nedávných diskusí mezi zástupci spotřebitelů a představiteli podnikatelské sféry, společná podpora federální úpravy naráží nepřekvapivě především na odlišné představy o jejím obsahu, nikoliv její potřebě. První skupina volá po robustních nástrojích na ochranu jednotlivců a přesunu břímě této problematiky ze spotřebitelů na podniky.[439] Zato druhá skupina plánuje využít jednotící federální úpravu ke zmírnění povinností, které mohou vyplývat z progresivnějších státních úprav.[440] Toto pouze utvrzuje propastný rozdíl perspektivy, který na problematiku mají podporovatelé zvýšené ochrany soukromí jednotlivce v online prostředí a zástupci podniků tvořících bázi sledovacího kapitalismu *(surveillance capitalism)*.[441]

3.4 Diskuse přínosu americké perspektivy pro tuto monografii

Na základě druhé kapitoly lze vnímat trend rostoucí četnosti, důsledků a složitosti případů porušení bezpečnosti. Nadto, jak bude diskutováno v následující čtvrté kapitole, nové technologie a postupný přesun většiny obchodních i sociálních interakcí do primárně virtuální komunikace přidávají na významu této problematice.

436 Srov. LAPOWSKY, Issie. Get Ready for a Privacy Law Showdown in 2019. *Wired* [online]. 2018 [cit. 24. 5. 2021].

437 Srov. SCHNEIER, Bruce. Facebook and Cambridge Analytica. *Schneier on Security* [online]. 29. 3. 2018 [cit. 24. 5. 2021]. Dostupné z: https://www.schneier.com/blog/archives/2018/03/facebook_and_ca.html

438 Viz As GDPR nears, Google searches for privacy are at a 12-year high. *The Economist* [online]. 2018 [cit. 24. 5. 2021].

439 Viz BLOOMBERG, Scott. Tech Industry & Consumer Advocates Share Support for Federal Data-Privacy Legislation, Differ on the Details. *Security, Privacy and the Law* [online]. 18. 10. 2018 [cit. 24. 5. 2021]. Dostupné z: https://www.securityprivacyandthelaw.com/2018/10/tech-industry-consumer-advocates-share-support-for-federal-data-privacy-legislation-differ-on-the-details/

440 Viz SCHNEIER, Bruce. California Passes New Privacy Law. *Schneier on Security* [online]. 3. 7. 2018 [cit. 24. 5. 2021]. Dostupné z: https://www.schneier.com/blog/archives/2018/07/california_pass.html

441 Srov. ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* [online]. 2015, roč. 30, č. 1.

Koncept notifikačních povinností, tak jak vznikl v právu Spojených států a byl následně přenesen do prostředí unijního práva, v tomto směru slouží jako potenciálně robustní regulatorní nástroj pro omezení následků pojících se k těmto škodlivým jevům. Reakce na porušení bezpečnosti musí být koordinovaná, aby byla účinná. Nepostačuje pouze reakce dotčeného správce či zpracovatele. Je na místě zapojit také dozorový orgán, který má celkový přehled o širším kontextu, a dále pak subjekty údajů, které mají hlavní zájem, aby upravili své jednání a reagovali tak na hrozící újmu. Tato otevřenost komunikace, transparentnost a koordinace, které jsou předpokladem efektivní reakce, však jak v rámci americké, tak unijní úpravy, narážejí na řadu překážek, které omezují funkční nasazení daného koncepčního řešení do procesů zpracování. I v kontextu americké úpravy vnímám, že dochází k přítomnosti překážek pro dodržování a funkční přínos předmětných povinností.

Prvně jde o překonání protichůdných zájmů a dosažení motivace povinným subjektům ke sdílení informací o případech porušení bezpečnosti, buďto skrze vyrovnávací výhody *(trade-off)* nebo důsledným vymáháním notifikačních povinností. Povinnost oznámit porušení bezpečnosti ze své podstaty vede ke konfliktu zájmů u povinného subjektu,[442] zvláště pokud právní úprava ukládá zavedení přiměřených opatření, čímž vyvstává hrozba sankce.[443] I pokud je hlavním společenským přínosem z oznamovací povinnosti prevence vzniku či navýšení hrozící újmy skrze vyrovnání informační asymetrie s dotčenými fyzickými osobami, povinné subjekty se rozhodují primárně s ohledem na své zájmy. Rozbor této perspektivy představím v páté kapitole.

Dále má na realizaci plnění povinností vliv také míra právní jistoty, kterou má povinný subjekt ohledně výkladu vzniku a obsahu dané povinnosti. Zatímco šíře ochrany osobních údajů v unijním právu zakládá zvýšenou výkladovou náročnost skrze rozsáhlé užití neurčitých právních pojmů a performativních pravidel, ve Spojených státech jsou povinnosti související s porušením bezpečnosti zpravidla formulovány úžeji a klíčové pojmy jsou jasněji dané. Řada úprav se omezuje pouze na elektronické záznamy

442 Zde jsou klíčové hrozící náklady v podobě náhrady újmy dotčeným jednotlivcům. Pravděpodobnost jejich realizace posiluje ve Spojených státech etablovanost skupinových žalob.

443 V americkém prostředí lze zvažovat především výše nastíněnou činnost FTC.

v nezašifrované podobě. Právní jistotu pak posilují též časté příkladné výčty údajů o jednotlivci, na které se úprava vztahuje.

V tomto ohledu je významné, aby pro specifické oblasti byla dostupná podrobná vodítka, tak jak tomu je v případě federální úpravy pro finanční a zdravotní sektor ve Spojených státech. V tomto směru je velmi pozitivní vydání vodítek Sboru s příklady scénářů porušení zabezpečení osobních údajů z počátku roku 2021.[444] Přesto lze pokládat aplikaci těchto povinností na konkrétní situace, zvláště s ohledem na dynamiku technologického vývoje, za přetrvávající výzvu. Metodologie, doporučení, osvědčená praxe a příklady vhodného řešení tak představují významné prvky umožňující dodržení souladu, přičemž jejich absence může naopak odrazovat povinné subjekty od dodržování notifikačních povinností. K tomuto řešení výkladové nejistoty se vrátíme v podkapitole 6.2.

S ohledem na překážky v motivaci povinných subjektů a výkladu složitých povinností pokládám za přínosné, aby se regulatorní úprava soustředila na postihování činností s nejvyšší mírou rizika. V rámci celkového spektra činností zpracování údajů o jednotlivcích lze poměrně snadno identifikovat oblasti, kde je zjevně vyšší inherentní riziko újmy při porušení bezpečnosti zpracovávaných údajů.

Elektronicky uchovávané a zpracovávané údaje mají mnohem vyšší potenciál úniku a zneužití než papírové záznamy. Užití šifrování zásadně snižuje přístup k informační hodnotě údajů. Bankovní sektor či zdravotnictví obecně zpracovávají rozsáhlé databáze vysoce citlivých údajů o jednotlivci, které hrozí snadným zneužitím. Ochrana některých databází údajů o jednotlivcích je úzce provázána s aktivy a podstatou činnosti dané entity,[445] zatímco u jiných je lze vnímat jako podružné a jejich narušení tedy za relativně nevýznamné z hlediska zájmů povinného subjektu, ačkoliv vzniklé riziko pro subjekty údajů může být značné.[446]

444 Srov. Guidelines 01/2021 on Examples regarding Data Breach Notification. *EDPB* [online]. Brusel: EDPB 2021 [cit. 10. 10. 2021].

445 Např. zachování důvěrnosti a integrity účetních záznamů klientů společnosti poskytující služby účetního poradenství.

446 Např. údaje získané provozovatelem distribuční soustavy z chytrých elektroměrů primárně pro lepší správu zátěže dané soustavy, ze kterých však lze dovodit určité informace o preferencích, pohybu či činnostech jednotlivce na odběrovém místě.

V rámci amerického regulatorního rámce nalézáme větší přizpůsobení notifikačních povinností těmto aspektům. Oproti tomu unijní regulatorní přístup vysoké úrovně celkové ochrany tuto diverzifikaci vnímá až jako druhotný krok v rámci výkladu, primárně vedený vodítky, doporučeními a kodexy chování. V tomto ohledu by prioritou dozorových úřadů měla být identifikace těchto oblastí a přednostní důraz na dodržování souladu v nich působícími subjekty.[447]

Je dále potřebné rozvíjet koordinaci a spolupráci pro včasné a účinné reakční opatření na rozsáhlé případy porušení bezpečnosti, které se významně dotýkají více členských států EU[448] nebo se kaskádově šíří napříč kyberprostorem bez specifického zaměření na určité subjekty či území.[449] V EU je toto předmětem *Pan-European Personal Data Breaches Exercises* organizovaných Společným výzkumným střediskem *(Joint Research Centre)* společně s Generálním ředitelstvím pro spravedlnost a spotřebitele *(Directorate-General for Justice and Consumers of the European Commission)* a dozorovými úřady členských států.[450] Ve Spojených státech je tato koordinace zajišťována především skrze sektorová uskupení pro sdílení informací označovaná jako centra pro analýzu a sdílení informací *(Information Sharing and Analysis Centres*, ISAC*)*. Jejich formát a výhody budou blíže představeny v podkapitole 6.3.

Přenositelné prvky americké úpravy s možnou přidanou hodnotou: Některé aspekty americké úpravy by mohly být prospěšné i v unijním kontextu. Za potenciálně hodnotný nejen pro informovanost subjektů údajů, ale též pro zvyšování obecného povědomí a podporu výzkumných a vzdělávacích činností považuji veřejně dostupný rejstřík ohlášených případů porušení bezpečnosti, podobný tomu, který vede na svých webových stránkách

447 Srov. SKROUPA, Christopher P. GDPR Priorities: Public Companies Must Urgently Handle Data Breaches. *Forbes* [online]. 2018 [cit. 25. 5. 2021].

448 Viz RODRIGUEZ, Salvador. Facebook hack affected 3 million in Europe, creating the first big test for privacy regulation there. *CNBC* [online]. 2018 [cit. 25. 5. 2021].

449 Srov. ZIMBA, Aaron; CHISHIMBA, Mumbi. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research* [online]. 2019, roč. 4, č. 1, s. 3 a násl.

450 Srov. MALATRAS, Apostolos et al. Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review* [online]. 2017, roč. 33, č. 4, s. 458 a násl.

HHS pro významné případy v sektoru zdravotnictví.[451] Návrh veřejného rejstříku byl přitom obsažen ve znění Obecné nařízení přijatého v prvním čtení Evropským parlamentem.[452]

Další úprava, která by mohla mít významný přínos pro překonání nízké motivace povinných subjektů k ohlašování porušení bezpečnosti je rozsáhlejší podpora oznamovatelů porušení *(whistleblower)*. V amerických reáliích má tato role ustálenou tradici založenou i pro oblast porušení bezpečnosti mimo jiné skrze *Sarbanes-Oxley Act* z roku 2002.[453] V EU přitom v nedávné době došlo k významnému posunu v harmonizaci této oblasti skrze přijetí směrnice 2019/1937.[454] Jelikož aktivita oznamovatelů v této oblasti již do určité míry narostla samotným přijetím Obecného nařízení,[455] nastiňuji očekávatelný přínos této úpravy blíže v podkapitole 6.6.

V tomto bodě bych rád stručně polemizoval nad možným přínosem amerických zkušeností se skupinovými žalobami ve vztahu k porušení bezpečnosti. Tradice skupinových žalob je v evropském prostředí v řadě členských států přítomná, avšak není příliš rozvinutá.[456] V současné době dochází k transpozici harmonizované unijní úpravy tohoto procesního nástroje na ochranu kolektivních zájmů spotřebitelů, pod které je vztažena i ochrana osobních údajů.[457]

---

451 Viz Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. *Office for Civil Rights* [online]. [cit. 25. 5. 2021]. Dostupné z: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

452 Srov. 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). *Evropský parlament* [online]. COM(2012)0011-C7-0025/2012-2012/0011(COD). Štrasburk: Evropský parlament, 2014, s. 178 [cit. 29. 4. 2021].

453 Srov. SWANSON, Kristofer, Thomas L. KIRSCH II a Ryan M. DUNIGAN. Data Breaches in a Whistleblower's World:What You Should Know, Why You Should Know It. *ABA Criminal Justice Section Newsletter*., 2013, s. 7.

454 Směrnice Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie.

455 Srov. RAM, Aliya. Reports from whistleblowers on data breaches almost triple. *Financial Times* [online]. 2018 [cit. 25. 5. 2021].

456 Srov. *Report from the Commisson on the implementation of the Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union law (2013/396/EU)* [online]. COM/2018/040 final. 2018 [cit. 25. 5. 2021].

457 Směrnice Evropského parlamentu a Rady (EU) 2020/1828 ze dne 25. listopadu 2020 o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES.

Přes nutnou omezenou přenositelnost na základě specifik vývoje této problematiky ve Spojených státech lze, dle mého názoru, přinejmenším dovodit, že přes rozsáhlou a hluboce zakořeněnou procesní tradici skupinových žalob, včetně posilujících nástrojů, jako je uložení náhrady újmy nad rámec doložené způsobené újmy jako forma sankce *(punitive damages)*, je zde přenášení vzniklé újmy z dotčených jednotlivců na postižené subjekty značně neefektivní.

Americká zkušenost poukazuje na nesnadné doložení či vyčíslení způsobené újmy v intencích tradičního procesního práva.[458] Byť vysokou míru odmítnutí žalob bychom měli připisovat americkým specifikům, domnívám se, že vysoká četnost mimosoudních smírů je spojena s významnou informační asymetrií, kterou není snadné překonat procesními nástroji.

Dovoluji si také pochybovat o rozsahu vynucovací funkce skupinových žalob, jelikož nízká pravděpodobnost uložení rozsáhlé finanční kompenzace nebude vytvářet tlak na dodatečné investice do opatření na ochranu zpracovávaných údajů. Vyšší úspěšnost žalob na základě oznámených případů porušení bezpečnosti by dokonce mohla působit negativně na rozhodování povinných subjektů včasně odhalovat a řádně sdílet informace o těchto incidentech, jelikož by se tím dobrovolně vystavovaly těmto žalobám, což zřejmě nebude v takové situaci racionální. Tuto argumentaci dále rozvedu v příslušné podkapitole 6.4.

V unijním rámci na ochranu osobních údajů byly nedostatky vynucování skrze žalobní nároky poškozených jednotlivců do značné míry vykompenzovány rozsáhlou rolí dozorových úřadů.[459] I zde jsou však znatelné limity, zvláště s ohledem na nepřiměřeně omezenou kapacitu některých úřadů, což otvírá prostor v rámci EU pro selektivní volbu místa usazení *(jurisdiction shopping)*[460] a vytváří tak riziko oslabení celkové úrovně bezpečnosti osobních údajů.[461]

458 Viz ROMANOSKY, Sasha, David HOFFMAN a Alessandro ACQUISTI. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, 2014, roč. 11, č. 1, s. 25.

459 Podobně jako ve výsledku pro překážky skupinových žalob působí alespoň částečně i ve Spojených státech *Attorney General* a FTC, jak bylo popsáno v oddílech 3.3.4 a 3.3.5.

460 Blíže viz WIKIMEDIA FOUNDATION. Jurisdiction shopping. *Academic Dictionaries and Encyclopedias* [online]. 2010 [cit. 15. 7. 2021]. Dostupné z: https://enacademic.com/dic.nsf/enwiki/1323290

461 Srov. VINOCUR, Nicholas. 'We have a huge problem': European regulator despairs over lack of enforcement. *POLITICO* [online]. 27. 12. 2019 [cit. 12. 7. 2021]. Dostupné z: https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/

Výhoda sjednocené právní úpravy: Fragmentovaný rámec povinností napříč Spojenými státy však poukazuje na významnou výhodu unijního přístupu skrze přímo použitelné Obecné nařízení. Ta spočívá ve snížení administrativní zátěže povinných subjektů skrze sjednocení pravidel. Současně je jí také dosahováno stejné minimální úrovně ochrany pro všechny fyzické osoby v rámci jurisdikce, což ve Spojených státech v tomto ohledu zcela neplatí.

Tudíž ačkoliv se může zdát současný americký přístup jako poskytující vyšší míru právní jistoty skrze lépe zaměřené a více specifické notifikační povinnosti, je jeho harmonizace výrazně větší překážkou než dočasná vyšší míra právní nejistoty v EU. Ta je totiž překonatelná jak zvýšením dostupnosti výkladových vodítek a sektorových doporučení, tak výkladem pojmů skrze rozhodovací činnost dozorových úřadů a soudů. Nadto může být tento obecný jednotný rámec snadněji doplněn o specifickou úpravu postihující vybraný sektor než lze dosáhnout sjednocení narůstajícího počtu fragmentovaných úprav v americkém prostředí.

Při nalézání možných zlepšení pro unijní úpravu je na místě zvažovat nejen míru rizika spojenou s určitým druhem činnosti, ale též při tom používané technologie. Tak se např. s rozvojem strojového učení, automatizované komunikace a cloudových zpracování dat *(cloud computing)*[462] pojí specifická rizika, která mohou zesilovat rizikovost určitých činností, či naopak nabízet technická opatření pro jejich snížení. Právě na vliv technologického vývoje pro nastíněné úvahy se zaměříme počínaje čtvrtou kapitolou.

3.5 Shrnutí kapitoly

Mým záměrem v rámci této rozsáhlé kapitoly bylo přiblížit řešenou problematiku z právní perspektivy. Její struktura přitom byla vedena především dílčí otázkou (1), tudíž jsem zkoumal, jak se proměnily nyní použitelné notifikační povinnosti v Obecném nařízení ve srovnání s předchozí unijní a paralelní americkou právní úpravou.

462 Blíže k pojmu viz např. ANTONOPOULOS, Nick a Lee GILLAM. *Cloud Computing: Principles, Systems and Applications*. Londýn: Springer, 2017.

Za tímto účelem jsem přistoupil nejprve k představení unijní úpravy, která předcházela použitelnosti Obecného nařízení.[463] Jedná se o stále relevantní specifickou úpravu pro poskytovatele veřejně dostupných služeb elektronických komunikací dle směrnice 2002/58/ES, o soukromí a elektronických komunikacích poté, co byla novelizována směrnicí 2009/136/ES a později doplněna nařízením Komise 611/2013.[464] Již zde přitom nalézáme dělení na ohlašovací, oznamovací a dokumentační povinnost, které je přeneseno i do Obecného nařízení, jakož i řadu dalších prvků těchto povinností, na které bylo navázáno. Přehled jsem také doplnil o stručné představení národních právních úprav, které předcházely Obecnému nařízení.[465]

V podkapitole 3.2 již přenáším pozornost na použitelnou úpravu podle článků 33 a 34 Obecného nařízení. Ty nejprve představuji z hlediska jejich legislativního vývoje, abych mimo jiné upozornil na prvky, které se objevovaly v návrzích jednotlivých institucí, ale nejsou součástí výsledného kompromisu.[466] V rámci celostního pojetí je zde krátce zmínka o dílčích transpozicích do národních právních řádů na základě směrnice 2016/680. Osvětleno je také, že vzhledem k odlišnostem nepodstatným z hlediska rozvoje internetu věcí nepokládám za významné dále přihlížet k případným dílčím specifikům české národní úpravy a vycházím tedy pro zbytek monografie z úpravy dle Obecného nařízení.

Na to navazuji podrobným rozborem povinností souvisejících s porušením zabezpečení.[467] Po krátkém osvětlení terminologické nejednotnosti českého znění Obecného nařízení, na kterou bylo upozorněno již v podkapitole 1.2,[468] představuji dokumentační povinnost dle článku 33 odst. 5 Obecného nařízení. U té se věnuji výkladu pojmů porušení zabezpečení osobních údajů, osobní údaj a zpracování, abych mohl vyložit obsah dokumentační povinnosti. Následně soustředím pozornost na ohlašovací povinnost dle článku 33

463 Viz podkapitola 3.1.
464 O té byla řeč v oddílu 3.1.1.
465 Viz oddíl 3.1.2.
466 Lze zmínit například veřejně dostupný přehled porušení zabezpečení, navrhovaný Evropským parlamentem. Srov. oddíl 3.2.1.
467 Viz oddíl 3.2.2.
468 Blíže jsem se tomuto věnoval v KASL, František. K pojmové nejednotnosti porušení zabezpečení/bezpečnosti osobních údajů v českém právu. *AUC IURIDICA* [online]. 2019, roč. 2019, č. 3.

Obecného nařízení, u které dále doplňuji výklad o pojem nepravděpodobné riziko, jakož i práva a svobody fyzických osob, abych mohl adekvátně popsat i obsah této povinnosti. Třetí pak představuji oznamovací povinnost dle článku 34 Obecného nařízení, u které přidávám ještě výklad pojmu vysoké riziko.

Na poskytnutý legislativní a obsahový přehled úpravy navazuji podrobnější diskusí významných aspektů úpravy povinností dle čl. 33 a 34 Obecného nařízení.[469] Nejprve nastiňuji systematickou provázanost s jinými prvky předpisu, čímž se dostávám k pojmu performativní pravidlo. Ten je vyložen a následně diskutován ve spojitosti s porušením zabezpečení, především s cílem odhalit předpoklady adekvátnosti uložení povinnosti sdílet informace.

V hlavní části diskuse se věnuji funkčnímu výkladu předmětné úpravy ve snaze o vymezení jejích účelů. K tomu přistupuji ve třech rovinách. Prvně, při nalézání účelu vyjádřeného ve vlastním textu úpravy, zjišťuji, že touto cestou je zachycen pouze účel povinnosti dokumentační. Po postoupení do druhé perspektivy, která sleduje účel zachycený v bodech odůvodnění, odhaluji účel povinnosti oznamovací. Pro ohlašovací povinnost však body odůvodnění nepřinášejí dostatečné osvětlení jejího účelu. Dovozuji tudíž její účel z jejího pojetí jako prvku chytré regulace, což považuji za třetí rovinu, tedy účel nalézaný z objektivního hlediska.

V další podkapitole 3.3 přecházím ke stručnému rozboru úpravy povinností při porušení bezpečnosti údajů o jednotlivci v právu Spojených států amerických. Jeho vhodnost a potřebnost zdůvodňuji především rozsáhlým odborným diskurzem založeným na dlouhé zkušenosti s notifikačními povinnostmi, které sloužily jako inspirace pro unijní úpravu. Ten následně využívám k posouzení obecnosti překážek úpravy identifikovaných v rámci předcházející diskuse, jakož i námětům řešení, kterým se věnuji především v šesté kapitole.

Po zdůraznění částečně odlišné terminologie[470] a nejvýznamnějších specifik americké právní úpravy[471] přistupuji k její vlastní struktuře na úrovni jednotlivých států.[472] Prvně věnuji pozornost vymezení pojmu porušení

469 Viz oddíl 3.2.3.
470 Srov. oddíl 3.3.1.
471 Srov. oddíl 3.3.2.
472 Srov. oddíl 3.3.3.

bezpečnosti údajů o jednotlivci. Následně se zaměřuji na kalifornský státní předpis z roku 2002, který byl první zvláštní úpravou zakládající notifikační povinnosti ve spojení s porušením bezpečnosti. Poskytuji i konsolidovaný přehled hlavních rysů předpisů v dalších státech Spojených států amerických. Významnou roli zde hraje judikatura a činnost státních *Attorney General*, o kterých pojednávám v oddílu 3.3.4. Následně pak představuji též federální rovinu úpravy,[473] konkrétně sektorové úpravy pro finanční sektor a pro sektor zdravotních služeb, činnost *Federal Trade Commission* a dosavadní neúspěšné snahy o jednotnou federální úpravu.

Poznatky o představených právních rámcích následně promítám do diskuse v podkapitole 3.4, která je vedena druhou částí dílčí otázky (1), tedy srovnáním úpravy v Obecném nařízení s paralelní americkou právní úpravou a čerpáním inspirace pro možná řešení odhalených překážek, která diskutuji podrobněji v šesté kapitole.

Předně zdůrazňuji potřebu koordinovaného přístupu povinných subjektů, dotčených jednotlivců a dozorového orgánu při řešení porušení bezpečnosti. Tomu však do značné míry stojí v cestě překážky v podobě kolize zájmů povinných subjektů a nejasného výkladu notifikačních povinností. Jeden z poznatků, který čerpám z americké zkušenosti, je přínos zaměření regulatorní pozornosti na činnosti s nejvyšší mírou rizika. Dále pak vnímám vhodnou inspiraci při sektorovém přístupu ke sdílení informací a spolupráci na řešení porušení bezpečnosti. Identifikuji i další přenositelné prvky americké úpravy s možnou přidanou hodnotou pro unijní prostředí, s čímž souvisí i polemika nad možným přínosem skupinových žalob. V závěru pak docházím k poznatku, že přes dnes významně negativně vnímanou zvýšenou výkladovou nejistotu má sjednocená právní úprava na základě Obecného nařízení zásadní výhodu nad fragmentovaným rámcem ve Spojených státech amerických, zvláště pokud bude využito nástrojů pro konkretizaci předmětných povinností a motivaci povinných subjektů, které představuji v šesté kapitole.

473 Viz oddíl 3.3.5.

4 PORUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ V KONTEXTU INTERNETU VĚCÍ

Projevy a důsledky spojené s rozvojem internetu věcí dosahují daleko za rovinu pouhé technologické proměny. Jde o mnohovrstvý jev, který doznává značné pozornosti jak v odborných, tak v populárních kruzích řady oborů.[474] Pojmosloví pro tuto proměnu technologického prostředí není zatím pevně zakotvené na jeden termín či definici. Různí autoři na něj odkazují např. jako na kyber-fyzické systémy *(cyber-physical systems)*[475], všudypřítomnou výpočetní technologii *(ubiquitous computing)*[476], ambientní inteligenci *(ambient intelligence)*[477] nebo eobjekty *(eObjects)*[478]. Za nejčastěji používané však platí označení internet věcí *(internet of things)*.

Pojem internet věcí je v současné době jedním z často zmiňovaných hesel spojovaných s nejmodernějšími technologickými trendy.[479] Souvisí s ním pokrok ve všech klasických oblastech informačních a komunikačních technologií. Díky tomu je již nejen technicky možné, ale především komerčně dostupné, instalovat komunikační moduly do předmětů každodenní potřeby. *Schneier* shrnuje tuto proměnu započatou v minulém desetiletí tak, že z věcí s počítači se staly počítače s věcmi.[480] Na trhu tak nalezneme řadu „chytrých" zařízení

474 Příkladem ALMEIDA, Virgilio A. F., Danilo DONEDA a Marília MONTEIRO. Governance Challenges for the Internet of Things. *IEEE Internet Computing* [online]. 2015, roč. 19, č. 4; MITTELSTADT, Brent. Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology* [online]. 2017, roč. 19, č. 3; WEBER, Rolf H. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, 2016, roč. 2016, č. 32.

475 Srov. BAHETI, Radhakisan a Helen GILL. Cyber-physical Systems. In: SAMAD, Tariq a Anuradha ANNASWAMY (eds.). *The Impact of Control Technology* [online]. New York: IEEE Control Systems Society, 2011, s. 161–166.

476 Viz WEISER, Mark. The computer in the 21st century. *Scientific American*, 1991, roč. 1991.

477 Srov. COSTA, Luiz. *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*. Cham: Springer International Publishing, 2016.

478 Viz MANWARING, Kayleen a Roger CLARKE. Surfing the Third Wave of Computing: A Framework for Research into eObjects. *Computer Law & Security Review: The International Journal of Technology Law and Practice* [online]. 2015, roč. 31, č. 5, s. 583–603.

479 Srov. THE ECONOMIST. Ubiquitous computing – Drastic falls in cost are powering another computer revolution. *The Economist* [online]. 2019 [cit. 15. 7. 2021].

480 *„The technological shift occurred during the last decade or so. It used to be that things had computers in them. Now they are computers with things attached to them."* Srov. SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 5.

(např. ledničky), schopných nad rámec běžných funkcí (uchovávání potravin v chladu) komunikovat dodatečné informace (např. blížící se expiraci potravin), zpracovávat nejrůznější formou shromažďované údaje (např. automatické doobjednání oblíbených produktů) a nabízet díky tomu dosud nedostupné funkce (např. doporučit recepty z dostupných potravin).[481]

Předpokládá se, že internet věcí postupně propojí skrze globální internetovou síť i předměty, u kterých se takové připojení vymyká našemu běžnému vnímání okolního světa.[482] Analytici předvídají, že půjde o jednou z nejzásadnějších změn v ICT v této dekádě.[483] Společnost *Cisco* odhaduje nárůst počtu zařízení internetu věcí z 6 miliard v roce 2018 na téměř 15 miliard v roce 2023. Se započtením mobilních telefonů, osobních počítačů, tabletů, televizí se přitom dle stejných odhadů počty všech připojených zařízení zvýší z 18 miliard v roce 2018 na téměř 30 miliard, což značí, že zařízení internetu věcí jsou kategorií, se kterou se spojuje většina očekávaného budoucího růstu na poli konektivity.[484]

Internet věcí slibuje vytvoření sítě propojených produktů od ledničky či termostatu v domácnosti přes čidla ve vozidlech až po senzory přímo v lidském těle.[485] To je však pouze část možností, které tento technologický posun přináší. Významné využití se již dnes rýsuje v podobě snížení nákladů výroby a poskytování služeb, především skrze zefektivnění logistiky (např. optimalizací *just-in-time*[486] dodávek), lepšího managementu skladování a distribuce, a obecně eliminace řady funkcí či činností, které bude možné přenechat

481 Srov. SAMSUNG. Family Hub Refrigerator – Overvierw. *Samsung* [online]. [cit. 19. 5. 2021]. Dostupné z: https://www.samsung.com/us/explore/family-hub-refrigerator/overview/; TAKAHASHI, Dean. Smarter's FridgeCam can guess when your food expires. *VentureBeat* [online]. 3. 1. 2017 [cit. 19. 5. 2021]. Dostupné z: https://venturebeat.com/2017/01/03/smarters-fridgecam-tells-you-when-your-food-will-expire/

482 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 6.

483 Srov. BRIGGS, Bill. *Tech Trends 2014, Inspiring Disruption* [online]. London: Deloitte Consulting, 2014, s. 55 [cit. 1. 6. 2021].

484 Srov. Cisco Annual Internet Report (2018–2023). *CISCO* [online]. San Jose, CA: Cisco, 2020, s. 6 a 8 [cit. 19. 5. 2021].

485 Viz KROES, Neelie. Ethical implications of tomorrow's digital society. In: SMITH, Ian. *Internet of Things 2012 New Horizons*. Halifax: IERC – Internet of Things European Research Cluster, 2012, s. 7.

486 K pojmu viz FINANCIAL AND BUSINESS TERMS. just-in-time. *Academic Dictionaries and Encyclopedias* [online]. 2012 [cit. 15. 7. 2021]. Dostupné z: https://business_finance.enacademic.com/21205/just-in-time

automatické komunikaci mezi zařízeními a výrobky nebo uživateli služeb.[487] V tomto lze spatřovat pouze počátek trendu, jelikož se jedná o využití, která jsou již v současné době aplikována a rozšiřována. Ke globální internetové síti je již dnes připojena řada běžných předmětů a zařízení, od spotřebičů a hraček po zdravotní zařízení.[488]

Lze vycházet z předpokladu, 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 nakonec převážně rozhodne trh a ekonomická úvaha, zda taková verze skýtá potenciál snížení nákladů např. v logistice nebo zda slibuje zvýšení výnosů např. skrze novou službu či lepší cílení reklamy.[489] S rostoucí konektivitou a za trvající platnosti tzv. *Mooreova zákona*[490] se současně otevírají nové možnosti funkcí a autonomních činností, které tyto předměty budou moci vykonávat. Mluví se o prolomení hranice mezi reálným a virtuálním světem, tedy o konceptu rozšířené reality *(augmented reality*[491] či *enhanced reality*[492]*)*, který se vyznačuje stavem všudypřítomného pokrytí dostupností informační sféry *(infosphere)*. Ta se přitom stává neopominutelnou (a neodstranitelnou) součástí běžného vnímání světa.[493]

U cílených urbanistických infrastrukturních řešení s významným zapojením prvků internetu věcí (především senzorů a jiných zařízení pro shromažďování informací) za účelem zvýšení efektivity se pak zažívá označení chytré

487 Srov. BACHLECHNER, Daniel et al. *IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht* [online]. Berlin: Bundesministerium für Wirschaft und Energie, 2016, s. 19–20 [cit. 25. 5. 2021].

488 Viz THE ECONOMIST. Things are looking app. *The Economist* [online]. 2016 [cit. 19. 5. 2021].

489 Srov. ANDERSON, Janna a Lee RAINIE. *The Internet of Things Will Thrive by 2025* [online]. Washington D.C.: Pew Research Center, 2014, s. 24 a násl. [cit. 19. 5. 2021]; SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 6–7.

490 Viz např. COFFMAN, Kerry a Andrew M. ODLYZKO. Internet Growth: Is There a "Moore's Law" for Data Traffic? [online]. 2002, roč. 4.

491 Srov. BARFIELD, Woodrow (ed.). *Fundamentals of Wearable Computers and Augmented Reality*. 2. vyd. Boca Raton: CRC Press, 2015; FLORIDI, Luciano (ed.). The Onlife Manifesto. In: FLORIDI, Luciano (ed.). *The Onlife Manifesto: Being Human in a Hyperconnected Era* [online]. Cham: Springer International Publishing, 2015, s. 7 a násl. [cit. 15. 7. 2021].

492 Srov. BOWSKILL, Jerry a John DOWNIE. Extending the capabilities of the human visual system: an introduction to enhanced reality. *ACM SIGGRAPH Computer Graphics* [online]. 1995, roč. 29, č. 2, s. 61 a násl.

493 Blíže viz FLORIDI, Luciano. *Information. A Very Short Introduction*. Oxford: Oxford University Press, 2010, s. 16.

město *(smart city)*[494]. Tato proměna veřejného prostoru přitom není cizí ani české urbanistice.[495]

4.1 Pojem internetu věcí

Značně rozšířené užívání slovního spojení internet věcí, jak bylo nastíněno výše, odráží různorodost a odlišnost vlastního obsahu daného pojmu, ve kterém ho daný autor vnímá. Jak je zjevné z podrobné monografie definic pojmu z pera autorského kolektivu *Minerva, Biru* a *Rotondi*, je přitom chápání možného obsahu značně různorodé.[496] Vzhledem k tomuto rozptylu definic nabízejí autoři vlastní neutrální dvoustupňovou definici, která odráží klíčové a nejčastěji reflektované vlastnosti akcentované ve spojitosti s tímto termínem. Jako taková je závislá na rozsahu a složitosti prostředí, ve kterém je internet věcí popisován.

Z hlediska prostředí malého rozsahu a složitosti jde o *„síť, která propojuje jedinečně identifikovatelné ‚věci' za pomoci sítě Internet. Tyto ‚věci' mají schopnost sběru informací za pomoci senzorů, případně aktivační systémy* [umožňující interakci s fyzickým světem] *a možnost programového nastavení. Skrze využití jedinečné identifikace a sběru informací za pomoci senzorů je možné shromažďovat údaje o „věci" a stav ‚věci' může být změněn odkudkoliv, kdykoliv a jakkoliv."*[497] Tato definice je zaměřena na vymezení jednotlivých zařízení v rámci dané sítě (tedy na pojetí věci v internetu věcí).

Pro představovanou monografii je však významnější definice pro rozsáhlá prostředí a složité sítě. V takovém kontextu je internet věcí tímto autorským kolektivem chápán jako *„samostatně se konfigurující, adaptivní, složitá síť, která propojuje ‚věci' se sítí Internet za využití standardních komunikačních protokolů. Tyto propojené věci*

494 Pro více informací viz např. BATTY, M. et al. Smart cities of the future. *The European Physical Journal Special Topics* [online]. 2012, roč. 214, č. 1, s. 481 a násl.

495 Srov. BROŽOVÁ, Jana. V Židlochovicích na Brněnsku vyroste ukázková čtvrť budoucnosti. *Bydlet.cz* [online]. 14. 7. 2020 [cit. 15. 7. 2021]. Dostupné z: https://www.bydlet.cz/551306-v-zidlochovicich-na-brnensku-vyroste-ukazkova-ctvrt-budoucnosti/; LUKÁČ, Petr. Prvním „chytrým" městem v Česku se stane Písek. Firma Schneider Electric bude řídit dopravu i vytápění. *Hospodářské noviny (iHNed.cz)* [online]. 2016 [cit. 15. 7. 2021].

496 Srov. MINERVA, Roberto, Abyi BIRU a Domenico ROTONDI. *Towards a definition of the Internet of Things (IoT)* [online]. Torino: IEEE, 2015, s. 70 [cit. 1. 6. 2021].

497 *„An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything."* Ibid., s. 73–74.

mají fyzickou či virtuální podobu v digitálním světě, schopnost sběru informací za pomoci senzorů, případně aktivační systémy a možnost programového nastavení. Jsou také jedinečně identifikovatelné. Zmíněná podoba obsahuje informace zahrnující identitu věci, její stav, umístění a další podnikové, společenské či soukromé relevantní informace. Věc poskytuje služby, s nebo bez lidského zásahu, za využití své jedinečné identifikace, shromažďování údajů, jejich komunikace a případné interakce s fyzickým světem. Tyto služby jsou užívány za pomoci inteligentních rozhraní a jsou dostupné kdekoliv, kdykoliv a za jakýmkoliv účelem, při zohlednění zajištění bezpečnosti."[498] Pojem internetu věcí v tomto vnímání sahá od komplexních řešení pro oblast zdravotnictví, energetiky, dopravní infrastruktury až po maloobchodní produkty pro zajištění bezpečnosti, pohodlí či zábavy.[499] Internet věcí je tak možné pokládat za rámcový posun v procesech a operacích, který zahrnuje široké spektrum dalších často zmiňovaných nových technologií jako jsou chytrá vozidla,[500] průmysl 4.0,[501] umělá inteligence,[502] robotika,[503] cloudová datová úložiště[504] či blockchain.[505, 506]

498 *„Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."* Ibid., s. 74.

499 Velmi výstižné je grafické zachycení viz BEECHAM RESEARCH LTD. M2M Sector Map. *Beecham Research Shaping the IoT Future* [online]. 2011 [cit. 1. 6. 2021]. Dostupné z: http://www.beechamresearch.com/download.aspx?id=18

500 Srov. ABIRESEARCH. *Smart Cars and the IoT* [online]. AN-1792. New York: ABIresearch. 2014 [cit. 15. 7. 2021].

501 Srov. LAMPROPOULOS, Georgios, Kerstin SIAKAS a Theofylaktos ANASTASIADIS. Internet of Things in the Context of Industry 4.0: An Overview. *International Journal of Entrepreneurial Knowledge* [online]. 2019, roč. 7.

502 Srov. DEVINNEY, Fran. Bringing the power of AI to the Internet of Things. *Wired* [online]. 2018 [cit. 15. 7. 2021].

503 Viz MATTHEWS, Kayla. The Internet of Robotic Things: How IoT and Robotics Tech Are Evolving Together. *IoT Times* [online]. 19. 6. 2019 [cit. 15. 7. 2021]. Dostupné z: https://iot.eetimes.com/the-internet-of-robotic-things-how-iot-and-robotics-tech-are-evolving-together/

504 Srov. STERGIOU, Christos et al. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems* [online]. 2018, roč. 78.

505 Srov. IEEE. The Potential of Blockchain for IoT. *IEEE Innovation at Work* [online]. 4. 9. 2019 [cit. 15. 7. 2021]. Dostupné z: https://innovationatwork.ieee.org/the-potential-of-blockchain-for-iot/

506 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 7.

4.2 Nové formy a vzorce zpracování osobních údajů v kontextu internetu věcí

S představenou mnohostí nových funkcí a užití informačních a komunikačních technologií v rámci internetu věcí se pojí významné důsledky pro sběr osobních údajů, jejich zpracování, sdílení a vytěžování. To je zvláště zjevné u inciativ, které byly připravovány již před světovou pandemií COVID-19, ale v jejím důsledku získaly mnohem snazší pozici pro rychlé a plošné nasazení navzdory problematickému posunování hranic informačního soukromí a navýšení intenzity profilování.[507] Zde pak nacházíme potvrzení vazby, která činí trendy v rozvoji internetu věcí vysoce relevantní z hlediska právního rámce ochrany osobních údajů, a s přihlédnutím k dále diskutovaným rizikům pak zvláště pro problematiku bezpečnosti zpracovávaných osobních údajů.

Neopominutelnou složkou internetu věcí, která je výsledkem nových technických možností, ale zároveň předpokladem jejich funkce, je intenzivní a rozsáhlé shromažďování, zpracování a sdílení údajů o uživatelích či jiných jednotlivcích.[508] 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. Může se jednat o čistě technické údaje, o metadata způsobilá za určitých okolností nebo v kombinaci identifikovat jednotlivce[509] nebo o osobní údaje přímo identifikující fyzickou osobu.[510]

Není zároveň vyloučeno, že shromažďování údajů shodným předmětem při plnění shodné funkce může v různých situacích představovat odlišnou míru zásahu do soukromí jednotlivce.[511] Je tudíž možné dovodit, že zařízení propojená pomocí internetu věcí mají potencionál zásadně zasahovat do osobní sféry jednotlivců.[512]

507 Srov. KLEIN, Naomi. Naomi Klein: How big tech plans to profit from the pandemic. *The Guardian* [online]. 2020 [cit. 15. 7. 2021].

508 Srov. TORRE, Ilaria et al. A framework for personal data protection in the IoT. In: *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* [online]. 2016.

509 Např. pohyb před senzorem, druh odebraného výrobku ze zařízení apod. v kombinaci se vzorcem chování daného uživatele nebo jeho virtuálním profilem.

510 Např. biometrické záznamy otisku prstů či tvaru obličeje.

511 Např. při použití v jednočlenné domácnosti v kontrastu s použitím ve veřejně přístupném zařízení.

512 Viz Fact Sheet of the European Commission. IoT Privacy, Data Protection, Information Security. *European Commission* [online]. Brussels: European Commission, 2016, s. 3 [cit. 12. 7. 2021].

Zpracování a sdílení osobních údajů v rámci internetu věcí představuje významný právní aspekt tohoto trendu. Datová propojenost stojí nejen u základu procesů v tomto kontextu, ale zaměření na individualizaci, optimalizaci a ambientní přítomnost podněcuje intenzivní snahy o maximalizaci shromažďovaných údajů a intenzivní kombinaci s údaji z jiných zdrojů za účelem profilování uživatelů či jiných relevantních fyzických osob. Již za účinnosti směrnice 95/46/ES bylo zřejmé, že *„[c]ílem 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."*[513]

Nové výzvy vzhledem k rozmanitosti kontextů a rozšíření M2M komunikace: Skutečnost, že zařízení v rámci internetu věcí často zpracovávají osobní údaje, nepředstavuje sama o sobě zásadně novou problematiku, na kterou by nepostačovalo vztáhnout dosavadní teoretické či praktické závěry a poznatky z oblasti ochrany osobních údajů. To, čím internet věcí představuje novou výzvu v této oblasti, je především nepřeberná různorodost dat, která za rozličných situací mohou být v různé intenzitě vztažena jako osobní údaje k jednotlivci.[514] Tato variabilita se dále umocňuje v situacích, kdy zařízení pro své funkce užívá autonomní komunikace s jinými zařízeními *(machine-to-machine*, M2M[515]*)*, ať již v důsledku možné akumulace osobních údajů, zranitelnosti těchto procesů a komunikace, či prosté nepředvídatelnosti podob a obsahu dílčích zpracování v důsledku rostoucí procesní autonomie zařízení.

513 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. wp223_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2014, s. 4 [cit. 12. 7. 2021].

514 Srov. KOZLOV, Denis, Jari VEIJALAINEN a Yasir ALI. Security and privacy threats in IoT architectures. In: *Proceedings of the 7th International Conference on Body Area Networks*. Oslo, Norway: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, s. 252 a násl. BodyNets '12.

515 Blíže k pojmu viz ANTON-HARO, Carles a Mischa DOHLER. *Machine-to-machine (M2M) Communications: Architecture, Performance and Applications*. Cambridge: Elsevier, 2014, s. 1–4.

Dalším významným faktorem, kterým se vyznačuje kontext internetu věcí, je potencionální všudypřítomnost zpracování, čímž dochází prakticky ke stavu, kdy subjekt údajů nemá nejen kontrolu, ale často ani povědomí o rozsahu zpracování, kterých je v daném okamžiku předmětem.[516] Zde lze pak zvláště 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.

Pro rámec ochrany osobních údajů představuje absence povědomí jednotlivce o skutečnosti, že v daném kontextu dochází či může docházet ke zpracování jeho osobních údajů, zásadní nedostatek.[517] Pracovní skupina dle článku 29 (nyní Sbor) k tomu uvádí, že *„[t]aková 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.“*[518] Domnívám se, že ještě významnějším problémem je nevědomost subjektu údajů v případě, že hrozí porušení bezpečnosti zpracovávaných údajů. Tím je podtrhován přetrvávající význam notifikačních povinností i v kontextu internetu věcí.

Právní konstrukce oprávněného zpracování údajů pak často v těchto situacích naráží na své limity, které lze jen stěží překonat extenzivním výkladem.[519] Jak výstižně shrnula Pracovní skupina dle článku 29 (nyní Sbor), *„[p]okud 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*

516 Srov. COSTA, Luiz. *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*. Cham: Springer International Publishing, 2016, s. 17.

517 Srov. ABDMEZIEM, Riad a Djamel TANDJAOUI. Internet of Things: Concept, Building blocks, Applications and Challenges. *ArXiv* [online]. 2014, roč. 2014.

518 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. wp223_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2014, s. 8 [cit. 12. 7. 2021].

519 Pro bližší vymezení nedostatků evropské koncepce práva ochrany osobních údajů, především s ohledem na přílišný důraz na souhlas subjektů, viz RUBINSTEIN, Ira S. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* [online]. 2013, roč. 3, č. 2.

funkcí."[520] Problematikou předvídatelnosti shromažďování osobních údajů pro subjekt údajů a vymezením rovnováhy mezi ochranou subjektů osobních údajů a efektivním využitím těchto údajů nejen v tomto kontextu se zabývala a zabývá řada autorů.[521] V tomto směru se také otevírá prostor pro diskusi o uplatnění a vymezení zásady omezení účelu, pro který byly osobní údaje shromážděny. Tato zásada doznala v Obecném nařízení úpravy, které předcházela rozsáhlá debata, jejímž výsledkem je znění článku 6 odst. 4 Obecného nařízení.[522] Podrobnější rozbor této problematiky je však nad rámec tématu této monografie.

Příklad nárůstu hrozeb v důsledku rozvoje internetu věcí u kamerových systémů: Kamerové systémy jsou typickým příkladem technického zařízení pro zpracování osobních údajů, na kterém byly testovány výše nastíněné limity právní úpravy ochrany osobních údajů co do přípustného účelu a rozsahu.[523] Doposud převažovala analýza rizik spojených s tímto zpracováním v návaznosti na činnosti příslušného správce. Převažujícím technologickým řešením byly totiž kamerové systémy na uzavřených lokálních okruzích *(closed-circuit television*, CCTV[524]*)*, které tudíž byly vystaveny pouze omezenému spektru vnějších rizik porušení bezpečnosti a zneužití příslušných záznamů.

Tato realita se však velmi rychle mění, jelikož mnoho kamerových systémů přechází na formát online konektivity a stává se tak součástí internetu věcí. Společnost *Gartner* pokládá trh s venkovními bezpečnostními kamerami za největší současnou složku trhu s koncovými zařízeními internetu věcí

520 Srov. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. wp223_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2014, s. 8 [cit. 12. 7. 2021].

521 Předně NISSENBAUM, Helen. Privacy As Contextual Integrity. *Washington Law Review*, 2004, roč. 79; Dále pak např. CUSTERS, Bart a Helena URŠIČ. Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection. *International Data Privacy Law;* [online]. 2016 [cit. 15. 7. 2021].

522 Blíže viz ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 03/2013 on purpose limitation* [online]. wp 203. Brussels: Article 29 Data Protection Working Party, 2013, s. 3 [cit. 12. 7. 2021].

523 Srov. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. K provozování kamerových systémů. *Úřad pro ochranu osobních údajů* [online]. 2. 5. 2018 [cit. 15. 7. 2021]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099

524 Blíže k pojmu např. ARMSTRONG, Gary a Clive NORRIS. *The Maximum Surveillance Society: The Rise of CCTV.* 1. vyd. Oxford; New York: Berg Publishers, 1999.

a předpokládá trvalý růst zájmu o tato zařízení, dále doplněný o nárůst množství kamerových systémů zabudovaných do vozidel.[525]

Dosavadní pojetí přípustného nastavení a potřebných opatření kamerových systémů, především co do bezpečnosti, se s tímto taktéž významně posouvají. Internetová konektivita těchto zařízení přináší množství nových bezpečnostních hrozeb, které staví tato zařízení do značné míry na roveň osobním počítačům či mobilním telefonům, avšak při převažující absenci odpovídajících bezpečnostních prvků.[526] To s sebou přináší i předpoklad častějších, významnějších a rozsáhlejších případů porušení bezpečnosti, které však nemusí být provozovateli kamerových systémů snadno odhalitelné, a proto může zůstávat působená újma subjektům údajům skryta.

Ambientní povaha zařízení internetu věcí: Riziko tohoto scénáře pak zvláště roste ve spojení s ambientními prvky internetu věcí,[527] u kterých je nepravděpodobné, že na ně budou subjekty údajů řádně upozorněny a budou tedy moci předvídat hrozby spojené s daným zpracováním. Již nyní, a zvláště pak do budoucna, přitom není vyloučeno, že kdejaké domácí zařízení či předmět osobní potřeby (např. zrcadlo,[528] zámek,[529] sprcha[530] či šatní

525 Viz GARTNER. Press release: Gartner Predicts Outdoor Surveillance Cameras Will Be Largest Market for 5G Internet of Things Solutions Over Next Three Years. *Newsroom* [online]. 17. 10. 2019 [cit. 15. 7. 2021]. Dostupné z: https://www.gartner.com/en/newsroom/press-releases/2019-10-17-gartner-predicts-outdoor-surveillance-cameras-will-be

526 K těmto hrozbám blíže viz BUGEJA, Joseph, Désirée JÖNSSON a Andreas JACOBSSON. An Investigation of Vulnerabilities in Smart Connected Cameras. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* [online]. 2018; CIMPANU, Catalin. New IoT Botnet Rises Feeding on Vulnerable Security Cameras. *BleepingComputer* [online]. 25. 4. 2017 [cit. 15. 7. 2021]. Dostupné z: https://www.bleepingcomputer.com/news/security/new-iot-botnet-rises-feeding-on-vulnerable-security-cameras/

527 Např. skrytá čidla na pracovišti či ve veřejně přístupných prostorách budov.

528 Srov. HOSSAIN, Anwar M., Pradeep K. ATREY a Abdulmotaleb El SADDIK. *Smart mirror for ambient home environment* [online]. 2007.

529 Srov. PARK, Yong Tae, Pranesh STHAPIT a Jae-Young PYUN. Smart digital door lock for the home automation. In: *TENCON 2009 – 2009 IEEE Region 10 Conference*: *TENCON 2009 – 2009 IEEE Region 10 Conference* [online]. 2009.

530 Srov. RODRIGUES, Rodolfo R. et al. An IoT-based Automated Shower System for Smart Homes. In: *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* [online]. 2018.

skříň[531]) bude mimo svého běžného určení také v určité míře zpracovávat též data (a často tak i osobní údaje).

Bude tedy daleko znatelněji než dnes nad možnosti (nejen) běžného uživatele rozpoznat, v jaké míře je jeho konání, byť v rámci prostorového soukromí jeho obydlí, transponováno do specifické digitální stopy. Přitom se zdůvodněním zlepšování uživatelského prožitku *(user experience)* lze předpokládat absenci „rušivých" průběžných upozornění o zpracování osobních údajů. Důsledkem je tudíž již zmiňovaná ambience, kterou internet věcí přináší do utváření datových záznamů o uživatelích. Při absenci povědomí o rozsahu zpracování, či o zpracování jako takovém, přitom významně narůstají rizika spojená s asymetrickou informací o případném porušení bezpečnosti osobních údajů. Nabývá tudíž na významu nejen role dozorového úřadu v zajištění důsledného dodržování povinností dle článku 32 Obecného nařízení a implementace přiměřených bezpečnostních opatření, ale též přínos včasné a důsledné notifikace případu porušení bezpečnosti.

Rizikovost zpracování osobních údajů v daném kontextu přitom dále zesiluje provázanost s technologií *cloud computingu*,[532] umožňujícího vytváření databází *big data*[533] a jejich následného vytěžování,[534] především pak za využití strojového učení a navazujících rostoucích uplatnění umělé inteligence.[535] Využití cloudových úložišť je součástí řady systémů internetu věcí[536] a kontinuální

531 Srov. LING, Sea, Maria INDRAWAN-SANTIAGO a Seng LOKE. RFID-based user profiling of fashion preferences: Blueprint for a smart wardrobe. *IJIPT* [online]. 2007, roč. 2.

532 Srov. MELL, Peter a Timothy GRANCE. *The NIST Definition of Cloud Computing* [online]. Gaithersburg, MA: National Institute of Standards and Technology, 2011, Special Publication 800-145 [cit. 15. 7. 2021].

533 Srov. MCAFEE, Andrew a Erik BRYNJOLFSSON. Big Data: The Management Revolution. *Harvard Business Review* [online]. 2012, October, s. 61 a násl. [cit. 15. 7. 2021].

534 Srov. FREITAS, Alex A. Data Mining Tasks and Concepts. In: FREITAS, Alex A. (ed.). *Data Mining and Knowledge Discovery with Evolutionary Algorithms* [online]. Berlin, Heidelberg: Springer, 2002, s. 13 a násl., Natural Computing Series [cit. 15. 7. 2021].

535 Srov. GORBENKO, Anna a Vladimir POPOV. Self-Learning Algorithm for Visual Recognition and Object Categorization for Autonomous Mobile Robots. In: HE, Xingui et al. (eds.). *Computer, Informatics, Cybernetics and Applications* [online]. Dordrecht: Springer Netherlands, 2012, s. 1289 a násl., Lecture Notes in Electrical Engineering.

536 Srov. CHAN, Mike. Why Cloud Computing is the Foundation of the Internet of Things. *Thorn Technologies* [online]. 15. 2. 2017 [cit. 15. 7. 2021]. Dostupné z: https://www.thorn-tech.com/2017/02/cloud-computing-foundation-internet-things/

sdílení dat mezi cloudovým úložištěm a sítí zařízení je vnímáno jako jedno z řešení omezené výpočetní a úložní kapacity jednotlivých zařízení.[537, 538]

Přístup uživatelů k ochraně osobních údajů a zesilující efekt internetu věcí: Interakci uživatelů s prvky internetu věcí přitom lze vnímat jako navazující na etablované vzorce a vztahy při užívání online služeb či mobilních aplikací. To je taktéž specifická oblast, kde dochází k problematickému nastavení parametrů zpracování osobních údajů, jelikož si zpravidla poskytovatelé těchto služeb a aplikací na základě značně jednostranných všeobecných smluvních podmínek zajišťují přístup k rozsáhlým souborům uživatelských osobních údajů, které jsou následně běžně obchodovány na trhu agregovaných dat pro nejrůznější účely.[539] Přestože unijní právní rámec ochrany osobních údajů dlouhodobě směřuje proti těmto postupům a nabízí normativní podklad pro posílení pozice jednotlivce při ochraně jeho osobních údajů, nelze vnímat současnou situaci na tomto poli za zvláště příznivou, což potvrzuje i nedávná studie *Claessona* a *Bjorstada* pro Norskou radu spotřebitelů *(Norwegian Consumer Council)*.[540]

Tato monografie potvrzuje domněnku, že většina uživatelů online služeb si stále není vědoma rozsahu, v jakém po sobě jejich užíváním zanechávají datovou stopou, a v jaké intenzitě je tato následně analyzována a zpracovávána celým odvětvím komerčních subjektů. Je tedy dle mého názoru nemístné se domnívat, že by data vyprodukovaná v rámci internetu věcí měla odlišný osud. Z toho lze tudíž extrapolovat, že situace uživatelů v kontextu srovnatelných služeb v rámci internetu věcí nebude příliš příznivější a nedostatky, které přetrvávají v systému ochrany osobních údajů ve vztahu k těmto formám zpracování, budou přeneseny společně s rozšířením služeb a aplikací do kontextu internetu věcí. Jak k tomu uvádí Pracovní skupina dle článku 29 (nyní Sbor), *„[n]árůst množství údajů vytvářených internetem věcí v kombinaci s moderními technikami souvisejícími s analýzou údajů a jejich křížovým přiřazováním může vést k sekundárnímu využívání těchto údajů, které může i nemusí*

537 Srov. VILLARI, Massimo et al. Osmotic Computing: A New Paradigm for Edge/Cloud Integration. *IEEE Cloud Computing* [online]. 2016, roč. 3, č. 6, s. 76 a násl.

538 Více pozornosti této perspektivě věnuji dále v oddílu 4.4.1.

539 Viz SPIEKERMANN, Sarah et al. The challenges of personal data markets and privacy. *Electronic Markets* [online]. 2015, roč. 25, č. 2, s. 161 a násl.

540 Srov. CLAESSON, Andreas a Tor E. BJØRSTAD. *"Out of Control" – A Review of Data Sharing by Popular Mobile Apps* [online]. 1.0. Oslo: Norwegian Consumer Council, 2020, s. 2 [cit. 15. 7. 2021].

souviset s účelem, k němuž bylo určeno jejich původní zpracování."[541] Tento vývoj je ostatně již dnes zaznamenán v souvislosti s osobními asistenty,[542] chytrými hračkami[543] či chytrými náramky.[544]

4.3 Problematika zajištění bezpečnosti osobních údajů v kontextu internetu věcí

Vedle vlastního nárůstu četnosti a různorodosti forem zpracování osobních údajů je hlavním zdrojem rizik pro práva a zájmy fyzických osob v rámci internetu věcí nedostatečná úroveň bezpečnosti u těchto zařízení. *Schneier* k tomu uvádí, že *„[b]ezpečnost je vždy záležitostí kompromisu. Často je jím bilancování bezpečnosti a pohodlí, ale někdy je to též bezpečnost na úkor vlastností či výkonnosti. To, že upřednostňujeme tyto ostatní hodnoty před bezpečností je hlavním důvodem, proč jsou počítače zranitelné, ale je též pravdou, že zabezpečení počítačů je skutečně obtížné.*"[545] U prvků internetu věcí je přitom kompromis na úkor bezpečnosti široce diskutovaným problémem.[546] U řady výrobků jsou již dnes zdokumentované četné zranitelnosti a bezpečnostní nedostatky.[547]

541 Srov. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. wp223_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2014, s. 9 [cit. 12. 7. 2021].

542 Viz CHEE, Foo Yun. Amazon's Alexa comes under scrutiny of Luxembourg privacy watchdog. *Reuters* [online]. 2019 [cit. 15. 7. 2021].

543 Srov. MYRSTAD, Finn. Connected toys violate European consumer law. *Forbrukerrådet* [online]. 6. 12. 2016 [cit. 15. 7. 2021]. Dostupné z: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

544 Srov. PAUL, Kari. "Tossed my Fitbit in the trash": users fear for privacy after Google buys company. *The Guardian* [online]. 2019 [cit. 15. 7. 2021].

545 *„Security is always a trade-off. Often it's security versus convenience, but sometimes it's security versus features or security versus performance. That we prefer all of those things over security is most of the reason why computers are insecure, but it's also true that securing computers is actually hard."* Srov. SCHNEIER, Bruce. *Click here to kill everybody.* New York: W.W. Norton & Company, 2018, s. 19.

546 Srov. FERNANDES, Earlence et al. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? *IEEE Security Privacy* [online]. 2017, roč. 15, č. 4; OORSCHOT, Paul C. van a Sean W. SMITH. The Internet of Things: Security Challenges. *IEEE Security Privacy* [online]. 2019, roč. 17, č. 5; SADEGHI, Ahmad-Reza, Christian WACHSMANN a Michael WAIDNER. Security and privacy challenges in industrial Internet of Things. In: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* [online]. 2015.

547 Viz SCHNEIER, Bruce. The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters. *Schneier on Security* [online]. 25. 7. 2016 [cit. 15. 7. 2021]. Dostupné z: https://www.schneier.com/essays/archives/2016/07/the_internet_of_thin_3.html

Vzhledem k technickým limitům zajištění jejich bezpečnosti, ať již s přihlédnutím k omezené kapacitě baterií, nízkému výkonu mikroprocesorů či omezené softwarové výbavě zařízení je implementace přiměřených bezpečnostních opatření zpravidla ve střetu s dosažením komerčně udržitelných výrobních nákladů. Tyto výzvy sice dávají prostor pro řadu inovativních řešení pro překonání těchto limitů, ať již na poli kryptografie[548] či skrze adaptivní bezpečnostní modely,[549] avšak daleko spíše vedou k nízké úrovni bezpečnosti bez ohledu na výsledná rizika pro data uživatelů.

Není to ovšem zcela tak, že by internet věcí přinášel zásadní nové technické výzvy na poli kyberbezpečnosti. Podstatným momentem je především rozšíření spektra produktů, pro které se kyberbezpečnost stává nepominutelným prvkem. Co dříve bylo specifikem vývoje a optimalizace osobních počítačů či mobilních telefonů je do budoucna nutno vnímat jako součást životního cyklu produktů sahajících od automobilů po rozvodny elektřiny.[550] Na rozdíl od společností působících na trhu s informačními technologiemi však v řadě odvětví, ať již jde o automobilový či hračkářský průmysl, nemají zde působící podniky zpravidla srovnatelné know-how na poli kyberbezpečnosti a jeho nabytí „za pochodu" je do značné míry charakterizující pro rozvoj internetu věcí.[551]

Jak bylo již nastíněno výše, s rostoucí všudypřítomností propojených zařízení narůstá složitost systému, který má být zabezpečen.[552] Složitost činí zajištění bezpečnosti náročnější, jelikož znamená více prvků, více interakcí, větší množství chyb a vyšší pravděpodobnost selhání uživatelů, např. používáním výchozího hesla či špatnou konfigurací sdílení dat.[553]

Specifickou výzvou je pak vytváření, a především aktualizace, firmware a záplatování softwarového vybavení. U zařízení internetu věcí je běžně očekávána

548 Viz PREMNATH, Sriram N. a Zygmunt J. HAAS. Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model. *IEEE Wireless Communications Letters* [online]. 2015, roč. 4, č. 3.

549 Viz AMAN, Waqas a Einar SNEKKENES. Managing security trade-offs in the Internet of Things using adaptive security. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* [online]. 2015.

550 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 8.

551 Srov. NEWMAN, Lily Hay. Medical Devices Are the Next Security Nightmare. *Wired* [online]. 2017 [cit. 15. 7. 2021].

552 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 7.

553 Ibid., s. 27.

dlouholetá funkčnost na základě jednoduchých přednastavených algoritmů, které ovšem nemusí umožňovat dodatečné aktualizace či úpravy.[554] I při jejich možnosti je pak nutno potýkat se s tržní realitou, která může přinést zánik společnosti, která aktualizace poskytovala[555] či absenci racionální motivace výrobců poskytovat dlouhodobou podporu starším výrobkům.[556] Při odhlédnutí od těchto dodatečných překážek na poli internetu věcí je pak nutné brát v potaz, že ani dnes není instalace aktualizací a oprav software u běžných zařízení, i při jejich dostupnosti, ze strany uživatelů ani příliš důsledná a ani včasná. Důvodem může být jejich pohodlí, neznalost či nedůvěra v přínos těchto aktualizací.[557]

Boom funkcionalit těchto zařízení přitom znamená větší množství software, který může obsahovat zranitelnosti, ať již na základě nízké úrovně provedeného programování nebo v důsledku rozsáhlého využívání již existujícího kódu *(code reuse)*[558].[559] Softwarová vybavenost zařízení internetu věcí pak činí tyto produkty zranitelné v podstatě stejným způsobem jako počítače, ať již jde o riziko malware, ransomware, navázání do botnetu či jiné formy porušení bezpečnosti zařízení a v něm zpracovávaných údajů.[560]

Řada těchto hrozeb má přitom charakter prolomení bezpečnostních opatření celé třídy produktů *(class break)*, kdy automatizovaný útok na určitou známou zranitelnost může ohrozit miliony zařízení, kterým je společná.[561]

554 Srov. ROMAN, Rodrigo, Jianying ZHOU a Javier LOPEZ. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* [online]. 2013, roč. 57, č. 10, Towards a Science of Cyber Security, s. 2266 a násl.

555 Srov. FINLEY, Klint. Nest's Hub Shutdown Proves You're Crazy to Buy Into the Internet of Things. *Wired* [online]. 2016 [cit. 15. 7. 2021].

556 To je ostatně realitou i ve vztahu k výrazně složitějším zařízením. Uvažte např. limity podpory starších operačních systémů pro osobní počítače či chytré telefony. Pro srovnatelné zkušenosti z prostředí zařízení internetu věcí viz Internet of Things. Privacy & Security in a Connected World. *Federal Trade Commission* [online]. Washington D.C.: Federal Trade Commission, 2015, s. 13–14, FTC Staff Report [cit. 14. 7. 2021].

557 Pro srovnání s tím, o kolik méně pravděpodobná je uživatelská důslednost u ambientních zařízení internetu věcí zvažte, kdo pravidelně kontroluje a instaluje aktualizace firmware na svém domácím routeru. Srov. SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 36–37.

558 Srov. ZEESHAN, Afzaal Ahmad. What Code Reuse is and Why We Use It. *C#Corner* [online]. 28. 3. 2015 [cit. 15. 7. 2021]. Dostupné z: https://www.c-sharpcorner.com/uploadfile/201fc1/what-is-code-reuse-and-why-we-use-it/

559 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 21.

560 Ibid., s. 26.

561 Ibid., s. 31.

Mezi mediálně nejznámější příklady takovýchto útoků cílících na zařízení internetu věcí se řadí botnet *Mirai*,[562] ransomware *WannaCry*[563] či malware *NotPetya*.[564] Riziko těchto útoků je významně znásobeno snadnou dostupností tohoto a mnoha dalšího škodlivého software, díky čemuž mohou automatizované či sofistikované kybernetické útoky provádět i „hackeři" s minimálními schopnostmi (tzv. *script kiddie*).[565] Na tržištích *dark webu*[566] je dnes velmi snadné (a levné) si za kryptoměny pořídit sofistikované malwarové nástroje.[567] To pouze umocňuje rizika, která přináší rozšiřování digitalizace a konektivity skrze rozmach internetu věcí.

4.4 Specifika porušení bezpečnosti v kontextu internetu věcí

Výše nastíněné charakteristiky prostředí z hlediska zajištění bezpečnosti a rozsahu zpracování osobních údajů se promítají do specifických výzev pro dodržování právních povinností spojených s porušením bezpečnosti zpracovávaných údajů.

562 Srov. CLOUDFLARE. What is the Mirai Botnet? *Cloudflare* [online]. 2020 [cit. 22. 5. 2021]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/; FRUHLINGER, Josh. The Mirai botnet explained: How IoT devices almost brought down the internet. *CSO Online* [online]. 9. 3. 2018 [cit. 22. 5. 2021]. Dostupné z: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

563 Srov. KASPERSKY. What is WannaCry ransomware? *Kaspersy* [online]. 6. 11. 2019 [cit. 22. 5. 2021]. Dostupné z: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry; WHITTAKER, Zack. Two years after WannaCry, a million computers remain at risk. *TechCrunch* [online]. 12. 5. 2019 [cit. 22. 5. 2021]. Dostupné z: https://social.techcrunch.com/2019/05/12/wannacry-two-years-on/

564 Viz GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired* [online]. 2018 [cit. 22. 5. 2021]; MCAFEE. What Is Petya and NotPetya Ransomware? [online]. 2020 [cit. 22. 5. 2021]. Dostupné z: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html

565 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 30.

566 Jedná se o část sítě Internet, která není dohledatelná skrze tradiční internetové vyhledávače, ale pouze za využití specifických nástrojů, jakým je například prohlížeč Tor. Blíže viz GUCCIONE, Darren. What is the dark web? How to access it and what you'll find. *CSO Online* [online]. 5. 3. 2020 [cit. 15. 7. 2021]. Dostupné z: https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html; CHERTOFF, Michael. A public policy perspective of the Dark Web. *Journal of Cyber Policy* [online]. 2017, roč. 2, č. 1.

567 Srov. CISOMAG. Darknet Markets Make Malware Buying Easy: Research. *Cyber Security Magazine* [online]. 2020 [cit. 22. 5. 2021].

Jelikož však je prostředí internetu věcí jako takové vysoce komplexní a různorodé, nevnímám výše nastíněné přiblížení problematiky za dostatečně podrobné pro účely této monografie. Shledávám totiž, že i vzhledem ke zpracování osobních údajů v tomto prostředí vystupuje do popředí několik významných aspektů, na které však nelze důsledně poukázat pouze na jednom scénáři. Pro jejich adekvátní rozbor a představení jsem tudíž na základě prvotní rešerše a studia dostupných materiálů zvolil tři významné perspektivy rozvoje internetu věcí, z nichž každá poukazuje na jiná specifika, která je na místě zohlednit při diskusi dopadů rozvoje internetu věcí na plnění povinností spojených s porušením bezpečnosti zpracovávaných údajů. Společně pak poskytují širokou škálu situací, které mohou představovat významné hrozby pro zpracování osobních údajů v kontextu internetu věcí.

Dopad automatizované komunikace na rozsah sdílení osobních údajů mezi zařízeními: První rovinou, která bude takto přiblížena, je automatizovaná komunikace mezi zařízeními a rozmach autonomně činných zařízení. Cílem je poukázat na centrálnost aspektu konektivity a sdílení osobních údajů v rámci internetu věcí. Snažím se tak dokreslit několik již zmíněných charakteristik tohoto prostředí. Shledávám za významné zdůraznit, že internet věcí nestojí na pouhém shromažďování osobních údajů zařízeními skrze senzory a následném zpracování, ale že je to právě sdílení těchto údajů mezi zařízeními a databázemi *big data*, které umožňuje optimalizovat a individualizovat poskytované služby cestou profilování. Zpracování osobních údajů zde tudíž probíhá v řadě navazujících rovin, které v důsledku propojenosti vystavují subjekty údajů novým rizikům a představují výzvu pro adekvátní bezpečnostní opatření.

Dynamika interakce v rámci chytrého města a *ad hoc* zpracování společnými správci: Jak však má za cíl naznačit druhá rovina, tato komunikace často je a bude vysoce proměnlivá, charakterizována složitou sestavou interagujících zařízení a nestálostí subjektů, které se na daném zpracování podílejí především v roli společných správců. Na množinu vrstev těchto síťových vztahů a jejich rostoucí *ad hoc* charakter nahlížím skrze koncept chytrého města.

Mikropodniky a jejich opomíjený význam: V tomto i v ostatních kontextech internetu věcí přitom v podstatě figurují tři kategorie subjektů. Předně

jde o subjekty údajů, kteří jsou buďto aktivními uživateli nebo pasivně zaznamenávanými „profilovými prvky". Dále lze pak předpokládat, že dominantní roli v tomto prostředí bude podobně jako v dosavadním rozvoji služeb informační společnosti v kyberprostoru zaujímat omezený okruh nadnárodních technologických společností, které nabídnou do značné míry ucelená řešení výrobků a služeb.[568] Nelze však opomíjet pozici a roli početní většiny ostatních správců a zpracovatelů, kteří budou nabízet dílčí prvky, služby či zařízení. Mikropodniky, tedy podniky s méně než 10 zaměstnanci a ročním obratem či rozvahou nižší než 2 miliony EUR, které tvoří významnou většinu podnikatelských subjektů v EU, budou také začleňovat prvky internetu věcí do svých podnikových sítí a využívat je pro nabízení či zlepšování svých služeb. Budou se tak, dle mého názoru, často nacházet v pozici odpovědného správce osobních údajů, který bude povinen zhodnotit dopad a bezpečnostní rizika spojená s implementací prvků internetu věcí a podniknout přiměřená opatření pro jejich omezení. S ohledem na množství mikropodniků a výše nastíněnou složitost zajištění bezpečnosti internetu věcí přitom bude mít dodržování povinností pojících se s porušením bezpečnosti u těchto správců rostoucí význam i pro celkové udržování vysoké úrovně bezpečnosti u velkých podniků, pro které mohou být interakce a vazby s nimi skrytou formou zranitelnosti.

Na základě poznatků z těchto perspektiv a výše představených obecných aspektů zpracování osobních údajů v kontextu internetu věcí zformuluji následně v podkapitole 4.5 hlavní formy proměny, které toto prostředí přináší do problematiky porušení bezpečnosti zpracovávaných údajů. Na to následně navazuji diskusí v podkapitole 4.6.

4.4.1 Automatizovaná komunikace mezi stroji a prostředí autonomních zařízení

S nárůstem významu zařízení s prvky umělé inteligence, ať již jde o roboty, chytrá vozidla či jiná autonomní zařízení, získává na relevanci zohlednění specifik činností a interakce těchto zařízení nejen se svým okolím, ale též mezi

568 Srov. MOORE, Martin a Damian TAMBINI. *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*. Oxford: Oxford University Press, 2018, s. 43; POWLES, Julia a Jat SINGH. Why the internet of things favours dominance. *The Guardian* [online]. 2015 [cit. 20. 5. 2021].

sebou.[569] V rámci tohoto oddílu jsou primárně zkoumány možné důsledky rozšíření těchto zařízení pro frekvenci, intenzitu a různorodost případů porušení bezpečnosti osobních údajů.

Za tímto účelem je představen možný dopad implementace technologie 5G na existující technologické standardy. Diskutovaný kontext se týká především automatizované komunikace mezi zařízeními (*machine-to-machine, M2M*) v rámci konceptů průmyslu 4.0, chytrého města či prostředí chytrého domova. S ohledem na zaměření monografie je přitom pozornost soustředěna na souvislosti s povinnostmi dle článků 33 a 34 Obecného nařízení.

Existuje několik klíčových technologických předpokladů, které umožnily příchod doby internetu věcí. Ty se týkají předně možnosti ekonomicky masově vyrábět výpočetní a komunikační moduly, které mohou být vloženy do jednotlivých výrobků a dodávat jim dodatečné funkce.[570] Výzvy v tomto směru představovala například výkonnost mikroprocesorů,[571] optimalizace spotřeby energie[572] či efektivita komunikace s těmito moduly.[573] Přesto však hlavní přínos z provozování souborů takovýchto zařízení spočívá v jejich propojenosti. Na významu tudíž získávají příslušné standardy a protokoly bezdrátové komunikace.

Komunikační standardy pro internet věcí: Tato oblast rozvoje internetu věcí zaznamenala v předchozích letech vytvoření dvou hlavních standardů pro komunikační technologie. Jde o eMTC (*enhanced Machine Type Communication*, často zahrnovaný pod širší kategorii LTE-M (*Long-Term Evolution for Machines*))

569 Srov. THE ECONOMIST. The Splinternet of Things threatens 5G's potential. *The Economist* [online]. 2019 [cit. 15. 7. 2021].

570 Srov. WORLD ECONOMIC FORUM. *Accelerating the Impact of IoT Technologies* [online]. Cologny: World Economic Forum. 2018 [cit. 17. 10. 2021]. *Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities*.

571 Srov. ADEGBIJA, Tosiron et al. Microprocessor Optimizations for the Internet of Things: A Survey. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* [online]. 2018, roč. 37, č. 1, s. 7 a násl.

572 Viz EL-RAZEK, Mohamed Abd, M. B. ABDELHALIM a Hanady H. ISSA. Dynamic power reduction of microprocessors for IoT applications. In: *2016 28th International Conference on Microelectronics (ICM)*: *2016 28th International Conference on Microelectronics (ICM)* [online]. 2016.

573 Srov. PURKOVIC, Dalibor, Marian HÖNSCH a Tobias Raphael Maria Karl MEYER. An Energy Efficient Communication Protocol for Low Power, Energy Harvesting Sensor Modules. *IEEE Sensors Journal* [online]. 2019, roč. 19, č. 2, s. 701.

a NB-IoT *(Narrowband Internet of Things)*.[574] Oba jsou dílem *3rd Generation Partnership Project* (3GPP),[575] tedy přední mezinárodní organizace pro standardizaci v oblasti mobilních technologií, která zajišťuje kompatibilitu prvků elektronických komunikací a zařízení napříč předními světovými trhy. Dle údajů *Global Mobile Suppliers Association* (GSA) přes 175 operátorů v 72 zemích v roce 2021 spustili sítě s podporou těchto standardů.[576]

Každý z těchto standardů je vytvořen pro odlišný segment komunikace v rámci internetu věcí. NB-IoT poskytuje nízkou rychlost přenosu dat, krátký dosah a možnost vysoké hustoty komunikace. Je tedy vhodný pro hustě obydlené prostředí s vysokou koncentrací zařízení, která jsou nenákladná a vyžadují nízkou spotřebu energie.[577] Výhodou tohoto standardu je také dobré pokrytí v budovách, využití tedy nachází např. v řešeních chytré domácnosti či správě životního cyklu domácích spotřebičů.[578] LTE-M oproti tomu nabízí relativně vysokou rychlost přenosu dat, je vhodný pro zařízení v pohybu a umožňuje přenos hlasu po síti, je však současně náročnější na potřebné využití šířky pásma a spotřebu energie.[579] Obecně tak poskytuje bezpečnou a výhodnou alternativu pro mnoho aplikací, kde by jinak bylo zapotřebí připojení k síti za pomoci Wi-Fi.[580]

Výše představené standardy umožnily „první generaci" zařízení internetu věcí, zvláště pak spotřebitelské produkty pro prostředí chytré domácnosti[581]

574 Viz 3GPP. Standards for the IoT. *The Mobile Broadband Standard* [online]. 2016 [cit. 16. 9. 2021]. Dostupné z: https://www.3gpp.org/news-events/1805-iot_r14

575 Viz 3GPP. About 3GPP. *The Mobile Broadband Standard* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.3gpp.org/about-3gpp

576 Viz GSA. More than 175 5G Commercial Networks Launched in 72 Countries/Territories totaltelecom [online]. 23. 8. 2021 [cit. 18. 10. 2021]. Dostupné z: https://www.totaltele.com/510680/GSA-More-than-175-5G-Commercial-Networks-Launched-in-72-CountriesTerritories

577 Viz SHARETECHNOTE. NB-IoT. *LTE Quick Reference* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: http://www.sharetechnote.com/html/Handbook_LTE_NB_LTE.html

578 Srov. NB-IoT Commercialisation Case Study: How China Mobile, China Telecom and China Unicom Enable Million More IoT Devices. *GSMA* [online]. 2019 [cit. 16. 9. 2021].

579 Viz LIGERO, Raquel. Differences between NB-IOT and LTE-M. *Accent Systems* [online]. 3. 5. 2018 [cit. 16. 9. 2021]. Dostupné z: https://accent-systems.com/blog/differences-nb-iot-lte-m/

580 Srov. GSMA. *LTE-M Commercialisation Case Study: How AT & T and Telstra Connect Million More IoT Devices* [online]. 2019 [cit. 16. 9. 2021].

581 Viz SOLIMAN, Moataz et al. Smart Home: Integrating Internet of Things with Web Services and Cloud Computing. In: *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*: *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* [online]. 2013.

nebo základní nástroje pro zvýšení efektivity v pracovním prostředí.[582] Jsou zde však limity pro využití těchto bezdrátových komunikačních standardů, která brání širšímu nasazení *„mesh"*[583] síťových řešení (pojem vysvětlím dále v textu), která by umožnila významnější „mezní přínosy" pojící se s rozmachem internetu věcí.[584] Řešením této překážky se zdá být nová generace standardů pro telekomunikační technologie nesoucí označení 5G.

V současné době je mnoho podnikatelských oblastí plno očekávání ohledně standardů 5G, které byly prvotně specifikovány ve výstupu 3GPP Release 15 v roce 2019,[585] plně upraveny pak v následujícím Release 16, který byl dokončen v polovině roku 2021.[586] Mnohými je tato technologie vnímána jako nezbytný aktivátor boomu internetu věcí a související digitální transformace mnoha podnikatelských modelů.[587] Širší komerční využití technologie 5G se očekává již brzy,[588] lze uvést příklady prvních síťových rámců z počátku roku 2020, které byly implementovány v Jižní Koreji či Singapuru.[589]

Hlavní výhodou, která se pojí s touto novou generací síťové technologie je významné navýšení rychlosti přenosu dat, značné snížení latence

582 Viz BACHLECHNER, Daniel et al. *IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht* [online]. Berlin: Bundesministerium für Wirschaft und Energie. 2016 [cit. 25. 5. 2021]; DIGITAL TRANSFORMATION MONITOR. *Germany: Industrie 4.0* [online]. Brusel: Evropská komise. 2017 [cit. 5. 8. 2021].

583 Srov. YU LIU et al. Wireless Mesh Networks in IoT networks. In: *2017 International Workshop on Electromagnetics: Applications and Student Innovation Competition* [online]. 2017.

584 Viz The Internet of Things will bring the internet's business model into the rest of the world. *The Economist* [online]. 2019 [cit. 17. 10. 2021].

585 Viz 3GPP. Release 15. *The Mobile Broadband Standard* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.3gpp.org/release-15

586 Viz 3GPP. Release 16. *The Mobile Broadband Standard* [online]. 2020 [cit. 12. 7. 2021]. Dostupné z: https://www.3gpp.org/release-16

587 Viz LOOZEN, Tom a Adrian BASCHNONGA. In the next wave of telecoms, are bold decisions your safest bet? *EY* [online]. 11/2019 [cit. 16. 9. 2021]. Dostupné z: https://www.ey.com/en_gl/tmt/in-the-next-wave-of-telecoms-are-bold-decisions-your-safest-bet

588 Viz COLLELA, Paolo. 5G and IoT: Ushering in a new era. *Ericsson* [online]. 27. 6. 2017 [cit. 16. 9. 2021]. Dostupné z: https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/5g-and-iot-ushering-in-a-new-era

589 Srov. ALSHAHAB, Sharifah Fadhilah a Derrick A. PAULO. After seven months, here's what South Korea can teach us about 5G. *CNA* [online]. 11/2019 [cit. 16. 9. 2021]. Dostupné z: https://www.channelnewsasia.com/news/cnainsider/what-south-korea-first-country-launch-5g-network-can-teach-us-12056726

a očekávatelné navýšení kapacity sítě jako takové.[590] Oba výše zmíněné standardy pro propojení internetu věcí umožňují budoucí adaptaci sítí na podporu technologického standardu 5G.[591] Hlavní posun, který se pro internet věci skrze tuto technologii předpokládá, je přesun z řešení založených na jednoúčelových zařízeních k digitálně automatizovaným službám.[592]

Jeden z prvků, který by měl tomuto vývoji přispět je funkce dělení sítě, která umožní odlišování více logických sítí se specifickými parametry pro potřeby konkrétního komunikačního rámce uvnitř jedné sítě.[593] Toto by mělo podpořit plný rozvoj internetu věcí v předpokládaných složitých prostředích chytrého města,[594] chytré mobility[595] či dopravních řetězců průmyslu 4.0.[596] Tyto silně na datech závislé služby budou poskytovat optimalizaci a individualizaci uživatelské interakce postavené na, ve zvyšující se míře všudypřítomném, využívání umělé inteligence a automatizovaného přenosu dat mezi zařízeními.

Nové možnosti propojitelnosti zřejmě také posílí užívání cloudových služeb, přenechávajících koncovým zařízením internetu věcí pouze roli sběru dat a následného provedení či zobrazení výstupu, zatímco vlastní zpracování bude probíhat na dálku.[597] To ale bude vyžadovat neustálou komunikaci množiny shromážděných dat a následnou závislost na stažení instrukcí či údajů z cloudového uzlu. Je dále pravděpodobné, že požadavky na funkcionalitu i uživatelské pohodlí postupně odstraní manuální vnášení údajů

590 Viz IEEE. 3 Key Benefits of 5G. *IEEE Innovation at Work* [online]. 20. 12. 2018 [cit. 16. 9. 2021]. Dostupné z: https://innovationatwork.ieee.org/3-key-benefits-of-5g/

591 Viz QUALCOMM TECHNOLOGIES. *Accelerating the mobile ecosystem expansion in the 5G Era with LTE Advanced Pro* [online]. 2018, s. 6 [cit. 17. 10. 2021].

592 Srov. KENWORTHY, Randal. The 5G And IoT Revolution Is Coming: Here's What To Expect. *Forbes* [online]. 11/2019 [cit. 17. 10. 2021]. Dostupné z: https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/

593 Viz ZHANG, Shunliang. An Overview of Network Slicing for 5G. *IEEE Wireless Communications* [online]. 2019, roč. 26, č. 3, s. 111 a násl.

594 Srov. FERDOUSI, Sifat. Network Slicing in Smart Cities [online]. 2018 [cit. 17. 10. 2021]. Dostupné z: http://networks.cs.ucdavis.edu/presentation2018/Sifat-08-17-2018.pdf

595 Viz ZHANG, Haijun et al. Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. *IEEE Communications Magazine* [online]. 2017, roč. 55, s. 138 a násl.

596 Viz KALOR, Anders et al. Network Slicing in Industry 4.0 Applications: Abstraction Methods and End-to-End Analysis. *IEEE Transactions on Industrial Informatics* [online]. 2018, roč. PP, s. 5419 a násl.

597 Srov. IOT SOLUTIONS WORLD CONGRESS. Advantages of 5G and how will benefit IoT. *Digitalizing Industries* [online]. 2. 4. 2019 [cit. 17. 10. 2021]. Dostupné z: https://www.iotsworldcongress.com/advantatges-of-5g-and-how-will-benefit-iot/

skrze automatizované shromažďování a sdělování mezi zařízeními, tak aby bylo dosaženo požadovaného ambientního charakteru poskytované služby.[598] V tomto vývoji spatřuji významnou výzvu z hlediska ochrany osobních údajů, specificky pro povinnosti spojené s porušením zabezpečení osobních údajů dle článků 33 a 34 Obecného nařízení.

Bezpečnostní výzvy spojené se zavedením 5G: Vedle široce zdokumentovaných[599] a obecně uznávaných[600] limitů prostředí internetu věcí bránit porušením bezpečnosti a omezit jejich dopad, přináší posílené toky dat v důsledku implementace technologie 5G další, bytostnější překážky pro realizaci notifikačních povinností.

Technické výzvy se váží k automatizaci komunikace mezi zařízeními a proměnlivému množství účastnících se zařízení. Přes snahy významných nadnárodních technologických společností uzavřít uživatele do homogenních sítí utvářených výhradně produkty daného poskytovatele zůstává přinejmenším pro veřejně přístupné prostředí chytrého města či podnikové sítě malých a středních podniků vysoce pravděpodobné, že se v nich budou setkávat zařízení řady výrobců s různými komunikačními a bezpečnostními parametry. Toto přinese složité scénáře kompatibility odlišných bezpečnostních či komunikačních standardů vedoucí ke skrytým zranitelnostem.[601] Správci tak vznikne jedinečná síť s mnoha možnými slabými místy.

***Mesh* sítě:** Automatizace komunikace mezi zařízeními přitom učiní správu datových toků a zajišťování bezpečnosti sítě a zařízení ještě složitějšími. Lze totiž předpokládat, že přinese nové vzorce datových toků, které budou nezbytné pro řádné fungování *mesh* sítí, tedy sítí s proměnlivou strukturou,[602]

598 Viz COSTA, Luiz. *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*. Cham: Springer International Publishing, 2016, s. 23–24.

599 Viz KREBS, Brian. New Mirai Worm Knocks 900K Germans Offline. *Krebs on Security* [online]. 30. 11. 2016 [cit. 20. 3. 2021]. Dostupné z: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

600 Srov. THE ECONOMIST. A connected world will be a playground for hackers. *The Economist* [online]. 2019 [cit. 17. 10. 2021].

601 Viz BAUWENS, Jan et al. Portability, compatibility and reuse of MAC protocols across different IoT radio platforms. *Ad Hoc Networks* [online]. 2019, roč. 86, s. 144 a násl.

602 Blíže k pojmu viz CILFONE, Antonio et al. Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies. *Future Internet* [online]. 2019, roč. 11, č. 4, s. 100.

ale budou činit obtíže z hlediska zajištění bezpečnosti.[603] Nová řešení síťové bezpečnosti na bázi heuristického vyhledávání za pomoci umělé inteligence či profilování datových toků zařízení mohou přinášet určitou protiváhu těmto tendencím.[604] S přihlédnutím k dosavadním zkušenostem na poli kyberbezpečnosti je však nepravděpodobné, že by mnoho správců v rychle se blížícím budoucím prostředí internetu věcí věnovalo významně vyšší pozornost a prostředky na zajištění bezpečnostních opatření a odhalování případů porušení bezpečnosti osobních údajů, než je tomu dnes.[605] Skutečný rozsah problému tedy bude zřejmě narůstat, byť bez vědomí příslušných odpovědných správců.

Shrnutí poznatků: U internetu věcí na bázi technologie 5G lze obecně očekávat více technologických bezpečnostních výzev pro ochranu osobních údajů, častější případy porušení bezpečnosti s citelnějšími dopady, ale také méně kontroly správců nad datovými toky v rámci jejich sítí a častější opominutí odhalení a řádného notifikování významného porušení bezpečnosti.

4.4.2 Přímé a nepřímé provázanosti sítí chytrého města

Chytré město představuje aplikaci internetu věcí v rozsáhlém, společensky významném kontextu. Vzhledem k množství dotčených a spolupůsobících subjektů, jakožto i prolínání soukromého a veřejného sektoru, zde dochází ke specifickým situacím a výzvám. Tato zvyšující se komplexita nejen datových toků, ale i vzájemných právních vztahů příslušných správců a zpracovatelů, vede ke znesnadnění plnění příslušných povinností dle právní úpravy ochrany osobních údajů.

Koncept chytrého města *(smart city)* je příkladem synergie nových technologií, které zahrnují internet věcí, *big data* a *cloud computing* do modelu propojeného

603 Srov. VARGA, Pal et al. Security threats and issues in automation IoT. In: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)* [online]. 2017.

604 Viz CU, Tung. Artificial Intelligence for Cybersecurity: A Review. *Faculty Research and Creative Activities Symposium* [online]. 2019.

605 Viz GORDON, Lawrence A. et al. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security* [online]. 2014, roč. 06, č. 01.

městského prostředí, které slibuje zlepšení udržitelnosti a kvality života.[606] Pojem zahrnuje implementaci ICT řešení, jakožto i širší socioekonomickou proměnu městského ekosystému zapojující do interakce řadu nových zúčastněných stran. Je příkladem složitého propojení technologií se sociálními, politickými a ekonomickými faktory, které se protínají v moderním metropolitním plánování.

Přes populární užívání pojmu chytré město v řadě kontextů pro něj neexistuje jednotící definice. V řadě případů pak dochází k překryvu s méně častým pojmem inteligentní město *(intelligent city)*.[607] Podle studie z roku 2014 pro Evropský parlament za účelem prozkoumání kontextu pro *European Innovation Partnership on Smart Cities and Communities* lze přijmout následující definici: *„Chytré město je město usilující o řešení veřejných problémů skrze řešení založená na ICT skrze bázi městského partnerství s množstvím zúčastněných stran. Tato řešení jsou vyvíjena a zlepšována skrze iniciativy chytrého města, buďto jako jednotlivé projekty nebo (častěji) jako síť překrývajících se aktivit.“*[608]

Směrodatným aspektem je přitom intenzivní úsilí o koordinaci a propojení dříve oddělených technologických řešení a dílčích služeb do integrovaných sítí k dosažení synergií a zlepšení kvality městského života.[609] Toto rostoucí propojení nových technologií s městským prostředím však také vede k nárůstu složitosti datových toků, což představuje rostoucí výzvu pro zajištění bezpečnosti a odolnosti *(resilience)* tohoto prostředí.

Souhra existující a nové infrastruktury a nepřímé modulární závislosti: Většina studií týkajících se chytrého města se soustředí na ověření

606 Viz NUAIMI, Eiman Al et al. Applications of big data to smart cities. *Journal of Internet Services and Applications* [online]. 2015, roč. 6, č. 1, s. 2; SUCIU, George et al. Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things. In: *2013 19th International Conference on Control Systems and Computer Science* [online]. 2013, s. 513.

607 Srov. BRIGGS, Guy. The Intelligent City: Ubiquitous Network of Humane Environment. In: JENKS, Michael a Nicola DEMPSEY. *Future Forms and Design for Sustainable Cities*. Routledge, 2005.

608 *„Smart City is a city seeking to address public issues via ICT based solutions on the basis of a multi-stakeholder, municipally based partnership. These solutions are developed and refined through Smart City initiatives, either as discrete projects or (more usually) as a network of overlapping activities.“* Srov. MANVILLE, Catriona et al. *Mapping Smart cities in the EU* [online]. Brusel: Directorate-General for Internal Policies, European Parliament, 2014, s. 17 [cit. 20. 5. 2021].

609 Viz BATTY, M. et al. Smart cities of the future. *The European Physical Journal Special Topics* [online]. 2012, roč. 214, č. 1.

uskutečnitelnosti obecných konceptů, celkovou strukturu a organizační rámce[610] nebo se omezuje na dílčí prvek a jeho specifické problémy a výzvy.[611] Do určité míry v pozadí zůstávají otázky kyberbezpečnosti a zajištění bezpečnosti zpracování osobních údajů, zvláště pak v kontextu souhry existující a nově vznikající městské infrastruktury, či nepřímé závislosti modulárních částí infrastruktury navzájem. Právě tyto dva kontexty vnímám z hlediska porušení bezpečnosti osobních údajů za klíčová místa zvýšeného rizika. U souhry existující a nové infrastruktury je překážkou kompatibilita a nepředvídatelnost situačního nastavení. U nepřímé modulární závislosti jde o dynamiku *ad hoc* situací a zvýšenou složitost prostředí skrze překrývající se vrstvy procesů a služeb.

Vznik chytrého města: Existence propojenosti mezi jednotlivými prvky městského ekosystému je jedním z definičních prvků urbanizace. Město je neustále se měnící organismus, který trvale pokouší své limity.[612] Vznik chytrého města se obecně odvíjí jedním ze dvou základních směrů.[613] Buď je město nebo městská část vybudována zcela nově s integrovanou vrstvou infrastruktury chytrého města, nebo jde o přeměnu existujících a fungujících městských částí sérií dílčích projektů s postupným začleňováním chytrých prvků.

Přístup skrze proměnu existujícího městského prostředí je zvláště reprezentativní pro evropský kontext. Již v roce 2011 měla dle studie pro Evropský parlament více jak polovina ze 468 měst v EU s více jak 100 000 obyvateli některou z charakteristik chytrého města, přičemž u 52 měst nad 500 000 obyvatel tomu tak bylo u 46 z nich. Jde tedy znatelně o fenomén velkých měst.[614] Významnou

610 Srov. ANTHOPOULOS, Leonidas, Marijn JANSSEN a Vishanth WEERAKKODY. A Unified Smart City Model (USCM) for smart city conceptualization and benchmarking. *International Journal of Electronic Government Research* [online]. 2016, roč. 12, č. 2.

611 Srov. LÉVY-BENCHETON, Cédric et al. *Cyber Security for Smart Cities – an Architecture Model for Public Transport* [online]. ENISA. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research, 2015 [cit. 20. 3. 2021].

612 Viz MATTONI, Benedetta, Franco GUGLIERMETTI a Fabio BISEGNA. A multilevel method to assess and design the renovation and integration of Smart Cities. *Sustainable Cities and Society* [online]. 2015, roč. 15.

613 Srov. ANGELIDOU, Margarita. Smart city policies: A spatial approach. *Cities* [online]. 2014, roč. 41, Supplement 1, Current Research on Cities.

614 Charakteristik chytrého města je v rámci studie identifikováno šest: *Smart Governance, Smart Economy, Smart Mobility, Smart Environment, Smart People a Smart Living.* Blíže viz MANVILLE, Catriona et al. *Mapping Smart cities in the EU* [online]. Brusel: Directorate-General for Internal Policies, European Parliament, 2014, s. 9 [cit. 20. 5. 2021].

roli v rozvoji chytrých měst v EU má rámcový program na podporu výzkumu a inovací Horizon 2020, prostřednictvím kterého jsou financovány projekty městského rozvoje *(Smart Cities and Communities Lighthouse Projects)*[615], do kterých jsou zapojena i česká města.[616] Tato míra podpory v rámci EU pramení ze snahy o udržení globální konkurenceschopnosti metropolitních oblastí.[617] Projekty tohoto typu se však zdaleka neomezují pouze na EU. Studie *Navigant Research* z poloviny roku 2019 identifikuje 443 významných projektů chytrého města ve 286 městech po celém světě.[618]

Odolnost chytrého města: Se zajištěním bezpečnosti v městském kontextu se prolíná otázka městské odolnosti (*resilience*) vůči nejrůznějším přírodním, sociálním či ekonomickým výzvám. Toto je dimenze, která přidává na významu strategickému plánování rozvoje chytrého města.[619] Na své aktuálnosti přitom dále získala v důsledku pandemie COVID-19.[620] I proto se mnoho velkých projektů chytrých měst zaměřuje primárně na zvyšování odolnosti městského ekosystému, tedy jeho kapacitu vypořádat se s problémy jako je přetížená dopravní síť, nedostatky veřejných služeb, místní nezaměstnanost, distribuční sítě pro vodu a energii, enviromentální hrozby, narušení veřejné bezpečnosti či hrozící následky extrémního počasí.

Skrze řešení těchto problémů dochází často k vrstvení nových prvků a sítí informačních a komunikačních technologií přes existující městskou infrastrukturu a celkovému navyšování provázanosti a propojenosti těchto vrstev.

615 Viz EIP-SCC. About Smart City Lighthouse Projects. *EIP-SCC* [online]. 2020 [cit. 15. 7. 2021]. Dostupné z: https://eu-smartcities.eu/projects/1972/description

616 Viz SCIS. Smart Cities and Communities Lighthouse projects. *EU Smart Cities Information System* [online]. 2020 [cit. 15. 7. 2021]. Dostupné z: https://smartcities-infosystem.eu/scc-lighthouse-projects

617 Srov. MANVILLE, Catriona et al. *Mapping Smart cities in the EU* [online]. Brusel: Directorate-General for Internal Policies, European Parliament, 2014, s. 104 [cit. 20. 5. 2021].

618 Viz BUSINESSWIRE. Navigant Research's Smart City Tracker 2Q19 Highlights 443 Projects Spanning 286 Cities Around the World. *Businesswire* [online]. 20. 6. 2019 [cit. 15. 7. 2021]. Dostupné z: https://www.businesswire.com/news/home/20190620005092/en/Navigant-Research%E2%80%99s-Smart-City-Tracker-2Q19-Highlights

619 Viz ERAYDIN, Ayda a Tuna TASAN-KOK. *Resilience Thinking in Urban Planning.* Springer Science & Business Media, 2012.

620 Srov. SMART CITIES WORLD. COVID-19 accelerates the adoption of smart city tech to build resilience. *Smart Cities World* [online]. 7. 5. 2020 [cit. 15. 7. 2021]. Dostupné z: https://www.smartcitiesworld.net/news/news/COVID-19-accelerates-the-adoption-of-smart-city-tech-to-build-resilience—5259

Tento nový stupeň konektivity však přináší městskému ekosystému svůj vlastní soubor zranitelností související s výše popsanými specifiky internetu věcí,[621] které vyžadují přiměřenou pozornost.

Vznik chytrého města jako postupný proces: Při pohledu na chytré město z obecné perspektivy jde zpravidla o soubor projektů vážících se k různým prvkům, který vede k postupné proměně existujících městských prostředí do integrované architektury.[622] K této proměně dochází časem a na základě stupňovitého procesu, ale celkové směřování lze zpravidla vymezit jako zvyšování propojenosti a závislosti mezi dílčími moduly a komponenty.

Městské plánování zahrnuje řadu technických, ekonomických, politických a dalších faktorů, které odrážejí vlastní složitost městského ekosystému. Z praktického hlediska mohou být projektanti omezeni přístupem k místu realizace, časovým oknem pro stavební práce, potřebou udržení jejich částečného přístupu či funkcionality. Zvláště chytrá přeměna nosné městské infrastruktury se může potkávat s těmito výzvami, nemine se jimi zřejmě ani změna administrativních či operačních systémů. Další překážky mohou být politického rázu,[623] rozpočtové, právní z hlediska požadavků na projektové výdaje z veřejného rozpočtu, administrativní či v důsledku nedostatku dodavatelů s přiměřenou odborností.[624]

Všechny tyto aspekty utvářejí z proměny města fragmentovaný proces, který vyžaduje nejen dlouhodobou vizi, ale i důslednou koordinaci a dohled nad funkční provázaností jednotlivých fází proměny. Skutečnost, že různé prvky infrastruktury jsou na různé úrovni novosti není ničím specifickým. Chytré komponenty však v tomto ohledu zpravidla přinášejí novou dimenzi konektivity, související se zvýšeným důrazem na sběr, sdílení a využívání dostupných dat. Přidáním těchto komunikačních vlastností prvkům, které

621 Srov. podkapitola 4.3.

622 Srov. MATTONI, Benedetta, Franco GUGLIERMETTI a Fabio BISEGNA. A multilevel method to assess and design the renovation and integration of Smart Cities. *Sustainable Cities and Society* [online]. 2015, roč. 15.

623 Viz AUERBACH, Gedalia. Urban planning: Politics vs. Planning and Politicians vs. Planners. *Horizons in Geography*. 2012, č. 79/80.

624 Srov. GARVIN, Alexander. *Urban Planning Today* [online]. NED-New edition. Minneapolis: University of Minnesota Press, 2006 [cit. 29. 3. 2021]. A Harvard Design Magazine Reader.

je tradičně nemají, dochází k vytvoření zcela nové bezpečnostní perspektivy na danou síť či systém.[625]

Z jednotlivých zařízení se stávají přístupové body a nástroje pro zpracování osobních a jiných údajů, které mohou být ohroženy či zneužity. Hrozby jsou následně zvýšeny nepředvídanými vazbami mezi systémy a prvky a skrytými závislostmi napříč městským ekosystémem.

Hrozby spojené s nepřímým vztahem mezi systémy mohou být posíleny v rámci stavebních úprav či implementací nových modulů, kdy dochází k utváření dočasných komunikačních rámců, náhradním fyzickým propojením, překlenovacím datovým tokům, dočasným odstavením systémů, zkušebním provozům či optimalizačnímu testování. Tato dynamika proměny města se pak odráží v dynamice scénářů zúčastněných subjektů na činnostech a datových tocích, čímž se stupňuje složitost jednotlivých situací.

Kyberbezpečnostní hrozby spojené s nepřímou provázaností modulů: Vedle průběžného charakteru proměny města hraje z hlediska zajištění bezpečnosti datových toků a zpracování osobních údajů roli též rostoucí přímý a nepřímý překryv mezi dílčími systémy a moduly.

Typickým projevem transformace na chytré město je zavedení moderního multi-modálního veřejného systému dopravy.[626] Inovace mohou zahrnovat síť'ovou koordinaci vedoucí k flexibilnímu trasování,[627] či dokonce autonomní vozidla veřejné dopravy.[628] Vedle veřejné dopravy se vize chytrého města zpravidla upínají k pokročilým formám správy dopravních toků.[629] Ty zahrnují propojené sítě chytrého dopravního značení, silničních senzorů,

625 Viz MANWARING, Kayleen a Roger CLARKE. Surfing the Third Wave of Computing: A Framework for Research into eObjects. *Computer Law & Security Review: The International Journal of Technology Law and Practice* [online]. 2015, roč. 31, č. 5, s. 586 a násl.

626 Srov. ANDERSON, Marie Karen, Otto Anker NIELSEN a Carlo Giacomo PRATO. Multimodal route choice models of public transport passengers in the Greater Copenhagen Area. *EURO Journal on Transportation and Logistics* [online]. 2014.

627 Viz HANDTE, M. et al. An Internet-of-Things Enabled Connected Navigation System for Urban Bus Riders. *IEEE Internet of Things Journal* [online]. 2016, roč. 3, č. 5.

628 Viz GROGAN, A. Driverless trains: It's the automatic choice. *Engineering & Technology* [online]. 2012, roč. 7, č. 5; MOHANAPRIYA, R. et al. Driverless Intelligent Vehicle for Future Public Transport Based on GPS. *International Journal of Advanced Research in Electrical, Electronic and Instrumentation Engineering,* 2014, roč. 3, č. 3.

629 Srov. YOUSEF, Khalil M., Jamal N. AL-KARAKI a Ali M. SHATNAWI. Intelligent Traffic Light Flow Control System Using Wireless Sensors Networks. *Journal of Information Science and Engineering,* 2010, roč. 26.

sledování dostupných parkovacích míst,[630] či systému včasného varování.[631] Tyto prvky poskytují permanentní datové toky o všech významných aspektech dopravní situace ve městě, umožňující flexibilní správu dopravní hustoty skrze úpravy intervalů, změny digitálního dopravního značení (např. doporučená cesta, rychlost, parkovací místa)[632] nebo úpravu intervalů semaforů na trase pro záchrannou službu či jiná zvláštní vozidla. Projekty z této oblasti jsou zaměřeny především na řešení rostoucího dopravního přetížení a související zátěže pro životní prostředí a prodloužení doby na cestě pro dojíždějící.[633]

Správa chytrého města vyžaduje zpracovávat vstupy z vlastních administrativních systémů, od jiných veřejných složek, od místních podniků a obyvatel i z jiných vnitřních a vnějších zdrojů. Toto představuje značnou koordinační výzvu, která je cílena řadou strategií chytrých měst.[634] Může jít o specializované operační systémy, administrativní prostředí, komunikační platformy, autorizační portály, přístupové nástroje, komponenty pro správu databází osobních údajů, dohledové nástroje, reaktivní a adaptabilní kyberbezpečnostní řešení, systémy včasného varování či automatizované havarijní či krizové systémy. Tato provázanost je vlastním zdrojem rizik, protože zranitelnost jedné sítě či systému může snadno vést k porušení bezpečnosti propojených sítí.[635]

Další relevantní projekty se věnují inženýrským sítím pro distribuci energie,[636] vody, odpadů či plynu.[637] Chytré prvky zahrnují nejrůznější senzory, zátěžové

630 Srov. WANG, Hongwei a Wenbo HE. A Reservation-based Smart Parking System. In: *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* [online]. 2011.

631 Viz KHEKARE, Ganesh S. a Apeksha V. SAKHARE. A smart city framework for intelligent traffic system using VANET. In: *2013 International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)* [online]. 2013.

632 Viz FAHEEM et al. A Survey of Intelligent Car Parking System. *Journal of Applied Research and Technology* [online]. 2013, roč. 11, č. 5.

633 Srov. SUNDAR, Rajeshwari, Santhoshs HEBBAR a Varaprasad GOLLA. Implementing Intelligent Traffic Control System for Congestion Control, Ambulance Clearance, and Stolen Vehicle Detection. *IEEE Sensors Journal* [online]. 2015, roč. 15, č. 2.

634 Viz SCHOLL, Hans Jochen a Suha AL AWADHI. Creating Smart Governance: The key to radical ICT overhaul at the City of Munich. *Information Polity: The International Journal of Government & Democracy in the Information Age* [online]. 2016, roč. 21, č. 1.

635 Srov. KHATOUN, Rida a Sherali ZEADALLY. Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Communications Magazine* [online]. 2017, roč. 55, č. 3.

636 Viz FANG, X. et al. Smart Grid – The New and Improved Power Grid: A Survey. *IEEE Communications Surveys Tutorials* [online]. 2011, roč. 14, č. 4.

637 Viz např. AAZAM, M. et al. Cloud-based smart waste management for smart cities. In: *2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)* [online]. 2016.

či kontrolní sondy, komunikační jednotky či průtokové měřiče. Ty se v zásadě doplňují na existující inženýrské sítě a jsou tak integrovány do existujících distribučních a údržbových opatření. Související oblastí je optimalizace správy budov, především s ohledem na snížení energetické náročnosti. Jde v zásadě o koordinovanou implementaci prvků chytré domácnosti ve velkém rozsahu pro administrativní či obytné budovy. Specifickým prvkem chytrého města je také síť řiditelného pouličního osvětlení se senzory zátěže životního prostředí či veřejnými body pro internetové připojení.[638]

Chytré město lze tudíž vnímat jako spleť služeb a sítí, často se překrývajících v různých dimenzích. S ohledem na propojenost datové a fyzické povahy těchto prvků[639] a jejich očekávanou vysokou koncentraci v městské infrastruktuře, mohou být tyto provázanosti nejen přímé, na základě datových toků mezi sítěmi a databázemi, ale též skryté v důsledku synergií či překryvů ve fyzickém prostředí. Například koordinace hromadné dopravy závisí na řízení dopravních toků skrze chytré značení, které zpracovává data přenášená ze senzorů napříč městem. Nadto jsou tato data součástí platforem otevřených dat, a na jejich vytěžování stojí tedy soubor dodatečných funkcí a služeb. V prostředí chytrého města tak může útok na určitý systém vést k ohrožení podružného, navazujícího či nadstavbového systému, čímž mohou být způsobená nejen porušení bezpečnosti zpracovávaných údajů, ale i hmotné škody a omezení dostupných služeb.

K tomu dále přistupují organizační výzvy spojené s dynamicky proměnlivými situacemi, ve kterých se tyto různé moduly a služby chytrého města nacházejí. Tím se proměňují i odpovědné subjekty účastnící se přenosů údajů a jejich zpracování v jednotlivém okamžiku. S rostoucí propojeností se zvyšuje riziko přenosu zranitelnosti, lze zde tedy nalézt paralelu k riziku využití zranitelností v rámci dodavatelského řetězce.[640]

638 Viz PIZZUTI, Stefano, Mauto ANNUNZIATO a Fabio MORETTI. Smart street lighting management. *Energy Efficiency* [online]. 2013, roč. 6, č. 3.

639 Srov. BOYES, Hugh, Roy ISBELL a Tim WATSON. Critical Infrastructure in the Future City: Developing Secure and Resilient Cyber-Physical Systems. In: *Critical Information Infrastructures Security 9th International Conference, CRITIS 2014, Limassol, Cyprus, October 13–15, 2014, Revised Selected Papers*. New York: Springer International Publishing, 2016.

640 Srov. SHACKLEFORD, Dave. *Combatting Cyber Risks in the Supply Chain* [online]. Bethesda, MA: SANS Institute. 2017 [cit. 3. 10. 2021].

Shrnutí poznatků: Na příkladě chytrého města lze plně vnímat možnou komplexitu síťových propojení, které umožňuje rozvoj internetu věcí. Ty budou sloužit především optimalizaci veřejných služeb, ale lze předpokládat i značný důraz na personalizaci a shromažďování údajů o subjektech údajů, čímž bude docházet k četným zpracováním osobních údajů. Ty přitom budou putovat mezi prvky infrastruktury a dílčími aktéry napříč moduly a službami, čímž je z hlediska práva ochrany osobních údajů utvářena série zpracování společnými správci. Ti přitom nemusejí být omezeni pouze na relativně stálé poskytovatele služeb, ale mohou se *ad hoc* měnit v závislosti na míře provázanosti infrastruktury a datových toků v rámci chytrého města.[641] Vzhledem k dynamické povaze těchto vztahů je nepravděpodobné očekávat jasná a transparentní ujednání o dělbě odpovědnosti předvídaná článkem 26 Obecného nařízení. Motivaci jednotlivých povinných subjektů ohlašovat bezpečnostní selhání v situacích, kdy je přiřčení odpovědnosti za daný incident konkrétnímu prvku sítě, a tudíž konkrétnímu odpovědnému subjektu, složité na zjištění a prokázání, pak obecně předpokládám za nízkou.[642] Možnému řešení této překážky se budu věnovat v podkapitole 6.1.

4.4.3 Prostředí podnikových sítí a specifická situace mikropodniků

Prostředí mikropodniků obsahuje řadu specifik, které se odrážejí mimo jiné v bezpečnostních hrozbách pro osobní údaje. Tato skutečnost je významná, jelikož mikropodniky představují převážnou část správců osobních údajů v rámci EU. Jejich limitované finanční zdroje, absence specializovaného personálu, různorodá architektura podnikových sítí, či relativně vysoká míra regulatorního zatížení je často vede do situace, kdy nemají k dispozici (či nepovažují za nezbytné vynaložit) přiměřené prostředky a know-how na svou

641 Významnou dílčí problematiku v tomto směru představuje i otevírání dat veřejné správy a následné utváření služeb a aplikacích pracujících s těmito daty. Přestože vlastní otevřená data nemusejí představovat citlivé či zvláště zneužitelné osobní údaje, jejich následné provázání do služeb a kombinace s dalšími údaji získanými např. na základě souhlasu subjektu údajů užívajících danou aplikaci je v takové mohou proměnit. Úměrně s citlivostí osobních údajů se následně stupňují i rizika, a tudíž potřeba opatření na jejich ochranu.

642 K podnětům snižujícím motivaci povinných subjektů k ohlašování porušení bezpečnosti viz BOASIAKO, Kwabena Antwi a Michael O'CONNOR KEEFE. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. *SSRN Electronic Journal* [online]. 2018, s. 8 [cit. 5. 9. 2021].

kyberbezpečnost. Přitom i Národní bezpečnostní úřad[643] vnímal, že *„[j]ejich systémy a data přitom mohou být stejně kritická jako u velkých podniků, případně mohou pracovat s kritickými daty nebo systémy v rámci zajišťování služeb pro jiné subjekty."*[644] Tyto hrozby dále umocňuje rozšíření internetu věcí.[645] Je složité představit si v zásadě jakékoliv podnikání v moderní ekonomice bez zapojení prvků ICT (např. terminál pro platbu kartou, elektronické vedení účetnictví, kamerové zabezpečení prostor) a bez připojení k internetu (např. komunikace se zákazníky, online marketing, cloudové úložiště dat). Současně modernizace postupuje neúnavným tempem a přináší na trh nespočet nových výrobků a řešení. I drobné lokální podniky jsou tak pod trvalým konkurenčním tlakem inovovat své služby, výrobky a procesy, což v řadě případů znamená v menší či větší míře adopci zařízení internetu věcí, nyní též do značné míry posíleném situací vyvolanou pandemií COVID-19.[646] Mikropodniky tak čelí často nepřiměřené výzvě při odhalování a řešení porušení bezpečnosti.

Mikropodniky z hlediska statistické i právní kategorizace spadají pod malé a střední podniky (MSP).[647] Ty jsou pro účely jednotného výkladu v unijním právu vymezeny Doporučením Komise 2003/361/EC o definici mikropodniků, malých a středních podniků.[648] Ukazateli pro určení MSP jsou počet zaměstnanců[649] a finanční obrat.[650] Mikropodniky mají méně než 10 zaměstnanců a roční obrat či rozvaha je nižší než 2 miliony EUR.[651] Ze statistického hlediska přitom v roce 2019 tvořily mikropodniky 93 % všech podniků v EU, zaměstnávaly téměř 30 % všech zaměstnanců a vytvořily přes 20 % přidané hodnoty.[652]

643 Dnes se již jedná o agendu spadající pod Národní úřad pro kybernetickou a informační bezpečnost.

644 Viz Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *Národní bezpečnostní úřad* [online]. Praha: Národní bezpečnostní úřad, 2015, s. 14 [cit. 12. 7. 2021].

645 Ibid., s. 13.

646 Srov. DROZDIAK, Natalia a Helene FOUQUET. Creepy Technologies Invade European Workplaces. *Bloomberg.com* [online]. 2020 [cit. 15. 7. 2021].

647 Srov. čl. 1 Přílohy Doporučení Komise 2003/361/EC.

648 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422).

649 Bod odůvodnění 4 Doporučení Komise 2003/361/EC.

650 Ibid.

651 Srov. čl. 2 odst. 3 Přílohy Doporučení Komise 2003/361/EC.

652 Viz Annual Report on European SMEs 2018/2019, Research & Development and Innovation by SMEs. *Executive Agency for Small and Medium-Sized Enterprises (EASME)* [online]. EASME/COSME/2017/031. Brusel: Evropská komise, 2019, s. 17 [cit. 21. 5. 2021].

Mikropodniky a internet věcí: Mezi mikropodniky nalezneme jak inovativní obchodní modely start-upů a pionýrů digitální ekonomiky,[653] tak velmi statické podniky, které se drží tradičních obchodních modelů a pomíjí či úmyslně odmítají nové technologické trendy.[654, 655] Přestože inovační potenciál mikropodniků je v relativním poměru k ostatním kategoriím podniků nižší,[656] je podpora malých a začínajících podniků vnímána jako významný předpoklad růstu zaměstnanosti, místního rozvoje, udržení konkurenčního prostředí a nárůstu rovných příležitostí, a jde tudíž o jednou z priorit EU.[657] Inovační potenciál MSP je pak vnímán jako klíčová složka rozvoje Jednotného digitálního trhu a EU poskytuje v tomto směru řadu podpůrných nástrojů.[658]

S plným vědomím limitů zobecňování ve vztahu k mikropodnikům, jakožto i rozdílů mezi členskými státy,[659] je možné vnímat silný trend k modernizaci, inovaci a digitalizaci podnikatelského prostředí MSP napříč EU.[660] S tím úzce souvisí posun k vyšší propojenosti, interoperabilitě a vzájemné závislosti, stejně jako adaptabilitě a logistice na bázi *just-in-time* dodávek.[661] Slovy tehdejšího viceprezidenta Evropské komise *Ansipa*: *„Pokud bych měl vyjádřit svůj pohled na digitální budoucnost – Evropy, či vlastně celého světa – postačilo by mi k tomu jediné slovo: data. Digitální ekonomika se točí okolo dat. Je to hnací síla za hlavními prvky*

653 Srov. 25 % MSP podniká v oblasti s velmi vysokou intenzitou výzkumu a vývoje, jako je programování, strojírenská výroba či farmaceutický průmysl.

654 Srov. 41 % MSP naopak podniká v oblastech s velmi nízkou mírou inovace, např. ubytování, stavebnictví či jako realitní makléř.

655 Ibid., s. 27.

656 Ibid., s. 132.

657 Viz EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES. *Evaluation of support services for would-be entrepreneurs and newly established businesses : final report.* [online]. EASME/COSME/2018/017. Brussels: European Commission, 2019, s. i [cit. 16. 7. 2021].

658 Srov. EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES. *Accelerating innovation in Europe: Horizon 2020 SME Instrument impact report* [online]. 2017 Edition. Brussels: European Commission. 2017 [cit. 1. 10. 2021].

659 Viz EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES (EASME). *Annual Report on European SMEs 2018/2019, Research & Development and Innovation by SMEs* [online]. EASME/COSME/2017/031. Brusel: Evropská komise, 2019, s. 110 [cit. 21. 5. 2021].

660 Srov. EUROPEAN COMMISSION. Integration of Digital Technology. In: *European Digital Services Report* [online]. Brussels. 2017, Listy 6 a 7 [cit. 12. 7. 2021].

661 Viz HOFMANN, Erik a Marco RÜSCH. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry* [online]. 2017, roč. 89.

produktivity, inovace a digitalizace."[662] Podnikové operace tak dnes již i u řady mikropodniků zahrnují zpracování širokého spektra osobních údajů. Je přitom poměrně zjevné, že současný stav digitalizace ekonomiky je jen určitým mezistupněm na cestě k větší míře všudypřítomného propojení a digitální ekonomice silně využívající datových toků v rámci internetu věcí.[663]

Podniky různých velikostí, tedy včetně mikropodniků, se stávají významnými hráči na poli internetu věcí. Jejich role sahají od vývoje, výroby, distribuce a propagace po vlastní odběr a implementaci těchto zařízení.[664] Odvětví průmyslového internetu věcí se rychle rozvíjí,[665] jelikož vhodné využití jeho možností zvyšuje efektivitu logistiky, produktivitu zařízení a zaměstnanců, přesnost výroby, či kvalitu služeb, a vede tak k optimalizaci vynaložených nákladů.[666] Ačkoliv hlavní míru inovací i implementace na tomto poli provádějí velké podniky, většina menších podniků se s ní s rozmachem internetu věcí bude muset v té či oné podobě vypořádat.[667] Digitalizaci podnikového prostředí je tak věnována značná pozornost v širším odborném diskurzu.[668]

662 *„If I had to express my views about the digital future – that of Europe or indeed, of the whole world – I could do it with one word: data. The digital economy revolves around data. It is the driving force behind those three main elements of productivity, innovation and digitalisation."* Srov. ANSIP, Andrus. Speech by Vice-President Ansip at Bruegel annual meeting: "Productivity, innovation and digitalisation – which global policy challenges?" *European Commission* [online]. 7. 9. 2015 [cit. 27. 10. 2021]. Dostupné z: https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/speech-vice-president-ansip-bruegel-annual-meeting-productivity-innovation-and-digitalisation-which_en

663 Více viz EUROPEAN COMMISSION. Integration of Digital Technology. In: *European Digital Services Report* [online]. Brussels, 2017 [cit. 12. 7. 2021].

664 Srov. WORLD ECONOMIC FORUM. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services* [online]. REF 020315. Cologny: World Economic Forum, 2015, s. 14 a násl. [cit. 10. 10. 2021].

665 Srov. COLUMBUS, Louis. 2018 Roundup Of Internet Of Things Forecasts And Market Estimates. *Forbes* [online]. 2018, roč. 2018, č. 13.12 [cit. 16. 4. 2020].

666 Viz WORLD ECONOMIC FORUM. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services* [online]. REF 020315. Cologny: World Economic Forum, 2015, s. 3 [cit. 10. 10. 2021].

667 Lze totiž očekávat, že je nevyhnutelná proměna podnikatelského prostředí skrze tržní síly, která eventuálně povede k významné transformaci tradičních obchodních modelů ve většině sektorů. Tento proces je již zahájen a zdá se nepravděpodobné, že by se vyhnul mikropodnikům.

668 Viz např. BUCHERER, Eva a Dieter UCKELMANN. Business Models for the Internet of Things. In: UCKELMANN, Dieter, Mark HARRISON a Florian MICHAHELLES (eds.). *Architecting the Internet of Things* [online]. Berlin, Heidelberg: Springer, 2011 [cit. 16. 7. 2021]; GROMOVA, Ekaterina, Dmitriy TIMOKHIN a Galina POPOVA. The role of digitalisation in the economy development of small innovative enterprises. *Procedia Computer Science* [online]. 2020, roč. 169, Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019 (Tenth Annual Meeting of the BICA Society), held August 15–19, 2019 in Seattle, Washington, USA; OKS, Sascha Julian, Albrecht FRITZSCHE a Claudia LEHMANN. The digitalisation of industry from a strategic perspective. In: *R & D Management Conference*. 2016.

Mezi mikropodniky je k nalezení řada pionýrů technologické proměny, kteří se musejí aktivně vypořádávat s výzvami digitální propojenosti,[669] a byť řada mikropodniků nemá přímou snahu o implementaci prvků internetu věcí do svých podnikových operací, lze identifikovat nepřímé cesty, kterými se pro ně tento trend přesto stává relevantním. Kromě nových systémů a rámců u jejich dodavatelů, odběratelů či dalších obchodních partnerů jsou to především aktivity a požadavky zaměstnanců, které dříve či později učiní zařízení internetu věcí relevantní pro podnikové sítě zaměstnavatelů všech velikostí.

Role zaměstnanců ve vztahu k rozšíření internetu věcí u mikropodniků: Podnikové politiky užití vlastních zařízení *(bring your own device*, BYOD*)* [670] jsou již dnes poměrně rozšířené. S rostoucí provázaností jednotlivců s jejich personalizovanými zařízeními lze očekávat, že se poptávka po těchto politikách ze strany zaměstnanců dále zvýší.[671] Jelikož se v řadě kontextů jedná o účinný nástroj pro zvýšení produktivity a zaměstnanecké loajality,[672] zůstane tento typ podnikové politiky zřejmě nadále relevantní a je na místě zohledňovat specifické bezpečnostní důsledky, které se s ním pojí.[673]

Je to přitom především prostředí mikropodniků, kde má politika BYOD významné místo. Mikropodniky mají pro svou komorní velikost zpravidla problémy jednoznačně oddělit soukromé a korporátní aktivity (a tudíž i datové toky) svých zaměstnanců či vlastníků.[674] Otevřená politika BYOD pak také

669 Pro konkrétní příklady viz DITEM. Blog & Case Studies. *Digital Transformation of European Micro Enterprises* [online]. 2019 [cit. 16. 7. 2021]. Dostupné z: https://www.ditem.eu/blog

670 K pojmu viz NEW WORDS. BYOD. *Academic Dictionaries and Encyclopedias* [online]. 2013 [cit. 16. 7. 2021]. Dostupné z: https://new_words.enacademic.com/36/BYOD

671 Viz ZAHADAT, Nima et al. BYOD security engineering: A framework and its analysis. *Computers & Security* [online]. 2015, roč. 55.

672 Podle dotazníkového šetření, které v roce 2016 provedl *The Economist* 45 % zaměstnanců pokládá mobilitu za přínos k jejich produktivitě a 30 % z nich by nepracovalo ve společnosti, která nepřipouští politiku BYOD. Srov. Mobility, performance and engagement. *Economist Intelligence Unit* [online]. London: The Economist. 2016 [cit. 27. 10. 2021].

673 Blíže viz ZAHADAT, Nima et al. BYOD security engineering: A framework and its analysis. *Computers & Security* [online]. 2015, roč. 55.

674 Uvažujte start-up s několika zaměstnanci, který je výrazně limitován finančními možnostmi a pro který je kontraproduktivní vynucovat striktní omezení ICT pro osobní a pracovní potřebu. Blíže pak viz CLARKE, Roger. The prospects of easier security for small organisations and consumers. *Computer Law & Security Review* [online]. 2015, roč. 31, č. 4, s. 539.

umožňuje mikropodniku využívat výhod nových technologií bez přímých investic do podnikového vybavení, jelikož jsou vlastnictvím zaměstnanců.[675]

Specifické postavení mikropodniků z hlediska kyberbezpečnosti: Z hlediska kyberbezpečnosti jsou přitom mikropodniky v unikátním postavení ve vztahu k této technologické proměně. Na jedné straně jde zpravidla o drobné korporátní zákazníky, závislé na výrobcích či řešeních od velkovýrobců či dominantních poskytovatelů služeb, zvláště na poli ICT. Jejich pozice v tomto směru tudíž není příliš odlišná od koncových uživatelů. Na druhé straně však vystupují také v roli správců či zpracovatelů osobních údajů, někdy ve velmi omezené míře (např. místní kadeřnictví), jindy v nepoměrně rozsáhlejší roli (např. vývojář a poskytovatel služby skrze mobilní aplikaci vytěžující otevřená data)[676]. Mikropodniky jsou také významnými inovátory, ať již na poli produktů, tedy jako výrobci či subdodavatelé zařízení internetu věcí, či jako pionýři v inovativní implementaci těchto zařízení do svých obchodních procesů a při interakci s koncovými zákazníky.[677] Přitom jde stále o podnikatelské subjekty, které podléhají srovnatelné regulatorní zátěži jako větší subjekty s rozsáhlejšími personálními kapacitami a rozpočtovými možnostmi.

Obecně byl v druhé kapitole dovozen trend rostoucí frekvence a škodlivosti bezpečnostních incidentů. Studie pro Evropský hospodářský a sociální výbor z roku 2018 pak specificky upozorňuje na rostoucí míru rizika porušení bezpečnosti u MSP v EU.[678] Studie společnosti *Hiscox* dále zdůrazňuje, že MSP, zvláště pak mikropodniky, jsou neúměrně zatíženy újmou v důsledku

675 Tuto formu úspor lze považovat za zvláště relevantní pro malé podniky v návaznosti na pandemii COVID-19 a související (dočasný) významný tlak na bezkontaktní podnikání, práci z domova a celkově skokovou digitalizaci obchodního modelu v zájmu ochrany zdraví. Srov. LUNDIN, Nannan. COVID-19 and digital transformation – What do we see now and what will we see soon? *Offices of Science and Innovation* [online]. 27. 4. 2020 [cit. 16. 7. 2021]. Dostupné z: https://sweden-science-innovation.blog/beijing/COVID-19-and-digital-transformation-what-do-we-see-now-and-what-will-we-see-soon/

676 Srov. EUROPEAN DATA PORTAL. Building apps with Open Data. *European Data Portal* [online]. 21. 4. 2017 [cit. 15. 7. 2021]. Dostupné z: https://www.europeandataportal.eu/en/news/building-apps-open-data

677 Srov. MATZLER, Kurt et al. Open innovation in small and micro enterprises. *Problems and Perspectives in Management*, 2013, roč. 11, s. 16–17.

678 Viz Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. *The Hague Centre for Strategic Studies* [online]. QE-01-18-515-EN-N. The Hague: The European Economic and Social Committee (EESC), 2018, s. 30 [cit. 15. 7. 2021].

bezpečnostních incidentů.[679] Tuto disproporci je přitom nutno podtrhnout vzhledem ke skutečnosti, že omezené finanční možnosti mikropodniků znamenají, že náklady spojené s porušením bezpečnosti mohou být pro mikropodnik více zatěžující, než je tomu v případě větších podniků.[680] To vede ke zvýšené újmě dotčených subjektů údajů, jelikož řešení případu porušení bezpečnosti nelze pokládat za prioritu mikropodniku v likvidaci.

MSP jsou přitom obecně pokládány za méně připravené na kyberbezpečnostní hrozby než větší entity. Nízká úroveň bezpečnostních opatření je často dána omezenou pozorností věnovanou těmto hrozbám. *Klahr* ve své studii MSP ve Velké Británii uvádí, že 39 % malých podniků či mikropodniků vůbec neinvestuje do kyberbezpečnosti, jelikož se pokládá za příliš nevýznamný cíl, přitom 45 % těchto podniků zaznamenalo porušení bezpečnosti v uplynulých 12 měsících.[681]

I při akceptování rizik, je však pro mikropodniky často prohibitivní výše nákladů spojených s přiměřenými kroky k zajištění kyberbezpečnosti.[682] *Klahr* uvádí, že medián[683] výše ročních nákladů na kybernetickou bezpečnost britských malých a mikropodniků je pouze 200 GBP.[684] Tato nepřipravenost a zranitelnost na poli kyberbezpečnosti se pak logicky překrývá s možnou nepřiměřenou

679 Data ve studii naznačují, že náklady přepočteny na jednoho zaměstnance jsou pro podniky s méně než 100 zaměstnanci průměrně nejméně pětkrát vyšší, než pro podniky s více než 1 000 zaměstnanců. Srov. HISCOX. *The Hiscox Cyber Readiness Report 2017* [online]. Bermunda: Hiscox, 2017, s. 5 [cit. 16. 7. 2021].

680 Viz STEINBERG, Scott. Cyberattacks now cost companies $ 200,000 on average, putting many out of business. *CNBC* [online]. 13. 10. 2019 [cit. 16. 7. 2021]. Dostupné z: https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

681 Srov. KLAHR, Rebecca et al. *Cyber Security Breaches Survey 2017* [online]. London: UK Department for Culture, Media & Sport, 2017, s. 32 a 39.

682 Srov. Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. *The Hague Centre for Strategic Studies* [online]. QE-01-18-515-EN-N. The Hague: The European Economic and Social Committee (EESC), 2018, s. 8 [cit. 15. 7. 2021].

683 Medián představuje prostřední hodnotu v souboru hodnot seřazených podle určitého parametru. K pojmu viz FINANCIAL AND BUSINESS TERMS. median. *Academic Dictionaries and Encyclopedias* [online]. 2012 [cit. 16. 7. 2021]. Dostupné z: https://business_finance.enacademic.com/21867/median

684 Tuto hodnotu je na místě brát s rezervou, jelikož 34 % z 829 dotazovaných podniků odpovědělo, že na kyberbezpečnost vynakládá 0 GBP. Z tohoto důvodu může být průměr reprezentativnější hodnotou než medián, ten je pak 2 600 GBP. Srov. KLAHR, Rebecca et al. *Cyber Security Breaches Survey 2017* [online]. London: UK Department for Culture, Media & Sport, 2017, s. 21.

úrovní opatření pro zajištění bezpečnosti zpracovávaných osobních údajů a kapacitou podniku včas odhalit a přiměřeně reagovat na porušení bezpečnosti.

Podnikové sítě mikropodniků mohou mít řadu nedostatků. Mohou využívat zastaralé či neefektivní detekční a bezpečnostní nástroje. Může být zavedena rozvolněná BYOD politika, která umožňuje zranitelným zařízením přístup do sítě bez řádné kontroly.[685] Je pravděpodobné omezené zaškolení a organizace zaměstnanců, kteří nemají povědomí o hrozbách a jednají bez pokynů ohledně postupů, které snižují riziko.[686] Toto výrazně posiluje pravděpodobnost neodhaleného případu porušení bezpečnosti a omezuje tak možnost včasné nápravy, což zvyšuje možnou újmu.

Podnikové sítě mikropodniků lze přitom vnímat za hodnotný cíl útoků. Mohou obsahovat významné databáze osobních či jiných údajů. Zranitelná zařízení v sítích mikropodniků mohou být zneužita k útokům na třetí strany. V neposlední řadě pak mohou sítě mikropodniků nabízet přístup do lépe chráněných systémů a sítí výše v dodavatelském řetězci.[687]

Pokládám za zřejmé, že s rozvojem internetu věcí bude docházet k vyšší provázanosti problematiky ochrany osobních údajů a kyberbezpečnosti podnikových sítí.[688] Povinnosti týkající se zpracování osobních údajů tudíž nelze vnímat ve vakuu, jelikož zranitelné mikropodniky mohou znamenat ohrožení širokého spektra třetích subjektů. Plošné zavádění prvků internetu věcí do takto slabě chráněných podnikových sítí mikropodniků by mohlo z hlediska kyberbezpečnosti přinést „dokonalou bouři" *(perfect storm)*.[689] Existují

685 Srov. WHITWELL, Joe. Small businesses should invest in cyber security. *The Telegraph* [online]. 2017 [cit. 10. 10. 2021].

686 Toto platí především pro správu hesel a datových přenosů, jakož i krizové procesy pro situace porušení bezpečnosti či podvodu na základě sociálního inženýrství. Blíže viz LOUTOCKÝ, Pavel a Kamil MALINKA. Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců. *Revue pro právo a technologie*, 2016, roč. 7, č. 14, s. 45 a násl.

687 Typickým je v tomto směru případ porušení bezpečnosti retailové společnosti *Target*, který ohrozil především finanční údaje až 110 milionů držitelů kreditních a debetních karet. Došlo k němu skrze subdodavatele, společnost *Fazio Mechanical*, která poskytuje služby chladících systémů. Blíže viz KASSNER, Michael. Anatomy of the Target data breach: Missed opportunities and lessons learned. *ZDNet* [online]. 2. 2. 2015 [cit. 16. 7. 2021]. Dostupné z: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

688 Srov. ENISA. *Guidelines for SMEs on the security of personal data processing*. 2016, s. 7 a 8.

689 Srov. WEBER, Rolf H. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, 2016, roč. 2016, č. 32, s. 16.

značné obavy, že rozsáhlá adopce prvků internetu věcí povede k nárůstu bezpečnostních incidentů.[690] Tato zařízení jsou i institucemi jako je Europol považována za „zesilovače hrozby",[691] jelikož zvyšují složitost sítových interakcí, rozšiřují možné vektory útoku a jsou zvláště snadno ovládnutelná (skrze *class break)*[692] do podoby botnetu.

Mikropodniky a povinnosti související s porušením zabezpečení dle Obecného nařízení: Unijní právní rámec na ochranu osobních údajů směřuje k vysoké úrovni ochrany osobních údajů jednotlivce. Stanoví proto přiměřené požadavky na podnikovou úroveň technických a organizačních opatření vztahujících se ke zpracování osobních údajů, které dopadají i na mikropodniky. Tyto povinnosti z větší části nejsou nové,[693] přesto však vytrvale přinášejí těmto subjektům potíže s implementací, mimo jiné i pro omezené množství a použitelnost dostupných vodítek a výkladových materiálů.[694]

Potřebná opatření se nevztahují pouze k technickým nástrojům, tedy správě přístupu, autentizaci uživatelů, zálohování, monitoringu či ohlašování, ale i k organizační rovině. Zvláště pro zabránění porušení zabezpečení v důsledku náhodného jednání a ochraně proti sociálnímu inženýrství[695] je významná práce se vzděláním, motivací a komunikací zaměstnanců.

Režim souladu podle Obecného nařízení primárně stojí na zásadě odpovědnosti správce,[696] vyžadujíce prokázání přiměřenosti realizovaných opatření. Tvůrci úpravy v tomto ohledu od počátku vnímali potřebu proporcionality a přihlížení k odlišnostem možností a postavení různých subjektů, zvláště pak

690 Viz MARINOS, Louis, Adrian BELMONTE a Evangelos REKLEITIS. *ENISA Threat Landscape 2015* [online]. Heraklion: ENISA, 2015, s. 74 a násl. [cit. 12. 7. 2021]; SYMANTEC. *Internet Security Threat Report 2017 Volume 22* [online]. 2017, s. 63 a násl. [cit. 12. 7. 2021].

691 Podle zprávy Europolu již nelze internet věcí považovat za novou hrozbu, ale za běžnou složku vyšetřování kyberkriminality. EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. The Hague: European Police Office, 2016, s. 52.

692 K pojmu viz výše závěr podkapitoly 4.3.

693 Současná úprava dle Obecného nařízení do značné míry odráží požadavky dle čl. 17 směrnice 95/46/ES.

694 Srov. ENISA. *Guidelines for SMEs on the security of personal data processing*. 2016, s. 5–6.

695 Viz MOUTON, Francois, Louise LEENEN a Hein S. VENTER. Social engineering attack examples, templates and scenarios. *Computers & Security* [online]. 2016, roč. 59, s. 207.

696 Viz čl. 24 odst. 1 Obecného nařízení.

MSP.[697] Použitelná úprava v současném výkladu však příliš odlehčení nepřiměřené zátěže MSP nenabízí. Příkladem uvažme, že přes výslovnou výjimku obsaženou v článku 30 odst. 5 Obecného nařízení, povinnost vést záznamy zpracování na většinu MSP stejně dopadá a těmto podnikům je i ze strany dozorových úřadů doporučováno vést řádné záznamy v souladu s tímto článkem.[698] To platí i pro dokumentační povinnost případů porušení zabezpečení. MSP dále nejsou nijak vyňaty z povinností provést přiměřená technická a organizační opatření pro zabezpečení zpracování a dopadají na ně bez výjimek i povinnosti ohlašování a oznamování případů porušení zabezpečení osobních údajů dle článků 33 a 34 Obecného nařízení.

Zvláště mikropodniky se tak, dle mého názoru, ocitají ve znevýhodněné pozici z hlediska poměru povinností a kapacit pro zajištění řádného souladu s právní úpravou ochrany osobních údajů. V důsledku širokého užití performativních pravidel, přenášejících výklad neurčitých právních pojmů na povinné subjekty v předmětné úpravě, je do značné míry nezbytné i pro tyto podniky podrobně se seznámit s koncepcí Obecného nařízení a být schopen důsledného výkladu požadavků pro specifika svých aktivit. Zde jsou pak především mikropodniky významně zatěžovány nedostatkem vlastní odborné know-how, umocněnou nedostupností konkrétně orientovaných vodítek a doporučení dobré praxe.[699] Byť ENISA vydala doporučení pro MSP již koncem roku 2016,[700] jejich obecnost je značně limitující pro snadnou aplikaci na konkrétní situaci. Spektrum situací, ve kterých

697 Viz DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. EU Data Protection Reform: What benefits for businesses in Europe? Fact sheet. *European Commission* [online]. Brussels: European Commission, 2016, s. 5 a 6 [cit. 29. 9. 2021].

698 Viz VAN CANNEYT, Tim; PROVOOST, Soo Mee. Belgian DPA publishes recommendation on GDPR record keeping obligation. *fieldfisher* [online]. 4. 7. 2017 [cit. 3. 10. 2021]. Dostupné z: http://privacylawblog.fieldfisher.com/2017/belgian-dpa-publishes-recommendation-on-gdpr-record-keeping-obligation/

699 Srov. FREITAS, Maria da Conceição a Miguel Mira da SILVA. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering and Management* [online]. 2018, roč. 3, č. 4; KAPOOR, Keshav, Karen RENAUD a Jacqueline ARCHIBALD. Preparing for GDPR: helping EU SMEs to manage data breaches. In: *2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security* [online]. Liverpool: Society for the Study of Artificial Intelligence and Simulation for Behaviour (AISB), 2018 [cit. 16. 7. 2021].

700 Srov. již výše citované ENISA. *Guidelines for SMEs on the security of personal data processing*. 2016.

se mikropodniky nacházejí je přitom velmi široké a s adopcí různých kombinací zařízení internetu věcí bude dále významně narůstat.

Shrnutí poznatků: Mikropodniky se nacházejí ve zvláště zranitelném postavení ve vztahu ke kyberbezpečnostním hrozbám. Již v současné době je dosahování přiměřené úrovně bezpečnostních opatření v podnikových sítích těchto subjektů problematické. Nové vektory zranitelností, které přinesou zařízení internetu věcí pak mohou značit závažný problém nejen pro dotčené subjekty údajů, ale též pro další subjekty v rámci dodavatelských řetězců. Hlavním problémem pro mikropodniky je neúměrný nárůst potřebných opatření ve vztahu k jejich kapacitám a odbornému know-how. Tento nepoměr je pouze nominálně reflektován právní úpravou a v současné době nejsou dostatečně dostupná a rozšířená praktická vodítka a příklady dobré praxe, která by mikropodnikům v nejrůznějších odvětvích usnadnila výklad a realizaci potřebných opatření dle požadavků Obecného nařízení a tím zlepšila jejich situaci tváří rostoucím hrozbám v kontextu internetu věcí.

4.5 Výzvy pro povinnosti spojené s porušením bezpečnosti v kontextu internetu věcí

Předcházející podkapitoly představily nejprve obecně a následně na třech významných dílčích perspektivách výzvy a překážky, které přináší internet věcí především pro oblast kyberbezpečnosti. Tu je však na místě brát za notně propojenou s požadavky na základě právního rámce na ochranu osobních údajů, zvláště pak ve spojitosti s porušením bezpečnosti.

Obecné nařízení bylo navrženo a přijímáno se zohledněním dynamiky technologického vývoje a z ní plynoucích výzev. Lze vnímat snahu o stabilitu normativního rámce navzdory proměnám regulovaného prostředí, který se odráží v technologické neutralitě normy, preferenci performativních pravidel, přítomnosti normativních nástrojů chytré regulace i dalších projevů abstraktnosti řady ustanovení. Obecné nařízení lze tak brát za pevnou základní normu, to však nevylučuje případnou vhodnost doplnění či rozšíření normativní struktury o speciální úpravu reagující na významné proměny regulovaného prostředí. To platí zvláště pro změny v procesech a vzorcích zpracování a sdílení osobních údajů. Tato adaptace normativního rámce lze

pokládat za nezbytnou pro kontinuitu vysoké úrovně ochrany osobních údajů a předvídá ji v tomto směru i samo Obecné nařízení.[701]

Na základě představeného rozboru charakteristik prostředí internetu věcí a souvisejících dopadů na zajištění bezpečnosti zpracovávaných osobních údajů pokládám tento technologický fenomén za příklad kontextu, kde lze o dodatečné normativní specifikaci v tomto duchu uvažovat. Zvláště významná je přitom narůstající složitost vícevrstvých síťových vztahů pro neustálé zachycování a sdílení osobních údajů a dalších dat. To souvisí na jedné straně s rozvojem technologických řešení, ať již se jedná o nové formáty *mesh* sítí zaváděné v rámci standardu 5G, rostoucí automatizaci M2M komunikace či převládající koncept centralizovaného zpracování údajů shromažďovaných koncovými zařízeními za pomoci *cloud computingu*.[702] Současně vnímám i organizační a společenskou proměnu vedenou rozvojem internetu věcí, která je nejlépe patrná na nových *ad hoc* vazbách a vícevrstvých propojeních utvářených v rámci chytrého města.[703] Nelze pak pomíjet, že rozšiřování internetu věcí nevyhnutelně vede k zapojení více subjektů do datových toků a více mikropodniků tudíž musí řešit zajištění přiměřených opatření na zabezpečení zpracovávaných osobních údajů, nejen v zájmu ochrany subjektů údajů, ale též pro zabránění vzniku kriticky zranitelných míst v rámci dodavatelských řetězců.[704]

Na základě shromážděných poznatků z těchto perspektiv a kontextů nyní naváži na obecné poznatky o trendech v četnosti a intenzitě porušení bezpečnosti představených v druhé kapitole. Pro celkové zachycení výzev a překážek, které přináší rozvoj internetu věcí pro povinnosti spojené s porušením bezpečnosti formuluji čtyři hlavní formy proměny. Těmi jsou:

1. zvýšení frekvence a množství případů porušení bezpečnosti;
2. zvýšení závažnosti újmy v důsledku porušení bezpečnosti;
3. znesnadnění odhalení porušení bezpečnosti;
4. nárůst složitosti a četnosti situací se společnými správci.

701 Srov. bod odůvodnění 10 Obecného nařízení.
702 Tyto perspektivy jsem podrobně představil v oddílu 4.4.1.
703 Tomu jsem věnoval pozornost v rámci oddílu 4.4.2.
704 O tom bylo pojednáno v oddílu 4.4.3.

4.5.1 Zvýšení frekvence a množství případů porušení bezpečnosti

Předpokládané masové rozšíření zařízení internetu věcí v podnikovém prostředí i v soukromém užití je často vnímáno s významnými obavami ohledně možného nárůstu bezpečnostních hrozeb. Provázaná povaha tohoto prostředí je považována za „zesilovač hrozby“,[705] zvláště s ohledem na dodatečnou složitost, která vytváří nové formy přímých či nepřímých zranitelností. Současné bezpečnostní nedostatky řady široce užívaných zařízení internetu věcí pak dále hrozí tím, že dosahování potřebné úrovně bezpečnostních opatření v prostředí s rostoucí mírou digitalizace bude stále složitější,[706] zvláště pro správce s omezenými kapacitami a know-how, mezi které lze zahrnout řadu mikropodniků. S tím lze předpokládat nejen růst neodhalených případů porušení bezpečnosti, ale především celkové hrozící újmy dotčeným subjektům údajů.

4.5.2 Zvýšení závažnosti újmy v důsledku porušení bezpečnosti

Internet věcí v širokém pojetí přináší kvalitativní proměnu možné formy újmy v důsledku bezpečnostního incidentu, vzhledem k významnému provázání fyzické a digitální povahy řady takto propojených zařízení.[707] Za nejvýznamnější lze v tomto směru vnímat hrozby pro život a zdraví např. při napadení ovládací jednotky moderního vozidla za jízdy.[708]

Nové funkcionality zařízení internetu věcí však taktéž zvyšují ohrožení jednotlivců v důsledku porušení bezpečnosti zpracovávaných osobních údajů, např. skrze neoprávněnou aktivaci a ovládání zařízení shromažďujícího osobní údaje kamerami či jinými senzory.[709] Vlastní všudypřítomnost

705 Srov. EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. The Hague: European Police Office, 2016, s. 52.

706 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 27–28.

707 Řada prvků internetu věcí má aktivní prvky řízené software (uvažujte robotiku, ale též podpůrné prvky při řízení vozidla či pilotování dronu). Dále se v současné době významně rozvíjí možnosti automatického řízení a rozhodování (až už jde o autonomní vozidla či domácí asistenty).

708 Viz GREENBERG, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired* [online]. 2015 [cit. 5. 8. 2021].

709 Příkladem může být riziko přítomnosti chytrého asistenta jako je *Alexa* v prostorách vnímaných z hlediska soukromí jako intimních, tedy např. v ložnici. Srov. CUTHBERTSON, Anthony. Alexa needs to be banned from the bedroom, privacy expert says. *The Independent* [online]. 17. 12. 2019 [cit. 16. 7. 2021]. Dostupné z: https://www.independent.co.uk/life-style/gadgets-and-tech/news/alexa-privacy-amazon-echo-delete-recordings-a9249951.html

a adaptibilita těchto prvků je pak předpokladem pro výrazně komplexnější a detailnější soubory osobních údajů a profilování fyzických osob.[710] Internet věcí je tak cestou k vyšší personalizaci služeb, optimalizaci procesů i uspokojování nových potřeb a preferencí. Související obohacení kyberprostoru o nové prvky datové stopy jednotlivců a celková digitalizace rostoucího množství mezilidských interakcí však zároveň promění vnímání soukromí a intimity.[711] Rostoucí závislost jednotlivce na virtuálních identitách a profilech na digitálních službách v rámci profesní, společenské či intimní komunikace[712] (jakož i pro vnímání sama sebe) je pak s to zvyšovat újmu (včetně stresu a duševního nepohodlí) při porušení bezpečnosti. Vlastní újmu pak může dále navýšit krádež identity, ztráta personalizovaného nastavení či zneužití shromážděných citlivých osobních údajů proti zájmům daného subjektu údajů.

4.5.3 Znesnadnění odhalení porušení bezpečnosti osobních údajů

Produkty internetu věcí mají již dnes řadu zdokumentovaných bezpečnostních nedostatků, které mohou činit monitorování či odstraňování porušení bezpečnosti osobních údajů složitější.[713] Potenciálně škodlivější než rozsáhlé, silně medializované případy porušení bezpečnosti jsou pak četná skrytá zneužití zranitelností, která umožňují dlouhodobé či pro jednotlivce citelné zneužití přístupu k datům a osobním údajům bez včasného varování ohrožených subjektů údajů.

Nárůst možných vektorů zranitelností[714] v kombinaci se zvyšujícím se množstvím zpracovávaných osobních údajů a omezenými kapacitami řady správců

710 Viz MARAS, Marie-Helen. Tomorrow's Privacy. Internet of Things: security and privacy implications. *International Data Privacy Law*, 2015, roč. 5, č. 2, s. 101.

711 Viz COSTA, Luiz. *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*. Cham: Springer International Publishing, 2016, s. 128–129.

712 Specifickou oblastí, na které lze sledovat tyto projevy rostoucího významu virtuálních identit je nárůst popularity aktivní tvorby v rámci platforem jako je *YouTube* mezi dětmi a mladistvými. Tomuto tématu jsem se podrobně věnoval v KASL, František. *Tvorba YouTuberů prizmatem práva na ochranu osobnosti dětí a mladistvých*. Rigorózní práce. Brno: Masarykova univerzita, Právnická fakulta, 2019.

713 Viz SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 30 a 31.

714 Srov. ENISA. *Baseline Security Recommendations for IoT* [online]. Report/Study. Heraklion: ENISA, 2017, s. 31–35 [cit. 16. 7. 2021].

a zpracovatelů (zvláště z řad mikropodniků) důsledně dodržovat požadavky zajištění bezpečnosti zpracovávaných osobních údajů přináší rostoucí riziko právě těchto skrytých porušení bezpečnosti. Bez adekvátního tlaku regulátora skrze vymahatelný a vymáhaný rámec povinností vyžadujících důslednou detekci, včasné ohlášení a účinné zmírnění následků těchto incidentů lze očekávat nárůst disparity mezi normativní strukturou na ochranu zájmů subjektů údajů (tedy právem zaručenou vysokou úrovní jejich ochrany) a reálnou kapacitou regulátora tuto ochranu zajišťovat (tedy jejich skutečnou úrovní ochrany).

4.5.4 Nárůst složitosti a četnosti situací se společnými správci

Významným aspektem regulatorního rámce Obecného nařízení je snadno uchopitelný mechanismus přiřazení odpovědnosti za dodržení souladu konkrétním povinným subjektům.

Komplexní struktury služeb v překrývajících se vrstvách,[715] které díky internetu věcí nalézáme především v prostředí chytrého města, zvyšují pravděpodobnost složitých, proměnlivých a celkově nepřehledných právních vztahů mezi povinnými subjekty. Mnohost subjektů zúčastněných na shromažďování, přenosu a zpracování osobních údajů povede v řadě situací k založení vztahu společných správců dle článku 26 Obecného nařízení.

Současný nárůst frekvence a autonomie M2M komunikace mezi prvky internetu věcí (např. s ohledem na významnější roli procesů koordinovaných umělou inteligencí)[716] povede k dynamičtějším *ad hoc* vztahům datových přenosů a kombinacím zpracovávaných osobních údajů napříč správci a zpracovateli, což se odrazí na méně zřetelném ujednání ohledně dělby rolí a povinností mezi těmito subjekty.

---

715 Na základní fyzické rovině nalézáme senzory, moduly pro shromažďování dat a další vstupy. Samostatnou rovinou jsou pak komunikační protokoly a síťové prvky pro datové přenosy. Nad nimi běží funkční a aplikační roviny, které obsahují vlastní služby a procesy využívající data shromážděná a komunikovaná nižšími vrstvami. Srov. YANG, Xue et al. A Multi-layer Security Model for Internet of Things. In: WANG, Yongheng a Xiaoming ZHANG (eds.). *Internet of Things*. Berlin/Heidelberg: Springer, 2012, s. 389, Communications in Computer and Information Science.

716 Srov. FANG, Junbin et al. Position Paper on Recent Cybersecurity Trends: Legal Issues, AI and IoT. In: AU, Man Ho et al. (eds.). *Network and System Security*. New York: Springer International Publishing, 2018, Lecture Notes in Computer Science.

S ohledem na nesnadné přesné určení časového okamžiku porušení bezpečnosti vzniká prostor pro ospravedlnění opomíjení notifikačních povinností ze strany potenciálně všech společných správců. Vyšší neurčitost rozsahu povinností jednotlivých subjektů ve vztahu k dané instanci zpracování osobních údajů se, dle mého názoru, projeví negativně především na plnění ohlašovací povinnosti vůči dozorovému úřadu. Lze totiž předpokládat, že subjekt, který dozorový úřad upozorní na porušení bezpečnosti, na sebe tímto přebírá hlavní odpovědnost za řešení dané situace, což vzhledem k předpokládaným s tímto spojovaným dodatečným nákladům nelze zpravidla vnímat jako racionální rozhodování podniku. Tuto perspektivu blíže rozvádím v následující páté kapitole.

4.6 Diskuse

Jak představeno v rámci této kapitoly, internet věcí s sebou přináší významnou proměnu procesů a vzorců zpracování osobních údajů a nové výzvy v oblasti zajištění bezpečnosti. Tím hrozí dosažením limitů současného právního rámce povinností pojících se s porušením zabezpečení osobních údajů dle Obecného nařízení, co se týká kapacity povinných subjektů (zvláště mikropodniků) včasně odhalit všechna porušení zabezpečení a řádně je ohlásit dozorovému úřadu či případně oznámit dotčeným subjektům údajů.

Rostoucí přítomnost propojených zařízení zpracovávajících osobní údaje, které jsou značně zranitelné ať již jednotlivě, či v důsledku svého propojení a přímých či nepřímých závislostí, zvyšuje potřebu koordinace a standardizace opatření na ochranu zpracovávaných osobních údajů napříč všemi segmenty správců a zpracovatelů.

Vyšší expozice jednotlivců skrze datovou stopu a podrobné profily v rámci digitalizovaných služeb moderní společnosti posílí jejich závislost na řádném fungování těchto procesů a vystaví je tak větším rizikům v případě porušení bezpečnosti. Zajištění vysoké úrovně ochrany osobních údajů je předpokladem důvěry uživatelů v tyto služby, což vyžaduje funkční normativní rámec příslušných povinností představených v rámci třetí kapitoly pro toto prostředí.

Klíčovým faktorem je přitom včasnost reakce na vzniklé porušení bezpečnosti. Přitom v tomto ohledu je již dnešní situace značně neuspokojivá, když

z bezpečnostní zprávy společnosti *Ponemon Institute* vyplývá, že průměrná doba mezi případem porušení bezpečnosti a jeho odhalením postiženou entitou dosahovala v roce 2019 tragických 206 dní (2017 to bylo 191 dní, 2018 pak 197 dní).[717] Při této úrovni obtíží povinných subjektů řádně odhalit případy porušení bezpečnosti přitom vyvstávají pochybnosti nejen o smysluplnosti přísné normativní lhůty 72 hodin pro ohlášení případu porušení dle článku 33 Obecného nařízení, ale především reálné kapacity většiny podniků a institucí odhalit alespoň závažné případy porušení bezpečnosti.[718]

Vzhledem k překážce střetu zájmů povinných subjektů, která byla identifikována ve spojitosti s porušením zabezpečení v rámci diskuse v předcházející třetí kapitole, u které nemám důvod pochybovat o platnosti i pro prostředí internetu věcí, je na místě před diskusí možných řešení blíže analyzovat motivaci k plnění či neplnění notifikačních povinností. Tím bude možné odhadnout realistické předpoklady pro vymahatelnost představených normativních povinností a přenést je do prostředí internetu věcí.

4.7 Shrnutí kapitoly

V rámci této kapitoly zaměřené na technologickou perspektivu proměny prostředí v důsledku rozvoje internetu věcí jsem nalézal odpovědi na soubor dílčích otázek, které jsou metodickým vodítkem při dosahování cíle představované monografie. Ten směřuje k posouzení, zda má současná právní úprava povinností při porušení zabezpečení osobních údajů dle Obecného nařízení účelné uplatnění i v prostředí internetu věcí, a pokud ano, pak jakými úpravami lze překonat zjištěné výzvy a překážky.

Nejprve jsem zde tedy přistoupil k vymezení pojmu internet věcí.[719] Následně jsem identifikoval nové formy a vzorce zpracování osobních údajů v tomto kontextu.[720] Ty souvisejí nejen s narůstajícím rozsahem zpracování osobních údajů, ale i s rozmanitostí struktury předmětných procesů a s rozšířením

717 Blíže viz PONEMON INSTITUTE. *Cost of a Data Breach Report 2019* [online]. Traverse City: IBM Security, 2019, s. 50 [cit. 22. 5. 2021].

718 Na zdroje formulující tyto pochybnosti jsem již odkazoval v rámci druhé kapitoly. Srov. BISOGNI, Fabio, Hadi ASGHARI a Michel J. G. VAN EETEN. Estimating the size of the iceberg from its tip. In: *16th Annual Workshop on the Economics of Information Security*: *WEIS 2017* [online]. San Diego: University of California, 2017 [cit. 12. 7. 2021].

719 Srov. podkapitola 4.1.

720 Srov. podkapitola 4.2.

M2M komunikace. Všudypřítomnost zpracování pak hrozí absencí povědomí subjektu údajů o tomto zpracování, což vede k nepředvídatelnosti jeho rozsahu, a tudíž možného rozsahu újmy v případě porušení bezpečnosti. Tento nárůstu hrozeb jsem popsal na příkladu rozvoje internetu věcí u kamerových systémů. V něm se výstižně projevuje i častá ambientní povaha zařízení internetu věcí. Nadto jsem přihlížel k zesilujícímu efektu *cloud computingu* a vytěžování databází *big data*.

Další rovinou, které jsem věnoval pozornost, byla problematika zajištění bezpečnosti.[721] Zde jsem upozornil na bezpečnostní limity řady zařízení internetu věcí, související mimo jiné s problémem aktualizace a opravy software. Pro lepší představu o nastíněných výzvách jsem dále přistoupil k podrobné analýze tří významných scénářů, z nichž každý výstižně poukazuje na odlišný aspekt proměny zpracování osobních údajů v tomto kontextu.[722] Věnoval jsem tak pozornost (i) dopadům automatizované komunikace na rozsah sdílení osobních údajů mezi zařízeními, (ii) dynamice interakce v rámci chytrého města a *ad hoc* zpracování společnými správci, a (iii) opomíjenému významu mikropodniků.

Při rozboru automatizované komunikace mezi stroji a prostředí autonomních zařízení[723] jsem nejprve představil existující komunikační standardy pro internet věcí a následně se zaměřil na novou generaci telekomunikačních standardů 5G. Zde jsem diskutoval význam cloudových služeb a nárůst sdílení osobních údajů, jakož i nové bezpečnostní výzvy spojené se zavedením 5G, např. v kontextu *mesh* sítí. Závěrem z této perspektivy je, že u internetu věcí na bázi technologie 5G lze očekávat častější případy porušení bezpečnosti s citelnějšími dopady, a také častější opominutí odhalení a řádného ohlášení významného porušení bezpečnosti.

Druhou specifickou perspektivou, které jsem věnoval pozornost byly přímé a nepřímé provázanosti sítí chytrého města.[724] Zde jsem nejprve vymezil pojem chytrého města a formy jeho vzniku. Následně jsem se zaměřil na důsledky souhry existující a nové infrastruktury a také na nepřímé modulární závislosti

721 Srov. podkapitola 4.3.
722 Srov. podkapitola 4.4.
723 Srov. oddíl 4.4.1.
724 Srov. oddíl 4.4.2.

mezi jednotlivými prvky. Chytré město je vhodným příkladem nového stupně propojenosti, kterou internet věcí přináší. Lze zde plně vnímat možnou komplexitu zpracování osobních údajů v rámci síťových propojení, ať již slouží k optimalizaci veřejných služeb, či personalizaci doprovodných služeb. Datové toky prostupují napříč moduly a službami mezi prvky infrastruktury a dílčími aktéry, čímž je z hlediska práva ochrany osobních údajů utvářena série zpracování společnými správci. Ti přitom nemusejí být omezeni pouze na relativně stálé poskytovatele služeb, ale mohou se *ad hoc* měnit v závislosti na míře provázanosti infrastruktury a datových toků v rámci chytrého města. To přináší dodatečné překážky pro motivaci jednotlivých povinných subjektů odhalovat a ohlašovat porušení bezpečnosti osobních údajů.

Třetí zkoumanou perspektivou bylo prostředí podnikových sítí a specifická situace mikropodniků.[725] Nejprve vymezuji pojem mikropodnik a následně poukazuji na relevanci rozvoje internetu věci a digitalizace i pro tuto rozsáhlou skupinu povinných subjektů. Vedle vlastních inovací podniku může být vazba utvořena např. skrze zaměstnance vnášením zařízení internetu věcí do podnikových sítí na základě politik BYOD. Zvláštní pozornost věnuji specifickému postavení mikropodniků z hlediska kyberbezpečnosti a jejich často nedostatečným bezpečnostním opatřením, které vedou k významným zranitelnostem. Ty mohou s rozvojem internetu věcí dále významně narůstat a ohrožovat subjekty údajů i další entity v rámci dodavatelských řetězců. Shledávám tak, že se mikropodniky nacházejí ve zranitelném postavení. Realizaci potřebných opatření přitom brání nejen omezené kapacity a know-how těchto podniků, ale též nedostatečná dostupnost praktických vodítek a příkladů dobré praxe, které by alespoň částečně snížily neúměrné zatížení těchto subjektů při výkladu povinností uložených Obecným nařízením.

Na základě výše představených poznatků formuluji čtyři základní oblasti, ve kterých vnímám významnou proměnu povinností souvisejících s porušením bezpečnosti v kontextu internetu věcí.[726] Jedná se o (i) zvýšení frekvence a množství případů porušení bezpečnosti, (ii) zvýšení závažnosti hrozící újmy v důsledku porušení bezpečnosti, (iii) znesnadnění odhalení porušení bezpečnosti a (iv) nárůst složitosti a četnosti situací se společnými správci.

725 Srov. oddíl 4.4.3.
726 Srov. podkapitola 4.5.

Tyto následně diskutuji, přičemž dovozuji přetrvávající či dokonce rostoucí potřebnost právního rámce notifikačních povinností, jakož i zásadní nedostatečnost včasného odhalení a ohlášení porušení zabezpečení již za současné situace.[727] Dále dovozuji, že internet věcí nic nemění na existenci střetu zájmů povinných subjektů při ohlašování porušení bezpečnosti, kterému věnuji hlavní pozornost v rámci následující páté kapitoly.

Výše shrnutá struktura kapitoly přitom sledovala soubor dílčích otázek, které jsem za tímto účelem formuloval v rámci podkapitoly 1.3. Jádro tvořila otázka (2), na kterou jsem zde nabídl odpověď napříč kapitolou a specificky pak v podkapitole 4.5. Ta zněla, zda prostředí internetu věcí přináší nové výzvy pro dodržování povinností souvisejících s porušením bezpečnosti osobních údajů?

Na kladné odpovědi se přitom projevily především kladné odpovědi na navazující (pod)otázky (3),[728] (4),[729] (5)[730] a (6).[731] Ty jsem reflektoval ve vymezení a diskusi hlavních výzev pro povinnosti spojené s porušením bezpečnosti v kontextu internetu věcí v podkapitole 4.5, konkrétně v příslušných oddílech 4.5.1 až 4.5.4. Takto vymezené výzvy a překážky nyní tvoří základ pro nalézání možných řešení, ke kterému přistupuji v šesté kapitole, tedy po nadcházejícím zohlednění dodatečných aspektů motivace povinných subjektů z ekonomické perspektivy.[732]

727 Srov. podkapitola 4.6.
728 Dochází v tomto prostředí k navýšení četnosti a rozsahu porušení bezpečnosti?
729 Narůstá zde též intenzita a škodlivý dopad případů porušení bezpečnosti?
730 Vyvstávají v něm nové překážky odhalení případů porušení bezpečnosti?
731 Přináší prostředí internetu věcí specifické výzvy pro určení povinných subjektů?
732 Srov. pátá kapitola.

5 MODELOVÁNÍ MOTIVACE POVINNÝCH SUBJEKTŮ PRO DODRŽOVÁNÍ POVINNOSTÍ

V předcházejících kapitolách jsem čtenáři postupně představil situace, ve kterých zpravidla dochází k porušení bezpečnosti,[733] evropské i americké právní rámce, které směřují k narovnání postavení dotčených subjektů a omezení hrozící újmy[734] a nové výzvy, kterými se technologická proměna světa kolem nás promítá do zpracování osobních údajů a rizik pro bezpečnost těchto procesů.[735]

Napříč perspektivami nastíněnými v předchozích kapitolách jsme opakovaně naráželi na potřebu zohlednění přístupu povinného subjektu k vyhodnocení rizika spojeného s následky porušení bezpečnosti a jeho motivace k dodržení notifikačních povinností. V těchto úvahách však nepostačuje čistě právní náhled na předmětnou problematiku, jelikož naše pozornost směřuje nikoliv toliko k vyváženosti práv a povinností dotčených subjektů na základě aplikovatelného normativního rámce, ale k možnosti modelovat a zhodnotit reakci povinných subjektů na právem uložené povinnosti a adekvátnost nastavení struktury dané normy jako takové. V této kapitole tudíž představuji řešenou problematiku z ekonomické perspektivy, přičemž mám za cíl pojmenovat a modelovat výzvy, které se pojí s rozhodováním povinných subjektů ohledně dodržování notifikačních povinností. Naplno přitom využívám dostupných zdrojů z amerického odborného diskurzu, který je právě v tomto směru výrazně rozsáhlejší než ten evropský.

Přestože již v předchozích kapitolách byla v duchu pragmatické metody v přístupu k řešené problematice provazována právní perspektiva s převážně technologickými či kyberbezpečnostními pohledy na dílčí otázky, zde právo dočasně ustupuje významně do pozadí. Zahrnutím této roviny zdůrazňuji multidisciplinární povahu představované monografie. Na vhodnost tohoto přístupu k otázkám z oblasti ochrany osobních údajů přitom usuzuji mimo jiné z prohlášení, které učinil *Bygrave*, že „[právní věda ochrany osobních

733 Srov. druhá kapitola.
734 Srov. třetí kapitola.
735 Tato proměna je zachycena jako rozvoj internetu věcí a představena v přecházející čtvrté kapitole.

údajů] *by měla také studovat regulatorní normy z perspektivy jiných oblastí a disciplín. Toto vyžaduje relativně otevřené a eklektické využívání zdrojových materiálů a metod studia, které spoléhají na prvky ze širokého okruhu disciplín zahrnujících informatiku, sociologii, filozofii, politické vědy, antropologii a ekonomii.*"[736]

Omezení na podnikatelské subjekty: Povinnými subjekty ve vztahu k řešené problematice porušení bezpečnosti osobních údajů jsou správci osobních údajů. Těmi mohou být nejrůznější fyzické či právnické osoby. Jsou jimi však v převážné míře komerční subjekty,[737] které zpracovávají osobní údaje v rámci podnikatelské činnosti, a tudíž jako součást souboru aktivit, které jsou z ekonomického hlediska vnímány jako racionální a primárně směřující k vytváření zisku.[738] Jednání takového subjektu je jedním z ústředních zaměření modelů ekonomické teorie, jelikož z něj lze dovozovat pravidla a zákonitosti na mikroekonomické úrovni a tím racionalizovat tržní jednání.[739] V rámci těchto úvah je s každým rozhodnutím spojováno posouzení předpokládaných přínosů a nákladů, tedy bilancování incentiv,[740] a následná

736 *„legal scholarship* […] *ought also to study the regulatory norms from the perspectives of other fields and disciplines. This necessitates a relatively open and eclectic use of source materials and study methods that rely on elements from a broad range of disciplines, including informatics, sociology, philosophy, political science, anthropology and economics."* Srov. BYGRAVE, Lee A. Legal Scholarship on Data Protection: Future Challenges and Directions. In: *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde Liber Amicorum Yves Poullet*. 1. vyd. Brussels: Larcier, 2018, s. 501.

737 Toto zúžení pojmu je nevyhnutelně omezující, z ekonomické perspektivy však nelze srovnatelně modelovat rozhodovací procesy subjektů, jejichž zájmy nejsou vedeny primárně ekonomickou úvahou. Přesto však nevnímám, že by toto zjednodušení mělo zásadní vliv na závěry této monografie. Ačkoliv nelze u subjektů založených za jiným účelem než k dosahování zisku vnímat srovnatelnou sílu motivačních nástrojů čistě ekonomické povahy, v rámci šesté kapitoly ani žádné takové nediskutuji. Jelikož tedy úvahy o možných řešeních nejsou vázány na nezbytnost čistě racionálního ekonomického uvažování povinného subjektu, vnímám zjednodušení přijaté v této kapitole za zpřehledňující již tak pro čtenáře poměrně náročné perspektivy.

738 Jinými účely existence právnických osob než dosahování zisku, může být např. plnění funkce uložené zákonem, správa majetku, organizace společného zájmu společníků či omezení rizika. K poslednímu zmíněnému účelu viz CHEN, James. What Is a Special Purpose Vehicle (SPV)? *Investopedia* [online]. 29. 6. 2020 [cit. 16. 7. 2021]. Dostupné z: https://www.investopedia.com/terms/s/spv.asp

739 Srov. SIMON, Herbert S. Rational Decision-Making in Business Organizations. Nobel Memorial Lecture, 8. 12. 1977. In: LINDBECK, Assar (ed.). *Economic Sciences, 1969–1980: The Sveriges Riksbank (Bank of Sweden) Prize in Economic Sciences in Memory of Alfred Nobel*. Singapore, New Jersey, London, Hong Kong: World Scientific, 1992, s. 343.

740 Incentivou je pobídka, která daný subjekt motivuje k dané aktivitě či volbě. K pojmu blíže viz MARTIMORT, David (ed.). *The Economic Theory of Incentives* [online]. Cheltenham: Edward Elgar Publishing, 2017, The International Library of Critical Writings in Economics series [cit. 16. 7. 2021].

volba relativně nejvýhodnějšího postupu. To bude podrobněji osvětleno dále v podkapitole 5.2.

Předtím ještě přiblížím pojem rizika a výzvy spojené s hodnocením rizika a správou.[741] Poznatky o riziku a racionálním rozhodování následně uplatním při rozboru dvou rovin řešené problematiky. Nejprve přihlédnu k rozhodování povinného subjektu ohledně přiměřenosti bezpečnostních opatření v kontextu rozpočtových omezení a optimálního přínosu dané investice z hlediska podniku a z hlediska společnosti (tedy subjektů údajů). Zde budu také zjišťovat, jaký význam má sdílení informací o porušení bezpečnosti s jinými subjekty a jaké jsou případné překážky jeho fungování.[742] Poté již přistoupím k vlastnímu dilema střetu zájmů podniku spojeného s povinností ohlásit případ porušení bezpečnosti dozorovému orgánu.[743] V tomto směru nejprve představím dva významné ekonomické modely, které můžeme užít k jeho zachycení, tedy *Garciův* model[744] a *Laubeho* a *Böhmeho* model,[745] a následně budu diskutovat význam těchto poznatků pro řešenou problematiku a jejich uplatnitelnost v kontextu internetu věcí.[746]

5.1 Riziko a hodnocení rizika

Klíčovým aspektem pojícím se s vyhodnocením vhodné reakce na porušení bezpečnosti je riziko. To se procesem prolíná v řadě kontextů. Pro oblast kybernetické bezpečnosti je pojem rizika vnímán ve třech rovinách. Jde o:

1. nebezpečí, možnost škody, ztráty, či nezdaru;
2. účinek nejistoty na dosažení cíle; či
3. možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.[747]

V kontextu ochrany osobních údajů lze pak tyto tři roviny odhalit taktéž. (i) Správce je dle článku 32 Obecného nařízení povinen vyhodnotit rizikovost

741 Srov. podkapitola 5.1.
742 Srov. podkapitola 5.3.
743 Srov. podkapitola 5.4.
744 Srov. oddíl 5.4.1.
745 Srov. oddíl 5.4.2.
746 Srov. podkapitola 5.5.
747 Viz JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti* [online]. Brno: Národní centrum kybernetické bezpečnosti, 2015, s. 85 [cit. 10. 1. 2021].

zpracování osobních údajů pro zavedení adekvátních ochranných opatření přiměřeně snižujícím pravděpodobnost neoprávněného zpracování osobních údajů. Přesto riziko překonání bezpečnostních opatření přetrvává a (ii) správce k němu musí přihlížet při aktivní snaze o detekci a vyhodnocení případného porušení bezpečnosti.[748] (iii) Při odhalení takového případu stojí před specifickým vyhodnocením z něj plynoucího rizika nejen pro svá aktiva (tzn. míru ohrožení sítí, systémů či databází), ale i pro dotčené subjekty údajů (tzn. rozsah, citlivost či snadnost zneužití zpřístupněných osobních údajů)[749].

Podstata rizika je intuitivně snadno představitelná, jelikož s ním každý z nás operuje na každodenní bázi. Pro operativní vymezení a správu rizik je však nutné zachytit dostatečně zřetelně hodnoty posuzovaných scénářů, aby o nich mohlo být transparentně rozhodováno.[750] Hodnoty ohrožené rizikem mohou nabývat nejrůznější podoby, přičemž ne všechny podoby je možné vyhodnotit srovnatelně snadno či přesně. Pro některé je možné najít obecně přijímané vyhodnocovací postupy (např. úmrtnost), pro jiné je samotná otázka spojení s hodnotou značně neurčitá (např. ohrožení spravedlnosti).[751] V souladu s body odůvodnění 75 a 76 Obecného nařízení je při hodnocení rizika na místě vycházet primárně z pravděpodobnosti a závažnosti dopadů spojených s daným rizikem. Pro případy porušení zabezpečení osobních údajů je přitom při vyhodnocení s tím souvisejícího rizika klíčové přihlížet k objektivně zhodnotitelné pravděpodobnosti a závažnosti hrozby.[752]

Kvantifikovat závažnost případu porušení zabezpečení je přitom značně nesnadné, což efektivně brání zavedení jednotné metodiky pro vyhodnocování rizik při zpracování osobních údajů. V rámci vodítek byla pro tyto účely identifikována kritéria jako druh porušení, citlivost dotčených osobních

748 Srov. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 13 [cit. 28. 2. 2021].

749 Ibid., s. 24–26.

750 Viz FISCHHOFF, Baruch a John KADVANY. *Risk. A Very Short Introduction*. Oxford: Oxford University Press, 2011, s. 22, Very Short Introductions.

751 Ibid.

752 Viz PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 23 [cit. 28. 2. 2021].

údajů, snadnost identifikace subjektů údajů či specifické charakteristiky správce.[753] Ta však zpravidla nevyhnutelně nabízejí značný prostor pro subjektivní zhodnocení. Řada těchto kritérií nemá jednoznačně kvantifikovatelné vyjádření (srov. specifické charakteristiky správce), a pokud ano, lze je vyjádřit pouze na škále (srov. citlivost dotčených osobních údajů). Značné obliby i v komplexních metodologiích rizika přitom nabývají slovní škály.[754] Ostatně vlastní právní úprava na těchto slovních zachyceních hodnot stojí.[755] Slovní zachycení hodnot je přitom značně subjektivní. *Fischhoff* a *Kadvany* k tomu uvádějí, že to, že je něco „pravděpodobné", může pro někoho znamenat 40 % možnost a pro jiného 70 %. Nadto pro jednu osobu může pravděpodobnost spojená se slovním vyjádřením „pravděpodobně" nabývat různých hodnot v závislosti na diskutovaném jevu.[756]

Objektivní vyjádření bezpečnostního rizika: Zachycení porušení zabezpečení jakožto jevu s objektivně vyjádřenou hodnotou rizika a nákladů je přitom klíčové pro celkovou systematiku správy rizik skrze určení přiměřených ochranných opatření a nastavení vhodných scénářů a procesů pro snížení rizikovosti daných operací ve vztahu ke zpracovávaným osobním údajům. *Shameli-Sendi, Aghababaei-Barzegar a Cheriet* nabízejí významný příspěvek do této problematiky skrze vytvořenou taxonomii přístupů k hodnocení informačních bezpečnostních rizik (*information security risk assessment,* ISRA), založenou na předcházejících 125 studiích z let 1995 až 2014.[757] Poukazují přitom na potřebu zohledňování dynamické proměny technologického prostředí (tzn. i zde pojímaný internet věcí) a kapacit zvažovaného útočníka. Přístupy k hodnocení rizik lze dělit do tří kategorií; založené na aktivech *(asset-driven)*, založené na službách *(service-driven)* a založené na podnikatelské

753 Ibid., s. 25–26.

754 Nízká / střední / vysoká / velmi vysoká závažnost. Srov. ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches [online]. 20. 12. 2013 [cit. 25. 10. 2021]. Dostupné z: https://www.enisa.europa.eu/publications/dbn-severity

755 Povinnost oznámení případu porušení subjektům údajů při pravděpodobnosti *vysokého rizika* pro práva a svobody fyzických osob. Srov. čl. 34 Obecného nařízení.

756 Srov. pravděpodobnost deště proti pravděpodobné výhře v utkání. Viz FISCHHOFF, Baruch a John KADVANY. *Risk. A Very Short Introduction*. Oxford: Oxford University Press, 2011, s. 94, Very Short Introductions.

757 Srov. SHAMELI-SENDI, Alireza, Rouzbeh AGHABABAEI-BARZEGAR a Mohamed CHERIET. Taxonomy of information security risk assessment (ISRA). *Computers & Security* [online]. 2016, roč. 57.

činnosti *(business-driven)*. Přístup založený na aktivech je převažující, vykazuje však nedostatky,[758] které se snaží kompenzovat další zmíněné přístupy. Významným aspektem, který zvyšuje přesnost hodnocení, ale současně přidává na jeho složitosti je zohlednění horizontálních a vertikálních závislostí mezi ohroženými prvky.[759] Autoři proto poukazují na přínosy hybridního hodnocení s důrazem na podnikatelské činnosti *(business-driven)*, oceněním aktiv ve vzájemné vertikální a horizontální závislosti a stanovení rizika za využití konceptu propagace *(risk measurement using propagation concept)*.[760]

Další zajímavý pohled na určení rizika porušení bezpečnosti přinášejí *Sen a Borle* ve své empirické studii zaměřené na odhadování kontextuálního rizika těchto jevů.[761] Přistupují přitom k jevu z kriminalistické perspektivy a aplikují teorii příležitosti k trestnému činu *(opportunity theory of crime)*[762], vycházející z racionality útočníka, který se zaměřuje na hodnotné cíle dosažitelné s nízkým úsilím a rizikem. Přihlížejí k sídlu entity, hlavní činnosti a minulým případům porušení bezpečnosti. Mezi zajímavé závěry jejich studie platí, že vyšší pravděpodobnost porušení bezpečnosti se odchylně od teorie příležitosti pojí se soukromými i veřejnými entitami, které vykazují vyšší investice do kyberbezpečnosti.[763]

5.2 Teorie rozhodování

Rozhodování je proces volby mezi dostupnými možnostmi na základě dostupných informací a s přihlédnutím k očekávané relativní výhodnosti příslušné volby. Výchozím modelem je prostředí jednoduchého rozhodování, kde každá možnost má porovnatelně kvantifikovaný výsledek. V případě nejistého výsledku je známá jeho pravděpodobnost, která umožňuje

758 Především vysoký počet prvků a náročnost přiřazení frekvence ohrožení či odlišení významných rizik.

759 Ibid., s. 25.

760 Ibid., s. 27.

761 Viz SEN, Ravi a Sharad BORLE. Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems* [online]. 2015, roč. 32, č. 2.

762 Blíže viz NATARAJAN, Mangai. *Crime Opportunity Theories: Routine Activity, Rational Choice and their Variants*. Abingdon: Routledge, 2017.

763 Srov. SEN, Ravi a Sharad BORLE. Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems* [online]. 2015, roč. 32, č. 2, s. 330 a násl.

určit jeho očekávanou hodnotu jako násobek pravděpodobnosti. Při různých nákladech spojených s jednotlivými možnostmi je na místě vztáhnout hodnotu k jednotnému denominátoru (např. snížená újma v důsledku porušení bezpečnosti na jednotku vynaložených nákladů).[764]

Teorie užitku: S přibližováním teoretických rámců praktických situacím však vyvstávají výše naznačené překážky přiřaditelnosti kvantifikovatelné hodnoty a objektivně určitelné pravděpodobnosti daného scénáře. Do hry také vstupují další aspekty, které mají vliv na racionalitu volby. Přiřazení hodnoty jednotlivým volbám se v ekonomii věnují především teorie užitku *(utility)*, kterou v rámci názorové školy utilitarismu zformuloval *Bentham*[765] a významně rozvinul mmj. *Mill*.[766] Užitek je přitom hodnota, která v ekonomické terminologii vyjadřuje uspokojení spotřebitele spojené s danou volbou ve spotřebě statků. Jde tedy o teoretický nástroj kvantifikace hodnoty možných variant jednání, který následně umožňuje formulovat principy nejvhodnější volby se zohledněním subjektivním preferencí a specifik situace a zakotvit tudíž rozhodování do rámce racionality.

Teorie užitku prošly značně rozsáhlým a komplexním vývojem, jelikož často stály u jádra jednotlivých ekonomických myšlenkových směrů a škol. Zachovaly však primární dělení na kardinalistické *(cardinal)* a ordinalistické *(ordinal)*, které se liší v principiálním vnímání možnosti vyjádření hodnoty užitku. Kardinalistické vnímání je založeno na možnosti konkrétního vyjádření hodnoty užitku (např. *Bentham* zavedl jednotku *util*). Významné je v tomto vnímání pravidlo klesající hodnoty dalšího stejného statku, tzn. zákon klesajícího mezního užitku,[767] který významně rozpracoval např. *Jevons*.[768] Ordinalistické pojetí užitku oproti tomu odmítá možnost jeho přímé kvantifikace, ale přijímá za možné pouze jeho relativní řazení. Je tedy možné určit, která volba

764 Viz FISCHHOFF, Baruch a John KADVANY. *Risk. A Very Short Introduction*. Oxford: Oxford University Press, 2011, s. 65–67, Very Short Introductions.

765 Blíže viz BENTHAM, Jeremy. *An Introduction to the Principles of Morals and Legislation* [online]. London: T. Payne and Son, 1780 [cit. 16. 7. 2021].

766 Srov. MILL, John Stuart. *Utilitarianism*. Revised edition. Oxford; New York: Oxford University Press, 1998.

767 Srov. DRENNAN, Matthew. Economies: Diminishing Marginal Utility. *Challenge*, 2006, roč. 49, č. 5.

768 Srov. JEVONS, William Stanley. The Mathematical Theory of Political Economy. *Journal of the Statistical Society of London* [online]. 1874, roč. 37, č. 4.

je vhodnější, nikoliv však již o kolik je vhodnější. Směrodatná je v tomto směru práce *Pareta*.[769]

Přestože původní zaměření teorií užitku je soustředěno na volbu spotřebitele s omezenými zdroji mezi nabízenými produkty v zájmu maximálního uspokojení jeho preferencí a potřeb, je její konceptuální struktura široce aplikovatelná na celé spektrum jednání spočívajícího ve volbě. Jedná se tak o konstrukt, který je základem normativní teorie rozhodování, která je podkladem pro ekonomické modelování racionálního, tedy logicky zdůvodnitelného, rozhodování.[770]

Axiomy teorie rozhodování na základě maximalizace užitku: Předpokladem možnosti racionálního rozhodování o riziku na základě maximalizace užitku je splnění základních axiomů teorie.

Prvním je axiom úplnosti *(completeness)*, který zajišťuje, že všechny varianty jsou navzájem porovnatelné, tedy že s každou možností je možné spojit relativní preferenci.

Druhým je axiom přenositelnosti *(transitivity)*, na základě kterého musí platit, že preference první možnosti před druhou a druhé před třetí znamená preferenci první před třetí. *Temkin* sice vznáší pochybnost o axiomatické povaze tohoto pravidla, zvláště při zcela subjektivním parametru hodnocení (např. líbivost),[771] ovšem při posuzování možností s přihlédnutím k souvisejícímu riziku je na místě upřednostnit postoj *Brooma*, dle kterého je přenositelnost samotným jádrem objektivně porovnatelné volby preference *(the very meaning of objective comparable desirability)*.[772, 773] Klíčové je přitom zachycení dílčích užitků, pro které byl směrodatný především *von Neumannův* a *Morgensternův* teorém vyjádření užitku.[774] V jeho rámci byly dovozeny dodatečné dva

769 Srov. PARETO, Vilfredo. The New Theories of Economics. *Journal of Political Economy*, 1897, roč. 5, č. 4.

770 Blíže viz ANAND, Paul. *Foundations of Rational Choice Under Risk*. Oxford, New York: Oxford University Press, 1995.

771 Blíže viz TEMKIN, Larry S. *Rethinking the Good: Moral Ideals and the Nature of Practical Reasoning*. Oxford: Oxford University Press, 2012.

772 Blíže viz BROOME, John. *Weighing Goods: Equality, Uncertainty and Time*. Oxford: Wiley-Blackwell, 1995.

773 Srov. STEELE, Katie a H. Orri STEFÁNSSON. Decision Theory. In: ZALTA, Edward N. (ed.). *The Stanford Encyclopedia of Philosophy* [online]. Winter 2016. Stanford: Metaphysics Research Lab, Stanford University, 2016 [cit. 16. 7. 2021].

774 Srov. NEUMANN, John von a Oskar MORGENSTERN. *Theory of Games and Economic Behavior. 60th Anniversary Commemorative Edition*. 2007.

axiomy umožňující matematické modelování rozhodování na základě užitku s pomocí kardinálních čísel.[775]

Třetím je tak axiom kontinuity *(continuity)*, dle kterého žádný výsledek není tak špatný, aby při rozhodnutí nebyla za určitých podmínek zvažována i volba, která jej zahrnuje jako možný.

Závěrečným, čtvrtým axiomem je požadavek nezávislosti *(independence)*, ze kterého dovozujeme, že při stejné pravděpodobnosti určitého výsledku u dvou možností by volba mezi těmito možnostmi měla být nezávislá na preferenci daného výsledku. Ve formálním zápise lze jednotlivé axiomy vyjádřit následovně:[776]

Pro každé $A, B \in S$: buďto $A \preceq B$ nebo $B \succeq A$.
Pro každé $A, B, C \in S$: pokud $A \preceq B$ a $B \preceq C$ potom $A \preceq C$.
Pokud $A \preceq B \preceq C$ platí, že je $p \in [0,1]$ pro které platí: $\{pA,(1\text{-}p)C\} \sim B$
Pokud $A \preceq B$ platí pro každé C a každé $p \in [0,1]$: $\{pA,(1\text{-}p)C\} \preceq \{pB,(1\text{-}p)C\}$

Behaviorální teorie rozhodování: Nahlížení na rozhodování skrze ekonomickou teorii racionálního rozhodování je nutně nedostatečně komplexní pro zachycení skutečného procesu rozhodování člověka, jelikož na jedné straně opomíjí vliv emocí či vnitřních hodnot jednotlivce a na straně druhé předpokládá všudypřítomné striktně logické vyvažování užitků bez zohlednění intuitivního jednání či zkratkovitého rozhodování bez důsledného zvažování alternativ.[777] Tyto nedostatky se snaží překonat zastánci behaviorální teorie rozhodování, např. *Edwards*.[778] Přibližování se reálným rozhodovacím procesům jednotlivce však přenáší problematiku hluboko na pole psychologie[779] a činí modelování rozhodování ekonomických aktérů v dílčích situacích neuchopitelně složitým.

775 *„V matematice se pojem kardinální číslo, někdy též kardinál, pojí s čísly používanými pro popis velikosti množin. Jelikož se matematika zabývá i nekonečnými objekty, kardinální čísla a mohutnosti množin popisují i nekonečné množiny."* Srov. *Kardinální číslo* [online]. 2017 [cit. 16. 7. 2021].

776 Viz STEELE, Katie a H. Orri STEFÁNSSON. Decision Theory. In: ZALTA, Edward N. (ed.). *The Stanford Encyclopedia of Philosophy* [online]. Winter 2016. Stanford: Metaphysics Research Lab, Stanford University, 2016, [cit. 16. 7. 2021].

777 Srov. FISCHHOFF, Baruch a John KADVANY. *Risk. A Very Short Introduction*. Oxford: Oxford University Press, 2011, s. 70, Very Short Introductions.

778 Srov. EDWARDS, Ward. Behavioral Decision Theory. *Annual Review of Psychology* [online]. 1961, roč. 12, č. 1.

779 Srov. SCIENCEDIRECT. Behavioral Decision-Making – an overview. *ScienceDirect Topics* [online]. 2020 [cit. 16. 7. 2021]. Dostupné z: https://www.sciencedirect.com/topics/psychology/behavioral-decision-making

Pro zde řešenou problematiku rozhodování správce ve spojitosti s porušením bezpečnosti osobních údajů není přitom opuštění racionální rozhodovací teorie nezbytné. Byť dílčí rozhodnutí činí jednotlivec, rozhodovací procesy při správě rizika podniku či srovnatelného subjektu jsou svou formalizací do značné míry oproštěny o behaviorální vlivy a jsou na ně tudíž uplatnitelné předpoklady racionálního rozhodování.[780]

Analýza a řízení rizik: Pokud ustoupíme z čistě teoretické roviny zjišťujeme, že správa rizika má své zavedené metody a osvědčené postupy. Ty pokrývají celé spektrum rizik, kterým podnik může čelit, ať již technologická, projektová, finanční, investiční, informační či právní. Pro vlastní stanovení výše rizika existuje normovaná metoda upravená v ČSN ISO/IEC 27005 (36 9790), která vychází ze součtové matice rizika o osách dopadu a pravděpodobnosti rizika.[781]

Vzhledem k rostoucí komplexnosti rizikových scénářů se také vyvíjí samotný koncept systému řízení rizika. Můžeme proto vnímat posun od *risk managementu* na finanční a provozní úrovni k *business risk managementu* na úrovni manažerské a nově rozvíjené úrovni *enterprise risk managementu* zaměřeném na vhodné nastavení strategie přístupu k riziku napříč celou společností a všemi zdroji hodnoty.[782]

Není nutné zde přihlížet k celé šíři pojetí správy rizika podniků, se zde řešeným tématem však úzce souvisí rostoucí role řízení informační bezpečnosti. Ta přitom směřuje k odpovídající ochraně všech údajů a informací organizace ve všech formách, přesahuje tudíž ochranu osobních údajů a vztahuje se též na obchodní tajemství, utajované informace či jiné formy důvěrných záznamů.[783] V souvislosti s digitalizací a rostoucí propojeností podnikových systémů nabývají na významu tzn. asymetrické hrozby, které jsou průvodním projevem i u rozmachu internetu věcí. V tomto smyslu jde o asymetrii snižujících se požadavků na kapacity a schopnosti útočníka a rostoucích dopadů a újmy

780 Srov. SIMON, Herbert A. Rational Decision Making in Business Organizations. *The American Economic Review*, 1979, roč. 69, č. 4; TOMER, John F. Rational organizational decision making in the human firm: A socio-economic model. *The Journal of Socio-Economics* [online]. 1992, roč. 21, č. 2.

781 Viz SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. aktualizované a rozšířené vyd. Praha: Grada, 2013, s. 133.

782 Ibid., s. 152.

783 Ibid., s. 281.

způsobených jeho útokem.[784] V kontextu těchto hrozeb narůstá význam bezpečnostních norem, o kterých bude zmínka podrobněji v rámci podkapitoly 6.2.

5.3 Investice do kyberbezpečnosti a přínosy sdílení informací

Porušení bezpečnosti je pro postiženého správce i dotčené subjekty údajů spojeno s přímými a nepřímými náklady, které se materializují s určitou pravděpodobností v závislosti na několika proměnných. Část těchto proměnných je z jejich hlediska exogenní.

Osud uniklých údajů jako exogenní proměnná: Za přední exogenní proměnnou, tedy takovou, která je mimo kontrolu jak správce, tak subjektu údajů, a která má významný vliv na realizaci újmy v důsledku porušení bezpečnosti, je jednání útočníka či třetí strany, která získala k dispozici kompromitované osobní údaje. Ať již jsou získány přímou činností,[785] skrze prostředníka,[786] či dílem náhody,[787] mohou tyto subjekty následně na základě svého rozhodování předmětné údaje zpracovávat bez ohledu na oprávnění, ať již za finančním či jiným cílem, k újmě subjektu údajů a postiženého správce. V závislosti na jednání těchto subjektů v konkrétním případě tak může i významné selhání správce vedoucí ke zpřístupnění rozsáhlého souboru nezabezpečených osobních údajů mít relativně malý dopad na dotčené subjekty údajů, či naopak relativně nevýznamný únik dat může být zneužit pro významné poškození jejich zájmů a aktiv.

Přes tento prvek exogenní nejistoty je však na místě při rozhodování ve vztahu k porušení bezpečnosti, a to ať v rámci preventivních opatření (tedy zde dále diskutovaných investic do kyberbezpečnosti) či reaktivních opatření (tedy následně diskutovaných notifikačních povinností), přiřadit kvantifikovatelnou hodnotu očekávatelné újmě a nákladům spojeným s jednotlivými scénáři.

Náklady spojené s porušením bezpečnosti: S porušením bezpečnosti se pojí řada přímých i nepřímých nákladů, které dávají příslušným

784 Zde připomínám pojem *script kiddie* uvedený v této souvislosti ke konci podkapitoly 4.3, kde jsou také přiblíženy projevy těchto hrozeb v kontextu internetu věcí. Ibid., s. 284.
785 Tzn. napadením databází správce.
786 Tzn. formou odkupu na nelegálním tržišti.
787 Tzn. v případě omylem zaslaných či zveřejněných osobních údajů.

rozhodováním primárně ekonomickou povahu.[788] Přímé náklady jsou zpravidla rozumně předvídatelné a odpovídají nákladům na obnovení řádné činnosti zasažených sítí a systémů, ztrátu spojenou s poškozenými či ztracenými daty a na ně navazující ušlé příjmy z podnikových operací. Lze sem řadit též očekávatelnou či diskontovanou[789] náhradou újmy poškozeným subjektům údajů či obchodním partnerům. Nepřímé náklady oproti tomu představují nesnadno kvantifikovatelný soubor dopadů porušení bezpečnosti na dobrou pověst podniku, vnímání ze strany investorů, důvěryhodnost u úvěrových institucí či pozornost dozorových orgánů. Spadá sem i související možnost dodatečných sankcí za nepřiměřenou úroveň zavedených opatření.[790] Přes potřebu zachycení nákladů spojených s případy porušení bezpečnosti pro příslušné rozhodovací procesy je však zjevná značná nejednotnost v přístupech k jejich určení. Na to poukazují *Algarni* a *Malaiya* ve své studii porovnávající výpočetní modely a předkládající předpoklady pro sjednocující přístup k vyjádření očekávaných nákladů.[791]

Výše přímých i nepřímých nákladů se kromě výše uvedené exogenní proměnné váží převážně ke třem formám opatření, které správce může (a na základě povinností dle čl. 32 Obecného nařízení má) implementovat s cílem zmenšit riziko porušení bezpečnosti i následné újmy.

Preventivní opatření: První skupinu představují preventivní opatření, tedy vhodná technická a organizační opatření pro zabezpečení zpracovávaných osobních údajů, která umožní předcházet předvídatelným formám porušení bezpečnosti[792] a minimalizovat hrozící újmu v případě neoprávněného

788 Srov. GAL-OR, Esther a Anindya GHOSE. The Economic Incentives for Sharing Security Information. *Information Systems Research* [online]. 2005, roč. 16, č. 2, s. 186 a násl.

789 Diskontování je matematický postup pro převedení budoucí hodnoty na současnou hodnotu. Čím vzdálenější je budoucí náklad, tím má nižší současnou hodnotu. Srov. *Diskontování* [online]. 2017, [cit. 16. 7. 2021].

790 Viz BOASIAKO, Kwabena Antwi a Michael O'CONNOR KEEFE. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. *SSRN Electronic Journal* [online]. 2018, s. 2 [cit. 5. 9. 2021].

791 Srov. ALGARNI, Abdullah M. a Yashwant K. MALAIYA. A consolidated approach for estimation of data security breach costs. In: *2016 2nd International Conference on Information Management (ICIM)* [online]. London: IEEE, 2016, s. 26 a násl.

792 Např. aktualizované a adekvátní firewally sítě a systémů, kontrola oprávnění a přístupu k datům, školení zaměstnanců o bezpečném užívání ICT, či pravidelné penetrační testování a interní bezpečnostní audit.

zpřístupnění těchto dat.[793] Tato proměnná tudíž snižuje pravděpodobnost případu porušení bezpečnosti v daném časovém horizontu a případně snižuje jeho závažnost. Jde tedy o zásadní komponentu podnikového zabezpečení a tím i oblast, do které jsou zpravidla koncentrovány investice do kyberbezpečnosti v rámci dané entity.

Detekční opatření: Vliv mají také zavedená detekční opatření technické[794] i organizační podoby.[795] Včasné zachycení neoprávněného přístupu do sítě a systému podniku, případně odhalení chybného nastavení přístupu k datům či špatného příjemce komunikovaných údajů je v kontextu digitálně uchovávaných osobních údajů klíčové. Již v rámci diskuse v podkapitole 4.6 bylo poukázáno na dostupné údaje o často značně opožděném odhalení porušení bezpečnosti.[796] Přitom se zvyšujícím se časovým odstupem vznikají dodatečné překážky řádné a komplexní analýze případu porušení bezpečnosti, a klesá tudíž přesnost vyhodnocení jeho rozsahu a dopadu. Co je však významnější, s rostoucí dobou od vzniku zranitelnosti bez vědomí správce, a tudíž i subjektů údajů, roste prostor pro třetí strany v přístupu k dotčeným osobním údajům a jejich neoprávněnému zpracování k újmě těchto subjektů.

Reakční opatření: Hrozící újmě lze zabránit či ji zmínit také po vlastním porušení bezpečnosti skrze reakční opatření. Jde především o nápravu bezpečnostní zranitelnosti a degradaci zpřístupněných dat, u kterých je to možné (zpravidla zneplatněním přístupových údajů a hesel). Nezbytným předpokladem je však včasné odhalení případů porušení. Za významné reakční opatření pak platí ohlášení a příp. oznámení případu porušení bezpečnosti dozorovému úřadu a dotčeným subjektům údajům, kterým je tak umožněno

793 Především pseudonymizace, šifrování, hashování a užití kryptografické soli při úschově přístupových hesel. Pojem kryptografická sůl *(salted hash)* značí doplnění šifrovaného záznamu o náhodné bity, které zvyšují jeho odolnost. Srov. *Sůl (kryptografie)* [online]. 2020 [cit. 16. 7. 2021].

794 Např. antivirová ochrana s využitím heuristické analýzy či umělé inteligence. K využití umělé inteligence v tomto kontextu viz např. IBM. Artificial Intelligence for Smarter Cybersecurity. *IBM Security* [online]. 2020 [cit. 16. 7. 2021]. Dostupné z: https://www.ibm.com/security/artificial-intelligence

795 Především školení zaměstnanců ohledně včasného hlášení podezřelých aktivit či případů porušení bezpečnosti, interní systém s jasnou hierarchií pro přijímání, analýzu a vyhodnocení těchto podnětů či mezipodniková spolupráce při sdílení informací o aktuálních bezpečnostních hrozbách.

796 Viz PONEMON INSTITUTE. *Cost of a Data Breach Report 2019* [online]. Traverse City: IBM Security, 2019, s. 50 a násl. [cit. 22. 5. 2021].

podniknout další reakční opatření, a koordinovat je se správcem pro minimalizaci hrozící újmy ze zpřístupnění osobních údajů.

Notifikační povinnosti jako incentiva pro investice do kyberbezpečnosti: Již v rámci diskuse v oddílu 3.2.3 jsem dovodil, že účel notifikačních povinností spočívá především v odstranění informační asymetrie mezi správcem a dozorovým úřadem či dotčenými subjekty údajů za účelem snížení hrozící újmy v důsledku porušení bezpečnosti. Jak však uvádějí *Laube* a *Böhme*, tato povinnost současně cílí na posílení incentiv správců k adekvátním investicím do kyberbezpečnosti,[797] tedy především do preventivních a detekčních opatření.

Racionálně řízené podniky založené za účelem dosahování zisku operují při rozhodování o vynaložení dostupných prostředků na základě bilancování předvídatelných přínosů a nákladů. Proti zájmům na zajištění vysoké úrovně kyberbezpečnosti ve smyslu ochrany hmotných a nehmotných aktiv podniku tak stojí kvantifikace a porovnání relativní návratnosti investic do kyberbezpečnosti s jinými možnostmi užití dostupných prostředků. Úvahy týkající se přiměřené výše těchto investic se zpravidla odvíjejí od předpokladů založených široce přijímanou analytickou prací *Gordona* a *Loeba* z roku 2002[798] a modelů na ně navazujících.

Model *Gordona* a *Loeba*: Tito autoři usilovali o vymezení optimální úrovně investic do kyberbezpečnosti. Za předpoklad svého modelu berou, že podnikům hrozí konstantní úroveň bezpečnostních hrozeb, kterou nemohou ovlivnit, ale dodatečné investice mohou snížit zranitelnost jejich sítí a systémů. Tyto investice však podléhají ekonomickému zákonu klesajících výnosů,[799] tedy každá další jednotka investice má nižší přínos. To je dáno tím, že dosažení dokonalé úrovně kyberbezpečnosti, která by zcela vyloučila bezpečnostní incidenty, by vyžadovalo zcela neúměrnou výši investic.[800]

---

797 Srov. LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1, s. 29.

798 Srov. GORDON, Lawrence A. a Martin P. LOEB. The economics of information security investment. *ACM Transactions on Information and System Security* [online]. 2002, roč. 5, č. 4.

799 K zákonu klesajících výnosů (*law of diminishing returns*) blíže viz SAMUELSON, Paul A. a William D. NORDHAUS. *Microeconomics*. 17. vyd. New York: McGraw-Hill Education, 2001.

800 Srov. SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. aktualizované a rozšířené vyd. Praha: Grada, 2013, s. 96.

Formálně je podstata modelu zachycena v následujících třech vzorcích. První vyjadřuje, že očekávané přínosy z investice do kyberbezpečnosti jsou funkcí očekávatelné újmy v důsledku porušení bezpečnosti, která závisí na míře zranitelnosti podniku a pravděpodobnosti porušení bezpečnosti. Při vyšších investicích přitom klesá riziko, a tudíž i přínos dodatečné investice. Tento pokles však není na bázi přímé úměry, je tudíž nutné zohledňovat nelinearitu dané funkce, což zachycuje druhý vzorec. Optimální výše investice je tudíž výsledkem komplexnější funkce na bázi přirozených logaritmů (ln),[801] jak vyjádřeno třetím vzorcem.

$$EBIS(z) = [v - S(z,v)]L \quad 802$$

$$S^{II}(z,v) = v^{z+1} \quad 803$$

$$z^{II*}(v) = \frac{\ln\left(\frac{1}{-vL(\ln v)}\right)}{\ln v} \quad 804$$

Popis proměnných:

z	Výše investice do kyberbezpečnosti
v	Míra zranitelnosti podniku
$S(z,v)$	Pravděpodobnost porušení bezpečnosti s ohledem na danou míru zranitelnosti a výši realizovaných investic do kyberbezpečnosti
$EBIS(z)$	Očekávané přínosy z investice do kyberbezpečnosti
L	Očekávaná újma v důsledku porušení bezpečnosti
$S^{II}(z,v)$	Nelineární funkce pravděpodobnosti porušení bezpečnosti
$z^{II*}(v)$	Optimální výše investice do kyberbezpečnosti pro nelineární funkci pravděpodobnosti porušení bezpečnosti

Modelová optimální výše investic do kyberbezpečnosti: Model směřuje ke stanovení optimální výše investic do kyberbezpečnosti, která odpovídá bodu s nejvyšším rozdílem celkového přínosu investic (tzn. snížení zranitelnosti) a celkových nákladů (tzn. celkové výše investice). Autoři toto optimum

801 Tzn. logaritmu, kde je základem Eulerovo číslo. K pojmu viz *Eulerovo číslo* [online]. 2020, [cit. 16. 7. 2021].

802 Viz GORDON, Lawrence A. a Martin P. LOEB. The economics of information security investment. *ACM Transactions on Information and System Security* [online]. 2002, roč. 5, č. 4, s. 444, vzorec (1).

803 Ibid., s. 448, vzorec (7).

804 Ibid., vzorec (8).

testují s ohledem na různou míru zranitelnosti (tzn. očekávanou újmu způsobenou bezpečnostním incidentem).

V rozporu s obecným očekáváním model udává, že by investice neměla být nekonečně rostoucí funkcí zranitelnosti, jelikož přínos zvýšených investic do zabezpečení vysoce zranitelných aktiv je příliš nízký, aby byl ekonomicky optimální. Jedním ze závěrů modelu je, s přihlédnutím k dílčím podmínkám a parametrům modelu, že maximální ekonomicky racionální rozsah investic do kyberbezpečnosti by měl dosahovat přibližně 37 % očekávatelné újmy v důsledku předvídatelných bezpečnostních incidentů.[805]

Tento závěr je pochopitelně velmi limitován pro praktickou použitelnost a může sloužit pouze pro rozvinutí dalších komplexnějších ekonomických úvah a modelů. Přináší však jistý vhled do základních incentiv motivujících podnik k investicím do kyberbezpečnosti s ohledem na vnímanou hrozbu, a především pak jejich limitů. Rozpočtová omezení (tzn. dostupné zdroje a výhodnost jejich alternativních investic) vedou podnik k hledání optimální výše nákladů na kyberbezpečnost v intencích posuzování analýzou nákladů a přínosů,[806] spíše než sledováním maximálního zabezpečení nejzranitelnějších informačních aktiv (jako jsou např. zvláštní kategorie osobních údajů).

Požadavek neoptimální výše investic vynucovaný právním rámcem: Zde je pak zjevná role normativních povinností, jako je požadavek přiměřených opatření dle článku 32 Obecného nařízení, které usměrňují tyto čistě ekonomicky racionální volby podniku v zájmu ochrany určité skupiny aktiv (zde tedy zpracovávaných osobních údajů). Problematické však je, že zpravidla vyžadují po podniku modelově vyšší než optimální úroveň investic z perspektivy daného podniku. Toho je dosahováno především skrze hrozbu administrativních sankcí při nedostatečném zabezpečení těchto aktiv, či případném porušení jiných s nimi spojených povinností, jako je ohlášení či oznámení případu porušení zabezpečení.

Limity modelu *Gordona* a *Loeba*: Na limity *Gordonova* a *Loebova* modelu poukázal výzkum dalších autorů v této oblasti, kteří na něj navazovali, a pokoušeli

805 GORDON, Lawrence A. a Martin P. LOEB. The economics of information security investment. *ACM Transactions on Information and System Security* [online]. 2002, roč. 5, č. 4, s. 452.

806 Analýza nákladů a přínosů (*cost benefit analysis*) patří k základním metodám hodnocení investičních záměrů. K pojmu viz *Analýza nákladů a přínosů* [online]. 2019 [cit. 16. 7. 2021].

se v dílčích aspektech rozšířit použitelnost dosažených závěrů či je testovat na komplexnějším modelovaném prostředí.

Yue a kol. se ve své studii z roku 2006 zabývali síťovými externalitami spojenými s investicemi do kyberbezpečnosti a změnou, kterou v úvahách o optimu vyvolá vnímání bezpečnostních opatření ve vrstvách spíše než jako jednotný blok.[807] Na to navazovala ve svém modelu z roku 2012 *Barysnikov*,[808] když sledovala ještě vyšší komplexnost kategorizace bezpečnostních opatření, a testovala residuální hrozbu v závislosti na úrovni investice do kyberbezpečnosti vůči každé vrstvě jednotlivě.

Oproti tomu *Huang, Hu a Behara* modelovali optimalizaci investic pro prevenci multi-vektorových útoků.[809] Z hlediska úvah o maximalizaci přínosu dokládají, že při omezeném rozpočtu je na místě soustředit ochranu na typ útoku s největším potenciálem újmy, spíše než investice rozkládat příliš široce.

Zohlednění externalit typu DDoS útoku: *Gordon* a *Loeb*, za přispění *Lucyshyna* a *Zhou*, následně v roce 2014 rozvinuli výše představený základní model o zohlednění externalit, tedy důsledků porušení bezpečnosti, které nejsou předvídatelnými sankcemi či náhradou újmy přeneseny do rozhodování daného podniku (tzv. *spillover effect*).[810] Příkladem jsou DDoS útoky, kdy porušení bezpečnosti podniku a přiřazení jeho zařízení do botnetu, který k danému útoku následně slouží, přispívá k újmě třetího subjektu, který je cílem daného DDoS útoku, byť na podnik tato újma není přímo ani nepřímo přenositelná.[811] Zohlednění těchto externalit se pak může významně odrazit v optimální výši investic do kyberbezpečnosti.

Zohlednění sdílení informací mezi podniky: Za další významné omezení pro *Gordonův* a *Loebův* základní model platilo, že nebere v potaz provázanost situace více podniků na poli kyberbezpečnosti, a tudíž možné přínosy

807 Srov. YUE, Wei T. et al. Network externalities, layered protection and IT security risk management. *Decision Support Systems* [online]. 2007, roč. 44, č. 1.

808 Viz BARYSHNIKOV, Yuliy. IT Security Investment and Gordon-Loeb's 1/e Rule. *WEIS Conference*, 2012, roč. 2012.

809 Viz HUANG, Derrick C., Qing HU a Ravi S. BEHARA. *Economics of information security investment in the case of simultaneous attacks*. 2006.

810 Srov. GORDON, Lawrence A. et al. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security* [online]. 2014, roč. 06, č. 01, s. 24 a násl.

811 Ibid., s 27.

spojené se sdílením informací o aktuálních hrozbách a jejich konkrétní podobě. Toho si autoři byli vědomi, a proto tento aspekt rozvinuli v navazující ekonomické analýze, kterou s nimi již v roce 2003 zpracoval *Lucyshyn*.[812] Sdílení informací může vést k vyšší úrovni zabezpečení podniků při stejném rozpočtu na investice do kyberbezpečnosti. Jak je však modelem ukázáno, předpokladem přínosů ze sdílení informací je funkční mechanismus incentiv k aktivní účasti všech podniků. Tím je bráněno situaci, kdy se každý podnik snaží ušetřit skrze spoléhání se na informace od druhých bez adekvátního přispění do systému skrze vlastní investice a sdílení informací.

Gal-Or a *Ghose* ve svém modelu z roku 2005 za využití teorie her *(game theory)*[813] odhalují, za jakých podmínek je pro podnik výhodné účastnit se dobrovolného sdílení informací.[814] Výsledky studie identifikují dvě roviny ekonomických incentiv, které vedou podniky k účasti na sdílení informací. První jsou přínosy s přímým efektem, které mají pozitivní vliv na poptávku po produktu podniku a druhou jsou přínosy se strategickým efektem, které snižují cenovou konkurenci. Tyto přínosy se zvyšují s velikostí podniku a úrovní konkurence v odvětví.[815] Jedním ze závěrů modelu pak také je, že tržně dosažená *Bertrand-Nashova* rovnováha nedosahuje úrovně sdílení informací a investic do kyberbezpečnosti, která by byla vhodná z hlediska společenského optima, a proto by měla přistoupit motivace ze strany veřejného regulátora.[816]

Zohlednění vzájemné závislosti mezi podniky: *Ogut a kol.* k tomu pojetí přispěli studií z roku 2005, která směřovala k modelovému zachycení parametru vzájemné bezpečnostní závislosti mezi podniky.[817] Poukázali přitom

812 Viz GORDON, Lawrence A., Martin P. LOEB a William LUCYSHYN. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* [online]. 2003, roč. 22, č. 6, s. 461 a násl.

813 Jedná se o oblast aplikované matematiky, která zkoumá rozhodovací scénáře v situacích se střetem zájmů a identifikuje nejvýhodnější strategii pro účastníky těchto konfliktů. Srov. *Teorie her* [online]. 2019 [cit. 16. 7. 2021].

814 V americkém prostředí k němu dochází skrze Centra pro analýzu a sdílení informací (ISAC). Těm se budu věnovat blíže v oddílu 6.3.1; Srov. GAL-OR, Esther a Anindya GHOSE. The Economic Incentives for Sharing Security Information. *Information Systems Research* [online]. 2005, roč. 16, č. 2, s. 186 a násl.

815 Ibid., s. 200.

816 Ibid.

817 Srov. OGUT, Hulisi, Nirup MENON a Srinivasan RAGHUNATHAN. Cyber Insurance and IT Security Investment: Impact of Interdependence Risk. In: *WEIS* [online]. 2005 [cit. 16. 7. 2021].

na skutečnost, že tyto fyzické či logické provázanosti efektivně snižují incentivy podniků zvyšovat investice do kyberbezpečnosti. Autoři tudíž podtrhují potřebu rámců pro sdílení informací a státem vynutitelných sankcí pro motivaci podniků k navýšení investic na společensky, nikoliv podnikově, optimální úroveň.[818]

Liu, Ji a *Mookerjee* se ve svém modelu z roku 2011 blíže věnují vzájemnému postavení podniků a jeho dopadu na rozhodnutí o sdílení informací a o výši investic do kyberbezpečnosti.[819] Identifikují dva nosné scénáře, podniky s komplementárními produkty a podniky s produktovými substituty. Pokud se produkty podniků vzájemně doplňují, existuje přirozená incentiva ke spolupráci a sdílení informací, úroveň investic je však v rovnovážném stavu nižší než společenské optimum a je na místě vnější (regulatorní) pobídka pro její zvýšení. V případě konkurenčních podniků nastává situace označovaná jako vězňovo dilema[820] a v rovnovážném stavu nedochází k dobrovolnému sdílení informací, i když by to bylo přínosné pro oba podniky. Je proto potřebný vnější vstup vedoucí podniky ke sdílení informací (regulátorem vynucovaná povinnost). Podniky však ani zde nebudou dosahovat společensky optimální úrovně investic, jelikož buďto konkurenční tlak povede k přeinvestování nebo se vynucené sdílení informací odrazí v podinvestování bezpečnostních opatření.

Významnou perspektivu problematiky rozpracovávají *Naghizadeh* a *Liu* ve studii z roku 2018, kde se na sdílení informací mezi podniky dívají z hlediska sekvenční teorie her, tedy vlivu opakované interakce mezi podniky na jejich strategii v přístupu ke sdílení informací.[821] Rozhodování podniků o dodržení dohody o sdílení informací je opět případ vězňova dilema, přičemž při jednom kole rozhodování je jako u předchozí studie *Nashova* rovnováha racionálně jednajících hráčů v poloze nedodržet dohodu a nesdílet informace, ačkoliv

818 Ibid., s. 23.

819 Srov. LIU, Dengpan, Yonghua JI a Vijay MOOKERJEE. Knowledge sharing and investment decisions in information security. *Decision Support Systems* [online]. 2011, roč. 52, č. 1, s. 95 a násl.

820 Jde o scénář teorie her s nenulovým součtem, kdy hráči, kteří nemohou komunikovat mohou dosáhnout lepší pozice, pokud spolupracují, ale bude jim na újmu, pokud druhá strana spolupráci neoplatí. K pojmu viz *Vězňovo dilema* [online]. 2020 [cit. 17. 7. 2021].

821 Srov. NAGHIZADEH, Parinaz a Mingyan LIU. Inter-Temporal Incentives in Security Information Sharing Agreements. In: *AAAI workshop on Artificial Intelligence for Cyber Security (AICS)* [online]. Phoenix: AAAI, 2016 [cit. 12. 7. 2021].

to není z obecné perspektivy nejvýhodnější postup.[822] Pro rozhodování s více koly je zásadní, jakou cestou má podnik možnost zjistit důvěryhodnost jednání druhého podniku. Jednou variantou je zjišťování informací o jednání ostatních každým podnikem individuálně. To vede k nezávislým a nedokonalým závěrům o jednání ostatních podniků.[823] Alternativou je situace, kdy jednání podniků sleduje třetí nezávislý subjekt (např. dozorový orgán či dobrovolná organizace pro sdílení informací), který hodnotí rozsah sdílených informací podnikem a výsledek hodnocení zveřejňuje.

Shrnutí poznatků: Klíčové závěry z představených modelů optimalizace investic do kyberbezpečnosti a sdílení informací o bezpečnostních hrozbách mezi podniky uplatnitelné v rámci další analýzy jsou dva.

V prvé řadě existuje ekonomické zdůvodnění založení normativních povinností zajištění přiměřených opatření na ochranu před porušením bezpečnosti, jelikož racionálně jednající podnik při volbě opatření přihlíží k rizikům pojícím se k jeho aktivům, nikoliv však již k externalitám, které hrozí jiným podnikům či dotčeným subjektům údajů. K tomu musí být motivován skrze regulatorní rámec, ať již přenesením vzniklé újmy či hrozbou sankce.

Druhým závěrem je, že i pokud lze sdílením informací mezi podniky o případech porušení bezpečnosti zvýšit efektivitu jejich investic do kyberbezpečnosti, bez dalšího není mezi konkurujícími podniky (např. v rámci odvětví) pravděpodobné, že ke sdílení informací v přiměřeném rozsahu přistoupí a nebudou se snažit získat výhody z informací sdílených jinými bez vlastního přispění. Jde tedy o variaci problému černého pasažéra *(free rider problem)*[824].[825]

Efektivitu sdílení informací přitom zvyšuje, pokud existuje třetí subjekt zajišťující transparentnost a důvěryhodnost jednání podniků, a tedy odhalující jejich nedodržování závazků sdílet informace, a současně je možné sankcionovat subjekty, které takto porušují svůj závazek. V tomto směru je tedy založeno ekonomické zdůvodnění ohlašovací povinnosti pro případy porušení bezpečnosti. Je však na místě se blíže podívat na rozhodování podniku, zda

822 Ibid., s. 3.
823 Ibid.
824 Srov. CHAPPELOW, Jim. What Is the Free Rider Problem? *Investopedia* [online]. [cit. 17. 7. 2021]. Dostupné z: https://www.investopedia.com/terms/f/free_rider_problem.asp
825 Závěry představených studií dále reflektuji v rámci podkapitoly 6.3.

plnit či neplnit normativně založenou ohlašovací povinnost a předpoklady pro fungování tohoto prvku chytré regulace.

5.4 Rozhodování podniku o ohlašování porušení bezpečnosti

Za hlavní problém motivace povinných subjektů při dodržování ohlašovací povinnosti vůči dozorovému úřadu identifikované v rámci diskuse právní úpravy v oddílu 3.2.3 platí střet zájmů. Těmi jsou předně společenský zájem na zveřejnění informací o porušení bezpečnosti a zájem podniku na minimalizaci sankcí a jiných nákladů v důsledku tohoto porušení. Modelování racionálního rozhodování podniku a vymezení incentiv, které umožní překonat tuto překážku plnění uložené povinnosti se podrobně věnovaly dva modely. Dřívější *Garciův* model je založen na americkém právním prostředí, které bylo představeno v podkapitole 3.3. Obdobně a zřejmě nezávisle na něm byla problematika později rozpracována *Laubem* a *Böhmem* pro evropské prostředí, již se zohledněním připravovaného Obecného nařízení. V této podkapitole představím oba modely a jejich nosné závěry, které pak budu diskutovat v návaznosti na cíl a dílčí otázky monografie v následující podkapitole 5.5.

5.4.1 *Garciův* model

Problematice se v roce 2013 v americkém kontextu ve své disertační práci podrobně věnoval *Garcia*.[826] V úvodní části své studie, podobně jako výše uvedení autoři, dovozuje, že investice do kyberbezpečnosti podniku nejsou ze společenské perspektivy na optimální úrovni, jelikož rozhodování podniku opomíjí náklady způsobené nedostatečnou úrovní bezpečnosti, které nesou jiné subjekty, tzn. externality porušení bezpečnosti.[827] Upozorňuje tudíž na problém morálního hazardu podniku vedoucího k investicím pod společensky optimální úrovní, který je nutno korigovat regulatorně, tzn. normativně internalizovat zmíněné externality pro jejich zahrnutí do rozhodování podniku.[828]

Ideální model regulatorního rámce: Jako koncepční řešení představil ideálně fungující regulatorní rámec pro zajištění přiměřené úrovně kyberbezpečnosti. Ten vychází z předpokladu, že regulátor má plné informace

826 Srov. GARCIA, Michael E. *The Economics of Data Breach: Asymmetric Information and Policy Interventions*. Disertační práce. Columbus, The Ohio State University, 2013.
827 Ibid., s. 70.
828 Ibid., s. 73–76.

o porušení bezpečnosti bez ohledu na jednání podniku, tzn. i bez potřeby ohlašování.[829] Současně pro zjednodušení opomíjí náklady podniku spojené se zjišťováním podrobností porušení bezpečnosti i případnou kompenzaci, kterou mohou na podniku nárokovat dotčení jednotlivci.[830] Jádrem modelu je možnost transparentního vyčíslení společenských nákladů případu porušení bezpečnosti, které jsou regulátorem přenášeny na postižený podnik v režimu předvídatelné a jisté sankce a zasahují tak do jeho rozhodování již *ex ante*.[831] Podnik je skrze znalost hrozící sankce schopen předvídat celospolečenské náklady spojené s porušením bezpečnosti a v rámci racionálního rozhodování je tudíž internalizuje a přiměřeně zvýší investici do kyberbezpečnosti.[832] Pro přenesení tohoto modelu blíže realitě je však klíčové, že regulátor nemá plné informace a u většiny případů závisí na ohlášení podniku, aby o existenci porušení bezpečnosti získal povědomí a mohl tak za ně uložit sankci.[833]

Asymetrická povaha informace o porušení bezpečnosti: Právě v tomto směru nabízí *Garciův* model hodnotný podklad pro diskusi v rámci této monografie. Po zakotvení představeného konceptu ideálně fungujícího regulatorního rámce totiž upíná pozornost právě na tuto specifickou nedokonalost reality, ve které se odráží další forma morálního hazardu *(moral hazard)*[834] při rozhodování podniku. Ten je spojený s asymetrickou povahou informace o existenci a parametrech případu porušení a problému nepříznivého výběru *(adverse selection)*[835] z hlediska společenského optima (a tedy zájmu dotčených jednotlivců) při rozhodování podniku o sdílení této informace s regulátorem.

829 Ibid., s. 76.
830 Ibid., s. 78.
831 Ibid., s. 81.
832 Ibid., s. 83.
833 Ibid., s. 86.
834 Morální hazard je zpravidla spojován se zlou vírou v rámci smluvních ujednání, obecně však zachycuje situaci, když daný subjekt podstupuje nepřiměřené riziko (ze společenské perspektivy) na základě incentivy vlastního zisku (resp. omezení nákladů). Srov. KENTON, Will. Moral Hazard Definition. *Investopedia* [online]. 10. 4. 2019 [cit. 17. 7. 2021]. Dostupné z: https://www.investopedia.com/terms/m/moralhazard.asp
835 Opět se jedná o pojem převážně ze smluvních vztahů kupujícího a prodávajícího, který však lze zobecnit na využívání (až zneužívání) odlišné informační vybavenosti mezi stranami ohledně podstatného parametru transakce (či zde jevu, který hrozí újmou) ve prospěch lépe informované strany (zde k omezení nákladů podniku skrze neohlášení porušení bezpečnosti). Srov. HAYES, Adam. Adverse Selection Definition. *Investopedia* [online]. 28. 5. 2020 [cit. 17. 7. 2021]. Dostupné z: https://www.investopedia.com/terms/a/adverseselection.asp

Ten má přitom možnost s určitou pravděpodobností získat informaci o porušení bezpečnosti i bez ohlášení zasaženým podnikem. Podnik je tudíž staven před nepříznivý výběr, zda ohlásit případ a čelit jistým nákladům s tím spojeným, či neohlásit a čelit za určité pravděpodobnosti navíc dodatečné sankci za neohlášení.[836]

Provázanost rozhodování podniku o investicích a o ohlášení: Tato situace tak staví podnik před dvojí rozhodování:

1. o výši investice do kyberbezpečnosti (v zájmu racionální minimalizace nákladů prevencí porušení bezpečnosti); a
2. o ohlášení případu porušení bezpečnosti v případě, že k němu dojde (v zájmu racionální minimalizace nákladů s přihlédnutím k možné sankci a dalším souvisejícím nákladům).

V obou případech tedy ekonomicky racionálně jednající podnik usiluje o minimalizaci vzniklých nákladů, tedy o maximalizaci svého jmění.[837] To je dle *Garcii* možné zapsat jako:

$$\max_{\eta,r} U_F^{DP} = \max_{\eta} \left\{ p(\eta_N) U_{FV}^{DP} + \left(1 - p(\eta_N)\right) \left(\max_{r} U_{FE}^{DP} \right) \right\}$$ [838]

Popis proměnných:

U_F^{DP}	Jmění podniku v závislosti na politice ohlašování porušení bezpečnosti
U_{FV}^{DP}	Jmění podniku v závislosti na politice ohlašování při hrozbě porušení bezpečnosti
U_{FE}^{DP}	Jmění podniku v závislosti na politice ohlašování poté, co došlo k porušení bezpečnosti
η_N	Výše investice do kyberbezpečnosti
p	Pravděpodobnost porušení bezpečnosti
r	Rozhodnutí podniku, zda ohlásí či neohlásí zjištěné porušení bezpečnosti

836 Srov. GARCIA, Michael E. *The Economics of Data Breach: Asymmetric Information and Policy Interventions*. Disertační práce. Columbus, The Ohio State University, 2013.
837 Ibid., s. 95.
838 Ibid., vzorec (28).

Při úpravě této rovnice získáme vyjádřeno, že součástí procesu rozhodování je zajištění minimalizace újmy podniku v důsledku porušení bezpečnosti. Zde je rozhodné porovnání očekávaného jmění podniku po ohlášení a při neohlášení násobeného pravděpodobností odhalení. To lze vyjádřit následovně:

$$\max_{\eta} \pi_P - \eta_N - \eta_D - (1 - p(\eta_N)) \left[D(\eta_D) + \min\{F(m,t) + \tau_I, q(F(m,t) + \tau_I + f)\} \right] \quad ^{839}$$

Popis proměnných:

π_P	Zisk podniku před případem porušení bezpečnosti
η_N	Výše investice do kyberbezpečnosti
p	Pravděpodobnost porušení bezpečnosti
$D(\eta_D)$	Újma podniku v důsledku porušení bezpečnosti
$F(m,t)$	Sankce za případ porušení bezpečnosti
m	Množství dotčených subjektů údajů
t	Citlivost dotčených údajů
τ_I	Náklady firmy na odhalení porušení bezpečnosti
q	Pravděpodobnost odhalení porušení regulátorem bez ohlášení podnikem
f	Dodatečná sankce za neohlášení porušení bezpečnosti

Význam pravděpodobnosti odhalení a sankce při neohlášení: Tato rovnice potvrzuje již výše uvedené, tedy že směrodatný pro rozhodování podniku je relativně nižší očekávaný náklad dané volby. U neohlášení hraje klíčovou roli pravděpodobnost odhalení tohoto porušení ohlašovací povinnosti a výše sankce s tím spojená. Pravděpodobnost odhalení však ve svém modelu *Garcia* bere jako exogenní proměnou, kterou není možné ovlivnit.[840] Domnívám se, že to je hlavní slabinou tohoto modelu, jelikož ovlivnění pravděpodobnosti odhalení porušení ohlašovací povinnosti považuji za možné.[841]

839 Ibid., s. 96 vzorec (29).

840 Ibid., s. 96.

841 V tomto směru je vhodnější pojetí v rámci modelu *Laubeho* a *Böhmeho*, který je představen v následující podkapitole. Vedle vlastní aktivity regulátora při bezpečnostním auditu vnímám za významnou roli oznamovatelů (*whistle-blower*). Tomuto aspektu věnuji pozornost v rámci podkapitoly 6.6.

S tímto omezením je však pro potřebnou motivaci podniku k ohlašování případů porušení, při stálosti všech ostatních parametrů *(ceteris paribus)*, směrodatná výše sankce za porušení ohlašovací povinnosti. Model přitom zjednodušuje situaci předpokladem jejího jistého a bezodkladného uložení a vymáhání. Potřebnou výši dolní sazby této sankce pak *Garcia* vyjádřil následovně:

$$f^* > \left(\frac{1-q}{q}\right)(F^*(m,t) + \tau_I) \quad [842]$$

$$F^*(m,t) \mapsto L(\eta_D) \quad [843]$$

Popis proměnných:

f^*	Minimální výše dodatečné sankce za neohlášení porušení bezpečnosti pro vynucení dodržování ohlašovací povinnosti
q	Pravděpodobnost odhalení porušení bezpečnosti regulátorem bez ohlášení podnikem
$F^*(m,t)$	Optimální sankce za porušení bezpečnosti
m	Množství dotčených subjektů údajů
t	Citlivost dotčených údajů
τ_I	Náklady podniku na odhalení porušení bezpečnosti
$L(\eta_D)$	Funkce společenské újmy v důsledku porušení bezpečnosti
η_D	Výše investice do zabezpečení dat (např. šifrování)

Ta je tedy funkcí internalizace vnějších nákladů (externalit, tzn. společenské újmy v důsledku porušení bezpečnosti) a nákladů na odhalení porušení bezpečnosti upravených pravděpodobností odhalení neohlášeného porušení bezpečnosti. Pro funkční motivaci podniku k ohlašování porušení bezpečnosti je tudíž významné, aby sankce za neohlášení dosahovala nezbytné minimální výše, která bude pro podnik dostatečně odrazující.[844] *Garcia* však zároveň upozorňuje na rizika spojená s nevhodným nastavením maximální výše sankce. Absence horní hranice sankce či nezohledňování velikosti a rozpočtových možností podniku může působit až jako překážka podnikání pro malé a střední podniky.[845]

842 Ibid., s. 96.
843 Ibid.
844 Ibid., s. 98.
845 Ibid., s. 170–171.

Ohlašovací povinnost jako motivace ke zvýšení investic do kyberbezpečnosti: Co se týče přínosu povinnosti ohlašování porušení bezpečnosti jako stimulace investic do kyberbezpečnosti podniku, shrnuje podmínku ekonomicky racionální politiky následující nerovnice:

$$\left(1 - p\left(\eta_N^{DP^*}\right)\right)\left(\left\{\frac{\partial F^*(m,t)}{\partial \eta_D}\right\}_{\eta_{FD}^{NR^*}} + \tau_I\right) < \left(p\left(\eta_N^{DP^*}\right) - p\left(\eta_{FN}^{NR^*}\right)\right)\frac{\partial D\left(\eta_{FD}^{NR^*}\right)}{\partial \eta_D}$$ [846]

Popis proměnných:

p	Pravděpodobnost porušení bezpečnosti
η_F^{DP*}	Optimální investice do zabezpečení sítě
$F^*(m,t)$	Sankce za porušení bezpečnosti
η_D	Výše investice do zabezpečení dat (např. šifrování)
η_{FD}^{NR*}	Optimální investice podniku do zabezpečení dat bez ohlašovací povinnosti
τ_I	Náklady podniku na odhalování porušení bezpečnosti
η_{FN}^{NR*}	Optimální investice podniku do zabezpečení sítě bez ohlašovací povinnosti
$D(\eta_{FD}^{NR*})$	Funkce nákladů podniku při porušení bezpečnosti

Omezení daná rozpočtem a vhodná alokace investic podniku: Tou je předně vyjádřeno, že podnik bude racionálně motivován zvyšovat investice do kyberbezpečnosti do té míry, dokud je mezní přínos dodatečné investice založené regulatorní povinností[847] nižší než mezní přínos investice na snížení výsledného negativního dopadu na jmění podniku po odečtení přínosu z investic do kyberbezpečnosti na základě regulatorních požadavků.[848] Za tímto složitým bilancováním je skryta myšlenka, že rozpočet podniku na kyberbezpečnost je omezen a investice do jednotlivých opatření je na místě zvažovat ve vzájemné konkurenci co do jejich přínosu pro zachování maximálního jmění podniku.

846 Ibid., s. 102 vzorec (34).

847 Za předpokladu dostatečného snížení pravděpodobnosti či výše sankce za nedodržení požadavků na přiměřené zabezpečení a nákladů na odhalení případů porušení.

848 Ibid., s. 102.

Shrnutí poznatků: Motivace podniku je vedena snahou o minimalizaci nákladů spojených s řešením případu porušení bezpečnosti. Toho může být částečně dosahováno preventivními opatřeními v podobě investic do kyberbezpečnosti, podnik však nebude motivován k těmto investicím v míře, která je optimální z hlediska subjektů údajů, jelikož na něj plně nedopadá (není zcela internalizována) celková újma v důsledku porušení bezpečnosti. Při rozhodování o ohlášení porušení bezpečnosti bude taktéž veden úvahou o minimalizaci nákladů, přičemž rozhodující roli v těchto úvahách bude hrát očekávaná efektivní[849] výše sankce za neohlášení. Dále je významná pravděpodobnost uložení této sankce, *Garcia* však tuto proměnnou bere jako exogenní, tedy danou bez možnosti ji v rámci modelu ovlivnit.

Garciův model tudíž potvrzuje, že regulatorní nastavení sankcí za nesplnění ohlašovací povinnosti musí být přiměřeně přísné, aby motivovalo podnik k odhalování a řádnému ohlašování porušení bezpečnosti.[850] Dále je však dovozeno, že vzhledem k omezené rozpočtové kapacitě podniků mohou tyto regulatorní požadavky při nevhodně nastavené zátěži spojené s touto povinností jít na úkor jiných složek investic do kyberbezpečnosti (např. na šifrování dat či reaktivní opatření). Stanovení vhodného rozmezí sankce je přitom komplikováno probabilistickou povahou porušení bezpečnosti, čímž je zamlžena linka mezi četností případů porušení a úrovní bezpečnosti podniku, kterou tak nelze snadno modelovat.[851]

5.4.2 *Laubeho* a *Böhmeho* model

Zřejmě nezávisle na představených závěrech *Garcii* poskytují srovnatelnou komplexní analýzu rozhodování podniku ohledně ohlašování porušení

849 Model přitom odhlíží od možných právních nástrojů pro pozdržení (významné z hlediska diskontování tohoto nákladu) či zabránění vymáhání (skrze řádné opravné prostředky či soudní napadení správního rozhodnutí regulátora). Vnímám tedy za nezbytné upravit tento závěr v tom směru, že kalkulace očekávané výše sankce, která ovlivňuje rozhodování podniku musí být přiměřeně diskontována právě na základě těchto faktorů.

850 Je zde na místě upozornit, že se jedná o čistě ekonomický model, který do značné míry nezohledňuje plnou komplexitu příslušných procesů, konkrétně např. reflexi principů správního trestání a limity, které jsou v tomto směru dány orgánu ukládajícímu příslušnou sankci.

851 Ibid., s. 102.

bezpečnosti dozorovému orgánu ve svém modelu z roku 2016 *Laube* a *Böhme*.[852] Ten je přitom příhodně formulován z evropské perspektivy a zohledňováno je jak v té době připravované Obecného nařízení, tak paralelně projednávaná harmonizace povinnosti hlásit kybernetické bezpečnostní incidenty na základě směrnice 2016/1148.[853]

Cílem této studie bylo vymezení, za jakých podmínek ohlašovací povinnost vede ke zvýšení celkové kyberbezpečnosti ve společnosti za současného snížení celkových s tím se pojících společenských nákladů. Autoři přitom využívají ekonomický model pána (regulátor) a správce (podnik) (*principal-agent model)*[854], dělený do tří částí. První část staví na modelování optimální výše investic do kyberbezpečnosti vycházejících ze základního modelu *Gordona* a *Loeba*, který byl představen v podkapitole 5.3. Významným dále využívaným podkladem je pak studie o vzájemné závislosti úrovně bezpečnosti mezi podniky, zpracovaná *Ogutem a kol.*[855] Tato závislost je pro účely modelu vyjádřena následující rovnicí:

$$P_i(x_i, x_{1-i}) = 1 - \left(1 - P(x_i)\right) \cdot \left(1 - \gamma \cdot P(x_{1-i})\right)$$ [856]

Popis proměnných:

x_i	Investice do kyberbezpečnosti prvního podniku
x_{1-i}	Investice do kyberbezpečnosti druhého podniku
$P(x_i)$	Funkce pravděpodobnosti porušení bezpečnosti v závislosti na investici prvního podniku
γ	Míra závislosti kyberbezpečnosti podniků navzájem

852 Srov. LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1.

853 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

854 Jde o do jisté míry analogickou aplikaci obecného modelu vlastníka aktiv a jeho správce, který se uplatňuje v řadě kontextů, ať již jde o vztah zaměstnavatele a zaměstnance či akcionářů a představenstva. Srov. BLACK'S LAW DICTIONARY. Principal-Agent Model Definition. *UpCounsel* [online]. 1999 [cit. 17. 7. 2021]. Dostupné z: https://www.upcounsel.com/principal-agent-model-definition

855 Srov. OGUT, Hulisi, Nirup MENON a Srinivasan RAGHUNATHAN. Cyber Insurance and IT Security Investment: Impact of Interdependence Risk. In: *WEIS* [online]. 2005 [cit. 16. 7. 2021].

856 Srov. LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1, s. 34, vzorec (2).

Předpoklad provázanosti úrovně kyberbezpečnosti mezi podniky: Je tedy modelováno, že určitou mírou prospívají investice do kyberbezpečnosti jednoho podniku i ke kyberbezpečnosti druhého podniku. Za předpoklad pro další úvahy je bráno, že podnik má do určité míry vlastní zájem na odhalování porušení bezpečnosti[857] a pro zjednodušení také, že detekční opatření jsou plně spolehlivá.[858] V případě založení ohlašovací povinnosti je pak podnik při zveřejnění informace o porušení bezpečnosti vystaven dodatečným nákladům.[859]

Konflikt zájmů podniku a regulátora: Autoři podobně jako výše docházejí k poznatku, že s plněním ohlašovací povinnosti se pojí riziko konfliktu zájmů podniku[860] a regulátora,[861] které lze charakterizovat jako problém morálního hazardu, jelikož podnik má omezenou motivaci jednat ve veřejném zájmu na úkor zájmu vlastního.

Laube a *Böhme*, podobně jako *Garcia*, následně zvažují možné nástroje regulátora pro motivaci podniků k plnění ohlašovací povinnosti z hlediska ekonomicky racionálního rozhodování. Zvažují tedy porovnání očekávaných nákladů podniku spojených s ohlášením a neohlášením v různých situacích. Přitom zohledňují vedle rozhodnutí podniku o plnění ohlašovací povinnosti též, zda bylo porušení bezpečnosti odhaleno nejprve podnikem a pak případně dozorovým orgánem. Pracují tedy s následujícími scénáři:[862]

Scénář	Náklady podniku
Nedojde k porušení bezpečnosti.	Žádné náklady podniku.
Dojde k porušení bezpečnosti, ale podnik jej buď neodhalí nebo se rozhodne neohlásit. Regulátor porušení bezpečnosti následně neodhalí.	Pouze náklady způsobené samotným porušením bezpečnosti.

857 Jde předně o přímou a nepřímou újmu, která podniku v této souvislosti vzniká bez ohledu na ohlášení porušení bezpečnosti, jelikož jsou zasaženy jeho aktiva.

858 *Lippmann a kol.* však poukázali na to, že spolehlivost těchto opatření je zpravidla blíže 80 %. Srov. LIPPMANN, Richard et al. The 1999 DARPA off-line intrusion detection evaluation. *Computer Networks: The International Journal of Computer and Telecommunications Networking* [online]. 2000, roč. 34, č. 4, s. 579 a násl.

859 Předně sankce za nedostatečná bezpečnostní opatření, reputační újma, snížená důvěra investorů a obchodních partnerů apod. Srov. LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1, s. 34.

860 Minimalizovat své náklady, a tudíž zásadně neohlásit.

861 Zajistit transparentnost, a tudíž vynucovat ohlašování.

862 Ibid., s. 35.

Scénář	Náklady podniku
Dojde k porušení bezpečnosti, ale podnik jej buď neodhalí nebo se rozhodne neohlásit. Regulátor porušení bezpečnosti následně odhalí.	Náklady způsobené porušením bezpečnosti, a dodatečné náklady v důsledku zveřejnění porušení včetně sankce za neohlášení porušení.
Dojde k porušení bezpečnosti, podnik jej odhalí a ohlásí.	Náklady způsobené porušením bezpečnosti a dodatečné náklady v důsledku jeho zveřejnění.

Výše sankce a pravděpodobnost odhalení neohlášení jako klíčové proměnné: Za směrodatné komponenty pro motivaci podniku k ohlášení porušení bezpečnosti autoři identifikují, srovnatelně s *Garciou*, výši sankce za neohlášení a pravděpodobnost odhalení neohlášeného případu porušení. Tu přitom již neberou jako exogenní proměnnou, ale modelují ji jako pravděpodobnost provedení bezpečnostního auditu ze strany regulátora, přičemž vycházejí z předpokladu, že audit vždy odhalí všechny neohlášené případy porušení.[863]

Autoři se blíže nevěnují otázce výše potřebné sankce za neohlášení, přejímají však závěry *Khouzani a kol.* o nevhodnosti neomezené horní sazby[864] a zakládají tedy předpoklad přiměřené a vymahatelné sankce na úrovni újmy spojené s případem porušení.[865] Jejich studie je tudíž komplementární s *Garciovým* modelem. Jejich model je nadto přínosný tím, že zohledňují dopady rozhodování podniku na situaci dalších podniků. To vyjadřuje funkce:

$$(x_i^+, t_i^+) = \arg min_{x_i,t_i} c_i(x_i, x_{1-i}, t_i, t_{1-i}, a), \quad \text{za podmínky, že } x_i \geq 0$$ [866]

863 I v tomto směru musíme tento model brát jako poměrně idealistický, zvláště s ohledem na výše zmíněné přetrvávající problémy dozorových úřadů kontrolovat plnění povinností dle Obecného nařízení, o kterých byla řeč v rámci podkapitoly 3.4. Možnostem posílení odborných kapacit dozorového úřadu v souvislosti s ohlašováním porušení zabezpečení je věnována podkapitola 6.5.

864 Srov. KHOUZANI, Arman, Viet PHAM a Carlos CID. Incentive Engineering for Outsourced Computation in the Face of Collusion. In: *Workshop on the Economics of Information Security (WEIS)* [online]. PA, US: Pennsylvania State University, 2014 [cit. 16. 7. 2021].

865 Viz LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1, s. 35.

866 Ibid., vzorec (12).

Popis proměnných:

arg $min_{x_i,t_i} c_i\,(x_i,x_{1-i},t_i,t_{1-i},a)$	Funkce argumentu minima pro náklady podniku v důsledku porušení bezpečnosti
c_i	Náklady podniku v důsledku porušení bezpečnosti
x_i	Investice do kyberbezpečnosti prvního podniku
t_i	Sklon k řádnému ohlašování porušení bezpečnosti prvním podnikem
a	Pravděpodobnost úspěšného auditu regulátorem

Rozhodování podniku o investicích do kyberbezpečnosti: Funkce modeluje nejvýhodnější rozhodnutí podniku o investicích do kyberbezpečnosti a ohlášení případu porušení v závislosti na rozhodnutích podniku druhého. Jde přitom o příklad nekooperativní hry více hráčů, kde je tudíž cílem nalezení *Nashovy* rovnováhy,[867] tedy situace, kdy ani jeden z podniků nedosáhne změnou svých rozhodnutí lepší pozice.

Rozhodování podniku o ohlášení porušení bezpečnosti je přitom závislé na s tím spojených nákladech v poměru k pravděpodobnému odhalení dozorovým orgánem. To lze vyjádřit jako:

$$\tilde{t}(\tilde{x},a) = \begin{cases} 1 & \text{pokud } a \geq a_{min} \vee q_2 = 0 \\ 0 & \text{v ostatních případech.} \end{cases}$$ [868]

$$a_{min} = \frac{q_2}{(q_2 + S)}$$

Popis proměnných:

$\tilde{t}$	Sklon podniku k řádnému ohlášení porušení bezpečnosti (dobrovolné ohlášení při hodnotě 1, zamlčení při hodnotě 0)
$\tilde{x}$	Investice podniku do kyberbezpečnosti
a	Pravděpodobnost úspěšného odhalení neohlášení dozorovým orgánem
a_{min}	Minimální pravděpodobnost odhalení dozorovým orgánem způsobilá ovlivnit rozhodování podniku o ohlašování porušení bezpečnosti

867 K pojmu viz NASH, John. Non-Cooperative Games. *Annals of Mathematics* [online]. 1951, roč. 54, č. 2.

868 Srov. LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1, s. 36, vzorec (15).

q_2	Dodatečné náklady podniku v důsledku zveřejnění porušení bezpečnosti
S	Sankce za neohlášení porušení bezpečnosti při jeho odhalení dozorovým orgánem (v rámci modelu předjímána na prakticky únosné úrovni rovné újmě podniku v důsledku vlastního porušení bezpečnosti, tedy $S= q_1$)

Potřebná úroveň pravděpodobnosti odhalení neohlášení dozorovým úřadem pro motivaci podniku: *Laube* a *Böhme* na základě výše popsaných vzorců komplexně zachycují dvě modelové situace, na kterých poukazují na souhru jednotlivých představených proměnných. Ty se přitom liší v míře vzájemné závislosti mezi dosahováním kyberbezpečnosti u modelovaných podniků. Jedním z výstupu projektů je vzorec pro stanovení nezbytné pravděpodobnosti úspěšného auditu regulátorem (), který je, za jinak nezměněných okolností *(ceteris paribus)*, způsobilý vést podnik k dobrovolnému plnění ohlašovací povinnosti.[869] Je přitom možné zvažovat, že lze skrze výši sankce za neohlášení do určité míry kompenzovat nižší frekvenci či úspěšnost auditů, je však také nutné přihlížet k realistické nemožnosti podniku odhalit všechny případy porušení.[870]

Vedle toho je z modelu patrné, že pokud újma v důsledku zveřejnění případu porušení bezpečnosti není nevýznamná, tak absence bezpečnostních auditů či jiných nástrojů pro kontrolu dodržování ohlašovací povinnosti činí její dodržování ze strany podniků ekonomicky neracionální a tudíž nepravděpodobné.[871] Dále pak autoři dovozují, že povinnosti ohlašování porušení bezpečnosti jako takové mají příznivý ekonomický dopad.[872] To ovšem pouze za splnění tří předpokladů:

1. vysoké vzájemné závislosti mezi dosahovanou úrovní kyberbezpečnosti u jednotlivých podniků,[873]

869 Ibid., s. 36.
870 Ibid., s. 38.
871 Ibid., s. 37.
872 Tzn. celkové náklady s ní spojené jsou nižší než její kvantifikovatelný společenský přínos.
873 Tedy pokud sdílení informací významně kompenzuje část přímých investic jednotlivých podniků. K významu dobrovolného sdílení informací o bezpečnostních hrozbách mezi podniky se vrátím v podkapitole 6.3.

2. vysoké efektivity dozorového orgánu sdílet a šířit účelné informace získané na základě ohlášení[874] a
3. nízkých dodatečných nákladů spojených pro podnik se zveřejněním informace o porušení bezpečnosti.[875, 876]

Shrnutí poznatků: Závěry představeného modelu *Laubeho* a *Böhmeho* vnímám jako příhodné doplnění výše představených závěrů *Garciova* modelu a současně potvrzení jejich platnosti i pro kontext povinností dle Obecného nařízení. Předně je poukázáno na význam, který má zohlednění provázanosti dosažené úrovně kyberbezpečnosti mezi podniky. To na jedné straně reflektuje riziko plynoucí z nepoměru bezpečnostních opatření mezi prvky dodavatelského řetězce a na druhé straně nabízí prostor pro zvýšení celkové úrovně kyberbezpečnosti skrze funkční rámec sdílení informací mezi podniky. Dále je věnována pozornost konfliktu zájmů ve vztahu k ohlašovací povinnosti a významu výše sankce a její pravděpodobnosti pro vynucování plnění této povinnosti. Oproti *Garciovu* modelu je pozornost soustředěna na modelování vlivu pravděpodobnosti odhalení neohlášení porušení bezpečnosti podnikem, tedy na úspěšnost bezpečnostního auditu dozorovým orgánem. Ta dle autorů závisí na souhře identifikovaných proměnných, pro což nabízejí modelové zachycení. Dovozují následně, že ohlašovací povinnost při této míře vymahatelnosti má společenský přínos, pokud je mezi úrovní kyberbezpečnosti podniků dostatečná provázanost, dozorový orgán je schopen účelně využít ohlášené informace a pro podnik se se zveřejněním těchto informací pojí pouze nízké dodatečné náklady.

5.5 Diskuse

V představených modelech lze nalézat ekonomické ospravedlnění ohlašovacích povinností jakožto nástrojů pro zefektivnění sdílení informací

874 Tedy pokud ohlášené informace jsou účelně využity pro zvýšení kyberbezpečnosti u dalších podobných podniků. K této podmínce se vrátím v rámci podkapitoly 6.5.

875 Tedy pokud sankce za nedostatečná bezpečnostní opatření, která vedla k porušení bezpečnosti není nepřiměřeně odrazující a spojení podniku s veřejně dostupnými informacemi o porušení bezpečnosti má pouze malé dopady na jeho dobrou pověst a postavení u zákazníků, investorů a obchodních partnerů. Tato podmínka je zvláště problematická a pokusím se jí alespoň částečně reflektovat při diskusi v podkapitole 6.2.

876 Srov. LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, roč. 2, č. 1, s. 37.

o případech porušení bezpečnosti a optimalizace investic do bezpečnostních opatření podniků skrze zpětné přenesení újmy, kterou přinášejí subjektům údajů. Současně však bylo poukázáno na nezbytné podmínky a limity, kterým je nutno přizpůsobit nastavení této povinnosti pro dosahování jejího společensky přínosného uplatňování. Tyto podmínky se týkají především tří momentů.

(i) Způsobilost podniku odhalit porušení bezpečnosti: Zaprvé je nezbytné, aby podnik byl způsobilý porušení bezpečnosti odhalit. Zde jsou klíčové investice do detekčních opatření. Pouze při vědomí porušení bezpečnosti je totiž podnik vystaven dilema rozhodování o jeho ohlášení a pouze podniky, které by měly a mohly být schopny odhalit případ porušení lze odůvodněně sankcionovat za nedodržení ohlašovací povinnosti. Jak bylo představeno v oddílu 4.5.3, internet věcí v tomto ohledu přináší nové výzvy, které mohou být překážkou především pro mikropodniky, na což bylo poukázáno v oddílu 4.4.3.

(ii) Nezbytnost vynucení plnění ohlašovací povinnosti: Druhým momentem je vlastní racionální proces rozhodování povinného subjektu o ohlášení odhaleného porušení bezpečnosti dozorovému orgánu. Oba modely představené v podkapitole 5.4 poukázaly na nedostatečnou výchozí motivaci podniku řádně ohlašovat porušení bezpečnosti, především protože se pro ně se zveřejněním pojí dodatečné náklady, příp. sankce. Vyvstává zde tudíž potřebnost adekvátního nástroje pro vynucení plnění této povinnosti, za který je oběma modely identifikována dodatečná sankce za neohlášení.

Potřeba jasného signálu o výši minimální sankce: Jak vyplývá z *Garciova* modelu, tato sankce musí dosahovat nezbytné minimální výše, které se povinný subjekt musí obávat, tak aby ji byl nucen zohlednit při svém rozhodování. Toto je relevantní poznatek z hlediska sankčního mechanismu správních pokut dle článku 83 Obecného nařízení, kde dolní hranice není stanovena. Absentuje zde tudíž jasný regulatorní signál, který by povinné subjekty mohly v rámci svého rozhodování zohlednit, zvláště pokud u dozorových orgánů není vysledovatelný srozumitelný vzorec pro stanovení výše uložené sankce. Jedním z možných řešení je buďto plynutí času a s ním nárůst souboru rozhodnutí dozorových úřadů o uložení pokut, ze kterého bude možné tento signál lépe vyčíst. Za vhodnější však pokládám zahrnutí tohoto

signálu srozumitelně a závazně do pokynů a stanovisek dozorových úřadů, samozřejmě za dodržení principů správního trestání, tedy např. vymezením rozhodných parametrů pro posouzení a zpřístupněním statistických údajů o uložených pokutách. Tím je možné na jedné straně koordinovat tento signál a reflektovat míru jeho zohlednění povinnými subjekty, a na druhé straně jasně komunikovat jeho případnou variaci s ohledem na směrodatné parametry daného podniku.[877]

Dostatečná pravděpodobnost odhalení neohlášení porušení bezpečnosti: Druhou komponentou motivace podniků k plnění ohlašovací povinnosti skrze uložení sankce je však možnost odhalení neohlášených případů porušení, a tudíž pravděpodobnost uložení této dodatečné sankce. Tomuto aspektu věnovali zvláštní pozornost ve své studii *Laube* a *Böhme,* a z jejich modelu vyplývá, že bez dostatečně vysoké pravděpodobnosti odhalení neohlášení nemá vlastní normativní hrozba dodatečnou sankcí potřebný vliv na motivaci povinného subjektu v zásadě bez ohledu na její hypotetickou výši. Překážkou v tomto směru je však nejen omezená kapacita dozorových úřadů provádět dostatečné množství přiměřeně hloubkových bezpečnostních auditů, ale též vlastní rostoucí složitost odhalení porušení bezpečnosti, kterému je vystaven již samotný povinný subjekt. Přesto se možnost získání informací o porušení bezpečnosti i jinou cestou, než skrze ohlášení povinného subjektu, jeví jako nezbytný předpoklad funkčního nastavení ohlašovací povinnosti. Z tohoto důvodu nastiňuji možná řešení v podkapitole 6.6.

(iii) Využití sdílených informací o porušení bezpečnosti: Třetím momentem je přínosnost samotných sdílených informací. Na tu lze přitom nahlížet ze dvou momentů. Jedním jsou dobrovolně sdílené informace mezi podniky a druhým je účelné využití ohlášených informací dozorovým úřadem.

Sdílení informací mezi podniky: Autoři studií zaměřujících se na dosahování společensky potřebné úrovně investic do kyberbezpečnosti, stejně tak jako *Laube* a *Böhme* v rámci svého modelu, poukazují na přínos dobrovolného sdílení informací o kyberbezpečnosti mezi podniky. Může přitom jít jak o doporučená opatření, zajištění kompatibility bezpečnostních prvků, identifikaci

877 Zde mám na mysli především avizovaný mírnější postup vůči nepřiměřeně zatěžovaným mikropodnikům či vůči podnikům v odvětvích s malým rizikem, který však ztrácí na informační hodnotě, pokud zůstává v rovině neurčitých formulací.

nových hrozeb, tak o informace o odhaleném porušení bezpečnosti. Pozitivní efekt této koordinace a spolupráce bude nabývat na významu především s rostoucí propojeností v rámci sítí a systémů internetu věcí. S tím však může narůstat i negativní důsledek identifikovaný v představených studiích na toto téma, tedy riziko narůstajícího spoléhání se povinných subjektů na aktivitu a investice ostatních. Toto nebezpečí jsem přitom identifikoval ve vztahu k internetu věcí zvláště v kontextu zpracování skrze společné správce v prostředí chytrého města, představeného v oddílu 4.4.2. Významnou podmínkou pro překonání tohoto nedostatku v rámci dobrovolného sdílení informací mezi podniky byla stanovena existence nezávislého zprostředkovatele, který na jedné straně ověřuje důvěryhodnost zúčastněných subjektů a na druhé straně právě potlačuje realizaci hrozby černého pasažéra. Vhodným příkladem nastavení těchto rámců spolupráce a informační výměny z amerického prostředí jsou centra pro analýzu a sdílení informací (ISAC). Jejich přenositelnosti do evropského kontextu tak věnuji podkapitolu 6.3.

Účelné využití ohlášených informací dozorovým úřadem: Pro adekvátní nastavení ohlašovací povinnosti není dostatečné nahlížet pouze na perspektivu povinných subjektů, ale vnímám za potřebné též zhodnotit činnost dozorového úřadu navazující na řádné ohlášení porušení bezpečnosti. To je totiž nezbytnou komponentou dosahování účelu této úpravy jakožto prvku chytré regulace, tak jak byl identifikován v rámci oddílu 3.2.3. Dozorový úřad by přitom měl dostupné informace od regulovaných subjektů využívat k jejich podpoře při řešení daného případu porušení bezpečnosti a tím přispět k omezení hrozící újmy pro dotčené subjekty údajů. Dále je celkový obrázek o kyberbezpečnostní situaci napříč sektory dosažitelný při řádném plnění ohlašovací povinnosti tak, jak je předvídána Obecným nařízením, vysoce detailní a aktuální. Může tak nejen umožňovat koordinaci a vhodné zaměření preventivní a kontrolní činnosti dozorového úřadu, ale lze uvažovat o jeho prospěšnosti v souvisejícím kontextu kybernetické bezpečnosti. Jak bylo identifikováno v rámci čtvrté kapitoly, rozšiřování internetu věcí zvyšuje složitost a rozsah prostředí, které je z tohoto pohledu relevantní. Orgány monitorující a koordinující kybernetickou bezpečnost tak musejí zohledňovat nová zařízení (např. ledničky, automobily či hračky) a nové aktéry (např. četné mikropodniky), a je pro ně tudíž přínosné získat přístup k dostupným údajům

o aktuálním vývoji jejich kybernetické bezpečnosti. Hodnota informací na základě ohlašovací povinnosti se přitom v tomto směru zvyšuje nejen s jejím důsledným a plošným plněním, ale též s přihlédnutím ke skutečnosti, že o kyberbezpečnostní situaci řady podniků jsou jinak dostupné pouze velmi sporadické informace. Z tohoto důvodu rozvíjím myšlenky možného propojení a spolupráce tohoto druhu v podkapitole 6.5.

5.6 Shrnutí kapitoly

V rámci této kapitoly jsem doplnil celostní pohled na problematiku porušení bezpečnosti o ekonomickou perspektivu. Zaměřil jsem se především na studium motivace povinných subjektů plnit povinnosti související s porušením bezpečnosti, ať již v podobě zavedení přiměřených opatření či ve formě řádného ohlašování dozorovému orgánu. S ohledem na limity dostupných ekonomických modelů jsem v úvodu upozornil na omezení přímé vazby zde představených závěrů pouze na podniky založené za účelem dosahování zisku. Nevnímám však toto omezení za limitující pro obecné závěry a diskusi možných řešení v následující kapitole.

Nejprve jsem přiblížil pojem rizika a nastínil překážky při jeho hodnocení.[878] V tomto směru jsem diskutoval možnost objektivního vyjádření bezpečnostního rizika a později jeho odraz při analýze a řízení rizik. V úvodu jsem také představil racionální teorii rozhodování, jakožto předpoklad dále diskutovaného modelování rozhodování podniků.[879] Jejím základem je přitom teorie užitku, u které jsem přiblížil jak kardinalistickou, tak ordinalistickou verzi. Poté jsem popsal základní axiomy založené na maximalizaci užitku. Zmínka byla též o behaviorálních teoriích rozhodování a limitech pro jejich užití v tomto kontextu.

Pozornost jsem následně přesunul k otázce dosahování přiměřených investic do kyberbezpečnosti a souvisejícímu zhodnocení přínosů sdílení informací mezi podniky.[880] Předně jsem zdůraznil, že osud uniklých údajů je v zásadě mimo kontrolu modelovaného jednání subjektů. Představil jsem formy nákladů podniku spojené s porušením bezpečnosti. Nastínil jsem pak funkční

878 Srov. podkapitola 5.1.
879 Srov. podkapitola 5.2.
880 Srov. podkapitola 5.3.

dělení ochranných opatření na preventivní, detekční a reakční, které umožnilo lepší provázání představovaných studií s kontextem publikace jako celku.

Výchozím bodem bylo shrnutí základního modelu *Gordona* a *Loeba*, který nastiňuje možnost určení optimální výše investic do kyberbezpečnosti a poukazuje na potřebu vynucování vyšších investic právním rámcem, pokud jimi má být dosahováno potřebné míry ochrany subjektů údajů. Tento základní model má však řadu významných limitů, které se snažili překonat četní navazující autoři. Tato doplnění obsahují především zohlednění externalit typu DDoS útoku, či zahrnutí problematiky sdílení informací mezi podniky s přihlédnutím k vzájemné závislosti mezi podniky, a případně též k důsledkům jejich konkurenčního postavení.

Klíčové závěry z těchto modelů jsou dva. Prvním je existence ekonomického zdůvodnění založení povinnosti přiměřených bezpečnostních opatření, tak jak ji nalézáme v článku 32 Obecného nařízení. Druhým je pak potenciální přínos dobrovolného sdílení informací mezi podniky, které však musí splňovat určité parametry pro překonání problému černého pasažéra.

V další podkapitole jsem již pozornost přesunul na dva modely řešící vlastní rozhodování podniku o ohlašování porušení bezpečnosti.[881] Dřívější *Garciův* model je zasazen do amerického prostředí.[882] Zde je nejprve nastíněna podoba ideálního modelu regulatorního rámce a následně již diskutována překážka asymetrické informace o porušení bezpečnosti. Rozhodování o investicích do kyberbezpečnosti a o ohlášení porušení bezpečnosti je přitom vnímáno jako provázané. Za klíčové proměnné při rozhodování o ohlášení jsou identifikovány pravděpodobnost odhalení a sankce při neohlášení. *Garcia* se dále zaměřuje na stanovení potřebné výše minimální sankce. Jeho předpokladem je, že motivace podniku je vedena snahou o minimalizaci nákladů. Toho může být využito pro vynucení ohlášení porušení bezpečnosti. Regulatorní nastavení sankcí za nesplnění této povinnosti však musí být přiměřeně přísné.

Tento závěr je následně doplněn a rozvinut v modelu *Laubeho* a *Böhmeho*, byť se zdá, že vznikl nezávisle na *Garciově* modelu.[883] Je jím však efektivně potvrzena obecná přenositelnost závěrů *Garciova* modelu do evropského prostředí,

881 Srov. podkapitola 5.4.
882 Srov. oddíl 5.4.1.
883 Srov. oddíl 5.4.2.

jelikož *Laube* a *Böhme* operují v tomto kontextu a zohledňují již i povinnosti dle Obecného nařízení. Zapracovávají přitom navíc jako relevantní proměnnou i rozsah provázanosti úrovně kyberbezpečnosti mezi podniky. I pro ně jsou však výše sankce a pravděpodobnost odhalení neohlášení klíčové pro motivaci podniku. Zaměřují se pak na rozdíl od *Garcii* na určení potřebné úrovně pravděpodobnosti odhalení neohlášení dozorovým úřadem pro motivaci podniku k dodržování této povinnosti. Výsledně dovozují, že ohlašovací povinnost při adekvátní míře vymahatelnosti má společenský přínos, pokud je mezi úrovní kyberbezpečnosti podniků dostatečná provázanost, dozorový orgán je schopen účelně využít ohlášené informace a pro podnik se se zveřejněním těchto informací pojí pouze nízké dodatečné náklady.

Představené studie poskytují mozaiku vztahů a závislostí, které hrají roli pro celostní vnímání porušení bezpečnosti, a především pak pro racionální očekávání ohledně provedení právní úpravou uložených opatření k jejich zamezení, odhalení a ohlášení. Přes nevyhnutelně zjednodušující logiku představených modelů je zřejmé, že řízení rizik souvisejících s ochranou osobních údajů zahrnuje značnou míru nejistoty, která je daná komplexností problematiky, a dále zesilována případnou omezenou personální či rozpočtovou kapacitou řady správců k jejímu překonání. Přes specifické zakotvení této úpravy v Obecném nařízení je zde pak na místě vnímat nevyhnutelnou propojenost s širším kontextem zajišťování kyberbezpečnosti, kterou prostředí internetu věcí dále posiluje. To může být přínosné především při nalézání vhodných řešení odhalených překážek pro plnění povinností vztahujících se k porušení zabezpečení dle Obecného nařízení.

Dosud shromážděné poznatky v závěru provazuji do diskutovaného kontextu internetu věcí.[884] K tomu jsem byl veden dílčí otázkou (7), týkající se motivace subjektů plnit povinnosti související s porušením bezpečnosti. Dovodil jsem, že i pro prostředí internetu věcí přetrvávají výzvy spojené s nízkou motivací podniků ohlašovat porušení bezpečnosti, které identifikovali autoři představených studií a modelů u této povinnosti obecně. Získal jsem však na jejich základě současně i podněty pro možná řešení.

Dále jsem zde přispěl k zodpovězení poslední dílčí otázky (8), ohledně relativního významu notifikačních povinností porušení bezpečnosti a jeho

884 Srov. podkapitola 5.5.

přetrvání v prostředí internetu věcí. V představených modelech shledáváme ekonomické ospravedlnění těchto povinností jakožto nástrojů pro zefektivnění sdílení informací a vynucení společensky přiměřené úrovně investic do bezpečnostních opatření podniků. Současně se však potvrdila přítomnost několika významných požadavků, které podmiňují tento přínos.

Předně jde o způsobilost podniku odhalit porušení bezpečnosti, která se v prostředí internetu věcí zhoršuje. Dále je pak nezbytné účinné vynucení plnění ohlašovací povinnosti, přičemž je na místě věnovat pozornost nejen šíření jasnému signálu o výši pravděpodobně hrozící sankce, ale též dosažení dostatečné pravděpodobnosti odhalení neohlášeného porušení bezpečnosti. V neposlední řadě vnímám za podstatné přihlížet k využití sdílených informací o porušení bezpečnosti, ať již jde o dobrovolné aktivity podniků nebo o otázku kapacity dozorových úřadů účelně využít ohlášených informací. Odhalil jsem zde však i některá možná řešení, kterým se budu dále věnovat v následující šesté kapitole.

6 POVINNOSTI SPOJENÉ S PORUŠENÍM BEZPEČNOSTI OSOBNÍCH ÚDAJŮ V PROSTŘEDÍ INTERNETU VĚCÍ

Napříč předcházejícími kapitolami jsem nejprve představil podobu a rozsah současné problematiky porušení bezpečnosti.[885] Následně jsem přiblížil právní rámce zakládající povinnosti s tímto jevem spojené,[886] přičemž zvláštní důraz byl kladen na úpravu porušení zabezpečení osobních údajů dle Obecného nařízení.[887] Poté byl představen kontext internetu věcí a související změny v procesech zpracování osobních údajů a nové výzvy pro jejich zabezpečení.[888] Doplněn byl též rozbor vlastního rozhodování povinných subjektů o plnění povinností souvisejících s porušením bezpečnosti, zvláště pak s ohledem na ohlašovací povinnost vůči dozorovému orgánu.[889]

Při tomto postupném nahlížení na problematiku z kyberbezpečnostní, právní, technologické a ekonomické perspektivy jsem odhaloval a pojmenovával limity a překážky, které vyvstávají při aplikaci na dílčí situace. Jde především o:

1. právní nejistotu ohledně výkladu vzniku a obsahu daných povinností,
2. nízkou motivaci povinných subjektů zavádět přiměřená bezpečnostní opatření, a zvláště pak sdílet s vrchnostenskými orgány informace o svých pochybeních a
3. omezené možnosti odhalení neohlášených případů.

Na základě těchto, i dalších odhalených překážek vnímám značnou mezeru mezi normativním konceptem předmětných povinností a jejich praktickou realizací. Jde tudíž o oblast, které je příznačná dichotomie normy a její aplikace, resp. doktríny a empirie, kterou obecně pojmenoval již v roce 1910 *Pound* ve svém příspěvku *„Law in Books and Law in Action"*.[890]

885 Srov. druhá kapitola.
886 Srov. třetí kapitola.
887 Srov. podkapitola 3.2.
888 Srov. čtvrtá kapitola.
889 Srov. pátá kapitola.
890 Srov. POUND, Roscoe. Law in Books and Law in Action. *44 American law Review,* 1910; K pojmu blíže též HALPERIN, Jean-Louis. Law in Books and Law in Action: The Problem of Legal Change. *Maine Law Review*, 2017, roč. 64, č. 1.

Jak jsem se dále snažil upozornit skrze zohlednění technologického vývoje zachyceného zde jako internet věcí, tato mezera je dále rozšiřována. Technologická realita se totiž vzdaluje od kontextu, na který byla normotvůrci příslušná právní úprava formulována a ve kterém byla přijímána. Tento jev *Marchant, Allenby* a *Herkert* označují jako problém tempa *(pacing problem)*.[891]

Příslušná úprava v článcích 33 a 34 Obecného nařízení byla, shodně s tímto předpisem jako celkem, koncipována nadčasově a bez vazby na konkrétní technologická řešení a možnosti. Přesto jsem identifikoval ve čtvrté kapitole specifika internetu věcí, která nelze adekvátně postihnout bez extenzivního výkladu či specifických doplnění příslušných normativních pravidel. Zde jde především o dynamické zpracování osobních údajů v prostředí chytrého města a související *ad hoc* vztahy společných správců, které zamlžují přiřazení povinností vážících se k porušení zabezpečení konkrétnímu subjektu.

Mým cílem v rámci této kapitoly je diskutovat možnosti dílčích úprav, doplnění či provázání se souvisejícími rovinami, která by při vhodné kombinaci a provedení byly s to zúžit mezeru mezi předmětným rámcem povinností dle Obecného nařízení a jeho praktickou aplikací, či alespoň omezit její rozšiřování v důsledku rozvoje internetu věcí. Představované úvahy *de lege ferenda* je na místě nevnímat odděleně, byť jejich vhodná a možná kombinace závisí na politických, institucionálních či ekonomických aspektech přesahujících rámec zde představované monografie.

Nejprve se zaměřím na možnosti posílení právní jistoty povinných subjektů skrze překonání nedostatečné srozumitelnosti či určitosti aplikace povinností souvisejících s porušením zabezpečení. Budu zde diskutovat cesty pro regulatorní reflexi specifik prostředí internetu věcí (podkapitola 6.1) i zprostředkování výkladu performativních pravidel a další cesty k usnadnění plnění předmětných povinností (podkapitola 6.2).

Následně přenesu pozornost k možnostem posílit motivaci povinných subjektů k realizaci preventivních opatření. Zde diskutuji přínosy spojené s koordinovaným dobrovolným sdílením informací (podkapitola 6.3)

891 Srov. MARCHANT, Gary E., Braden R. ALLENBY a Joseph R. HERKERT (eds.). *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*. Dordrecht: Springer, 2011, The International Library of Ethics, Law and Technology, 7.

a také možnosti rozsáhlejší přenositelnosti újmy vzniklé subjektům údajů na povinné subjekty (podkapitola 6.4).

Na závěr se budu věnovat problematice řádného ohlašování porušení zabezpečení. Zde přednesu tezi o možném účelném posílení kapacit Úřadu včasně zpracovávat a vyhodnocovat ohlašované informace skrze systematickou spolupráci v rámci veřejné správy (podkapitola 6.5). V poslední podkapitole pak diskutuji možné přístupy k překonání překážky nesnadného odhalení porušení zabezpečení ať již povinným subjektem, či dozorovým úřadem (podkapitola 6.6).

6.1 Regulatorní reflexe specifik zpracování osobních údajů v prostředí internetu věcí

Ze své podstaty je prostředí internetu věcí v rámci unijního práva postihováno celým spektrem právních předpisů, z nichž Obecné nařízení dopadá pouze na dílčí aspekt zohledňující častou osobní povahu zpracovávaných a přenášených údajů a s tím spojená rizika pro dotčené fyzické osoby. Vzhledem k rozsáhlé použitelnosti[892] a obecně stanoveným požadavkům a povinnostem přesahujícím do souvisejících rovin regulace[893] se Obecné nařízení uplatní na celé spektrum rozmanitých kontextů, ve kterých dochází k rozvoji internetu věcí.[894] Nelze však opomíjet, že řada sektorových užití podléhá dodatečné specifické regulatorní úpravě, která je harmonizována či sjednocena na úrovni unijního práva, ať již se jedná o dopravní prostředky,[895]

892 Povinnými správci a zpracovateli dle Obecného nařízení jsou všechny fyzické či právnické osoby soukromého či veřejného práva, které zpracovávají osobní údaje, na které dopadá tento předpis. Pro většinu oblastí vyňatých z této věcné působnosti pak nalézáme specifickou národní úpravu, např. na základě transpozice směrnice 2016/680. Blíže viz podkapitola 3.2.

893 Příkladem jsou požadavky na zabezpečení zpracování dle čl. 32 Obecného nařízení, které v sobě nevyhnutelně zahrnují též opatření pro zvýšení úrovně kyberbezpečnosti.

894 Příklady automatizace M2M datových toků, prostředí chytrého města i podnikových sítí i těch nejmenších podniků byly představeny v rámci podkapitoly 4.4, čímž bylo poukázáno na šíři a rozmanitost tohoto spektra.

895 Příkladem viz nařízení Evropského parlamentu a Rady (ES) č. 661/2009 ze dne 13. července 2009 o požadavcích pro schvalování typu motorových vozidel, jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla z hlediska obecné bezpečnosti nebo nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě.

zdravotnická zařízení[896] či inteligentní měření a související prvky energetických distribučních či přenosových sítí.[897]

6.1.1 Provázanost regulatorních rovin dopadajících na internet věcí

Aktivní fyzické prvky řady zařízení internetu věcí znamenají, že se v nich potkávají tři bezpečnostní perspektivy:

1. fyzická bezpečnost zařízení (lépe zachycená anglickým výrazem *safety*),
2. bezpečnost ve smyslu integrity zařízení (lépe zachycená anglickým výrazem *security*) a
3. ochrana zpracovávaných či uchovávaných dat a jejich informační hodnoty, především ve smyslu ochrany osobních údajů a soukromí příslušných fyzických osob.

Dodatečnou čtvrtou perspektivou, kterou lze spojovat se složitými systémy a sítěmi internetu věcí zastřešujících významné služby a funkce, např. v kontextu chytrého města, je dále kybernetická odolnost *(cyber resilience)* ve smyslu *„schopnosti nepřetržitě poskytovat zamýšlené výstupy i přes nepříznivé kybernetické události"*.[898]

Fyzická bezpečnost: Tato rovina je do značné míry upravena harmonizujícím rámcem, který zahrnuje na jedné straně směrnici Rady 85/374/EHS o odpovědnosti za vadu výrobku[899] a na druhé straně pak směrnice upravující požadavky na zařízení dodávaná na vnitřní trh, tedy v daném kontextu předně směrnici

896 Příkladem směrnice Evropského parlamentu a Rady 2007/47/ES ze dne 5. září 2007, kterou se mění směrnice Rady 90/385/EHS o sbližování právních předpisů členských států týkajících se aktivních implantabilních zdravotnických prostředků, směrnice Rady 93/42/EHS ze dne 14. června 1993 o zdravotnických prostředcích a směrnice 98/8/ES ze dne 16. února 1998 o uvádění biocidních přípravků na trh či nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU.

897 Příkladem směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU či nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou.

898 *„The ability to continuously deliver the intended outcome despite adverse cyber events."* Srov. BJÖRCK, Fredrik et al. Cyber Resilience – Fundamentals for a Definition. In: ROCHA, Alvaro et al. (eds.). *New Contributions in Information Systems and Technologies* [online]. Cham: Springer International Publishing, 2015, s. 312, Advances in Intelligent Systems and Computing.

899 Směrnice Rady 85/374/EHS ze dne 25. července 1985 o sbližování právních a správních předpisů členských států týkajících se odpovědnosti za vadné výrobky.

2014/53/EU,[900] harmonizující požadavky na bezpečnost rádiových koncových zařízení a směrnici 2014/35/EU,[901] upravující požadavky na elektrická zařízení.[902]

Bezpečnost ve smyslu integrity: Zde vystupuje do popředí především otázka kyberbezpečnosti, resp. kybernetické bezpečnosti,[903] která doznala významné harmonizace národních úprav na základě směrnice 2016/1148[904] a nedávno též nařízením 2019/881, aktem o kybernetické bezpečnosti.[905]

Ochrana informační hodnoty zpracovávaných či uchovávaných dat: Vedle v této monografii ústřední perspektivy ochrany osobních údajů do této roviny zahrnujeme též obecnější perspektivu ochrany soukromí.[906] Dále nelze opomíjet rámce na ochranu dat z jiných hodnotových perspektiv, jako jsou ochrana duševního vlastnictví,[907] obchodního tajemství[908] či utajovaných informací.[909]

900 Směrnice Evropského parlamentu a Rady 2014/53/EU ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES.

901 Směrnice Evropského parlamentu a Rady 2014/35/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se dodávání elektrických zařízení určených pro používání v určitých mezích napětí na trh.

902 Provázanost těchto směrnic je přitom dána bodem odůvodnění 7 směrnice 2014/53/EU, ve kterém je uvedeno, že *„[c]íle stanovené směrnicí 2014/35/EU, které se týkají požadavků na bezpečnost, postačují pro rádiová zařízení, a měly by proto sloužit jako reference a být uplatňovány na základě této směrnice. Aby se zbytečně neopakovala tatáž ustanovení, kromě ustanovení o takových požadavcích, neměla by se směrnice 2014/35/EU vztahovat na rádiová zařízení."*

903 Pojem kyberbezpečnosti je širší a zachycuje problematiku včetně technických a dalších rovin, zatímco pojem kybernetické bezpečnosti je vlastní právním předpisům vztahujícím se na tuto problematiku.

904 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

905 Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti").

906 Její harmonizované pojetí přitom prostupuje mezinárodními smlouvami a lze ji tak míti do určité míry za vlastní napříč jurisdikcemi. K jejímu zakotvení a obsahu jsem se vyjádřil blíže v KASL, František. 9 Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 396 a násl.

907 Přehled o relevantních právních předpisech pro tuto tematicky bohatou oblast právní úpravy nabízí např. KOUKAL, Pavel et al. *Právo duševního vlastnictví* [online]. 2020 [cit. 18. 7. 2021].

908 Směrnice Evropského parlamentu a Rady (EU) 2016/943 ze dne 8. června 2016 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním.

909 V této oblasti je významné předně Rozhodnutí Rady 2013/488/EU ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU a dále pak soubor dohod o bezpečnostních postupech pro výměnu a ochranu utajovaných informací mezi EU a třetími státy.

Nařízení o soukromí a elektronických komunikacích: Jak již bylo podrobně vylíčeno v rámci třetí kapitoly, ochranu osobních údajů v EU zastřešuje předně Obecné nařízení. Dodatečné zohlednění specifik internetu věcí (by) přitom mělo být[910] obsaženo v nařízení o soukromí a elektronických komunikacích.[911] To je v řádném legislativním procesu již od počátku roku 2017, o finálním znění však přetrvává intenzivní debata a vyjednávání, což se odráží v řadě úprav a doplnění, která již nyní významně proměnila původní návrh. Ve znění návrhu z 6. března 2020, zpracovaného v rámci prvního čtení Radou EU, nalézáme upravená ustanovení týkající se internetu věcí.[912] V nově přeformulovaném bodu odůvodnění 12 navrhovaného nařízení je kladen důraz na vnímání internetu věcí jako služby elektronických komunikací. To odráží preferenci regulatorního přístupu zaměřeného na podobu služeb a procesů. Je přijímána rostoucí role automatizované M2M komunikace a potřeba zajištění její důvěrnosti.

Význam tohoto nařízení však do budoucna vnímám jako omezený. Na jedné straně je to dáno tím, že příslušná ustanovení nedopadají na neveřejné sítě, tedy typicky vnitropodniková prostředí internetu věcí a na druhé straně nejsou povinnými subjekty poskytovatelé služeb na úrovni aplikaci, jelikož ti jsou bráni na roveň s koncovými uživateli.[913] Byť nelze předvídat, jaké konečné podoby text nařízení nabyde v době přijetí, i v současném znění nacházím několik bodů, které přispějí k přiblížení regulatorního rámce ochrany osobních údajů nově vznikající technologické realitě. Jde především o ustanovení návrhu nařízení týkající se zajištění důvěrnosti, které upravuje přípustné účely zpracování dat elektronických komunikací, zahrnující mimo jiné odhalení a prevenci bezpečnostních hrozeb a útoků jak v rámci přenosu, tak v zařízeních koncových uživatelů.[914]

910 Původně mělo být toto nařízení přijato společně s Obecným nařízením, příslušný legislativní proces však stále není ukončen a není tedy zjevné, zda a případně kdy bude skutečně přijato.

911 Srov. návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).

912 Srov. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). *Council of European Union* [online]. 6543/20. Brussels: Council of the European Union. 2020 [cit. 18. 7. 2021].

913 Ibid., s. 14 bod odůvodnění 12 návrhu.

914 Ibid., s. 61 čl. 6 odst. 1 písm. b) a c) návrhu.

6.1.2 Přiřazení povinností v situacích ad hoc společných správců

Specifickou výzvou identifikovanou v rámci představované monografie, kterou přináší prostředí internetu věcí pro řešení případů porušení zabezpečení osobních údajů, je neurčitost přiřazení rolí ve složitých sítích s prvky automatizované M2M komunikace. Primárně odpovědným subjektem při porušení zabezpečení osobních údajů je, jak bylo nastíněno v podkapitole 3.2, správce. Tím je dle článku 4 bodu 7 Obecného nařízení subjekt, který *„sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů."*[915] V souladu s výkladem SDEU ve věci *Wirtschaftsakademie Schleswig-Holstein*, C-210/16,[916] je na místě v zájmu zajištění vysoké úrovně ochrany subjektů údajů vykládat pojem správce široce.[917] V daném případě byli za společné správce ve vztahu k zájmové stránce na sociální síti určeni jak poskytovatel dané služby informační společnosti (společnost *Facebook*), tak administrátor dané stránky *(Wirtschaftsakademie Schleswig-Holstein)*, byť s možností zohlednění rozdílného podílu na odpovědnosti za dané zpracování osobních údajů.[918]

Společní správci v prostředí internetu věcí: Jak nastíněno výše,[919] do budoucna lze za takto nastavených parametrů očekávat stále častější situace, kdy kontrola nad zpracováním připadá v určité míře více subjektům a dochází tedy k situaci společných správců dle článku 26 Obecného nařízení. Ten předjímá ujednání mezi těmito správci ohledně podílu na plnění povinností, není však zřejmé, jak tohoto ujednání bude dosahováno v případě *ad hoc* zpracování osobních údajů, zvláště pokud půjde o proces automatizované či dokonce autonomní M2M komunikace. Absence zjevné dělby povinností společných správců je zvláště problematická ve vztahu k ohlašovací a oznamovací povinnosti, kdy nelze na základě závěrů páté kapitoly předpokládat motivaci jednotlivého správce ohlašovat porušení zabezpečení bez dostatečně silné incentivy. Tu přitom rozhodně neposiluje nastavení práva subjektu údajů na náhradu újmy, pro které je v článku 82 odst. 4 Obecného nařízení stanovena společná a nerozdílná odpovědnost společných správců vůči

915 Srov. čl. 4 bod 7 Obecného nařízení.
916 Rozhodnutí SDEU ze dne 5. 6. 2018 ve věci *Wirtschaftsakademie Schleswig-Holstein,* C-210/16.
917 Bod 28 rozhodnutí C-210/16.
918 Bod 43 rozhodnutí C-210/16.
919 Srov. především oddíl 4.4.2.

subjektu údajů bez ohledu na podíl daného společného správce, s následnou možností regresního nároku vůči ostatním společným správcům dle podílu na odpovědnosti.[920] Správce, který by notifikoval porušení zabezpečení se tak dobrovolně vystavuje celému rozsahu těchto nároků,[921] což je v rozporu s podmínkou funkčního nastavení ohlašovací povinnosti identifikovanou v podkapitole 5.5 ohledně nízkých dodatečných nákladů spojených se sdílením této informace.

Míra odpovědnosti je sice v souladu s článkem 83 odst. 1 písm. d) Obecného nařízení zohledňována dozorovým úřadem při ukládání případné správní pokuty, to se však bez dalšího nezdá být dostatečnou incentivou pro společné správce k proaktivnímu plnění ohlašovací povinnosti.

Určitý prostor pro zlepšení situace zde vnímám při zavedení a sjednocení praxe dozorových úřadů ve formě programu aplikace mírnějšího režimu při ukládání pokut *(leniency program)* po vzoru osvědčené praxe v kartelových otázkách práva hospodářské soutěže. Dozorové úřady mají prostor pro tuto formu správního uvážení na základě článku 83 odst. 2 písm. h) Obecného nařízení, který ukládá, aby správní pokuta odrážela mimo jiné i *„způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře"*.[922] Na to, aby se tato proměnná adekvátně odrazila v rozhodování povinných subjektů, je však nezbytné, aby byla transparentně a jednoznačně zakotvena pravidla a rozsah zohlednění tohoto kritéria. V otázkách práva hospodářské soutěže je toho dosahováno cestou příslušného oznámení Úřadu pro ochranu hospodářské soutěže,[923] resp. oznámení Komise.[924] Zkušenosti z tohoto prostředí však poukazují na potřebu důsledného a vyváženého nastavení podmínek mírnějšího režimu

920 To odpovídá obecným pravidlům odpovědnosti za škodu více škůdců. Srov § 2915 odst. 1 zákona 89/2012 Sb.

921 Možnost regresu v tomto směru nelze považovat za klíčovou, jelikož vymáhání příslušné části náhrady újmy po ostatních společných správcích je značně procesně náročné ve standardních situacích a může být v podstatě nemožné v kontextu *ad hoc* zpracování v rámci internetu věcí.

922 Srov. čl. 83 odst. 2 písm. h) Obecného nařízení.

923 Viz Oznámení Úřadu pro ochranu hospodářské soutěže ze dne 4. listopadu 2013 o aplikaci § 22ba odst. 1 zákona o ochraně hospodářské soutěže (program leniency). *Úřad pro ochranu hospodářské soutěže* [online]. Brno: Úřad pro ochranu hospodářské soutěže, 2013 [cit. 17. 7. 2021].

924 Viz Oznámení Komise o ochraně před pokutami a snížení pokut v případech kartelů. Úř. věst. C 298, 8. 12. 2006, s. 17–22.

a současnou hrozbu vysokých sankcí mimo tento režim.[925] To ovšem odpovídá normativnímu nastavení Obecného nařízení a zavedení srovnatelného programu tak nabízí, dle mého názoru, motivační nástroj pro řešení ohlašování porušení zabezpečení u společných správců.

6.1.3 Koordinovaný regulatorní přístup a certifikace zařízení internetu věcí

S ohledem na časté základní nedostatky bezpečnostních opatření u zařízení internetu věcí, na které jsem upozornil v podkapitole 4.3, je dále potřebné, aby regulatorní důraz směřoval do preventivní roviny, kdy je snižováno riziko samotného vzniku porušení zabezpečení a případně opominutí jeho odhalení. Požadavky na opatření za tímto účelem zakládá vedle ochrany osobních údajů většina z výše nastíněných regulatorních rovin.

Jejich vzájemné postavení v konkrétním případě je přitom zpravidla nepřehledné a jak zdůrazňují *Leverett, Clayton* a *Anderson* ve své studii pro Komisi z roku 2017, doposud nepříliš koordinované.[926] Autoři dospívají k souboru doporučení, která lze do značné míry provázat s rovinami diskutovanými v rámci této kapitoly. Vedle hlavního doporučení vytvořit společnou agenturu pro bezpečnostní inženýrství (*European Safety and Security Engineering Agency*), která by poskytla institucionální přemostění mezi agendami a působnostmi jednotlivých regulátorů a umožnila důsledné řešení bezpečnostních incidentů přesahujících jednotlivé agendy,[927] rozebírají přínosy bezpečnostní certifikace zařízení internetu věcí.[928]

Autoři prosazují začlenění požadavků na autocertifikaci *(self-certification)* bezpečnosti zařízení při připojení do sítě a možnosti online aktualizace jeho software jako součást požadavků kladených na výrobce zařízení pro získání

925 Srov. MARVÃO, Catarina a Giancarlo SPAGNOLO. *What Do We Know about the Effectiveness of Leniency Policies? A Survey of the Empirical and Experimental Evidence* [online]. Working Paper. 28. SITE Working Paper, 2014, s. 23 [cit. 18. 7. 2021].

926 Viz LEVERETT, Eireann, Richard CLAYTON a Ross ANDERSON. *JRC Technical Reports: Standardisation and certification of safety, security and privacy in the 'Internet of Things'* [online]. Brussels: European Commission, 2018, s. 20 [cit. 18. 7. 2020].

927 Ibid., s. 66–67.

928 Ibid., s. 25; K tomu se přitom část spoluautorů studie vyjádřila již dříve ve zprávě ANDERSON, Ross et al. *Security Economics and the Internal Market* [online]. Report/Study. Heraklion: ENISA. 2008 [cit. 18. 7. 2021].

označení CE osvědčující shodu výrobku s příslušnými harmonizovanými unijními právními předpisy.[929, 930]

Prostor v tomto směru vzniká především skrze certifikaci kybernetické bezpečnosti na základě nedávno použitelného nařízení 2019/881, aktu o kybernetické bezpečnosti.[931] Metodologická vodítka pro tento certifikační rámec byla vydána v září 2021.[932] Internet věcí byl v tomto ohledu identifikován jako jedna ze čtyř oblastí pro rozvoj unijního certifikačního schématu pro kybernetickou bezpečnost.[933] Výzkumný tým ENISA v tomto směru provedl analýzu podmínek pro kyberbezpečnostní certifikaci zařízení internetu věcí v EU.[934] Poukazují přitom na skutečnost, že ačkoliv některá odvětví (automobilový průmysl, zdravotnická zařízení, průmyslové systémy) vytvářejí vlastní standardy a regulatorní rámce, certifikace spotřebních zařízení internetu věcí je s těmito komplementární.[935]

Prvním zvažovaným certifikačním schématem je schéma *Eurosmart IoT*,[936] které je připravováno se zohledněním požadavků aktu o kybernetické bezpečnosti a v řadě ohledů sleduje strukturu *Common Criteria*.[937] Překážkou pro jeho užití napříč zařízeními internetu věcí je především jediná úroveň požadavků,

929 K podmínkám získání označení CE blíže viz čl. 30 nařízení Evropského parlamentu a Rady 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení č. 339/93.

930 Srov. LEVERETT, Eireann, Richard CLAYTON a Ross ANDERSON. *JRC Technical Reports: Standardisation and certification of safety, security and privacy in the 'Internet of Things'* [online]. Brussels: European Commission, 2018, s. 69 [cit. 18. 7. 2020].

931 Této úpravě se v českém akademickém prostředí mmj. věnoval *Vostoupal*. Blíže viz VOSTOUPAL, Jakub. Certifikace kyberbezpečnostních technologií. *Revue pro právo a technologie* [online]. 2019, roč. 10, č. 20.

932 Methodology for a Sectoral Cybersecurity Assessment. EU Cybersecurity Certification Framework". *ENISA* [online]. ENISA 2021 [cit. 20. 10. 2021].

933 Srov. BARREIRA, Inigo et al. *Standards Supporting Certification. Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes* [online]. Report/Study. Heraklion: ENISA, 2020, s. 5 [cit. 18. 7. 2021].

934 Ibid., s. 8.

935 Ibid., s. 9.

936 Srov. Eurosmart IoT Certification Scheme. *Eurosmart IoT Certification Scheme* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.eurosmart.com/eurosmart-iot-certification-scheme/

937 *Common Criteria for Information Technology Security Evaluation* (CC) je nejšíře mezinárodně uznávaný standard pro uznání shody bezpečnosti IT produktů (software, hardware i firmware). Srov. Common Criteria. *CC Portal* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.commoncriteriaportal.org/

která směřuje na výrobky s vysokými požadavky na bezpečnost a není tudíž nezbytná ani vhodná pro výrobky s nízkým bezpečnostním rizikem. V rámci tohoto schématu nepřichází tudíž příliš v úvahu široce užívaná alternativa certifikace skrze certifikační autoritu, tedy prohlášení výrobce o shodě (autocertifikace).[938] Alternativou je certifikační schéma *ETSI 303 645*,[939] které umožňuje i autocertifikaci pro výrobky se základní úrovní bezpečnosti.[940] Vlastní formát a procesy tohoto certifikačního schéma stále získávají finální kontury, směrodatným podkladem je znění publikované 19. června 2020.[941]

Zavedení plošné certifikace zařízení internetu věcí může představovat významný přínos pro zajištění realizace povinností souvisejících s porušením zabezpečení dle Obecného nařízení. Certifikační schéma *Eurosmart IoT* zakládá podrobné požadavky správy bezpečnostních zranitelností a incidentů. To zahrnuje nejen opatření vedoucí k odhalení porušení zabezpečení, např. skrze penetrační testování, ale též řádné plnění ohlašovací povinnosti a případně též účast na platformách pro sdílení informací o bezpečnostních zranitelnostech, o kterých je pojednáno v podkapitole 6.3.[942] Stejně tak certifikační schéma *ETSI 303 645* předpokládá transparentní a veřejně dostupnou politiku pro sdělování zranitelností *(vulnerability disclosure policy)*,[943] jakož i zakotvení technických opatření souvisejících s ochranou osobních údajů[944] a zajišťujících řádné plnění požadavků dle článku 32 Obecného nařízení.

938 Srov. BARREIRA, Inigo et al. *Standards Supporting Certification. Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes* [online]. Report/Study. Heraklion: ENISA, 2020, s. 9 a 12 [cit. 18. 7. 2021].

939 Srov. PANDZA, Jasper. Details of „REN/CYBER-0048" Work Item. *ETSI* [online]. 29. 6. 2020 [cit. 18. 7. 2021]. Dostupné z: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=57991

940 Srov. BARREIRA, Inigo et al. *Standards Supporting Certification. Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes* [online]. Report/Study. Heraklion: ENISA, 2020, s. 13 [cit. 18. 7. 2021].

941 Viz ETSI. *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements* [online]. ETSI EN 303 645 V2.1.1 (2020-06). Valbonne: ETSI. 2020 [cit. 17. 7. 2021].

942 Viz *Technical Report [TR-e-IoT-SCS-Part-2] Generic Protection Profile Pilot v1.2 RELEASE* [online]. [e-IoT-SCS-Part-2] GPP v1.2. Brussels: Eurosmart, 2019, s. 32–34 [cit. 17. 7. 2021].

943 Srov. ETSI. *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements* [online]. ETSI EN 303 645 V2.1.1 (2020-06). Valbonne: ETSI, 2020, s. 14 [cit. 17. 7. 2021].

944 Ibid., s. 24–25.

Byť bezpečnostní certifikace nesměřuje přímo k překonání identifikovaných limitů ohlašovací povinnosti porušení zabezpečení, při plošném uplatnění je způsobilá posílit tendence povinných subjektů přijímat přiměřená ochranná opatření, která sníží riziko porušení zabezpečení i následnou újmu.

6.2 Usnadnění výkladu a plnění příslušných povinností

Certifikaci lze však mít pouze za jeden z nástrojů, který usnadní pozici povinných subjektů skrze přeložení normativně uložených povinností, často ve formě performativních pravidel, do technicky exaktních požadavků. Obecné nařízení přikládá výkladu a specifikaci uložených povinností pro dílčí kontexty významnou roli a předvídá pro ně především tři zdroje: výkladové aktivity dozorových úřadů, vypracování kodexů chování sektorovými organizacemi a specifická osvědčení souladu udělovaná akreditovanými subjekty.

6.2.1 Pokyny, doporučení a osvědčené postupy

Přední vodítko při výkladu ustanovení Obecného nařízení představují pokyny, doporučení a osvědčené postupy vydávané v souladu s článkem 70 Obecného nařízení Sborem. Ta díky tomu, že Sbor sdružuje představitele dozorových úřadů ze všech členských států,[945] mají širokou validitu. Odst. 1 písm. g) a h) tohoto článku přímo ukládají Sboru vypracovat vodítka pro ustanovení článků 33 a 34 Obecného nařízení, resp. pro:

1. zjištění případů porušení zabezpečení osobních údajů,
2. určení zbytečného odkladu podle článku 33 odst. 1 a 2,
3. stanovení konkrétních okolností, za nichž jsou správce a zpracovatel povinni porušení ohlásit a
4. určení okolností, za jakých je pravděpodobné, že porušení zabezpečení osobních údajů bude mít z následek vysoké riziko pro práva a svobody fyzických osob.

K tomuto účelu slouží *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679*,[946] na které bylo odkazováno napříč

945 Srov. čl. 68 odst. 3 Obecného nařízení.

946 Srov. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29. 2018 [cit. 28. 2. 2021].

podkapitolou 3.2, při výkladu příslušných ustanovení. Tyto pokyny Sboru poskytují obecný výklad aplikovatelný napříč sektory a činnostmi. Jsou pak doplněny novějšími vodíky s konkrétními příklady řešených situací,[947] které výrazně zvyšují srozumitelnost a praktickou využitelnost tohoto souboru výkladových materiálů ze strany povinných subjektů pro řešení konkrétních situací a výklad dílčích nejasností souvisejících se specifiky dané podnikatelské aktivity.

6.2.2 Kodexy chování a standardizace

Pro specifikaci povinností pro jednotlivá odvětví předpokládá Obecné nařízení klíčovou roli dobrovolných kodexů chování *(code of conduct)*, vypracovaných v souladu s článkem 40 Obecného nařízení. Dle *Pokynů 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679*,[948] které vydal Sbor v polovině roku 2019, *„představují praktickou, potenciálně nákladově efektivní a smysluplnou metodu pro dosažení větší míry jednotnosti ochrany práv na ochranu osobních údajů* […] a] *[p]oskytují rovněž příležitost pro konkrétní odvětví, aby zohlednila společné činnosti v oblasti zpracování údajů a dohodla se na specifických a praktických pravidlech ochrany údajů, která uspokojí potřeby odvětví, jakož i požadavky obecného nařízení o ochraně osobních údajů.“*[949]

Jako takové bylo ustanovení vyzývající ke vzniku kodexů chování obsaženo již v předchozí úpravě dle směrnice 95/46/ES. Docházelo však pouze k jejich sporadickému utváření a z hlediska povinných subjektů nebyl tento nástroj vnímán za příliš užitečný.[950] Mimo EU však doznávají značné popularity v zemích s právním systémem *common law*, jako například v Kanadě.[951]

Jelikož jsou kodexy dobrovolným nástrojem vycházejícím z aktivity odvětvových uskupení a sdružení, nebyl jejich potenciál co do jejich množství

947 Viz Guidelines 01/2021 on Examples regarding Data Breach Notification. *EDPB* [online]. Brusel: EDPB 2021 [cit. 10. 10. 2021].

948 Srov. Pokyny 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679. *Evropský sbor pro ochranu osobních údajů* [online]. 1/2019 verze 2.0. Brusel: Evropský sbor pro ochranu osobních údajů, 2019, s. 679 [cit. 17. 7. 2021].

949 Ibid., s. 5.

950 Srov. KAMARA, Irene. Article 40. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 718.

951 Ibid., s. 720.

a obsahu doposud zdaleka naplněn. Obecné nařízení nadto nestanoví žádná specifická kritéria pro vymezení subjektů, které mohou přijmout kodex chování, což zakládá potenciál pochybností o jejich vymahatelnosti či široké uplatnitelnosti, pokud jsou již nějaké kodex vytvořeny a schváleny příslušným dozorovým úřadem.[952] Z těchto důvodů se domnívám, že role kodexů chování při usnadnění zajištění souladu s Obecným nařízením v kontextu internetu věcí nebude ani do budoucna příliš významná, v souvislosti s porušením zabezpečení však vnímám alternativu v podobě standardizace.

Standardizace: Vzhledem k provázanosti povinností z ochrany osobních údajů s dalšími rovinami bezpečnosti nastíněnými v předchozí podkapitole namísto toho přikládám rostoucí význam bezpečnostním standardům a kodexům správné praxe *(code of practice)* upravených specificky pro prostředí internetu věcí. Již ke konci roku 2018 bylo možné identifikovat značnou aktivitu v tomto směru napříč uskupeními a sdruženími jako je *IoT Security Foundation*,[953] *Industrial Internet Consortium*[954] či *IoT Security Initiative*[955].[956] Studie ENISA z konce roku 2018 pak propojuje existující standardy mezinárodních (ISO/IEC, ITU) a evropských (CEN, CENELEC, ETSI) organizací s požadavky předpisů upravujících kybernetickou bezpečnost a ochranu osobních údajů pro internet věcí.[957]

Standardizace nabízí nejen funkční vodítko jednotlivým povinným subjektům pro zavedení přiměřených a vhodných opatření v souladu s osvědčenou praxí, ale zakládá taktéž podmínky pro kompatibilitu a interoperabilitu mezi řešeními od různých výrobců a minimální úrovní opatření, která jsou v rámci daného odvětví očekávána. Vzhledem k provázané povaze prostředí

952 Ibid., s. 721.

953 Viz Framework. *IoT Security Foundation* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.iotsecurityfoundation.org/tag/framework/

954 Viz Technical & White Papers. *Industrial Internet Consortium* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.iiconsortium.org/white-papers.htm

955 Viz Open security knowledge. *IoT Security Initiative* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.iotsi.org

956 Srov. Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security. *Department for Digital, Culture, Media and Sport* [online]. London: Department for Digital, Culture, Media and Sport, 2018, s. 6–7 [cit. 17. 7. 2021].

957 Srov. ANDRUKIEWICZ, Elżbieta, Scott CADZOW a Sławomir GÓRNIAK. *IoT Security Standards Gap Analysis* [online]. Report/Study. v 1.0. Heraklion: ENISA. 2018 [cit. 18. 7. 2021].

internetu věcí, širokému spektru použití a rozmanitosti dílčích řešení od řady výrobců typické pro vysoce dynamické a inovativní tržní prostředí je zde potřeba standardizace dále umocněna.

Nedávný výstup projektu H2020 *CREATE-IoT* výstižně shrnuje složitost standardizace internetu věcí zohledněním jednotlivých vrstev, ve kterých jí má být dosaženo. Je představeno pojetí interoperability na bázi vrstev, které rozlišuje:

1. technickou vrstvu, tzn. na úrovni komunikačních protokolů,
2. syntaktickou vrstvu, tzn. formáty dat a techniky datové komprese,
3. sémantickou vrstvu, tzn. sjednocení významu komunikovaného obsahu a
4. organizační vrstvu, tzn. zajištění efektivní kooperace a procesů sdílení informací napříč systémy, infrastrukturami, místy a kulturami.[958]

Pro ucelené zachycení prostředí internetu věcí za účelem standardizace byl pak v rámci tohoto projektu formulován trojrozměrný referenční model architektury internetu věcí, který provazuje úrovně *(layers)* z pohledu funkcionality (např. fyzická úroveň senzorů, úroveň síťové komunikace či aplikační úroveň), průřezové funkce *(cross-cutting functions)* jako je bezpečnost, soukromí či spolehlivost a vlastnosti *(properties)* jako je interoperabilita či škálovatelnost.[959] Tento model lze následně využít k zachycení zaměření jednotlivých standardizačních procesů a rozsahu jejich aplikovatelnosti.[960]

Na význam utváření standardů pro internet věcí upozorňují i *Leverett, Clayton* a *Anderson* ve studii zmiňované již v podkapitole 6.1. Poukazují na množinu existujících mezinárodně či evropsky přijímaných standardů pro prostředí informačních a komunikačních technologií, které však mohou mít odlišnou použitelnost pro konkrétní řešení v rámci internetu věcí, což tvoří toto prostředí z hlediska současných standardů složitým a nepřehledným.[961] Nabízejí

958 Srov. RAGGETT, Dave et al. *Final report on IoT standardisation activities* [online]. Deliverable 06. 06. CREATE IoT, 2020, s. 9–10 [cit. 17. 7. 2021]. *Cross Fertilisation through Alignment, Synchronisation and Exchanges for IoT.*

959 Ibid., s. 11–12.

960 Ibid., s. 30 a násl.

961 Srov. LEVERETT, Eireann, Richard CLAYTON a Ross ANDERSON. *JRC Technical Reports: Standardisation and certification of safety, security and privacy in the 'Internet of Things'* [online]. Brussels: European Commission, 2018, s. 37 [cit. 18. 7. 2020].

také přehled nejvýznamnějších dostupných standardů, které lze považovat za relevantní pro bezpečnostní aspekty prostředí internetu věcí.[962]

Z hlediska povinností spojených s porušením zabezpečení osobních údajů doznávají na významu zvláště dva standardy. *ISO/IEC 29147:2018*, který upravuje vhodné nastavení komunikačních kanálů pro ohlášení možných zranitelností vůči danému výrobci či poskytovateli služby a navazujících procesů pro reakci na tato ohlášení a řešení takto odhalených zranitelností.[963] Dále pak také *ISO/IEC 30111:2019* upravující procesy pro verifikaci interně či externě ohlášených zranitelností a distribuci nápravy.[964, 965]

Systematika procesů a dokumentace na základě těchto standardů lze vnímat za vhodný podklad opatření pro snižování rizika případů porušení zabezpečení, jejich včasné detekce a adekvátního řešení.[966]

6.2.3 Vydávání osvědčení a zavedení pečetí a známek

Třetím možným zdrojem usnadnění výkladu je akreditace činnosti specializovaných subjektů dle článku 43 Obecného nařízení, které by vydávali správcům a zpracovatelům osvědčení o ochraně údajů, jakož případně i pečeti či známky dokládající ochranu údajů pro účely prokázání souladu s požadavky nařízení.[967] Tento formát potvrzení správnosti zvolených postupů by mohl být zvláště přínosný pro mikropodniky, jelikož jasná pravidla vydání osvědčení by jim usnadnila překonat znalostní mezeru, kterou mohou trpět ve vztahu k řádnému výkladu požadavků dle Obecného nařízení. Současně může být doložení osvědčení požadavkem v rámci dodavatelských řetězců, čímž lze zajistit dosahování minimální úrovně bezpečnostních opatření a tím

962 Ibid., s. 37–41.

963 Srov. ISO/IEC JTC 1/SC 27; INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION; ISO. ISO/IEC 29147:2018. *ISO* [online]. říjen 2018 [cit. 18. 7. 2021]. Dostupné z: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/23/72311.html

964 Srov. ISO/IEC JTC 1/SC 27; INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION. ISO/IEC 30111:2019. *ISO* [online]. říjen 2019 [cit. 18. 7. 2021]. Dostupné z: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/97/69725.html

965 Srov. LEVERETT, Eireann, Richard CLAYTON a Ross ANDERSON. *JRC Technical Reports: Standardisation and certification of safety, security and privacy in the 'Internet of Things'* [online]. Brussels: European Commission, 2018, s. 49–50 [cit. 18. 7. 2020].

966 Ibid., s. 52.

967 Srov. čl. 42 Obecného nařízení.

snížit riziko porušení zabezpečení v důsledku využití mikropodniků jako nejslabšího článku.

Ve své podstatě je tento formát specifickou formou certifikace řádné ochrany osobních údajů srovnatelný spíše s bezpečnostní certifikací skrze certifikační autoritu než s autocertifikací či dodržováním standardů.[968] Certifikace souladu s požadavky ochrany osobních údajů je sice nově zakotvena v Obecném nařízení, nejedná se však o nový koncept. Poměrně dlouhou tradici má například osvědčení *EuroPriSe*.[969] Nelze však pokládat tuto praxi v rámci EU za příliš rozšířenou a s ohledem na nedávné přijetí nařízení 2019/881, aktu o kybernetické bezpečnosti, se do značné míry přesouvá pozornost a očekávání spíše k připravovaným unijním certifikačním schématům pro kybernetickou bezpečnost, o kterých bylo pojednáno v oddílu 6.1.3.[970] Rozšíření vydávání osvědčení v souladu s Obecným nařízením může nadále stát v cestě značná odlišnost pojetí těchto nástrojů od již široce etablovaných formátů certifikačních schémat (např. ISO certifikace). Články 42 a 43 Obecného nařízení užívají řadu neurčitých pojmů, které nemají srovnatelné prvky v těchto rámcích.[971] To představuje překážku pro vlastní vytváření těchto mechanismů případnými akreditačními autoritami, ale především plošnému přijetí a převzetí těchto nástrojů ze strany povinných subjektů, zvláště pak pokud se jedná o mezinárodně působící subjekty, a jsou-li k dispozici jiné, vhodnější alternativy, např. na základě nařízení 2019/881.

6.3 Podpora sdílení informací pro zvýšení kooperace a synergií mezi podniky

V rámci páté kapitoly byl při diskusi racionální motivace podniků pro zajišťování adekvátních opatření na ochranu před porušením zabezpečení osobních údajů nastíněn možný přínos sdílení informací o kyberbezpečnosti

968 Viz LEENES, Ronald. Article 42. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 733.

969 Srov. Product and Service Privacy Certification. *European Privacy Seal* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.european-privacy-seal.eu/EPS-en/Product-and-Service-Privacy-Certification

970 Srov. LEENES, Ronald. Article 42. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 735.

971 Ibid., s. 737.

mezi podniky. Potenciálně významnou roli těmto dobrovolným uskupením přiznává pro zvýšení přínosů a snížení nákladů zajištění bezpečnosti v rámci datově i fyzicky propojených sítí a systémů jednotlivých podniků též ENISA.[972] V rámci amerického prostředí se přitom jedná o zavedený koncept, který tam má poměrně dlouhou tradici.

6.3.1 Centra pro analýzu a sdílení informací

Pro tuto síť uskupení zaměřených na sdílení informací o bezpečnostních hrozbách je ve Spojených státech užíváno označení Centra pro analýzu a sdílení informací *(Information Sharing and Analysis Centre*, ISAC). Jsou to neziskové organizace koordinující nejen výměnu informací mezi podniky určitého odvětvového zaměření, ale i obousměrné sdílení informací s příslušnými složkami veřejné správy.[973] V roce 2003 zde byla nadto pro spolupráci mezi jednotlivými ISACy založena národní rada *(National Council of ISACs)*, která dnes sdružuje 25 sektorových organizací.[974]

Dosavadní zkušenosti ze Spojených států s fungováním těchto organizací poukazují na jejich přínos pro zajištění vysoké úrovně kyberbezpečnosti.[975] Přispívají k ní především utvářením prostředí, které buduje důvěru mezi zúčastněnými subjekty a umožňuje sdílení zkušeností, které má pozitivní přínos zvláště pro podniky nově vystavené výzvám kyberbezpečnosti[976] či malé a střední podniky, které se tak mohou čerpat z osvědčené odvětvové praxe. Vytvářejí současně vhodnou platformu pro sdílení informací mezi soukromým a veřejným sektorem, což lze označit za složku budování regulatorního prostředí s prvky chytré regulace. Sdílení informací o hrozbách a zranitelnostech na jedné straně a dostupných analýz a znalostí řešení na straně druhé umožňuje lepší sladění zájmů regulátora a regulovaných subjektů, což

972 Srov. ENISA. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security* [online]. Report/Study. Heraklion: ENISA, 2010, s. 5 [cit. 18. 7. 2021].

973 Viz ENISA. *Information Sharing and Analysis Center (ISACs). Cooperative models* [online]. Report/Study. Heraklion: ENISA, 2017, s. 7 [cit. 18. 7. 2021].

974 Srov. Member ISACs. *National Council of ISACs* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.nationalisacs.org/member-isacs

975 Viz ENISA. *Information Sharing and Analysis Center (ISACs). Cooperative models* [online]. Report/Study. Heraklion: ENISA, 2017, s. 7 [cit. 18. 7. 2021].

976 Např. výrobci spotřebních zařízení jako jsou lednice či hračky, která se skrze rozšíření o ICT moduly stávají zařízeními internetu věcí, jak bylo podrobně představeno v podkapitole 4.2.

je považováno za nezbytný předpoklad pro nasazení performativních pravidel.[977] Jak bylo dovozeno v oddílu 3.2.3, platí totéž i pro povinnost ohlášení porušení zabezpečení jakožto identifikovaný prvek chytré regulace. Uvedené mě vede k závěru o přínosnosti rozšíření uskupení pro sdílení informací týkajících se kyberbezpečnosti mezi podniky i v evropském kontextu.

6.3.2 Iniciativy směřující ke sdílení informací v rámci EU

Zde však prozatím nemají uskupení typu ISAC rozsáhlou tradici. Jsou přitom pro ně v rostoucí míře utvářeny příhodné podmínky, např. skrze směrnice 2016/1148[978] ve spojitosti s kategorií provozovatelů informačních systémů základních služeb.[979] Řada členských států (např. Nizozemsko[980]) již určitými organizacemi v tomto ohledu disponuje, ačkoliv častěji než s formátem organizace typu ISAC se lze zatím setkat s jinými, zpravidla volnějšími strukturami spolupráce veřejného a soukromého sektoru *(public-private partnership*, PPP).[981]

Spolupráce veřejného a soukromého sektoru: PPP je pojem pro dlouhodobé dohody o spolupráci mezi subjekty z veřejného a soukromého sektoru, který může nabývat širokého spektra podob a lze jej nalézt v řadě oblastí (např. výstavba a provoz dopravní či komunikační infrastruktury, vzdělávání, zdravotnictví či podpora výzkumu a vývoje). Konkrétní podoba spolupráce a role jednotlivých partnerů se přitom značně liší v závislosti na cíli a struktuře dané dohody. Může se jednat o institucionální PPP, která obstarává bezpečnost prvku kritické infrastruktury, jako je *Riigi Infosüsteemi Amet*[982] v Estonsku

977 Srov. POLČÁK, Radim. 1 Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 14.

978 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

979 Srov. ENISA. *Information Sharing and Analysis Center (ISACs). Cooperative models* [online]. Report/Study. Heraklion: ENISA, 2017, s. 7 [cit. 18. 7. 2021].

980 Srov. EUROPEAN CYBER SECURITY ORGANISATION. *Position Paper. European Sector-Specific ISACs* [online]. WG 3 Sectoral demand. Brussels: European Cyber Security Organisation, 2018, s. 12 [cit. 17. 7. 2021].

981 Viz ENISA. *Information Sharing and Analysis Center (ISACs). Cooperative models* [online]. Report/Study. Heraklion: ENISA, 2017, s. 8 [cit. 18. 7. 2021].

982 Srov. Home. *Riigi Infosüsteemi Amet* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.ria.ee/en

či *Rządowe Centrum Bezpieczeństwa*[983] v Polsku.[984] Případně může jít o spolupráci založenou za dosažením dílčího cíle jako v případě *AEI Ciberseguridad y Tecnologías Avanzadas*[985] ve Španělsku či *SECURITYMADEIN.LU*[986] v Lucembursku.[987] Další variantou je spolupráce ve formě outsourcingu služby veřejného sektoru na soukromoprávní subjekt, což je případ *Kuratorium Sicheres Österreich*[988] v Rakousku či *KRITIS*[989] v Německu.[990]

Formálnější organizační struktura na bázi ISAC je zpravidla utvářena na popud soukromého sektoru.[991] Hlavní motivací je sdílení informací o aktuálních hrozbách a vývoji na poli kyberbezpečnosti. Formát kooperativního sdružení je ekonomicky efektivní pro jeho členy, což činí účast v něm atraktivní pro podniky z daného odvětví. Sdílení zkušeností a dobré praxe významných podniků s jejich dodavateli či menšími obchodními partnery pak snižuje rizikovost prostředí a dodavatelských řetězců, což posiluje motivaci k této formě spolupráce na obou stranách. Koordinace komunikace v rámci odvětví vůči veřejnosti dále umožňuje lépe prezentovat informace o odhalených případech porušení zabezpečení. Tím může být snížena nejen újma dotčených subjektů údajů, ale i újma na dobré pověsti postižených podniků či příslušného odvětví jako celku.[992]

Sdílení informací mezi podniky na celounijní úrovni: Přes nastíněné příklady však není rozšíření sdílení informací souvisejících s porušením zabezpečení mezi podniky v EU dosud příliš rozvinuté, a to platí zvláště pro další

983 Srov. O RCB. *Rządowe Centrum Bezpieczeństwa* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://rcb.gov.pl/

984 Viz ENISA. *Public Private Partnerships (PPP). Cooperative models* [online]. Heraklion: ENISA, 2017, s. 21 [cit. 17. 7. 2021].

985 Srov. About AEI. *AEI Ciberseguridad y Tecnologías Avanzadas* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.aeiciberseguridad.es/index.php/About_AEI_1

986 Srov. About SECURITYMADEIN.LU. *SECURITYMADEIN.LU* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://securitymadein.lu//contact/about/

987 Srov. ENISA. *Public Private Partnerships (PPP). Cooperative models* [online]. Heraklion: ENISA, 2017, s. 24 [cit. 17. 7. 2021].

988 Srov. Startseite. *Kuratorium Sicheres Österreich* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://kuratorium-sicheres-oesterreich.at/

989 Srov. Startseite. *Schutz Kritischer Infrastrukturen* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html

990 Srov. ENISA. *Public Private Partnerships (PPP). Cooperative models* [online]. Heraklion: ENISA, 2017, s. 28 [cit. 17. 7. 2021].

991 Viz ENISA. *Information Sharing and Analysis Center (ISACs). Cooperative models* [online]. Report/Study. Heraklion: ENISA, 2017, s. 12 [cit. 18. 7. 2021].

992 Ibid., s. 13.

úroveň spolupráce a koordinace, tedy mezi případnými sektorovými či národními uskupeními. Situace v jednotlivých členských státech je značně rozdílná a rámce pro spolupráci na celounijní úrovni jsou vzácné. Ty, které existují, vznikly v zásadě za přičinění unijních institucí, jako je tomu u *European Energy ISAC*,[993] který vznikl na základě projektu *DENSEK* financovaného EU.[994] Roli ISACů v EU taktéž oslabuje absence koordinačního orgánu, jakým je výše zmíněná národní rada pro ISACy v americkém prostředí.

Zvýšení počtu podniků zapojených do ISACů a jejich rozšíření do více odvětví napříč členskými státy může ovlivnit výše nastíněné prosazení certifikace zařízení internetu věcí, kde např. certifikační schéma *Eurosmart IoT* předvídá účast podniku v uskupení na bázi ISAC.[995] Utváření těchto uskupení by dále mělo být iniciováno dozorovými úřady ve spolupráci s orgány koordinujícími otázky kybernetické bezpečnosti, ačkoliv zde je současně významný i rozvoj spolupráce a koordinace mezi dozorovými úřady samotnými, jak bylo nastíněno již ve třetí kapitole při diskusi významu cvičení pro řešení panevropských případů porušení zabezpečení osobních údajů.[996]

6.3.3 Překážky sdílení informací

Jako hlavní překážku pro utváření organizací typu ISAC identifikovala ENISA ve své studii nedostatek expertů na oblast kyberbezpečnosti, což činí podniky neochotné sdílet své vzácné personální kapacity s ostatními subjekty či veřejným sektorem.[997]

Z obecnějších překážek sdílení informací na poli kyberbezpečnosti, které již dříve identifikovala ENISA a které částečně vyplývají z ekonomických studií představených v podkapitole 5.3, stojí za zmínku především problém černého

993 Srov. Home. *European Energy Information Sharing & Analysis Centre* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.ee-isac.eu/

994 Srov. ENISA. *Information Sharing and Analysis Center (ISACs). Cooperative models* [online]. Report/Study. Heraklion: ENISA, 2017, s. 24 [cit. 18. 7. 2021].

995 Srov. *Technical Report [TR-e-IoT-SCS-Part-2] Generic Protection Profile Pilot v1.2 RELEASE* [online]. [e-IoT-SCS-Part-2] GPP v1.2. Brussels: Eurosmart, 2019, s. 33 [cit. 17. 7. 2021].

996 Viz MALATRAS, Apostolos et al. Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review* [online]. 2017, roč. 33, č. 4.

997 Srov. ENISA. *Information Sharing and Analysis Center (ISACs). Cooperative models* [online]. Report/Study. Heraklion: ENISA, 2017, s. 36 [cit. 18. 7. 2021].

pasažéra.[998] Ten se pojí na jedné straně s ekonomickou povahou sdílení informací v rámci dobrovolných podnikových uskupení jako externality. Tato aktivita tudíž nemá odpovídající přínos pro sdílející podnik, ale je ku prospěchu především pro příjemce stran ostatních účastníků sdružení.[999] Vliv má též konkurenční postavení mezi účastníky, které může ukotvovat zažité vnímání potřeby chránit své know-how i utajovat své zranitelnosti a být tak v rozporu s budováním důvěry a spolupráce na základě sdílení informací.[1000]

Výstupy z cvičení vedeného ENISA však naznačují, že riziko černého pasažéra je v tomto kontextu menší a méně významné pro účastníky aktivně sdílející informace, než vyplývá z ekonomických modelů racionálního rozhodování podniků.[1001] Přesto je na místě klást důraz na vyváženou vzájemnost při sdílení informací, ať již mezi podniky, či v přiměřené míře i mezi soukromým a veřejným sektorem. Taktéž by se měla prosazovat snaha o maximální anonymizaci sdílených údajů a dat, která omezí riziko zneužití a současně zajistí potřebný soulad s právními rámci jako je Obecné nařízení.

6.4 Posílení přenositelnosti vzniklé újmy zpět na odpovědné subjekty

Pozornost, kterou správci věnují prevenci a odhalení případů porušení zabezpečení, může dále ovlivnit vyšší pravděpodobnost, že ponesou plnou tíži následků, kterou v jejich důsledku pociťují jako újmu dotčené subjekty údajů.

6.4.1 Nárok na náhradu újmy dle Obecného nařízení

Rámec ochrany osobních údajů je spojen především s dozorovou činností příslušných úřadů a hrozbou uložení přiměřeně odrazujících sankcí v souladu s článkem 83 Obecného nařízení. Subjektům údajů je ovšem současně výslovně zakládáno právo na účinnou soudní ochranu vůči správci či zpracovateli na základě článku 79 Obecného nařízení, zvláště pak při uplatnění

998 Viz NAGHIZADEH, Parinaz a Mingyan LIU. Inter-Temporal Incentives in Security Information Sharing Agreements. In: *AAAI workshop on Artificial Intelligence for Cyber Security (AICS)* [online]. Phoenix: AAAI, 2016, s. 8 [cit. 12. 7. 2021].

999 Viz ENISA. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security* [online]. Report/Study. Heraklion: ENISA, 2010, s. 31 [cit. 18. 7. 2021].

1000 Ibid., s. 35.

1001 Ibid., s. 32.

nároku na náhradu újmy v souladu s článkem 82 Obecného nařízení. Nárok pokrývá hmotnou i nehmotnou újmu a na správce se vztahuje objektivní odpovědnost s možností jejího zproštění, pouze pokud prokáže, že nenese žádným způsobem odpovědnost za událost, která vedla ke vzniku újmy.[1002] Úprava nároku touto formou v unijním nařízení není běžná a měla by vést k posílení postavení subjektů údajů, jelikož se jedná o přímo použitelný nárok. *Zanfir-Fortuna* tudíž dovozuje, že subjekt údajů se na něj může spolehnout i při vnitrostátních soukromoprávních sporech.[1003] Jde přitom o odraz článku 47 Listiny základních práv a svobod EU, který musí být respektován při jeho výkladu a aplikaci.[1004] Oproti americké úpravě se nárok vztahuje i na újmu způsobenou jinak než v důsledku porušení zabezpečení, což lze vnímat jako vyjádření celostního významu práva na informační sebeurčení v evropském právním systému,[1005] tedy zde možnost kontroly nad svými osobními údaji.[1006] Jak však upozorňuje *Rychlý*, optimistická očekávání spojená s přímou použitelností tohoto nároku do značné míry narážejí na různorodost národních úprav členských států, které se dosud nevypořádaly s adekvátní adaptací příslušných procesních norem na hladké začlenění tohoto procesního nástroje.[1007] Tudíž lze pouze konstatovat, že jeho využitelnost v blízké budoucnosti nejspíše zůstane primárně předmětem teoretického diskurzu, spíše než praktické aplikace.

6.4.2 Právní rámce pro skupinové žaloby v EU

I při překonání současných překážek uplatnění výše popsaného nároku na náhradu újmy a práva na účinnou soudní ochranu je významnou překážkou jejich dosažení nejen nedostatečné povědomí subjektů údajů, ale i procesní

1002 Čl. 82 odst. 1 a 3.

1003 Viz ZANFIR-FORTUNA, Gabriela. Article 82. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1163.

1004 Ibid., s. 1164.

1005 K tomu blíže viz POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 303.

1006 Srov. ZANFIR-FORTUNA, Gabriela. Article 82. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1164.

1007 Srov. RYCHLÝ, Tomáš. Posudek oponenta disertační práce „Právní a ekonomické aspekty porušení bezpečnosti osobních údajů v kontextu internetu věcí". 2021

náročnost soudního řízení, ve kterém je případný nárok uplatňován.[1008] Na to bylo upozorňováno Agenturou Evropské unie pro základní práva[1009] ve zprávě z roku 2013 o přístupu k prostředkům nápravy újmy při ochraně osobních údajů v jednotlivých členských státech.[1010] Zde byl obsažen podnět k posilování veřejného povědomí o dostupných právních nástrojích a posílení kapacit a role dozorových úřadů a společenských organizací poskytujících osvětu a vzdělávání subjektům údajů. Bylo zde však také doporučeno zvážit při přípravě Obecného nařízení zakotvení úpravy dávající těmto organizacím oprávnění vznášet stížnosti či zastupovat subjekty údajů před soudy formou skupinového žaloby.[1011]

Skupinové zastoupení dle Obecného nařízení: Tato zpráva se následně odrazila ve znění článku 80 Obecného nařízení.[1012] Tím je upraveno právo subjektů údajů na (skupinové) zastoupení skrze neziskový subjekt, organizaci nebo sdružení, založené ve veřejném zájmu a činné v oblasti ochrany osobních údajů.[1013] K zastoupení jsou tudíž oprávněny především uskupení na ochranu spotřebitelů, případně lze uvažovat i např. o odborových organizacích.[1014] Oprávnění k zastoupení na základě článku 80 Obecného nařízení vychází z režimu *opt-in*, daná entita musí tudíž být prvně zmocněna příslušnými subjekty údajů, než je započne procesně zastupovat při ochraně jejich práv.[1015] Ustanovení článku 80 odst. 2 Obecného nařízení však dává členským státům prostor pro odchylnou úpravu, která entitu zmocní

1008 Srov. GONZÁLEZ FUSTER, Gloria. Article 80. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1144.

1009 Srov. Agentura Evropské unie pro základní práva (FRA). *Evropská unie* [online]. 8. 6. 2020 [cit. 18. 7. 2021]. Dostupné z: https://europa.eu/european-union/about-eu/agencies/fra_cs

1010 Srov. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Access to data protection remedies in EU Member States* [online]. Vienna: European Union Agency for Fundamental Rights, 2013 [cit. 18. 7. 2021].

1011 Ibid., s. 53.

1012 Viz GONZÁLEZ FUSTER, Gloria. Article 80. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1143.

1013 Srov. čl. 80 odst. 1 Obecného nařízení.

1014 Viz PATO, Alexia. The Collective Private Enforcement of Data Protection Rights in the EU. In: *Privatizing Dispute Resolution* [online]. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2019, s. 131–132.

1015 Ibid., s. 133.

i k vystupování bez potřeby předchozího projevu vůle dotčených subjektů údajů (tzn. režim *opt-out*).[1016] Příkladem je úprava zastoupení kvalifikovanými subjekty na ochranu spotřebitelů bez předchozího mandátu ve Francii rozšířená od roku 2016 též na ochranu osobních údajů.[1017]

Přestože lze mechanismus založený článkem 80 Obecného nařízení považovat za prvek usnadnění přenositelnosti vzniklé újmy, je na místě upozornit na kritiku, dle které dané ustanovení ponechává vlastní formát zastoupení v přílišné míře na členských státech, což je v kontrastu s osvědčeným unijním přístupem k otázkám ochrany spotřebitele.[1018] Problematické jsou zvláště situace přesahující jeden členský stát, kde není subjektům údajů k dispozici podpora, která by byla srovnatelná se Sítí evropských spotřebitelských center,[1019] která zajišťuje stabilní a harmonizovaný rámec pro ochranu spotřebitelů napříč vnitřním trhem.[1020]

6.4.3 Právní úprava zástupných žalob

Výše kritizovanou fragmentaci úpravy má do značné míry napravit harmonizace na základě směrnice o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů z konce roku 2020.[1021] Jak vyplývá z bodu odůvodnění 13, v rámci směrnice je na místě vnímat rozšířené pojetí relevantních oblastí ochrany spotřebitele, mezi které spadá i ochrana osobních údajů. Transpoziční lhůta pro zástupné žaloby do právních řádů členských států

1016 Viz GONZÁLEZ FUSTER, Gloria. Article 80. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1149.

1017 Srov. PATO, Alexia. The Collective Private Enforcement of Data Protection Rights in the EU. In: *Privatizing Dispute Resolution* [online]. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2019, s. 134.

1018 Viz GONZÁLEZ FUSTER, Gloria. Article 80. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1150.

1019 Srov. Síť evropských spotřebitelských center – síť ESC. *Evropská komise* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://ec.europa.eu/info/live-work-travel-eu/consumers/resolve-your-consumer-complaint/european-consumer-centres-network-ecc-net_en

1020 Viz GONZÁLEZ FUSTER, Gloria. Article 80. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1150.

1021 Směrnice Evropského parlamentu a Rady (EU) 2020/1828 ze dne 25. listopadu 2020 o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES.

je 25. prosince 2022 pro přijetí a zveřejnění příslušných změnových zákonů a 25. června 2023 pro jejich použití. I vzhledem k množícím se průtahům s transpozicí řady jiných unijních směrnic, ať již v důsledku pandemie COVID-19 či vzhledem k rostoucímu napětí ohledně budoucího politického i institucionální uspořádání Evropské unie ovlivněného řadou událostí posledních let je poměrně nejisté, k jakému datu lze skutečně očekávat použitelnost tohoto procesního nástroje i v českém kontextu.

Návrh národní úpravy hromadných žalob: Paralelně s unijním legislativním procesem směřujícím k přijetí směrnice o zástupných žalobách probíhala v českém prostředí zákonodárná aktivita ohledně procesní úpravy hromadných žalob,[1022] která byla následně jako sněmovní tisk 775 a doprovodný sněmovní tisk 776 rozeslána poslancům, ovšem její projednávání bylo přerušeno[1023] a není zřejmé, jaký bude její další legislativní osud, ať již s ohledem na politický vývoj na podzim 2021 či v důsledku výše zmíněné lhůty pro transpozici zástupných žalob do českého práva na základě přijaté směrnice. Za zmínku stojí, že původní návrh hromadných žalob nabýval charakteru výrazně bližšího americkému prostředí, než který přináší unijní směrnice.[1024] Snaha o umožnění komerčního charakteru hromadných žalob a o široké uplatnění principu *opt-out* se však setkala se silnou kritikou.[1025] Upravená verze návrhu pak již v mnohém odpovídala přijaté unijní směrnici. Nad její rámec však návrh stále ponechával určitý prostor i pro *opt-out* typ hromadné žaloby a bylo předpokládáno širší uplatnění tohoto procesního nástroje než pouze na spotřebitelské spory.

Zkušenosti se skupinovými žalobami z prostředí Spojených států: Z amerických zkušeností, které byly ve stručnosti nastíněny v oddílu 3.3.7, lze

1022 Srov. MINISTERSTVO SPRAVEDLNOSTI. *Návrh zákona o hromadném řízení* [online]. KORNBA9EXSST. Praha: Portál ODok, 2019 [cit. 18. 7. 2021].

1023 Srov. Schválený pořad a stav projednávání 49. schůze. *Poslanecká sněmovna Parlamentu ČR* [online]. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.psp.cz/sqw/ischuze.sqw?o=8&s=49

1024 Viz VÁLOVÁ, Irena. Hromadné žaloby: Ministerstvo navrhuje povinné zastoupení advokátem i investorské financování. *Česká justice* [online]. 10. 4. 2019 [cit. 18. 7. 2021]. Dostupné z: https://www.ceska-justice.cz/2019/04/hromadne-zaloby-ministerstvo-navrhuje-povinne-zastoupeni-advokatem-i-investorske-financovani/

1025 Srov. SAIDAMOVÁ, Suzan. Zákon o hromadných žalobách po prudké kritice opět přepracován. *epravo.cz* [online]. 7. 2. 2020 [cit. 18. 7. 2021]. Dostupné z: https://www.epravo.cz/top/clanky/zakon-o-hromadnych-zalobach-po-prudke-kritice-opet-prepracovan-110572.html

převzít, že nevhodně nastavené procesní požadavky značně omezují prostor pro uplatnění tohoto procesního nástroje v intencích motivace povinných subjektů významněji zohledňovat externality způsobené subjektům údajů v důsledku nedostatečných opatření na ochranu osobních údajů či opominutí povinností souvisejících s případem porušení bezpečnosti.

Současně však nelze vnímat americký přístup ke skupinovým žalobám na roveň s pojetím zástupných žalob v unijním prostředí, ať již na základě článku 80 Obecného nařízení či dle směrnice o zástupných žalobách. Vzhledem ke klíčové roli neziskových organizací založených za účelem ochrany práv fyzických osob „stojí a padá" motivační a kompenzační efekt zástupných žalob v evropském prostředí s adekvátností personálních a rozpočtových kapacit těchto subjektů pro množství případů, které se vyskytnou. Je pak nepominutelné, že rámec ochrany spotřebitele významně přesahuje problematiku ochrany osobních údajů, byť se část organizací specializuje primárně na ni.

Vezměme přitom v potaz předpokládaný nárůst uplatnitelných nároků v důsledku nárůstu porušení zabezpečení ve spojení s rozvojem internetu věcí, tak jak jej nastínil pro americké prostředí *Robinson*.[1026] Lze pak snadno dojít k závěru, že kapacity daných organizací budou jen stěží odpovídat potřebám na zástupné žaloby v tomto kontextu. To může být významně umocněno, zvláště pokud nedojde v blízké době a v dostatečné míře k prosazení certifikace či standardizace zařízení internetu věcí, o kterých bylo pojednáno v předchozích podkapitolách, a dále tak zesílí bezpečností rizika prostředí, která podrobně popsal *Schneier*[1027] a která byla přiblížena v rámci podkapitoly 4.3.

Také lze zvažovat, zda relativní složitost této agendy[1028] v porovnání s jinými problémy v rámci ochrany spotřebitele, nepovede příslušné zastupující entity k alokaci svých omezených zdrojů přednostně na ochranu spotřebitelů v jiných oblastech, kde je jistě také v rostoucí míře potřeba.

1026 Srov. ROBINSON, Dallin. Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Things with Class Action Litigation. *Richmond Journal of Law & Technology*, 2020, roč. 26, č. 1, s. 52 a násl.

1027 Srov. SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018.

1028 Především s ohledem na specifika právní oblasti ochrany osobních údajů a provázanost s technickými aspekty a nadto také specializovanou problematikou kyberbezpečnosti.

Ve výsledku tak dospívám k názoru, že byť hrozba zpětné přenositelnosti újmy má ekonomické opodstatnění jako motivační nástroj, její reálná dosažitelnost na základě zástupných žalob pouze na bázi neziskových organizací pravděpodobně nebude dosahovat potřebného efektu, resp. není ho v současné době dosahováno na základě úpravy dle článku 80 Obecného nařízení a harmonizační úprava zástupných žalob na ochranu kolektivních zájmů spotřebitelů zřejmě situaci příliš nezmění.

6.5 Účelné propojení s hlášením kybernetických bezpečnostních incidentů

Předchozí podkapitola vyznívá pesimisticky ohledně zlepšení vynucování dodržování povinností dle Obecného nařízení skrze soukromoprávní nároky na náhradu vzniklé újmy, byť je k jejich usnadnění k dispozici procesní nástroj zástupných žalob. Vynucování těchto povinností cestou kontrolní a rozhodovací činnosti dozorových úřadů bohužel nevnímám v řadě členských států v současné době o mnoho příznivěji.

To platí zvláště ve spojitosti s řešením případů porušení zabezpečení, resp. ve směru zajišťování chytré regulace dozorovými úřady na základě těchto ohlášení. Jsem toho názoru, že dozorové úřady v této roli čelí srovnatelným výzvám, jako organizace na ochranu spotřebitelů při zástupných žalobách dle Obecného nařízení, tedy omezené specializované odborné kapacitě a současné relativní neatraktivnosti této agendy ve srovnání s jinými v rámci činností dozorového úřadu.

Nedostatek odborných kapacit dozorových úřadů: O zhodnocení, že v rámci státní, resp. veřejné správy panuje dlouhodobě značný nedostatek specialistů na agendy ICT, není mnoho pochyb.[1029] Lze předpokládat, že tento nedostatek je zvláště citelný u odborníků se zaměřením na kyberbezpečnost, jelikož jde o oblast, kde je významný nedostatek specialistů celosvětovým problémem, jak ve veřejném, tak v soukromém sektoru.[1030] Jak bylo nastíněno v podkapitole 2.1, nejvýznamnější podobou případu porušení

[1029] Příkladem viz ODBOR HLAVNÍHO ARCHITEKTA EGOVERNMENTU. *Digitální Česko. Informační koncepce České republiky. Navazující dokument č. 1: Metody řízení ICT veřejné správy ČR* [online]. verze 1.0. Praha: Ministerstvo vnitra, 2019, s. 88 [cit. 18. 7. 2021].

[1030] Srov. (ISC)2. *Strategies for Building and Growing Strong Cybersecurity Teams* [online]. Clearwater: (ISC)2, 2019, s. 8 [cit. 18. 7. 2021].

zabezpečení osobních údajů je bezpečnostní incident, což bude nadále umocňováno s rozšiřováním internetu věcí. Tím se agenda ochrany osobních údajů přibližuje problematice kyberbezpečnosti, resp. kybernetické bezpečnosti, a dále narůstají požadavky na odborné kapacity dozorového úřadu s touto specializací.

Možná spolupráce v rámci české veřejné správy: Jelikož i pro Úřad platí, že budování vlastních kapacit tohoto druhu je velmi obtížné, pokládám za příhodné diskutovat možnost kompenzace jejich absence skrze spolupráci s jinými složkami veřejné správy. Konkrétně považuji za vhodnou možnost systematickou spolupráci s vládním CERTem[1031] spadajícím pod Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) a národním CERTem, který je zaštiťován organizací CZ.NIC. Jde totiž o institucionální příjemce hlášení kybernetických bezpečnostních incidentů dle ZoKB.

6.5.1 Hlášení kybernetických bezpečnostních incidentů

S ohledem na rostoucí význam prvků informační infrastruktury pro fungování důležitých veřejných i soukromých služeb ve společnosti je dnes zajištění kybernetické bezpečnosti státu jednou z klíčových výzev.[1032] Příslušný právní rámec směřuje předně k zakotvení pravidel pro zajištění vysoké úrovně důvěrnosti, integrity a dostupnosti (tzv. CIA triáda) nosné informační infrastruktury a jí přenášených dat.[1033] Povinnosti na základě ZoKB ovšem dopadají pouze na poměrně úzce vymezené skupiny (zpravidla velkých) subjektů provozujících či spravujících významné prvky informační infrastruktury,

1031 Jedná se o skupinu pro reakci na počítačové hrozby (*computer emergency response team,* CERT), tedy tým odborníků na informační bezpečnost, jejichž úkolem je řešit bezpečnostní incidenty. Viz JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti* [online]. Brno: Národní centrum kybernetické bezpečnosti, 2015, s. 91 [cit. 10. 1. 2021]; Srovnatelným označením je skupina pro reakce na počítačové bezpečnostní incidenty (*computer security incident response team*, CSIRT). Ke vztahu obou pojmů viz POLČÁK, Radim. 12 Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 614–615.

1032 Srov. důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Dz, s. 2.

1033 Viz POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. *Právní problémy kybernetické bezpečnosti* [online]. Brno: Masarykova univerzita, Právnická fakulta, 2016, s. 156 [cit. 2. 1. 2021].

přičemž i mezi těmito skupinami zákon činí rozdíly a nepodřizuje všechny stejnému rozsahu povinností.[1034]

Pojem kybernetického bezpečnostního incidentu: Paralelu k pojmu porušení zabezpečení v kontextu ochrany osobních údajů zde představuje pojem kybernetický bezpečnostní incident, který je zákonem vymezen jako *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události“,*[1035] tedy události, *„která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“*[1036] Za cyklickou obecností představené definice se skrývá především mnohotvárnost situací, které je nutno tímto pojmem postihnout, jak bylo nastíněno v druhé kapitole.

V rámci právní úpravy kybernetické bezpečnosti je povinnost bezodkladně hlásit kybernetické bezpečnostní incidenty příslušnému bezpečnostnímu týmu vnímána za jeden ze základních kamenů.[1037] Tímto mechanismem jsou příslušným složkám veřejné moci v aktuálním čase poskytovány potřebné informace o bezpečnostní situaci na nejvýznamnější informační infrastruktuře.[1038] Vedle vlastního řešení konkrétní situace jsou tyto informace potřebné pro sledování dlouhodobějších trendů,[1039] resp. včasnou přípravu na nově vystupující hrozby. Způsob komunikace a obsah hlášení upravuje vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti (VoKB).

Obsah hlášení: Za podstatné náležitosti platí vedle identifikace odesílatele a uvedení okamžiku zjištění incidentu především označení postiženého prvku informační infrastruktury a vlastní popis incidentu.[1040] V rámci popisu incidentu je pak příslušný bezpečnostní tým vhodné informovat též o dosud provedených opatřeních, především co do nápravy vzniklých

1034 Srov. důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Dz, s. 64.
1035 Srov. § 7 odst. 2 ZoKB.
1036 Srov. § 7 odst. 1 ZoKB.
1037 Srov. POLČÁK, Radim. 12 Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 593.
1038 Srov. POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 92.
1039 Viz KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 492.
1040 Viz § 4 VoKB.

následků zranitelnosti a prevence jejich rozšíření, a o případné kontrole účinnosti zavedených opatření.[1041] Odpovídající informovanost bezpečnostních týmů a dozorového orgánu je předpokladem vhodného nasazení reaktivních a ochranných opatření[1042] účinně reagujících na vzniklé ohrožení regulované informační infrastruktury.[1043] V tomto lze vnímat příklad chytré regulace, realizované skrze normativní tlak na bezodkladnou transparentnost vůči příslušné složce veřejné moci pro umožnění její adekvátní reakce.[1044]

Okruh povinných subjektů: Jelikož zmíněná právní úprava směřuje především na zachování funkcionality významnější informační infrastruktury, je okruh subjektů povinných k hlášení kybernetických bezpečnostních incidentů dle § 8 ZoKB relativně úzký. Lze přitom vysledovat dvě verze této povinnosti. Striktnímu režimu hlášení všech kybernetických bezpečnostních incidentů podléhají správci (případně provozovatelé[1045]) informačních a komunikačních systémů kritické informační infrastruktury,[1046] významných informačních systémů,[1047] informačních systémů základní služby[1048] a orgány nebo osoby zajišťující významnou síť.[1049] Provozovatelé základních služeb nadto ohlásí, pokud daný incident má závažný dopad na kontinuitu poskytování dané služby, ať již jde o incident v jejich informačním systému či u poskytovatele digitální služby, na níž je základní služba závislá, neboť zpravidla pouze oni jsou schopni posoudit reálné dopady daného incidentu.[1050]

Mírnější režim se pak vztahuje na poskytovatele digitálních služeb (tedy poskytovatele on-line tržiště, internetového vyhledávače či *cloud computingu*),[1051] kteří mají povinnost hlásit pouze kybernetické bezpečnostní incidenty,

1041 Viz KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 493.
1042 Srov. § 13–15a ZoKB.
1043 Srov. důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Dz, s. 53.
1044 Viz POLČÁK, Radim. 12 Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 593.
1045 Srov. § 8 odst. 5 ZoKB.
1046 Srov. § 8 odst. 1 v kombinaci s § 3 písm. c) a d) ZoKB.
1047 Srov. § 8 odst. 1 v kombinaci s § 3 písm. e) ZoKB.
1048 Srov. § 8 odst. 1 v kombinaci s § 3 písm. f) ZoKB.
1049 Srov. § 8 odst. 1 v kombinaci s § 3 písm. b) ZoKB.
1050 Viz § 8 odst. 1 a 8 ZoKB a také důvodovou zprávu k zákonu č. 205/2017 Sb., kterým se mění zákon o kybernetické bezpečnosti ve znění zákona č. 104/2017 Sb., a některé další zákony, 205/2017 Dz, s. 33–34.
1051 Pojem digitální služby je přitom pro účely zákona omezen na vybrané kategorie. Srov. § 2 písm. l) ZoKB.

které mají významný dopad na poskytování digitální služby, a o nichž mají k dispozici informace, které jim umožní posoudit závažnost dopadu incidentu.[1052] V tomto směru lze shledávat aplikaci performativního pravidla, jelikož je ponecháno na poskytovateli dané digitální služby, aby v rámci interního systému kvalifikace bezpečnostních hrozeb posoudil, zda je na místě ohlášení konkrétního incidentu.[1053] Je zde současně možné vnímat paralelu s určením vzniku povinnosti ohlašovat případ porušení zabezpečení osobních údajů dle článku 33 Obecného nařízení, jak bylo rozebráno v oddílu 3.2.2. Na poskytovatele služby elektronických komunikací a subjekty zajišťující síť elektronických komunikací se ohlašovací povinnost dle § 8 ZoKB nevztahuje.

Poskytovatelé digitálních služeb a orgány nebo osoby zajišťující významnou síť provádějí hlášení národnímu CERTu, kterým je CSIRT.CZ[1054] zajišťovaný sdružením CZ.NIC.[1055] Ostatní povinné subjekty hlásí incidenty vládnímu bezpečnostnímu týmu CERT (GovCERT.CZ[1056]), jehož činnost je zajišťována Národním centrem kybernetické bezpečnosti (NCKB), které je výkonnou sekcí NÚKIB.[1057]

Množství hlášených incidentů: Dle statistik incidentů bylo roce 2020 bezpečnostnímu týmu CSIRT.CZ, tedy ze strany poskytovatelů digitálních služeb a orgánů nebo osob zajišťujících významnou síť, ohlášeno celkem 1267 kybernetických bezpečnostních incidentů, tedy nejvíce za dobu vedení statistiky.[1058] Potvrdilo se tedy, že pokles ohlášených incidentů v roce 2019 pod tisíc byl výjimkou, nikoliv změnou trendu z předchozích let.[1059] Zde

1052 Srov. § 8 odst. 2 ZoKB a také důvodová zpráva k zákonu č. 205/2017 Sb., kterým se mění zákon o kybernetické bezpečnosti ve znění zákona č. 104/2017 Sb., a některé další zákony, 205/2017 Dz, s. 33.

1053 Srov. § 29 odst. 1 VoKB. Vyhláška sice skrze § 31 nabízí kategorizaci kybernetických bezpečnostních incidentů a použitelná kritéria, jde však stále o do značné míry obecná vodítka, která vyžadují specifikaci pro posouzení jednotlivých situací.

1054 Blíže viz CSIRT.CZ. O nás. *CZ.NIC* [online]. 2019 [cit. 26. 2. 2021]. Dostupné z: https://csirt.cz/cs/o-nas/

1055 Srov. § 8 odst. 3 ZoKB.

1056 Blíže viz NÚKIB. GovCERT.CZ. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 26. 2. 2021]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/

1057 Srov. § 8 odst. 4 ZoKB. Dále také NÚKIB. Co je NCKB. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 26. 2. 2021]. Dostupné z: https://www.govcert.cz/cs/

1058 Viz CSIRT.CZ. CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ (národní CSIRT ČR) za rok 2020* [online]. Praha: CSIRT.CZ, 2021, s. 4 [cit. 20. 10. 2021].

1059 Ibid.

je však na místě dodat, že incidenty reportované CSIRT.CZ ze strany příslušných subjektů jsou charakterizovány buďto jako:

1. přetrvávající problémy, které subjekt nebyl vlastním úsilím schopen vyřešit,
2. problémy, u kterých není jednoduché identifikovat původce či subjekt příslušný k jejich řešení nebo
3. incidenty se závažným dopadem na informační infrastrukturu v ČR.[1060]

Jde tedy zpravidla o komplexnější případy s rozsáhlejšími důsledky. Bezpečnostnímu týmu GovCERT.CZ bylo v roce 2020 podáno 468 hlášení incidentů, což odpovídá stabilnímu růstovému trendu.[1061] K významnému nárůstu došlo u incidentů ve zdravotnictví, které byly též předmětem značné pozornosti medií. Nejvýznamnějším bylo zašifrování systémů Fakultní nemocnice Brno v březnu 2020.[1062]

Trendy kybernetické bezpečnosti: Trvalým trendem je narůstající sofistikovanost a četnost kybernetických bezpečnostních incidentů, zvláště v podobě *spear-phishingu*[1063] s cílem získání přístupu do významných sítí a systémů či k důvěrným databázím.[1064] Roste tím také okruh prvků informační infrastruktury relevantních z hlediska kybernetické bezpečnosti, zvláště pokud jde o rizika spojená s útoky skrze slabá místa v dodavatelském řetězci na hodnotnější či kritičtější cíle.[1065] I proto je zjevná snaha bezpečnostních týmů efektivně pracovat s maximálním okruhem dostupných a relevantních informacích o aktuálním stavu napříč informační infrastrukturou.[1066] K tomuto v posledních letech směrují aktivity CSIRT.CZ na výzkumném projektu Predikce a ochrana před kybernetickými incidenty (PROKI), který

1060 Ibid.

1061 Srov. NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. Brno: NÚKIB, 2021, s. 13 [cit. 20. 10. 2021].

1062 Ibid., s. 14.

1063 Jedná se o sofistikovanější útok typu *phishing*, který využívá předem získané informace o oběti. Těmi přitom jsou osobní údaje, zpravidla získané v důsledku porušení zabezpečení. Srov. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti* [online]. Brno: Národní centrum kybernetické bezpečnosti, 2015, s. 95 [cit. 10. 1. 2021].

1064 Srov. NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. Brno: NÚKIB, 2021, s. 17 a 21 [cit. 20. 10. 2021].

1065 Ibid., s. 18.

1066 Srov. KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 497.

shromažďuje informace o incidentech z řady dodatečných zdrojů a dává je k dispozici dotčeným subjektům.[1067] Ke zvýšení informační báze ostatně směřuje i nové výslovné ustanovení § 8 odst. 6 ZoKB o dobrovolném hlášení incidentů subjekty, na které nedopadá vlastní ohlašovací povinnost, kterým je transponováno ustanovení směrnice 2016/1148, o které byla zmínka již v rámci podkapitoly 6.1.[1068] V roce 2020 představovala hlášení těchto subjektů třetinu všech hlášení GovCERT.CZ, což představuje desetinásobný nárůst oproti roku 2019.[1069] Nalézání nových zdrojů relevantních informací o incidentech je tedy pro bezpečnostní týmy přetrvávající a stále aktuální výzvou. Za zvláště hodnotné lze pak, dle mého názoru, považovat ty, které jsou již dnes dostupné v rámci veřejné správy, zvláště pokud je nesnadné je shromáždit jinou cestou. Tak je tomu v případě ohlášených případů porušení zabezpečení osobních údajů.

6.5.2 Rostoucí obsahový překryv v prostředí internetu věcí

Problematika ochrany osobních údajů a kybernetické bezpečnosti je zvláště v kontextu povinností a opatření směřujícím k zabránění porušení zabezpečení blízká. Srovnatelná je např. kvalifikace, že porušení zabezpečení se může dotýkat rovin důvěrnosti, dostupnosti či integrity osobních údajů.[1070] Srovnatelné je taktéž užití regulatorních mechanismů performativních pravidel. Ať již v kontextu technických a organizačních opatření, které mají být provedena pro minimalizaci rizika vzniku porušení zabezpečení zpracovávaných osobních údajů,[1071] tak ve vlastní kvalifikaci naplnění podmínek vzniku povinnosti notifikovat dozorový úřad o určitém porušení zabezpečení.[1072] Na druhou stranu je na místě zohlednit, že případy porušení

1067 Viz CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ (národní CSIRT ČR) za rok 2018* [online]. Praha: CSIRT.CZ, 2019, s. 6 [cit. 26. 2. 2021].

1068 Čl. 20 směrnice 2016/1148, blíže také bod odůvodnění 67 této směrnice.

1069 Srov. NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. Brno: NÚKIB, 2021, s. 13 [cit. 20. 10. 2021].

1070 Srov. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29, 2018, s. 8 [cit. 28. 2. 2021].

1071 Srov. čl. 32 Obecného nařízení.

1072 Srov. čl. 33 odst. 1 Obecného nařízení.

zabezpečení se neomezují pouze na elektronicky uchovávané osobní údaje, ale i např. na ztrátu tištěných dokumentů.

Jelikož jsou k ohlašování případů porušení zabezpečení vůči dozorovému úřadu povinováni všichni správci,[1073] má tato úprava dle článku 33 Obecného nařízení potenciál být podkladem pro širší sběr informací. To se týká především stavu kybernetické bezpečnosti napříč prvky informační infrastruktury, které nepostihuje výše představená povinnost hlášení kybernetických bezpečnostních incidentů.

Případnou informační hodnotu však zamlžuje nízko nastavený práh pro založení povinnosti, který se váže k pouhé pravděpodobnosti rizika pro práva a svobody dotčených fyzických osob.[1074] Toto je ze své podstaty velmi hrubé síto, které vede povinné subjekty k ohlašování většiny incidentů,[1075] což v důsledku zvyšuje požadavky na dozorový úřad ve schopnosti řádně a včas zanalyzovat získané podklady a stanovit jejich informační hodnotu. Příval hlášení na základě této povinnosti vedl dozorové úřady v některých členských státech ke zdůrazňování, že ne všechny incidenty jim musejí být touto cestou hlášeny.[1076]

Ohlašovací povinnosti jsou do značné míry reakcí na rozšiřování informačních a komunikačních technologií a jejich rostoucí význam v procesech na všech úrovních.[1077] Tato proměna prostředí přitom neustává. Regulatorní rámec obecně, a zvláště v kontextu dynamického prostředí technologií, čelí

1073 Jak bylo opakovaně uvedeno výše, správcem je dle čl. 4 bodu 7 Obecného nařízení fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Okruh povinných subjektů je tedy velmi výrazně širší než u hlášení kybernetických bezpečnostních incidentů.

1074 Srov. čl. 33 odst. 1 Obecného nařízení.

1075 Viz BYGRAVE, Lee A. a Luca TOSONI. Article 4(1). In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 646.

1076 Ibid., s. 645.

1077 Příkladem vlivu technologického vývoje na úpravy hlášení kybernetického bezpečnostního incidentu je rozšíření okruhu povinných subjektů v souladu s transpozicí směrnice 2016/1148 na provozovatele základních služeb a vybrané poskytovatele digitálních služeb. Podobný signál přitom přišel i se zavedením obecné ohlašovací povinnosti dle Obecného nařízení nad rámec přechozí úpravy omezující se na poskytovatele veřejně dostupných služeb elektronických komunikací.

problému opožděné reakce na aktuální vývoj a trendy.[1078] Rozmach nových technologií jako je internet věcí přitom významně posouvá výzvy spojené s kybernetickou bezpečností a ochranou zpracovávaných osobních údajů, jak jsem se snažil poukázat v této monografii, především ve čtvrté kapitole.[1079]

Současný a budoucí překryv ohlašovacích povinností: Překryv vzniku představených ohlašovacích povinností u jednotlivých povinných subjektů není v současné době natolik problematickým jevem, vzhledem k relativně úzkému okruhu povinných subjektů dle ZoKB.[1080] S internetem věcí však významně narůstá množství subjektů, jejichž ohrožení se stává relevantním z hlediska kybernetické bezpečnosti. Objevují se nové vektory útoků, přitom do intenzity aktivit útočníků i požadavků na přiměřenou ochranu bude vstupovat rozvoj umělé inteligence a rozšíření sítí 5G.[1081] S ohledem na obecně nevalné bezpečnostní charakteristiky zařízení internetu věcí[1082] vzroste pravděpodobnost hrozeb, které mají nepřímý vliv na významné prvky informační infrastruktury. Může se jednat o rizika vyvstávající v rámci napadení článků dodavatelského řetězce, dílčích obchodních partnerů či nadstavbových služeb. Pro bezpečnostní týmy tedy bude stále významnější mít co nejucelenější přehled o dění na poli bezpečnostních incidentů napříč spektrem propojených subjektů.

Zároveň však roste složitost a „skrytost" incidentů, což zvyšuje potřebu specializovaného personálu nejen pro jejich odhalení a ohlášení, ale též pro podpůrnou činnost ze strany dozorového úřadu vůči správcům a související účelnou analýzu a vyhodnocení hlášených informací. V tomto ohledu pak pod Úřad spadá rozsáhlá agenda s množstvím povinných subjektů, kterou

1078 Srov. MARCHANT, Gary E., Braden R. ALLENBY a Joseph R. HERKERT (eds.). *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*. Dordrecht: Springer, 2011, The International Library of Ethics, Law and Technology, 7.

1079 Ty jsou dále umocněny vývojem od počátku roku 2020 v důsledku celosvětové pandemie a bezprecedentními karanténními opatřeními, která činí z informačních a komunikačních technologií (dočasně) zcela nepostradatelný nástroj pro alespoň omezenou realizaci řady jinak dosud nedigitalizovaných činností.

1080 Všechny povinné subjekty dle ZoKB jsou však zpravidla současně správci či zpracovateli dle Obecného nařízení. S výjimkou incidentů, které se nijak netýkají osobních údajů na ně tudíž dopadají obě ohlašovací povinnosti paralelně.

1081 Viz NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018* [online]. Brno: NÚKIB, 2019, s. 53 [cit. 26. 2. 2021].

1082 Srov. SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 19 a násl.

při řádném plnění ohlašovacích povinností povinnými subjekty[1083] není, dle mého názoru, Úřad s to pokrýt.[1084]

Kompatibilita těchto ohlašovacích povinností: Hlášení kybernetického bezpečnostního incidentu a ohlašování porušení zabezpečení osobních údajů jsou koncepčně obdobné povinnosti, které se vztahují na blízké či stejné události dotýkající se prvků informační infrastruktury a přenášených či uchovávaných dat. Přes jisté odlišnosti v perspektivě těchto úprav jsou hlavní cíle vzájemně provázané.

Právní rámec ochrany osobních údajů směřuje proti zásahům do distributivních práv fyzických osob, hrozícím při náhodném či neoprávněném zpřístupnění zpracovávaných osobních údajů, tedy dat uchovávajících citlivé informace o jednotlivci.[1085] Česká úprava kybernetické bezpečnosti přitom také stojí na ochraně distributivních práv jednotlivců skrze opatření pro udržování a zvyšování informační a síťové bezpečnosti.[1086] Ochranu dat v podobě ochrany osobních údajů přitom nelze oddělovat od ochrany prvků informační infrastruktury a naopak, jelikož z hlediska prostředí jde o technologicky provázané složky.[1087]

Obě ohlašovací povinnosti tedy směřují k podobnému účelu, nejvýznamnější odlišností (mimo institucionálního recipienta a okruh povinných subjektů) je pak do jisté míry vlastní obsah hlášení. Zatímco vůči bezpečnostním týmům je jádrem popis hrozby a zavedených opatření, vůči Úřadu tyto informace správci doplňují také o posouzení ohrožení osobních údajů co do rozsahu

1083 Dle dostupných statistik bylo v roce 2020 Úřadu nahlášeno 311 případů. S ohledem na údaje z velikostně srovnatelných členských států (např. 9132 ohlášených případů v Dánsku, 4908 ve Švédsku, 4001 ve Finsku, 1683 na Slovinsku, či 869 v Rakousku) lze vycházet z předpokladu, že značná část porušení zabezpečení v České republice není Úřadu hlášena. Srov. DLA PIPER'S CYBERSECURITY AND DATA PROTECTION TEAM. *DLA Piper GDPR data breach survey: January 2021* [online]. Londýn: DLA Piper, 2021, s. 11 [cit. 20. 10. 2021].

1084 Úřad má celkově cca 100 zaměstnanců, z nichž však pouze několik bude mít odbornou kapacitu potřebnou pro řešení agendy ohlašovaných porušení zabezpečení, vzhledem k obecnému nedostatku specialistů na kyberbezpečnost nastíněnou výše. Viz Návrh závěrečného účtu kapitoly 343 – Úřad pro ochranu osobních údajů za rok 2018. Průvodní zpráva. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2019, s. 10 [cit. 26. 2. 2021].

1085 Srov. čl. 1 odst. 2 Obecného nařízení.

1086 Viz POLČÁK, Radim. 12 Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 589.

1087 Srov. KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 99–100.

a závažnosti. Lze tedy říci, že hlášení dle Obecného nařízení jsou informativní pro bezpečnostní týmy, ovšem hlášení dle ZoKB nepostačují Úřadu, jelikož absentují akcent na perspektivu osobních údajů.

6.5.3 Přínosy systematické institucionální spolupráce

Domnívám se, že navázání systematické spolupráce mezi Úřadem a bezpečnostními týmy ohledně sdílení informací o ohlášených porušení zabezpečení a odborné podpory při jejich analýze a řešení je funkčním řešením nastíněných výzev, které přináší v tomto ohledu pro činnost Úřadu rozšíření internetu věcí.

Systematická spolupráce ve výsledku přispěje k lepší činnosti obou složek veřejné správy, přičemž přinese výhody regulovaným i chráněným subjektům. Je sice na místě respektovat, že jak Úřad, tak NÚKIB, jsou nezávislé úřady,[1088] v tom však nevnímám významnou překážkou pro založení této provázanosti.

Pro bezpečnostní týmy tato spolupráce přinese přehled o situaci u širokého spektra subjektů, které jinak informace o stavu svého zabezpečení příliš nesdílí.[1089] Jelikož pak tyto bezpečnostní týmy disponují v rámci veřejné správy nejrozsáhlejším odborným aparátem s touto specializací,[1090] mohou jistě poskytnout nazpět přiměřenou podporu Úřadu při řešení této agendy a komunikaci s postiženými správci.

1088 Resp. že národní CERT je spravován soukromoprávním subjektem na základě veřejnoprávní smlouvy dle § 19 ZoKB. To jej však dle mého názoru ve výsledku činí flexibilnějším, jelikož není limitován zásadou enumerativnosti veřejnoprávních pretenzí, a spolupráce s ním tak může být navázána bez specifického zákonného zmocnění, za dodržení podmínek této veřejnoprávní smlouvy.

1089 A nelze tudíž předpokládat, že k nim bezpečnostní tým získá přístup např. činností jako je výše zmíněný výzkumný projekt PROKI. Tyto informace mohou vést k odhalení významných trendů či hrozeb, které jsou sice jednotlivě pominutelné, ale z agregovaného hlediska nabývají na významu. Zranitelnosti v podružných, nadstavbových či navazujících prvcích informační infrastruktury pak mohou naznačovat jinak skryté riziko pro významné prvky, které může být sníženo včasným opatřením.

1090 Dle dostupných informací zaměstnává jen NÚKIB v současné době okolo 200 zaměstnanců, z velké části specializovaných na problematiku kybernetické bezpečnosti. Lze přitom do budoucna předpokládat další rozšiřování, ač připravované navýšení stavů v loňském roce nebylo realizováno. Viz MAGDOŇOVÁ, Jana. Kyberúřadu chybí IT specialisté a technici. Plánoval jich přijmout 48, ale povolení dostal jen na osm. *iROZHLAS* [online]. 2019 [cit. 2. 4. 2020]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/skrty-mista-urednici-schillerova-narodni-kyberneticky-urad_1907030657_kno

Tuto spolupráci mezi složkami veřejné správy by měly přivítat i ohlašující subjekty. Dostane se jim tím kvalitnější odborná podpora a současně poskytnuté informace přispějí ke zvýšení kybernetické bezpečnosti napříč prostředím, tedy i u jejich obchodních partnerů či poskytovatelů služeb. Shledávám tak tento přístup v souladu se závazky veřejné správy k optimalizaci poskytování digitálních služeb a minimalizaci neúčelné administrativní zátěže fyzických a právnických osob požadavky, které je možné vyřešit uvnitř veřejné správy.[1091] Užší spolupráce s bezpečnostními týmy pak s ohledem na jejich celostní pohled na situaci a řadu dalších zdrojů informací může přispět ke kapacitě Úřadu odhalit neohlášená porušení zabezpečení. Přitom již obecné vnímání navýšení možností Úřadu v tomto směru dle mého názoru přispěje k vyšší motivaci povinných subjektů řádně odhalovat a ohlašovat porušení zabezpečení. Větší množství hlášení pak dále posílí přínos této systematické spolupráce.

Taktéž z hlediska dotčených subjektů údajů jde, dle mého názoru, o přínosné nastavení datových toků v rámci veřejné správy. Na všech stranách lze předpokládat vysokou úroveň implementovaných organizačních a technických opatření na ochranu zpracovávaných osobních údajů. Předávána by přitom byla převážně technická data a agregované informace (popis povahy daného případu porušení zabezpečení, jeho pravděpodobné důsledky, učiněná či plánovaná opatření[1092]), která zpravidla ani nemají povahu osobních údajů. Přitom tato spolupráce pro ně znamená posílení kybernetické bezpečnosti obecně a z toho plynoucí pozitivní vliv na snížení hrozeb pro jejich údaje. To může být dále umocněno, pokud by došlo k výše naznačenému posílení motivace povinných subjektů k ohlašování porušení zabezpečení.

Systematickou spolupráci mezi Úřadem a bezpečnostními týmy tudíž pokládám za všeobecně prospěšnou úpravu sdílení informací a odborných kapacit v rámci veřejné správy. Vlastní podoba této spolupráce závisí

1091 Srov. POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 92–93; Jedním z nedávných zdůraznění aktuality těchto závazků je přijetí zákona č. 12/2020 Sb., o právu na digitální služby. K tomu blíže viz MATES, Pavel. Právo na digitální služby. *Revue pro právo a technologie* [online]. 2020, roč. 11, č. 21, s. 73 a násl.

1092 Srov. obsah hlášení dle čl. 33 odst. 3 Obecného nařízení. Informace týkající se rozsahu či druhu dotčených osobních údajů nevnímám z hlediska bezpečnostních týmů za podstatné a neočekávám tudíž jejich systematické předávání.

na nejvhodnějším technickém provázání příslušných informačních systémů, shledávám za smysluplnou určitou neutrální platformu pro sdílení informací, která případně do budoucna může být sdílena i s dalšími složkami veřejné správy (např. orgány činnými v trestním řízení).

6.6 Usnadnění odhalení neohlášených případů porušení zabezpečení

Spolupráce se specializovanými bezpečnostními týmy však nepokládám za jedinou cestu, jak usnadnit odhalování případů porušení zabezpečení. V rámci této podkapitoly nastíním nástroje pro využívání externích odborníků pro odhalování zranitelností a porušení zabezpečení, které jsou již nyní široce využívány v souvislosti s vývojem a distribucí softwarových produktů.

Tyto poznatky následně propojím se závěry páté kapitoly, kde bylo dovozeno, že pro řádnou motivaci povinných subjektů k ohlašování porušení zabezpečení nepostačuje pouze hrozba vysoké sankce, ale je nutná i přiměřená pravděpodobnost odhalení tohoto neohlášení. Hlavním nástrojem dozorového úřadu pro odhalování pochybení správců a zpracovatelů jsou audity.[1093] Vzhledem k jejich současné četnosti a hloubce[1094] však neočekávám odhalení neohlášeného případu porušení zabezpečení bez adekvátního přičinění dalších osob. Těmi mohou být někdy subjekty údajů za využití mechanismu stížností dle článku 77 Obecného nařízení.[1095] Pokud však porušení zabezpečení již pocítil subjekt údajů jako významnou újmu, která ho vedla k podání stížnosti, lze to považovat za systematické selhání regulatorního rámce na ochranu osobních údajů. Je tedy na místě se poohlédnout po osobách,

[1093] Srov. čl. 58 odst. 1 písm. b) Obecného nařízení. Audit probíhá na základě § 54 odst. 1 písm. a) zákona č. 110/2019 Sb. o zpracování osobních údajů podle zákona č. 255/2012 Sb., kontrolního řádu.

[1094] Kontrolní plán Úřadu pro rok 2021 obsahuje 25 kontrol. Srov. Kontrolní plán ÚOOÚ pro rok 2021. *Úřad pro ochranu osobních údajů* [online]. 2021 [cit. 18. 10. 2021]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=52202

[1095] Ty představují podnět o porušení povinností, vedoucí případně k zahájení kontroly Úřadem. V roce 2020 obdržel Úřad 1855 stížností a podnětů, které se týkaly celého spektra záležitostí včetně řady bagatelních pochybení. Z informací o řešení těchto stížností poskytnutých ve Výroční zprávě Úřadu za rok 2020 vyplývá, že 125 vedlo ke kontrole nebo jinému řízení, 452 bylo vyřízeno upozorněním správce na možné porušení a 1278 bylo vyřízeno jinak. Srov. Výroční zpráva 2020. *Úřad pro ochranu osobních údajů* [[online]. Praha: Úřad pro ochranu osobních údajů, 2021, s. 8 [cit. 18. 10. 2021].

které mohou na porušení zabezpečení upozornit dříve. Těmi mohou být buďto interní oznamovatelé porušení nebo externí odborníci na kyberbezpečnost. Zvýšení jejich motivace k ohlašování porušení zabezpečení vnímám tudíž za významnou cestu, jak dozorový úřad může včas získat informace o tomto jevu bez ohledu na aktivitu povinného subjektu. Ten je pak tudíž silně motivován porušení zabezpečení řádně a včas ohlásit, aby v souladu s představenou teorií racionálního rozhodování ohledně ohlašování předešel pravděpodobným dodatečným nákladům v podobě sankce.

6.6.1 Zavedené postupy pro odhalování zranitelností

K odhalení porušení zabezpečení jsou dobře situovaní odborně kvalifikovaní zaměstnanci daného správce či zpracovatele, či případně výzkumníci a další třetí osoby specializující se na odhalování zranitelností či analýzu bezpečnostních hrozeb.

Činnost těchto osob má tradici v prostředí ICT, ačkoliv primárně nesměřuje na ochranu osobních údajů, ale na zvyšování kyberbezpečnosti. Zodpovědné odhalení zranitelnosti *(responsible vulnerability disclosure)*, je dnes již etablovanou součástí kultury spolupráce v tomto odvětví. Skrze organický vývoj nabyla stabilizovanou podobu dočasného zatajení odhalených zranitelností před veřejností a poskytnutí původci software či hardware sjednané období na opravu zranitelnosti před jejím plným zveřejněním *(full disclosure)*.[1096]

Příkladem může být odhalení významné zranitelnosti bezpečnostních klíčů chytrých karet nabízených společností *Infineon Technologies AG* výzkumným týmem působícím na pracovišti CRoCS *(Centre for Research on Cryptography and Security)* Fakulty informatiky Masarykovy univerzity, kdy bylo pro nápravu společnosti poskytnuto období osmi měsíců před veřejným odhalením.[1097] Toto období umožňuje minimalizovat riziko zneužití zranitelnosti, aniž by pominula silná motivace původce software či hardware k její urychlené

1096 Srov. LEVERETT, Eireann, Richard CLAYTON a Ross ANDERSON. *JRC Technical Reports: Standardisation and certification of safety, security and privacy in the 'Internet of Things'* [online]. Brussels: European Commission, 2018, s. 24 [cit. 18. 7. 2020].

1097 Srov. NEMEC, Matus et al. ROCA: Vulnerable RSA generation (CVE-2017-15361). *CRoCS wiki* [online]. 16. 10. 2017 [cit. 19. 7. 2021]. Dostupné z: https://crocs.fi.muni.cz/public/papers/rsa_ccs17

opravě než bude veřejně známá. K zodpovědnému odhalení zranitelnosti zpravidla dochází zprostředkovaně skrze neutrální subjekt, např. CERT.[1098]

S rozvojem internetu věcí a množícími se zranitelnostmi je významné rozšiřovat tyto osvědčené praktiky i do nových odvětví. Jelikož se však nejedná o normativně zakotvený proces, dochází k jeho vývoji a uplatnění v širším okruhu odvětví nekoordinovaně. To může být problém zvláště s ohledem na mezinárodní povahu trhu se zařízeními a službami internetu věcí a rostoucí napětí mezi významnými geopolitickými hráči.

Přestože nemají tyto procesy přímou vazbu na ohlašování porušení zabezpečení a směřují zpravidla vůči správci či zpracovateli namísto dozorového úřadu, lze v nich nalézat inspiraci pro možný nástroj k posílení odhalení neohlášených porušení zabezpečení. V případě, že dozorový úřad vstoupí do neutrální zprostředkovatelské role, která bude směřovat k omezení dopadů zjištěné hrozby pro zpracovávané osobní údaje, nabízí se prostor pro vznik mechanismu posilujícího vymahatelnost příslušných povinností.

Motivaci k účasti výše zmíněných osob v takovém mechanismu lze konstruovat na základě dvou zavedených nástrojů sloužících pro tyto účely. Vůči zaměstnancům správce či zpracovatele je relevantním podkladem rámec na ochranu oznamovatelů porušení povinností před nepříznivými důsledky této aktivity pro jejich postavení. Vůči nezávislým výzkumníkům jsou pak osvědčeným nástrojem programy odměn za odhalení chyb.

6.6.2 Ochrana oznamovatelů porušení unijního práva

Osoby v závislém postavení zaměstnance vůči příslušnému správci či zpracovateli jsou ohroženy nepříznivými následky své aktivity, přestože mohou být cenným zdrojem důležitých informací pro zabránění či zmírnění újmy subjektů údajů v důsledku porušení zabezpečení. V EU do nedávna chyběl harmonizovaný rámec na ochranu těchto osob, což se však změnilo na podzim 2019, kdy byla přijata směrnice 2019/1937, směřující právě k tomuto účelu.[1099]

1098 Srov. LEVERETT, Eireann, Richard CLAYTON a Ross ANDERSON. *JRC Technical Reports: Standardisation and certification of safety, security and privacy in the 'Internet of Things'* [online]. Brussels: European Commission, 2018, s. 24 [cit. 18. 7. 2020].

1099 Směrnice Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie.

Její aplikovatelnost na ohlášení vztahující se k ochraně osobních údajů je zvláště zdůrazněna v bodě odůvodnění 14. Ten přitom upozorňuje i na provázanost ohlašování porušení zabezpečení a hlášení kybernetických bezpečnostních incidentů, o kterém bylo pojednáno v předchozí podkapitole. *„Oznamování ze strany oznamovatelů v této oblasti je obzvláště cenné pro předcházení bezpečnostním incidentům, jež by se nepříznivě dotkly klíčových hospodářských a sociálních činností a široce využívaných digitálních služeb, jakož i předcházení porušování pravidel Unie pro ochranu údajů. Toto oznamování napomáhá zajistit kontinuitu služeb, jež jsou nezbytné pro fungování vnitřního trhu a blaho společnosti.“*[1100]

Směrnice sjednocuje základní podobu oznamovacích procesů, které mají členské státy zaměstnavatelům uložit. Hlavní role dle článku 7 směrnice přísluší interním kanálům pro oznamování, které by měly v souladu s článkem 8 směrnice zřídit subjekty veřejného sektoru, jakož i soukromoprávní zaměstnavatelé s více jak 50 zaměstnanci, případně v závislosti na povaze podnikatelské činnosti i méně. Pro malé a střední podniky by se přitom měl uplatnit mírnější režim povinností. Směrnice dále v článku 9 stanoví hlavní parametry, které by tyto oznamovací kanály měly splňovat. Významná role je dále přikládána externímu oznamování za pomoci kanálů zřízených dozorovými či jinými příslušnými orgány. Tomu přitom dle článku 10 směrnice nemusí nezbytně nutně předcházet oznámení za pomoci interního kanálu.

Ústředním harmonizujícím prvkem směrnice jsou ustanovení článků 19 až 24, která zakládají ochranná opatření nejen pro oznamovatele, ale též pro další osoby, skrze které by mohl být oznamovatel odvetně postihován. Může jít o kolegy a příbuzné, ale též právní subjekty, které oznamovatel vlastní, pracuje pro ně nebo je s nimi jinak spojen v pracovním kontextu.[1101] Odvetná opatření, která jsou vůči těmto osobám zakázána mají být vymezena široce bez ohledu na konkrétní formu.[1102] Lhůta pro transpozici těchto požadavků do národních právních řádů členských států uplyne 17. prosince 2021.[1103]

Tento nástroj má značný potenciál přivést k pozornosti dozorového úřadu případy porušení zabezpečení, které povinný subjekt odhalí, ale řádně

1100 Srov. bod odůvodnění 14 směrnice 2019/1937.
1101 Blíže viz čl. 4 směrnice 2019/1937.
1102 Srov. čl. 19 směrnice 2019/1937.
1103 Srov. čl. 26 směrnice 2019/1937.

neohlásí. Vedle ochrany před odvetnými opatřeními na tato ohlášení vůči osobám v pracovněprávním vztahu k příslušnému správci či zpracovateli je však na místě zvažovat možnou dodatečnou motivaci oznamovatelů, výzkumníků či bezpečnostních analytiků k těmto oznámením.

6.6.3 Přínosy a překážky využití motivačních nástrojů

V prostředí vývoje software a odhalování významných zranitelností na poli kybernetické bezpečnosti plní roli motivačního nástroje zpravidla programy odměn za odhalení chyb *(bug bounty programs)*.

Ty jsou organizovány buďto přímo původci softwarového produktu, či skrze platformu, která příslušný program odměn koordinuje a poskytuje jako službu.[1104] Program může být veřejně přístupný všem zájemcům, či soukromě limitovaný pouze na předem vybranou skupinu výzkumníků.[1105]

Obecně jde o účinný nástroj pro odhalení chyb v software a bezpečnostních zranitelností. Zpravidla se však potýká s nízkou kvalitou řady příspěvků, což lze řešit správou kvality skrze výše zmíněnou platformu.[1106] Dalším rizikem je neefektivní alokace úsilí účastníků programu v podobě časté duplikace ohlášených chyb, přičemž odměněn je pouze první příspěvek.[1107] Zde pak hraje roli koordinace a zpětná vazba o již odhalených chybách, která umožní účastníkům soustředit se na jiné části programu či rizika. Programy tohoto druhu jsou vnímány jako důležitá složka zlepšování kyberbezpečnosti v prostředí internetu věcí.[1108]

Motivační mechanismus tohoto charakteru vnímám za uplatnitelný i pro problematiku odhalování případů porušení zabezpečení. Poskytování odměny

1104 Srov. LIMON DE JESUS, Gianluca. *Enhancing Vulnerability Management for IoT Devices with Bug Bounty Programs and Responsible Disclosure* [online]. Delft, 2019, s. 36 [cit. 19. 7. 2021]. Master's Thesis. Technical University Delft.

1105 Viz LASZKA, Aron et al. The Rules of Engagement forBug Bounty Programs. In: *22nd International Conference on Financial Cryptography and Data Security (FC 2018)* [online]. 2018, s. 5 [cit. 17. 7. 2021].

1106 Srov. ZHAO, Mingyi et al. Crowdsourced Security Vulnerability Discovery: Modeling and Organizing Bug-Bounty Programs. In: *HCOMP Workshop on Mathematical Foundations of Human Computation* [online]. 2016, s. 1 [cit. 18. 7. 2021].

1107 Ibid.

1108 Viz LIMON DE JESUS, Gianluca. *Enhancing Vulnerability Management for IoT Devices with Bug Bounty Programs and Responsible Disclosure* [online]. Delft, 2019, s. 40 [cit. 19. 7. 2021]. Master's Thesis. Technical University Delft.

za oznamování porušení ze strany dozorového úřadu je sice poněkud sporný koncept, který vyžaduje důsledné nastavení pravidel, která zabraňují zneužitelnosti systému a zajišťují účelné vynaložení veřejných financí, není to však koncept v této souvislosti neznámý. V rámci slovenského zákona na ochranu oznamovatelů je zakotvena možnost poskytnutí odměny za oznámení do výše 50násobku minimální mzdy.[1109]

Podpora aktivního odhalování chyb a zranitelností skrze odměny by však měla v souladu s rozvíjenou praxí být primárně iniciována ze strany zainteresovaných soukromých subjektů. Pro koordinaci a možný vstup ze strany dozorového úřadu se tak jeví jako vhodné zajišťování programu odměn skrze odvětvové organizace pro sdílení informací o kyberbezpečnosti mezi podniky, o kterých bylo pojednáno v podkapitole 6.3. V tomto duchu je již delší dobu koordinovaným programům odměn za odhalení chyb předvídán značný rozvoj napříč nově digitalizovanými odvětvími.[1110]

6.7 Shrnutí kapitoly

Tato kapitola směřovala za využití poznatků shromážděných o porušení bezpečnosti v kontextu internetu věcí z kyberbezpečnostní, právní, technologické a ekonomické perspektivy k diskusi možných řešení identifikovaných překážek pro praktickou aplikaci úpravy dle Obecného nařízení. Tyto diskutované prvky nelze vnímat odděleně, jelikož pouze jejich účelná a koordinovaná kombinace je s to alespoň omezit rozšiřování mezery mezi příslušnou právní úpravou a technologickou realitou, na kterou je aplikována.

Nejprve jsem věnoval pozornost regulatorní reflexi specifik zpracování osobních údajů v prostředí internetu věcí.[1111] Zde jsem zdůraznil, že se jedná o kontext postihovaný celým spektrem právních předpisů, z nichž Obecné nařízení dopadá pouze na dílčí aspekt, byť průřezově. Dále jsem přiblížil provázanost těchto regulatorních rovin, které byly pro zpřehlednění

[1109] Srov. § 9 zákona č. 54/2019 Z. z. o ochrane oznamovateľov protispoločenskej činnosti a o zmene a doplnení niektorých zákonov.

[1110] Srov. LOHRMANN, Dan. Why Offering Bug Bounties Will Be Widespread, Even in Government. *Government Technology* [online]. 16. 7. 2017 [cit. 19. 7. 2021]. Dostupné z: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/why-offering-bug-bounties-will-be-widespread-even-in-government.html

[1111] Srov. podkapitola 6.1.

kategorizovány jako zaměřené primárně na (i) fyzickou bezpečnost *(safety)*, (ii) bezpečnost ve smyslu integrity *(security)* a (iii) ochranu informační hodnoty zpracovávaných či uchovávaných dat, kam spadá i ochrana osobních údajů dle Obecného nařízení. To mělo být přitom doplněno nařízením o soukromí a elektronických komunikacích, jehož možný přínos jsem též diskutoval.

Poté jsem přesunul pozornost k problému přiřazení povinností v situacích *ad hoc* společných správců, který jsem identifikoval v rámci této monografie ve čtvrté kapitole. Za tímto účelem jsem představil současné široké pojetí pojmu správce na základě judikatury SDEU a navrhl, že pro překonání tohoto problému je možným řešením adaptace programu mírnějšího režimu při ukládání pokut *(leniency program)* osvědčeného v prostředí soutěžního práva.

Dalším dílčím tématem byla potřeba koordinovaného regulatorního přístupu a možný přínos certifikace zařízení internetu věcí. Zde jsem diskutoval především bezpečnostní certifikace, u kterých dochází v poslední době k významnému posunu a vývoji.

V další podkapitole jsem soustředil pozornost na možnosti usnadnění výkladu a plnění příslušných povinností souvisejících s porušením zabezpečení.[1112] Prvním takovým nástrojem byly pokyny, doporučení a osvědčené postupy dozorových úřadů, ty jsou však omezeny svou obecností. Sektorovou specifikaci by měly přinést kodexy chování, poukazuji však na důvody, proč se nejedná a zřejmě ani nebude jednat o významný nástroj pro usnadnění výkladu diskutovaných povinností. Daleko větší potenciál oproti tomu spatřuji v současném vývoji standardizace. Ta nabízí nejen funkční vodítko jednotlivým povinným subjektům pro zavedení přiměřených a vhodných opatření v souladu s osvědčenou praxí, ale zakládá taktéž podmínky pro kompatibilitu a interoperabilitu mezi řešeními od různých výrobců a minimální úrovní opatření, která jsou v rámci daného odvětví očekávána. Třetím zmíněným nástrojem předvídaným Obecným nařízením jsou osvědčení, pečeti a známky, tedy specifický formát certifikace souladu s požadavky ochrany osobních údajů. Vzhledem k odlišnosti pojetí této certifikace od mezinárodně uznávaných formátů certifikačních schémat však očekávám upřednostňování bezpečnostní certifikace formou prohlášení výrobce o shodě (autocertifikace).

1112 Srov. podkapitola 6.2.

Třetím diskutovaným řešením byla podpora sdílení informací mezi podniky pro zvýšení jejich kooperace a výsledných synergií pro ochranu osobních údajů.[1113] Za vzor jsem zde přitom bral americká centra pro analýzu a sdílení informací (ISAC). Poukázal jsem na aktivity ENISA ve směru podpory utváření těchto organizací i v evropském kontextu, současně jsem však konstatoval, že nejde doposud o příliš rozšířený formát. Rozšířenější jsou spíše méně formální spolupráce veřejného a soukromého sektoru (PPP) za různými účely souvisejícími se zabezpečením osobních údajů. Následně jsem diskutoval překážky sdílení informací mezi podniky, jako je problém černého pasažéra, a jejich vnímání praxí.

V další podkapitole jsem se zaměřil na možnosti posílení přenositelnosti vzniklé újmy zpět na odpovědné subjekty.[1114] Nejprve jsem přiblížil úpravu nároku na náhradu újmy dle Obecného nařízení a pak jsem věnoval pozornost otázce právního rámce pro skupinové žaloby. Na tu jsem nahlížel nejen z perspektivy skupinového zastoupení dle Obecného nařízení, ale i se zohledněním směrnice o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů. V diskusi jsem pak zohlednil i zkušenosti se skupinovými žalobami z prostředí Spojených států.

Tématem páté podkapitoly byla možnost účelného propojení ohlašování porušení zabezpečení s hlášením kybernetických bezpečnostních incidentů.[1115] S ohledem na nedostatek odborných kapacit dozorových úřadů pro řešení porušení zabezpečení jsem navrhl systematickou spolupráci mezi Úřadem a bezpečnostními týmy zaměřenými na kybernetickou bezpečnost. Těm jsou již dnes směřována hlášení kybernetických bezpečnostních incidentů, která jsem zde přiblížil co do obsahu, okruhu povinných subjektů i množství hlášených incidentů. Také jsem poukázal na současné trendy kybernetické bezpečnosti, které naznačují rostoucí obsahový překryv s problematikou porušení zabezpečení v prostředí internetu věcí. Argumentoval jsem, že systematická spolupráce by měla přínos nejen pro bezpečnostní týmy a Úřad, ale též pro ohlašující a chráněné subjekty.

1113 Srov. podkapitola 6.3.
1114 Srov. podkapitola 6.4.
1115 Srov. podkapitola 6.5.

Poslední dílčí problematikou byly možnosti usnadnění odhalení neohlášených případů porušení zabezpečení.[1116] Zde jsem upozornil na již existující postupy pro odhalování zranitelností jako je zodpovědné odhalení zranitelnosti *(responsible vulnerability disclosure)* skrze výzkumníky či jiné nezávislé subjekty. Poukázal jsem na rostoucí význam těchto mechanismů napříč sektory v důsledku rozvoje internetu věcí. Jako možné zdroje informací o neohlášených porušeních zabezpečení pro dozorový úřad vnímám vedle výzkumníku především zaměstnance upozorňující na porušení správce či zpracovatele. V tomto směru je významná směrnice o ochraně oznamovatelů porušení unijního práva, která harmonizuje nejen požadavky na interní a externí oznamovací procesy, ale především rozsah ochrany oznamovatele, čímž je zaručena jeho větší ochota vystoupit a ohlásit zjištěné porušení. Často je však zapotřebí dodatečná motivace, což platí i pro výše zmíněné odhalování zranitelností. Za tímto účelem se při vývoji software osvědčil mechanismus programů odměn za odhalení chyb. Diskutoval jsem tudíž přínosy a limity přenesení tohoto motivačního nástroje i na ohlašování porušení zabezpečení, ať již vůči dozorovému úřadu či spíše vůči sektorové organizaci sdružující podniky za účelem sdílení informací.

V této kapitole byly reflektovány všechny dílčí otázky na základě předchozích zjištění, které jsem k nim shromáždil napříč představovanou studií. Pozornost přitom byla soustředěna na dosažení vlastního cíle monografie, tedy stanovení, zda má současná právní úprava povinností při porušení zabezpečení osobních údajů dle Obecného nařízení účelné uplatnění i v prostředí internetu věcí, a pokud ano, pak jakými úpravami lze překonat případné zjištěné výzvy a překážky.

Již v rámci předchozích kapitol jsem dovodil, že význam těchto povinností v prostředí internetu věcí při vhodném nastavení a řádném plnění ze strany povinných subjektů pouze narůstá. Je to dáno nejen předpokládanou vyšší četností porušení zabezpečení, ale i rostoucí hrozící újmou, kterou v takových případech mohou subjekty údajů pociťovat. Význam této úpravy může být dále umocněn i zakotvením systematické spolupráce s bezpečnostními týmy pro oblast kybernetické bezpečnosti, pro které se jedná o potenciálně

[1116] Srov. podkapitola 6.6.

významný zdroj jinak nedosažitelných informací.[1117] Přesto je nutné zohledňovat identifikované podmínky vhodného nastavení a řádného plnění. Ty byly postupně rozkrývány a diskutovány napříč perspektivami představenými v této publikaci, v úvodu kapitoly jsem je však zobecnil na tři hlavní požadavky:

1. posílení právní jistoty povinných subjektů při výkladu a aplikaci uložených povinností,
2. posílení motivace povinných subjektů k realizaci preventivních opatření a
3. zajištění řádného ohlašování porušení zabezpečení a využití takto získaných informací.

Pro každý z těchto požadavků jsem pak napříč touto kapitolou nabídl diskusi souvisejících regulatorních nástrojů a mnou vnímaných možných řešení pro adaptaci příslušných povinností na rozšiřování internetu věcí.

V rámci posílení právní jistoty bude zřejmě hrát klíčovou roli zavedení požadavků na bezpečnostní certifikaci zařízení internetu věcí, doplněné o dostupné standardy uzpůsobené prostředí internetu věcí. Problematické postavení *ad hoc* společných správců pak může být překonáno zavedením programu aplikace mírnějšího režimu při ukládání pokut.

Motivovat povinné subjekty k přiměřeným bezpečnostním opatřením by měly především sektorové organizace na sdílení informací a zkušeností. Dalším impulsem pro to, aby se správci zabývali prevencí intenzivněji, může být zavedení funkčních rámců skupinových žalob a tím reálná hrozba zpětné přenositelnosti újmy subjektů údajů.

Ohlašování vůči dozorovému úřadu bylo shledáno za nejvíce problematický prvek regulatorního rámce vztahujícího se k porušení zabezpečení.[1118] Hlavní překážku zde tvoří kolize zájmů, kdy z hlediska racionálního rozhodování není pro povinný subjekt zpravidla výhodné, aby k ohlášení bez dalšího přistupoval. Plnění této povinnosti může být vynuceno, pokud za její neplnění hrozí dostatečně vysoká sankce a odhalení neoznámeného případu je přiměřeně pravděpodobné.[1119] Sankce, které lze na základě Obecného nařízení

1117 Srov. oddíl 6.5.3.
1118 Srov. třetí kapitola.
1119 Srov. pátá kapitola.

uložit v tomto směru nepředstavují překážku, problém je spíše nízká pravděpodobnost odhalení. Pro tu jsem navrhl tři možná řešení. Předně jde o systematickou spolupráci dozorového úřadu s bezpečnostními týmy, která mimo jiné navýší odbornou kapacitu dozorového úřadu a mohou mu zpřístupnit nové informace z prostředí kybernetické bezpečnosti, které umožní lépe odhalit neohlášené případy. Další možností jsou zaměstnanci správce jako oznamovatelé porušení, přiměřeně chránění napříč EU v souladu se směrnicí před odvetnými opatřeními zaměstnavatele. Nakonec pak jde o výzkumníky a externí specialisty, motivované programy odměn k nezávislému odhalování a ohlašování porušení. Podstatné přitom je uvést, že na základě zjištění o racionálním rozhodování podniku v páté kapitole není nezbytně nutné, aby kterékoliv z těchto řešení skutečně rozsáhle odhalovalo neohlášené případy porušení zabezpečení. Podniky při svém rozhodování kalkulují s očekávanými náklady ohlášení a neohlášení. Vnímaná vyšší předpokládaná pravděpodobnost odhalení neohlášení s ohledem na rozšíření možností dozorového úřadu, jak dospět k této informaci, by tak pro ně měla být sama o sobě impulsem pro řádné a důsledné ohlašování porušení zabezpečení.

Závěrečným poznatkem je zdůraznění rostoucí provázanosti dílčích rámců a regulatorních mechanismů přesahujících povinnosti dle Obecného nařízení k úspěšnému řešení bezpečnostní situace ICT podniků a dalších entit, i v zájmu ochrany subjektů údajů. S tím pak souvisí potvrzení obecně poznatelné premisy, že je nezbytné nalézat cesty ke koordinaci napříč odbornými perspektivami a regulatorními rovinami. Příslušné povinnosti jsou totiž účelně aplikovatelné pouze při zachování souladu s ostatními regulatorními nástroji, které byly nastíněny v rámci této kapitoly. To je nejen podmínkou jejich účinnosti, ale též cestou k předcházení nadbytečné administrativní zátěže, výkladových nejasností či nových aplikačních překážek, jejichž četné současné příklady byly identifikovány napříč touto publikací.

7 ZÁVĚR

V představené monografii jsem si kladl za cíl zkoumat, zda má současná právní úprava povinností při porušení zabezpečení osobních údajů dle Obecného nařízení účelné uplatnění i v prostředí internetu věcí, a pokud má, pak jakými úpravami lze překonat případné zjištěné výzvy a překážky, které jí v tomto prostředí vyvstávají. K tomu jsem přistoupil systematicky výkladem nosných prvků problematiky, přičemž mi tento postup umožnil na ni též postupně nahlédnout z více perspektiv.

Perspektiva kyberbezpečnostní: Nejprve jsem v rámci druhé kapitoly poskytl obecný úvod, vymezující pojem porušení bezpečnosti formu bezpečnostního incidentu a poukazující na rozsah a význam tohoto jevu v dnešní digitalizované společnosti.

Jedná se přitom o hrozbu inherentně spojenou s užíváním informačních a komunikačních technologií ke společenské interakci. Nárůst četnosti, jakož i intenzita a škodlivý dopad porušení bezpečnosti se tudíž zásadně stupňuje s rozvojem digitalizace společnosti, nárůstem konektivity a přibývajícím množstvím zpracovávaných údajů. Tento obecný trend, podložený nejen příklady významných porušení bezpečnosti, ale též dostupnými statistikami poskytl výchozí bod pro další analýzu proměny prostředí v důsledku rozšíření internetu věcí.

Z představených informací o aktuální situaci dále vyplývá, že problematika porušení bezpečnosti nabývá velkého a stále rostoucího rozsahu, což značí, že se jedná o významné téma se značným společenským dopadem. V konkrétních případech přitom může být situace velmi různorodá, jak jsem se v rámci této kapitoly snažil poodhalit. Je možné identifikovat velmi rozsáhlé případy porušení bezpečnosti zpracovávaných údajů, které přivodili značnou újmu milionům dotčených osob. Daleko častěji však dochází k převážně přehlíženým či dokonce neodhaleným případům porušení bezpečnosti menšího rozsahu či u méně exponovaných subjektů, které však jsou i tak s to přivodit zásadní újmu jednotlivcům. Za nejvážnější formu újmy pro fyzické osoby jsem dovodil krádež identity, tedy zjevnou či skrytou ztrátu (výlučné) kontroly nad částí svých uživatelských účtů či nad jinými projevy virtuální identity.

Perspektiva právní: Následně jsem se ve třetí kapitole přesunul k rozboru nejen unijního, ale i amerického regulatorní rámce stanovujícího soubor povinností pojících se k porušení bezpečnosti a omezení jeho výskytu a následků. Jde přitom o preventivní zajištění bezpečnostních opatření, dokumentaci případů porušení bezpečnosti, jejich ohlášení dozorovému orgánu a případně i oznámení dotčeným jednotlivcům.

Nejprve jsem přistoupil k představení unijní úpravy, která předcházela použitelnosti Obecného nařízení.[1120] Jedná se o stále relevantní úpravu pro poskytovatele veřejně dostupných služeb elektronických komunikací.[1121] Hlavní pozornost jsem ovšem soustředil na použitelnou úpravu podle Obecného nařízení.[1122] Na tu jsem nahlížel jak z hlediska legislativního vývoje,[1123] tak podrobným rozborem povinností souvisejících s porušením zabezpečení.[1124] V rámci celostního pojetí je zde i zmínka o dílčích transpozicích do národních právních řádů na základě směrnice 2016/680. Osvětlil jsem také, že vzhledem k odlišnostem nepodstatným z hlediska rozvoje internetu věcí nepokládám za významné dále přihlížet k případným dílčím specifikům české národní úpravy a vycházím tedy z úpravy dle Obecného nařízení. Na poskytnutý legislativní a obsahový přehled unijní úpravy jsem navázal podrobnější diskusí, v jejíž hlavní části jsem se věnoval funkčnímu výkladu ve snaze o vymezení účelů představených povinností. K tomu jsem přistoupil ve třech rovinách. Nalézal jsem (i) účel dle vlastního textu úpravy, (ii) účel zachycený v bodech odůvodnění a (iii) účel z objektivního hlediska.

Poskytl jsem dále stručný rozbor úpravy povinností při porušení bezpečnosti zpracovávaných údajů v právu Spojených států amerických. Jeho vhodnost a potřebnost jsem zdůvodnil především rozsáhlým odborným diskurzem založeným na dlouhé zkušenosti s notifikačními povinnostmi, které sloužily jako inspirace pro unijní úpravu, a který jsem využil při identifikaci vhodných řešení identifikovaných výzev. V této kapitole jsem v závěru pojmenoval významné překážky pro dosahování účelu těchto povinností. Konkrétně u ohlašovací povinnosti jde o kolizi zájmů, která odrazuje povinný subjekt

1120 Viz podkapitola 3.1.
1121 O té byla řeč v oddílu 3.1.1.
1122 Srov. podkapitola 3.2.
1123 Lze zmínit například veřejně dostupný přehled porušení zabezpečení, navrhovaný Evropským parlamentem. Srov. oddíl 3.2.1.
1124 Viz oddíl 3.2.2.

od plnění ohlašovací povinnosti a omezené možnosti dozorového orgánu získat příslušné informace jinou cestou.

Perspektiva technologická: Záměrem však nebylo omezit se v této monografii pouze na statickou diskusi této úpravy z dnešní perspektivy, ale konfrontovat ji s vysoce dynamickým trendem proměny postupů a vzorců zpracování osobních údajů, pro který jsem zvolil označení internet věcí. Přiblížení tohoto kontextu jsem věnoval čtvrtou kapitolu. Nejprve jsem zde přistoupil k vymezení pojmu internet věcí.[1125] Následně jsem odhalil nové formy a vzorce zpracování osobních údajů v tomto kontextu.[1126] Ty souvisejí nejen s narůstajícím rozsahem zpracování osobních údajů, ale i s rozmanitostí struktury předmětných procesů a s rozšířením automatizované komunikace mezi stroji. Všudypřítomnost zpracování pak vede k hrozící absenci povědomí subjektu údajů o tomto zpracování, což činí jeho rozsah, a tedy i rozsah možné újmy v důsledku porušení bezpečnosti nepředvídatelný. Tento nárůst hrozeb jsem popsal na příkladu rozvoje internetu věcí u kamerových systémů. V něm se výstižně projevuje i častá nenápadná povaha zařízení internetu věcí. Nadto jsem věnoval pozornost zesilujícímu efektu *cloud computingu* a vytěžování databází *big data*.

Další rovinou, které jsem věnoval pozornost byla problematika zajištění bezpečnosti.[1127] Zde jsem upozornil na bezpečnostní limity řady zařízení internetu věcí, související mimo jiné s problémem aktualizace a opravy software. Pro lepší představu o nastíněných výzvách jsem dále přistoupil k rozboru tří významných scénářů, z nichž každý poukazuje na odlišný aspekt proměny zpracování osobních údajů v tomto kontextu.[1128] Věnoval jsem tak pozornost (i) dopadům automatizované komunikace na rozsah sdílení osobních údajů mezi zařízeními, (ii) dynamice interakce v rámci chytrého města a *ad hoc* zpracování společnými správci, a (iii) narůstajícímu významu mikropodniků.

Při rozboru automatizované komunikace mezi stroji a v prostředí autonomních zařízení[1129] jsem nejprve představil existující komunikační standardy pro internet věcí. Následně jsem se zaměřil na novou generaci telekomunikačních standardů 5G. Závěrem z této perspektivy je, že u internetu věcí lze očekávat

1125 Srov. podkapitola 4.1.
1126 Srov. podkapitola 4.2.
1127 Srov. podkapitola 4.3.
1128 Srov. podkapitola 4.4.
1129 Srov. oddíl 4.4.1.

častější případy porušení bezpečnosti s citelnějšími dopady, jakož i častější opominutí odhalení a řádného ohlášení významného porušení bezpečnosti.

Druhou specifickou perspektivou byly přímé a nepřímé provázanosti sítí chytrého města.[1130] Zde jsem se zaměřil na důsledky souhry existující a nové infrastruktury a také na nepřímé modulární závislosti mezi jednotlivými prvky. Odhalil jsem nová rizika složitých zpracování v rámci síťových propojení, čímž je z hlediska práva ochrany osobních údajů utvářena série *ad hoc* zpracování společnými správci. To přináší dodatečné překážky pro dostatečnou motivaci jednotlivých povinných subjektů plnit příslušné povinnosti.

Do třetice jsem se zaměřil na internet věcí u mikropodniků.[1131] Nejprve jsem vymezil pojem mikropodnik. Následně jsem věnoval zvláštní pozornost specifickému postavení mikropodniků z hlediska kyberbezpečnosti a jejich často nedostatečným bezpečnostním opatřením, které vedou k významným zranitelnostem. Ty mohou s rozvojem internetu věcí dále významně narůstat a ohrožovat subjekty údajů i další entity v rámci dodavatelských řetězců. Shledal jsem také, že mikropodnikům v realizaci potřebných opatření brání nejen omezené kapacity a know-how, ale též nedostupnost praktických vodítek a příkladů dobré praxe.

Na základě výše představených poznatků jsem zformuloval čtyři základní oblasti, ve kterých vnímám významnou proměnu povinností souvisejících s porušením bezpečnosti v kontextu internetu věcí.[1132] Jedná se o (i) zvýšení frekvence a množství případů porušení bezpečnosti, (ii) zvýšení závažnosti újmy v důsledku porušení bezpečnosti, (iii) znesnadnění odhalení porušení bezpečnosti a (iv) nárůst složitosti a četnosti situací se společnými správci. V jejich kontextu jsem pak dále rozvíjel poznatky o předmětných povinnostech skrze jejich konfrontaci se specifiky internetu věcí. Dospěl jsem tak k odhalení dodatečných překážek, které lze v tomto kontextu očekávat, především co do včasného odhalení případů porušení bezpečnosti, jakož i přiřazení povinností v rámci *ad hoc* zpracování společnými správci.

Perspektiva ekonomická: Jelikož jsem za ústřední překážku ve spojení s diskutovanými povinnostmi stanovil motivaci povinných subjektů k jejich

1130 Srov. oddíl 4.4.2.
1131 Srov. oddíl 4.4.3.
1132 Srov. podkapitola 4.5.

dodržování, doplnil jsem v rámci páté kapitoly monografii o modelování racionálního rozhodování povinného subjektu v těchto situacích. Za tímto účelem jsem nejprve přiblížil pojem rizika a nastínil překážky při jeho hodnocení.[1133] Blíže jsem pak představil racionální teorii rozhodování, jejímž základem je teorie užitku.[1134]

Pozornost jsem následně přesunul k otázce dosahování přiměřených investic do kyberbezpečnosti. Výchozím bodem byl model *Gordona* a *Loeba*, který nastiňuje možnost určení optimální výše investic. Tento základní model má však řadu významných limitů, které se snažili překonat četní navazující autoři. Tato doplnění zahrnují především zohlednění externalit typu DDoS útoku, či zahrnutí problematiky sdílení informací mezi podniky s přihlédnutím k vzájemné závislosti mezi podniky a případně též k důsledkům jejich konkurenčního postavení. Klíčové závěry z těchto modelů jsou dva. Prvním je existence ekonomického zdůvodnění založení povinnosti přiměřených bezpečnostních opatření, tak jak ji nalézáme v článku 32 Obecného nařízení. Druhým je pak potenciální přínos dobrovolného sdílení informací mezi podniky.

V další podkapitole jsem již pozornost soustředil na dva modely řešící vlastní rozhodování podniku o ohlašování porušení bezpečnosti.[1135] Dřívější *Garciův* model je zasazen do amerického prostředí.[1136] Zde je diskutována překážka asymetrické informace o porušení bezpečnosti. Za klíčové proměnné při rozhodování o ohlášení jsou identifikovány pravděpodobnost odhalení a sankce při neohlášení. *Garcia* se dále zaměřuje na stanovení potřebné výše minimální sankce. Jeho předpokladem je, že motivace podniku je vedena snahou o minimalizaci nákladů. Toho může být využito pro vynucení ohlášení porušení bezpečnosti. Regulatorní nastavení sankcí za nesplnění této povinnosti však musí být přiměřeně přísné.

Tento závěr je doplněn a rozvinut v modelu *Laubeho* a *Böhmeho*, byť se zdá, že vznikl nezávisle na *Garciově* modelu.[1137] Je jím však efektivně potvrzena obecná přenositelnost závěrů *Garciova* modelu do evropského prostředí. *Laube* a *Böhme* navíc zohledňují jako relevantní proměnnou i rozsah

1133 Srov. podkapitola 5.1.
1134 Srov. podkapitola 5.2.
1135 Srov. podkapitola 5.4.
1136 Srov. oddíl 5.4.1.
1137 Srov. oddíl 5.4.2.

provázanosti úrovně kyberbezpečnosti mezi podniky. I pro ně jsou však výše sankce a pravděpodobnost odhalení neohlášení klíčové pro motivaci podniku. Zaměřují se pak na rozdíl od *Garcii* na určení potřebné úrovně pravděpodobnosti odhalení. Výsledně dovozují, že ohlašovací povinnost při adekvátní míře vymahatelnosti má společenský přínos, pokud je mezi úrovní kyberbezpečnosti podniků dostatečná provázanost, dozorový orgán je schopen účelně využít ohlášené informace a pro podnik se se zveřejněním těchto informací pojí pouze nízké dodatečné náklady.

Přes nevyhnutelně zjednodušující logiku představených modelů je zřejmé, že řízení rizik souvisejících s ochranou osobních údajů zahrnuje značnou míru nejistoty, která je daná komplexností problematiky, a dále zesilována případnou omezenou personální či rozpočtovou kapacitou řady správců k jejímu překonání. Dovodil jsem přitom, že investice do bezpečnostních opatření mohou být vynuceny skrze zpětnou přenositelnost vzniklé újmy na povinný subjekt a případně jejich potřeba může být snížena při koordinaci mezi vzájemně propojenými podniky, zpravidla skrze organizace pro sdílení informací o kyberbezpečnosti. Dále jsem určil, že největší překážka v podobě kolize zájmů vyvstává pro ohlašovací povinnost vůči dozorovému úřadu. Zde přitom může být řádné a včasné plnění na povinném subjektu efektivně vynuceno v zásadě pouze skrze kombinaci dostatečně odrazující dodatečné sankce za neohlášení a přiměřeně vysoké pravděpodobnosti odhalení tohoto případu i bez přispění povinného subjektu.

Dílčí otázky: Před představením šesté kapitoly a v ní obsažené diskuse, která se váže k cíli představované monografie, je na místě doplnit, že mě v rámci nahlížení na řešenou problematiku z těchto perspektiv provázelo a udržovalo na správném kurzu osm dílčích otázek, na které jsem při shromažďování poznatků napříč příslušnými kapitolami nalézal odpovědi.

(1): První z nich směřovala na to, jak se proměnily notifikační povinnosti v Obecném nařízení ve srovnání s předchozí unijní a paralelní americkou právní úpravou? Odpověď jsem poskytl v rámci třetí kapitoly, kde jsem ukázal nejen na zachovanou linku mezi těmito úpravami, ale též nové prvky, které přineslo Obecné nařízení. Hlavním poznatkem přitom bylo, že úprava v Obecném nařízení do značné míry čerpala ze zkušeností z předchozího rámce pro poskytovatele veřejně dostupných služeb elektronických komunikací.

Většina potřebné sektorové specifikace však byla normotvůrcem přenechána výkladu, což vede k přetrvávající nejistotě při aplikaci povinnými subjekty. Ta je výrazná i při porovnání s americkou úpravou, oproti té je však zásadní výhodou Obecného nařízení jednotnost napříč sektory i členskými státy.

(2): Dále jsem si kladl otázku, zda přináší prostředí internetu věcí nové výzvy pro dodržování povinností souvisejících s porušením bezpečnosti osobních údajů? Odpověď jsem nalézal ve čtvrté kapitole a je kladná, jelikož zde vznikají v řadě ohledů nové formy a vzorce zpracování osobních údajů.[1138] Roste nejen rozmanitost daných procesů a náročnost zajištění jejich bezpečnosti, ale i složitost vazeb mezi společnými správci a koordinace plnění příslušných povinností. Významným aspektem je také značně nenápadná povaha funkcí řady zařízení internetu věcí a s tím související neurčitost rozsahu probíhajícího zpracování i hrozící újmy.

(3), (4), (5), (6): Následně jsem formuloval v podstatě čtyři podotázky, které předjímaly možné nové hrozby spojené s technologickým pokrokem s ohledem na porušení bezpečnosti. Jejich obecný trend byl zaznamenán již ve druhé kapitole, všechny se pak následně potvrdily jako významné i pro kontext internetu věcí ve čtvrté kapitole. Je tedy nutné přihlížet nejen k hrozícímu navýšení četnosti a rozsahu porušení bezpečnosti, ale též nárůstu jejich intenzity a škodlivého dopadu. Současně jsem identifikoval předpoklady pro nové překážky odhalení těchto porušení bezpečnosti, ať již vzhledem ke složitosti síťových vazeb, nenápadnosti funkcí zařízení či omezenému know-how povinných subjektů v kategorii mikropodniků. Také jsem stanovil, že prostředí internetu věcí, jakým je i chytré město, přináší specifické výzvy pro určení povinných subjektů, což souvisí s již zmíněným přiřazováním povinností *ad hoc* společným správcům.

(7): Kapitola pátá byla do značné míry věnována zodpovězení otázky, zda se tyto proměny prostředí odrážejí v motivaci subjektů plnit povinnosti související s porušením bezpečnosti? Byť představované modely rozhodování o plnění povinností nezohledňují technologickou proměnu jako takovou, bylo možné provázat jejich klíčové prvky s proměnami, které jsem vymezil na základě předcházejících podotázek v souvislosti s internetem věcí. Dospěl jsem tudíž k závěru, že výstupy těchto modelových situací jsou nejen nadále

[1138] Srov. podkapitola 4.2.

platné i pro prostředí internetu věcí, ale dochází v řadě ohledu k jejich posílení. To platí nejen pro zvyšující se provázanost úrovně kyberbezpečnosti mezi podniky, ale též pro potřebu dodatečných cest, jak překonat informační asymetrii mezi povinným subjektem a dozorovým úřadem a ověřit tak plnění ohlašovací povinnosti. Rostoucí obtížnost odhalení porušení bezpečnosti a složitější struktury společných správců v kontextu internetu věcí totiž budou dále snižovat motivaci povinných subjektů důsledně dodržovat preventivní a ohlašovací povinnosti.

(8): Závěrečnou otázkou jsem se zamýšlel nad relativním významem, který lze přikládat notifikačním povinnostem porušení bezpečnosti v prostředí internetu věcí. V jejím rámci jsem se vypořádával nejen s hrozbu reálné nevymahatelnosti a rozsáhlého opomíjení těchto povinnosti ze strany příslušných správců, ale též s relativním poklesem významu s ohledem na rozšiřování souvisejících regulatorních rámců, jakým je např. právo kybernetické bezpečnosti. V rámci šesté kapitoly jsem přitom argumentoval ve prospěch závěru, že notifikační povinnosti porušení bezpečnosti mají stejný či dokonce větší význam v kontextu internetu věcí, pokud dojde k vhodnému nastavení podmínek pro jejich aplikaci. To souvisí nejen se srozumitelností obsahu těchto povinností všem správcům, tedy i mikropodnikům, ale též s překonáním nedostatečné motivace buďto zvýšením podpory, které se správcům dostává nebo zvýšením pravděpodobnosti odhalení neplnění povinností a s tím spojené hrozby dodatečné sankce. Ohledně relativního významu v porovnání s jinými rámci jsem pak poukázal na potřebu koordinace a přijetí rostoucí provázanosti, např. skrze systematickou spolupráci mezi dozorovým úřadem a bezpečnostními týmy zajišťujícími otázky kybernetické bezpečnosti.

Cíl monografie: Soubor takto shromážděných informací a poznatků mi umožnil dospět k cíli monografie, tedy stanovení, zda má současná právní úprava povinností při porušení zabezpečení osobních údajů dle Obecného nařízení účelné uplatnění i v prostředí internetu věcí, a pokud ano, pak jakými úpravami lze překonat případné zjištěné výzvy a překážky. To jsem diskutoval především v šesté kapitole.

Ohledně účelného uplatnění úpravy v prostředí internetu věcí jsem dovodil, že význam představených povinností dle Obecného nařízení v tomto kontextu dále narůstá, ovšem za předpokladu vhodného nastavení podmínek

pro jejich řádné plnění ze strany povinných subjektů a následné reakce ze strany dozorových úřadů. K tomu mě vedlo nejen očekávání rostoucí intenzity hrozeb, ale i jejich případného dopadu, který může postihnout dotčené subjekty údajů. S novou technologickou realitou nadto poroste složitost procesů zpracování a vztahů mezi správci, což bude znamenat vyšší potenciál nepřímých zranitelností a nárůst neodhalených porušení zabezpečení, která budou působit o to vyšší újmu. Celkově se přitom jedná o problematiku významnou nejen z perspektivy ochrany osobních údajů, ale též kyberbezpečnosti, resp. práva kybernetické bezpečnosti.

Dílčí překážky pro aplikaci příslušných povinností na prostředí internetu věcí vyplynuly průběžně při zohledňování jednotlivých perspektiv. Za hlavní jsem přitom označil následující tři:

1. právní nejistotu ohledně výkladu vzniku a obsahu daných povinností,
2. nízkou motivaci povinných subjektů zavádět přiměřená bezpečnostní opatření, a zvláště pak sdílet s vrchnostenskými orgány informace o svých pochybeních a
3. omezené možnosti odhalení neohlášených případů porušení zabezpečení.

Ty přitom vnímám jako odraz mezery mezi normativním konceptem předmětných povinností a jejich praktickou realizací, která je dále rozšiřována s rozmachem internetu věcí. V šesté kapitole jsem proto představil možná řešení pro adaptaci příslušných povinností na rozšiřování internetu věcí, směřující k překonání těchto tří překážek.

V rámci posílení právní jistoty přikládám klíčovou roli zavedení požadavků na bezpečnostní certifikaci zařízení internetu věcí,[1139] doplněné o dostupné standardy uzpůsobené prostředí internetu věcí.[1140] Problematické postavení *ad hoc* společných správců jsem pak navrhl překonat zavedením programu aplikace mírnějšího režimu při ukládání pokut.[1141]

Motivovat povinné subjekty k přiměřeným bezpečnostním opatřením by měly dle mého názoru především sektorové organizace na sdílení informací a zkušeností.[1142] Za další impuls pro to, aby se správci zabývali prevencí

1139 Srov. oddíl 6.1.3.
1140 Srov. oddíl 6.2.2.
1141 Srov. oddíl 6.1.2.
1142 Srov. podkapitola 6.3.

intenzivněji než nyní, pak vnímám zavedení funkčních rámců skupinových žalob a tím reálnější hrozbu zpětné přenositelnosti újmy ze subjektů údajů zpět na správce.[1143]

Dostatečně pravděpodobné odhalení neohlášených porušení zabezpečení dozorovým úřadem jsem vymezil za jeden z hlavních předpokladů vynutitelnosti řádného plnění ohlašovací povinnosti dle Obecného nařízení.[1144] Pro zvýšení pravděpodobnosti odhalení jsem navrhl tři dílčí řešení. Předně jde o systematickou spolupráci dozorového úřadu s bezpečnostními týmy, která navýší odbornou kapacitu dostupnou dozorovému úřadu a může mu zpřístupnit nové informace z prostředí kybernetické bezpečnosti, které mu umožní lépe odhalit neohlášené případy.[1145] Další možností je motivovat zaměstnance správce či zpracovatele k ohlášení porušení povinností dle Obecného nařízení i proti vůli tohoto zaměstnavatele. Tomu by měl přispět harmonizovaný rámec jejich ochrany před odvetnými opatřeními. V neposlední řadě pak považuji za vhodné využít kapacity nezávislých výzkumníků a externích specialistů a motivovat je programy odměn k odhalování neohlášených porušení. Pro všechna tato řešení přitom předpokládám, že nemusí být sama o sobě plně účinná, jelikož již samotná obava povinného subjektu ze snazšího odhalení nesplnění ohlašovací povinnosti by měla postačovat ke zvýšení racionální motivace ve větším měřítku řádně a důsledně ohlašovat odhalená porušení zabezpečení.

Prostor pro další výzkum: Řada nástrojů či řešení usnadňujících adaptaci rámce povinností vztahujících se k porušení zabezpečení osobních údajů na kontext internetu věcí, o kterých bylo v této monografii pojednáno, již nabyla či nabývá konkrétní podoby a lze v budoucnu očekávat jejich uplatnění. Prostor pro další výzkum tudíž shledávám nejen v podrobnější analýze těchto dílčích řešení, především pak bezpečnostní certifikace zařízení internetu věcí, utváření sektorových organizací pro sdílení informací o kyberbezpečnosti mezi podniky či systematické spolupráce mezi dozorovým úřadem a bezpečnostními týmy, ale především v nalézání vhodné souhry a synergie mezi těmito účelově provázanými prvky.

1143 Srov. podkapitola 6.4.
1144 Srov. podkapitola 5.5.
1145 Srov. podkapitola 6.5.

SUMMARY – PERSONAL DATA BREACH IN THE CONTEXT OF THE INTERNET OF THINGS

In the research publication presented here, I set out to examine whether the current legal framework for data breach obligations under the General Data Breach Regulation has a viable application in the Internet of Things environment and, if so, what adjustments can be made to overcome any identified challenges and obstacles to it in this environment. I have approached this issue from multiple perspectives.

Cybersecurity Perspective: First, in Chapter Two, I provided a general introduction, defining the concept of a personal data breach as a form of security incident and highlighting the scope and significance of this phenomenon in today's digitized society.

As such, it is a threat inherently associated with the use of information and communication technologies for social interaction. The increase in the frequency, intensity and harmful impact of personal data breaches is therefore fundamentally increasing with the growing digitalisation of society, the increase in connectivity and larger and larger amount of data being processed. This general trend, supported not only by examples of significant personal data breaches, but also by available statistics, has provided a starting point for further analysis of the changing environment due to the spread of the Internet of Things.

The current situation also shows that the issue of personal data breaches is becoming widespread and growing, which means that it is an important topic with a significant social impact. In specific cases, the situation can be very diverse, as I have tried to show in this chapter. It is possible to identify very large-scale personal data breaches that have caused significant harm to millions of individuals. Far more often, however, there are largely overlooked or even undetected personal data breaches of a smaller scale or by less exposed entities, which are nevertheless threatening substantial harm to individuals. I have identified identity theft, meaning the overt or covert loss of (exclusive) control over part of one's user accounts or other manifestations of virtual identity, as the most serious form of harm to individuals caused by personal data breach.

Legal Perspective: I then moved on in Chapter Three to analyse not only the EU but also the US regulatory framework setting out a set of obligations relating to personal data breaches and limiting their occurrence and consequences. This includes the provisions on appropriate protective measures, the documentation of personal data breaches, their reporting to the supervisory authority and, where appropriate, notification to the individuals concerned.

First, I presented the EU regulation that preceded the applicability of the GDPR. This is the still relevant regulation for providers of publicly available electronic communications services. However, my main focus has been on the applicable provisions of GDPR. I have looked at this both in terms of legislative development and by analysing in detail the obligations related to personal data breaches. As part of the holistic approach, there is also a mention of the related provisions transposed into national laws of Member States on the basis of Directive 2016/680. I then offered a more detailed discussion, in the main part of which I have focused on the functional interpretation in an attempt to define the purposes of the presented GDPR provisions. I approached this in three ways. I found (i) the purpose according to the text of the provision, (ii) the purpose captured in the recitals, and (iii) the purpose from an objective point of view. I further provided a brief analysis of the regulation of security breach obligations in US law.

I conclude this chapter by identifying significant obstacles to achieving the purpose of these obligations. Specifically, in the case of the reporting obligation, there is a conflict of interest that discourages the obliged entity from complying with the reporting obligation and the limited ability of the supervisory authority to obtain relevant information through other means.

Technological perspective: However, the intention in this publication is not to limit myself to a static discussion of current regulatory landscape, but to confront it with the highly dynamic trend of new practices and patterns of personal data processing, for which I have chosen the term Internet of Things. I have devoted Chapter Four to an introduction to this context. Here I first proceeded to define the concept of the Internet of Things. Subsequently, I revealed new forms and patterns of personal data processing in this context. These are related not only to the increasing scope of personal data processing, but also to the diversity of the structure of the processes

in question and the proliferation of automated machine-to-machine communication. The ubiquity of the processing then leads to an impending lack of awareness of the data subject of this processing, which makes its scope, and thus the extent of the potential harm resulting from a personal data breach, unforeseeable. I have described this increase in threats using the example of the development of the Internet of Things in video surveillance systems. It aptly reflects the often-stealthy nature of these devices. In addition, I have paid attention to the amplifying effect of cloud computing and the offloading of databases to big data.

Another level I paid attention to was the issue of security assurance. Here, I pointed out the security limitations of many Internet of Things devices, related, among other things, to the problem of updating and patching software. To get a better idea of the challenges outlined, I then proceeded to analyse three important scenarios, each of which highlights a different aspect of the transformation of personal data processing in this context. Thus, I have paid attention to (i) the impact of automated communication on the extent of personal data sharing between devices, (ii) the dynamics of smart city interaction and ad hoc processing by joint controllers, and (iii) the growing importance of micro-enterprises.

In analysing automated machine-to-machine communication in autonomous device environments, I first introduce existing communication standards for the Internet of Things. Subsequently, I focus on the 5G telecommunication standards. The conclusion from this perspective is that more frequent personal data breaches with more noticeable impacts can be expected in the Internet of Things environment, as well as more frequent failures to detect and properly report significant personal data breaches.

The second specific perspective was the direct and indirect interdependencies of smart city networks. Here, I focused on the implications of the interplay between existing and new infrastructure, as well as the indirect modular dependencies between elements. I uncovered new risks of complex processing within networked interconnections, thus shaping a series of ad hoc processing by joint controllers from a data protection law perspective. This poses additional obstacles to sufficiently motivating individual obliged entities to comply with their respective obligations.

Thirdly, I have focused on the Internet of Things for micro-enterprises. I first defined the concept of micro-enterprise. I then paid particular attention to the specific position of micro-enterprises in terms of cybersecurity and their often-inadequate security measures that lead to significant vulnerabilities. These can continue to grow significantly with the development of the Internet of Things and threaten data subjects and other entities in supply chains. I also found that micro-enterprises are hindered in implementing the necessary measures not only by limited personnel, budget and know-how, but also by the lack of specific guidance and good practice examples.

Based on the findings presented above, I have formulated four key areas in which I perceive a significant transformation of obligations related to personal data breaches in the context of Internet of Things. These are (i) an increase in the frequency and quantity of personal data breaches, (ii) an increase in the severity of harm due to personal data breaches, (iii) an increase in the difficulty of detecting personal data breaches, and (iv) an increase in the complexity and frequency of situations with joint controllers. I came to discover the additional obstacles that can be expected in this context, especially with regard to the timely detection of personal data breaches.

Economic perspective: Having identified the motivation of obliged entities to comply with the obligations discussed as a central obstacle in conjunction with the obligations, I supplemented the publication in Chapter Five by modelling the rational decision-making of the obliged entity in these situations. To this end, I first introduced the concept of risk and outlined the obstacles to its assessment. I then introduced a rational decision theory based on utility theory.

Then I shifted my attention to the issue of achieving adequate investment in cybersecurity. The starting point was the *Gordon* and *Loeb* model, which outlines the possibility of determining the optimal level of investment. However, this basic model has a number of significant limitations that numerous follow-up authors have sought to overcome. These extensions include, in particular, the consideration of externalities such as DDoS attacks, or the inclusion of benefits from information sharing, taking into account the interdependencies between entities and, where appropriate, the implications of their competitive position. The key conclusions from these

models are twofold. The first is the existence of an economic justification for the establishment of an obligation of appropriate security measures as found in Article 32 of GDPR. The second is the potential benefits of voluntary information sharing between entities.

In the next subsection, I focus on two models addressing the firm's decision to report personal data breaches. The earlier *Garcia* model is set in the US environment. Here the obstacle of asymmetric information about security breaches is discussed. The probability of detection and the penalties for failure to report are identified as key variables in the firm's decision whether to report or not. *Garcia* then focuses on determining the necessary level of sanction. His assumption is that a firm's motivation is driven by the desire to minimize costs. This can be used to enforce the reporting of security breaches. However, the regulatory setting of penalties for non-compliance must be reasonably severe.

This conclusion is complemented and developed in *Laube* and *Böhme's* model, although it appears to have been developed independently of *Garcia's* model. However, it effectively confirms the general transferability of the conclusions of *Garcia's* model to the European environment. In addition, *Laube* and *Böhme* also consider the extent of interdependence in the level of cyber security between firms as a relevant variable. However, even for them, the level of sanction and the probability of detection of non-reporting are crucial for the firm's decision. Unlike *Garcia*, they then focus on determining the necessary level of disclosure probability. As a result, they suggest that a reporting obligation, given an adequate level of enforcement, has social benefits if there is sufficient interdependence between the level of cybersecurity of firms, the supervisory authority is able to make meaningful use of the reported information, and there is little additional cost to the firm in disclosing the information.

Despite the inevitably simplistic logic of the models presented, it is clear that managing the risks associated with personal data protection involves a significant degree of uncertainty, which is due to the complexity of the issue, and further amplified by the potentially limited personnel or budgetary capacity of many controllers to overcome it. In doing so, I have inferred that investment in security measures may be enforced through the reverse

transferability of the harm incurred to the obliged entity and, where appropriate, the need for them may be reduced when measures are coordinated between firms, typically through cybersecurity information sharing organisations. Further, I have determined that the greatest obstacle in the form of a conflict of interest arises for the reporting obligation to a supervisory authority. Here, however, proper and timely compliance can only be effectively enforced on the obligated entity, in principle, through a combination of a sufficiently deterrent sanction for non-reporting and a reasonably high likelihood of detection of the personal data breach even without the obligated entity's report.

Research objective of the publication: The body of information and insights gathered in the previous chapters enabled me to arrive at the publication's research objective, i.e. to determine whether the current regulation of data breach obligations under GDPR has a viable application in the Internet of Things environment and, if so, what adjustments can be made to overcome identified challenges and obstacles. I discuss this primarily in Chapter Six.

Regarding the meaningful application of the regulation in the Internet of Things environment, I have concluded that the importance of the introduced obligations under GDPR in this context is further increasing, provided, however, that the conditions for their proper implementation by the obliged entities and the subsequent response by the supervisory authorities are set appropriately. This was prompted not only by the expectation of the increasing intensity of the threats, but also of their potential impact that may affect the data subjects concerned. Moreover, with the new technological reality, the complexity of processing processes and relationships between controllers will increase, which will mean a higher potential for indirect vulnerabilities and an increase in undetected breaches, which will cause all the more harm. Overall, this is an important issue not only from a data protection perspective, but also from a cybersecurity perspective.

Partial obstacles to the application of the relevant obligations to the Internet of Things environment have emerged in the course of this research

publication by taking the different perspectives into account. I have identified the following three as the main ones:

1. legal uncertainty regarding the interpretation of the incurrence and substance of the respective notification obligation,
2. the low motivation of obliged entities to implement adequate security measures and, in particular, to report their misconduct to the supervisory authority; and
3. limited possibilities of the supervisory authority to detect unreported personal data breaches.

I see these as a reflection of the gap between the normative concept of the obligations in question and their practical implementation, which is further widened with the rise of the Internet of Things. In Chapter Six, I therefore present possible solutions for adapting the relevant obligations to the proliferation of the Internet of Things, aimed at overcoming these three obstacles.

In order to enhance legal certainty, I attribute a key role to the introduction of security certification requirements for Internet of Things devices, complemented by available standards adapted to the Internet of Things environment. I then propose to overcome the problematic position of ad hoc joint controllers by introducing a leniency programme, as known from the competition law context.

In my opinion, sectoral initiatives to share information and experience should motivate obliged entities to take appropriate security measures. I see the introduction of functional class action frameworks as a further incentive for controllers to engage in prevention more intensively than they do now, and a more functional transfer of harm from data subjects back to controllers as motivation for their compliance.

I have identified the sufficiently probable detection of unreported breaches by the supervisory authority as one of the main prerequisites for the enforceability of proper compliance with the notification obligation under GDPR. To increase the likelihood of detection, I have proposed three solutions. Firstly, systematic cooperation between the supervisory authority and CSIRT teams, which will increase the professional capacity available to the supervisory authority and may give it access to new information from the

cybersecurity environment that will enable it to better detect unreported cases. Another option is to incentivise employees of the controller or processor to report breaches of obligations under GDPR as whistle-blowers. The recently harmonised EU framework to protect them from retaliation should contribute to this. Last but not least, I consider it appropriate to make use of the capacities of independent researchers and external specialists and to motivate them with reward schemes to detect unreported personal data breaches. For all of these solutions, I assume that they may not be fully effective in themselves, but the mere awareness of the obliged entity about the increasing ease of detection of non-compliance could be sufficient to increase its incentive to properly and consistently report detected personal data breaches.

Further research: A number of tools or solutions facilitating the adaptation of the framework of obligations related to personal data breaches to the Internet of Things context discussed in this research publication have already taken or are taking concrete form and can be expected to be applied in the future. Therefore, I see room for further research not only in a more detailed analysis of these solutions, in particular the security certification of Internet of Things devices, the formation of sectoral organisations for the sharing of cybersecurity information or the systematic cooperation between supervisory authorities and CSIRT teams, but above all in finding the appropriate balance and synergy between these interrelated solutions.

LITERATURA A DALŠÍ POUŽITÉ ZDROJE

Právní předpisy

Národní právní předpisy

Zákon č. 127/2005 Sb. o elektronických komunikacích, ve znění pozdějších předpisů.

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti.

Primární právo EU

Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts. In: EUR-Lex.

Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství, podepsaná v Lisabonu dne 13. prosince 2007.

Smlouva o fungování Evropské unie.

Sekundární právo EU

Směrnice Rady 85/374/EHS ze dne 25. července 1985 o sbližování právních a správních předpisů členských států týkajících se odpovědnosti za vadné výrobky.

Směrnice Rady 93/42/EHS ze dne 14. června 1993 o zdravotnických prostředcích.

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Směrnice 98/8/ES ze dne 16. února 1998 o uvádění biocidních přípravků na trh.

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422).

Oznámení Komise o ochraně před pokutami a snížení pokut v případech kartelů. Úř. věst. C 298, 8. 12. 2006.

Směrnice Evropského parlamentu a Rady 2007/47/ES ze dne 5. září 2007, kterou se mění směrnice Rady 90/385/EHS o sbližování právních předpisů členských států týkajících se aktivních implantabilních zdravotnických prostředků.

Nařízení Evropského parlamentu a Rady (ES) č. 661/2009 ze dne 13. července 2009 o požadavcích pro schvalování typu motorových vozidel, jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla z hlediska obecné bezpečnosti.

Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.

Nařízení Komise (EU) 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.

Rozhodnutí Rady 2013/488/EU ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU a dále pak soubor dohod o bezpečnostních postupech pro výměnu a ochranu utajovaných informací mezi EU a třetími státy.

Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě.

Směrnice Evropského parlamentu a Rady 2014/35/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se dodávání elektrických zařízení určených pro používání v určitých mezích napětí na trh.

Směrnice Evropského parlamentu a Rady 2014/53/EU ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES.

Nařízení Evropského parlamentu a Rady (EU) 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.

Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

Směrnice Evropského parlamentu a Rady (EU) 2016/943 ze dne 8. června 2016 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním.

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU.

Nařízení Evropského parlamentu a Rady (EU) 2018/644 ze dne 18. dubna 2018 o službách přeshraničního dodávání balíků.

Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES. In: EUR-Lex

Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti").

Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou.

Směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU.

Směrnice Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie.

Směrnice Evropského parlamentu a Rady (EU) 2020/1828 ze dne 25. listopadu 2020 o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES.

Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).

Americké právní předpisy

Gramm–Leach–Bliley Act of 1999, Public Law 106–102, 113 Stat. 1338. In: *govinfo.gov*

110 STAT. 1936 Public Law 104-191 Health Insurance Portability and Accountability Act, 1996. In: *govinfo.gov*

Kansas Statute, 2006. In: *ksrevisor.org*

Pennsylvania Statutes Title 73 Chapter 43, 2006. In: *privacylaw.proskauer.com*

Ohio Revised Code Title 13 Chapter 1349, 2007. In: *codes.ohio.gov*

Wisconsin Statutes Chapter 134, 2007. In: *docs.legis.wisconsin.gov*

123 STAT. 226 Public Law 111-5 Health Information Technology for Economic and Clinical Health Act, 2009. In: *hhs.gov*

Maine Revised Statute Title 10 Chapter 210-B, 2009. In: *mainelegislature.org*

Texas Business and Commerce Code Chapter 521, 2009. In: *statutes.capitol.texas.gov*

Tennessee Code Title 47, 2010. In: *law.justia.com*

Utah Code Title 13 Chapter 44, 2010. In: *law.justia.com*

Louisiana Revised Statute 51, 2011. In: *law.justia.com*

Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) (2012). In: *govinfo.gov*

Rhode Island General Laws Title 11, 2012. In: *law.justia.com*

Florida Statute Chapter 501, 2014. In: *leg.state.fl.us*

Idaho Statute Title 28 Chapter 51, 2014. In: *legislature.idaho.gov*

Kentucky Revised Statute Chapter 365, 2014. In: *law.justia.com*

North Carolina Statute, 2015. In: *ncleg.net*

Washington Statute Title 19 Chapter 255, 2015. In: *app.leg.wa.gov*

California Civil Code, 2017. In: *leginfo.legislature.ca.gov*

Delaware Code Title 6 Chapter 12B, 2017. In: *delcode.delaware.gov*

Indiana Code Title 24 Article 4.9, 2017. In: *iga.in.gov*

Iowa Statute Title 16 Chapter 715C, 2017. In: *legis.iowa.gov*

Montana Code Title 30 Chapter 14 Part 17, 2017. In: *leg.mt.gov*

Nevada Revised Statute Chapter 603A, 2017. In: *leg.state.nv.us*

North Dakota Century Code, 2017. In: *legis.nd.gov*

Alaska Statute Title 45 Chapter 48, 2018. DOI: https://doi.org/10.1525/9780520962026-011

Oregon Revised Statute Chapter 646A, 2018. In: *oregonlaws.org*

Wyoming Statues Title 40 Chapter 12, 2018. In: *advance.lexis.com*

Arkansas Code Title 4 Chapter 110, 2019. In: *advance.lexis.com*

Code of Georgia Title 10 Chapter 1, 2019. In: *advance.lexis.com*

Hawaii Revised Statute, 2019. In: *capitol.hawaii.gov*

Laws of Puerto Rico Title TEN, 2019. In: *advance.lexis.com*

Massachusetts General Law Part I Title XV Chapter 93H, 2019. In: *malegislature.gov*

Mississippi Code Title 75 Chapter 24, 2019. In: *advance.lexis.com*

The Laws of New York General Business Article 39-F, 2019. In: *nysenate.gov*

Ostatní právní předpisy

Bundesdatenschutzgesetz, BGBl. I S. 66, alte Fassung. In: *dejure.org*

Zákon č. 54/2019 Z. z. o ochrane oznamovateľov protispoločenskej činnosti a o zmene a doplnení niektorých zákonov. In: *slov-lex.sk*

Judikatura

Soudní dvůr Evropské unie

Rozhodnutí SDEU ze dne 19. 10. 2016 ve věci *Breyer*, C-582/14.

Rozhodnutí SDEU ze dne 5. 6. 2018 ve věci *Wirtschaftsakademie Schleswig-Holstein,* C-210/16.

Nejvyšší soud Spojených států amerických

Rozhodnutí SC USA ve věci *Clapper proti Amnesty International*, 568 U.S. 398 (2013).

Rozhodnutí SC USA ve věci *Spokeo, Inc. proti Robins*, 136 S.Ct. 1540 (2016).

Další americké soudy

Rozhodnutí United States Court of Appeals for the Ninth Circuit ve věci *Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018).

Rozhodnutí United States Court of Appeals for the Fourth Circuit ve věci *Hutton proti Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018).

Monografie, odborné články, sborníky a další online zdroje

3GPP. Standards for the IoT. *The Mobile Broadband Standard* [online]. 2016 [cit. 16. 9. 2021]. Dostupné z: https://www.3gpp.org/news-events/1805-iot_r14

3GPP. About 3GPP. *The Mobile Broadband Standard* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.3gpp.org/about-3gpp

3GPP. Release 15. *The Mobile Broadband Standard* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.3gpp.org/release-15

3GPP. Release 16. *The Mobile Broadband Standard* [online]. 2020 [cit. 12. 7. 2020]. Dostupné z: https://www.3gpp.org/release-16

AAZAM, M. et al. Cloud-based smart waste management for smart cities. In: *2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)* [online]. 2016, s. 188–193. DOI: https://doi.org/10.1109/CAMAD.2016.7790356

ABDMEZIEM, Riad a Djamel TANDJAOUI. Internet of Things: Concept, Building blocks, Applications and Challenges. *ArXiv* [online]. 2014, roč. 2014. Dostupné z: https://arxiv.org/pdf/1401.6877.pdf

ABIRESEARCH. Smart Cars and the IoT. *ABIresearch* [online]. AN-1792, 2014 [cit. 15. 7. 2020]. Dostupné z: https://www.abiresearch.com/market-research/product/1019236-smart-cars-and-the-iot/

ABRAMS, Rachel. Target to Pay $18.5 Million to 47 States in Security Breach Settlement. *The New York Times* [online]. 2017 [cit. 4. 3. 2020]. ISSN 0362-4331. Dostupné z: https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

ADAMS, Maurice a Jacco BOMHOFF (eds.). *Practice and Theory in Comparative Law* [online]. Cambridge: Cambridge University Press, 2012 [cit. 14. 7. 2020]. ISBN 978-1-107-01085-7. DOI: https://doi.org/10.1017/CBO9780511863301

ADEGBIJA, Tosiron et al. Microprocessor Optimizations for the Internet of Things: A Survey. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* [online]. 2018, roč. 37, č. 1, s. 7–20. ISSN 1937-4151. DOI: https://doi.org/10.1109/TCAD.2017.2717782

ALGARNI, Abdullah M. a Yashwant K. MALAIYA. A consolidated approach for estimation of data security breach costs. In: *2016 2nd International Conference on Information Management (ICIM)* [online]. London: IEEE, 2016, s. 26–39. DOI: https://doi.org/10.1109/INFOMAN.2016.7477530

ALMEIDA, Virgilio A. F., Danilo DONEDA a Marília MONTEIRO. Governance Challenges for the Internet of Things. *IEEE Internet Computing* [online]. 2015, roč. 19, č. 4, s. 56–59. ISSN 1089-7801. DOI: https://doi.org/10.1109/MIC.2015.86

ALSHAHAB, Sharifah Fadhilah a Derrick A. PAULO. After seven months, here's what South Korea can teach us about 5G. *CNA* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.channelnewsasia.com/news/cna-insider/what-south-korea-first-country-launch-5g-network-can-teach-us-12056726

AMAN, Waqas a Einar SNEKKENES. Managing security trade-offs in the Internet of Things using adaptive security. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* [online]. 2015, s. 362–368. DOI: https://doi.org/10.1109/ICITST.2015.7412122

An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. *California legislative information* [online]. 26. 9. 2002 [cit. 13. 7. 2020]. Dostupné z: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200120020SB1386

ANAND, Paul. *Foundations of Rational Choice Under Risk*. Oxford, New York: Oxford University Press, 1995, 174 s. ISBN 978-0-19-877442-6.

ANDERSON, Janna a Lee RAINIE. *The Internet of Things Will Thrive by 2025* [online]. Washington D.C.: Pew Research Center 2014 [cit. 19. 5. 2020]. Dostupné z: https://www.pewresearch.org/internet/2014/05/14/internet-of-things/

ANDERSON, Marie Karen, Otto Anker NIELSEN a Carlo Giacomo PRATO. Multimodal route choice models of public transport passengers in the Greater Copenhagen Area. *EURO Journal on Transportation and Logistics* [online]. 2014, s. 1–25. ISSN 2192-4376, 2192-4384. DOI: https://doi.org/10.1007/s13676-014-0063-3

ANDERSON, Ross et al. *Security Economics and the Internal Market* [online]. Report/Study. Heraklion: ENISA 2008 [cit. 18. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/archive/economics-sec

ANDRUKIEWICZ, Elżbieta, Scott CADZOW a Sławomir GÓRNIAK. *IoT Security Standards Gap Analysis* [online]. Report/Study v 1.0. Heraklion: ENISA 2018 [cit. 18. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

ANGELIDOU, Margarita. Smart city policies: A spatial approach. *Cities* [online]. 2014, roč. 41, Supplement 1, Current Research on Cities, s. 3–11. ISSN 0264-2751. DOI: https://doi.org/10.1016/j.cities.2014.06.007

ANSIP, Andrus. Speech by Vice-President Ansip at Bruegel annual meeting: "Productivity, innovation and digitalisation – which global policy challenges?" *European Commission* [online]. 2015 [cit. 27. 9. 2021]. Dostupné z: https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/speech-vice-president-ansip-bruegel-annual-meeting-productivity-innovation-and-digitalisation-which_en

ANTHOPOULOS, Leonidas, Marijn JANSSEN a Vishanth WEERAKKODY. A Unified Smart City Model (USCM) for smart city conceptualization and benchmarking. *International Journal of Electronic Government Research* [online]. 2016, roč. 12, č. 2, s. 77–93. ISSN 1548-3886. DOI: https://doi.org/10.4018/IJEGR.2016040105

ANTON-HARO, Carles a Mischa DOHLER. *Machine-to-machine (M2M) Communications: Architecture, Performance and Applications*. Cambridge: Elsevier, 2014, 427 s. ISBN 978-1-78242-110-8. DOI https://doi.org/10.1016/B978-1-78242-102-3.00001-0

ANTONOPOULOS, Nick a Lee GILLAM. *Cloud Computing: Principles, Systems and Applications*. Londýn: Springer, 2017. ISBN 978-3-319-54645-2.

ARMSTRONG, Gary a Clive NORRIS. *The Maximum Surveillance Society: The Rise of CCTV*. 1. vyd. Oxford; New York: Berg Publishers, 1999, 256 s. ISBN 978-1-85973-226-7.

AUERBACH, Gedalia. Urban planning: Politics vs. Planning and Politicians vs. Planners. *Horizons in Geography*. 2012, č. 79/80, s. 49–69. ISSN 0334-3774.

AURONEN, Lauri. Asymmetric Information: Theory and Applications. *Semin. Strateg y Int. Business*. 2003.

BAHETI, Radhakisan a Helen GILL. Cyber-physical Systems. In: SAMAD, Tariq a Anuradha ANNASWAMY (eds.). *The Impact of Control Technolog y* [online]. New York: IEEE Control Systems Society, 2011, s. 161–166. Dostupné z: http://ieeecss.org/general/impact-control-technology

BACHLECHNER, Daniel et al. IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten Abschlussbericht. *Bundesministerium für Wirschaft und Energie* [online]. 2016 [cit. 25. 5. 2020]. Dostupné z: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf?__blob=publicationFile&v=4

BAKER, Tom. On the Genealogy of Moral Hazard. *Texas Law Review*, 1996, roč. 75, s. 237.

BARFIELD, Woodrow (ed.). *Fundamentals of Wearable Computers and Augmented Reality*. 2. vyd. Boca Raton: CRC Press, 2015, 739 s. ISBN 978-1-4822-4350-5.

BARREIRA, Inigo et al. Standards Supporting Certification. Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes. *ENISA* [online]. Report/Study ISBN 978-92-9204-329-2. Heraklion: ENISA, 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-ii

BARYSHNIKOV, Yuliy. IT Security Investment and Gordon-Loeb's 1/e Rule. *WEIS Conference,* 2012, roč. 2012, s. 6.

BATTY, M. et al. Smart cities of the future. *The European Physical Journal Special Topics* [online]. 2012, roč. 214, č. 1, s. 481–518. ISSN 1951-6355, 1951-6401. DOI: https://doi.org/10.1140/epjst/e2012-01703-3

BAUTISTA, Gregory, Jeremy T. MERKEL a Alex MOH. (Another) Federal Data Breach Notification Law Introduced in Congress. *The National Law Review* [online]. 2017 [cit. 24. 5. 2021]. Dostupné z: https://www.natlawreview.com/article/another-federal-data-breach-notification-law-introduced-congress

BAUWENS, Jan et al. Portability, compatibility and reuse of MAC protocols across different IoT radio platforms. *Ad Hoc Networks* [online]. 2019, roč. 86, s. 144–153. ISSN 1570-8705. DOI: https://doi.org/10.1016/j.adhoc.2018.11.013

BENTHAM, Jeremy. *An Introduction to the Principles of Morals and Legislation* [online]. London: T. Payne and Son, 1780 [cit. 16. 7. 2020]. DOI https://doi.org/10.1093/oseo/instance.00077240. Dostupné z: http://www.koeblergerhard.de/Fontes/BenthamJeremyMoralsandLegislation1789.pdf

BETTS, Mitch. DP crime bill toughened. *Computerworld*, 1984, roč. 18, č. 27, s. 2. ISSN 0010-4841.

BISOGNI, Fabio, Hadi ASGHARI a Michel J. G. VAN EETEN. Estimating the size of the iceberg from its tip. In: *16th Annual Workshop on the Economics of Information Security*: *WEIS 2017* [online]. San Diego: University of California, 2017 [cit. 12. 7. 2020]. Dostupné z: https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_54.pdf

BJÖRCK, Fredrik et al. Cyber Resilience – Fundamentals for a Definition. In: ROCHA, Alvaro et al. (eds.). *New Contributions in Information Systems and Technologies* [online]. Cham: Springer International Publishing, 2015, s. 311–316, Advances in Intelligent Systems and Computing. ISBN 978-3-319-16486-1. DOI: https://doi.org/10.1007/978-3-319-16486-1_31

BLACK'S LAW DICTIONARY. Principal-Agent Model Definition. *UpCounsel* [online]. 1999. [cit. 17. 7. 2020]. Dostupné z: https://www.upcounsel.com/principal-agent-model-definition

BLOOMBERG, Scott. Tech Industry & Consumer Advocates Share Support for Federal Data-Privacy Legislation, Differ on the Details. *Security, Privacy and the Law* [online]. 2018 [cit. 24. 5. 2021]. Dostupné z: https://www.securityprivacyandthelaw.com/2018/10/tech-industry-consumer-advocates-share-support-for-federal-data-privacy-legislation-differ-on-the-details/

BOASIAKO, Kwabena Antwi a Michael O'CONNOR KEEFE. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. *SSRN Electronic Journal* [online]. 2018 [cit. 5. 9. 2021]. ISSN 1556-5068. DOI: https://doi.org/10.2139/ssrn.3191692

BOGDAN, Michael. *Comparative Law*. Stockholm: Springer, 1994, 250 s. ISBN 978-90-6544-861-3.

BOWSKILL, Jerry a John DOWNIE. Extending the capabilities of the human visual system: an introduction to enhanced reality. *ACM SIGGRAPH Computer Graphics* [online]. 1995, roč. 29, č. 2, s. 61–65. ISSN 0097-8930. DOI: https://doi.org/10.1145/204362.204378

BYOD. *Academic Dictionaries and Encyclopedias* [online]. 2013 [cit. 16. 7. 2020]. Dostupné z: https://new_words.enacademic.com/36/BYOD

BOYES, Hugh, Roy ISBELL a Tim WATSON. Critical Infrastructure in the Future City: Developing Secure and Resilient Cyber-Physical Systems. In: *Critical Information Infrastructures Security 9th International Conference, CRITIS 2014, Limassol, Cyprus, October 13–15, 2014, Revised Selected Papers*. New York: Springer International Publishing, 2016. ISBN 978-3-319-31663-5.

BRACY, Jedidiah a Sam PFEIFLE. WP29 Weighs In on the GDPR Trilogue Process. *IAPP* [online]. 2015. [cit. 13. 7. 2020]. Dostupné z: https://iapp.org/news/a/wp29-weighs-in-on-the-gdpr-trilogue-process-2/

BRIGGS, Bill. Tech Trends 2014, Inspiring Disruption. *Deloitte Consulting* [online]. 2014 [cit. 1. 6. 2020]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology/gx-cons-tech-trends-2014-inspiring-disruption.pdf

BRIGGS, Guy. The Intelligent City: Ubiquitous Network of Humane Environment. In: JENKS, Michael a Nicola DEMPSEY. *Future Forms and Design for Sustainable Cities*. Routledge, 2005, s. 31–53. ISBN 978-0-7506-6309-0.

BROOME, John. *Weighing Goods: Equality, Uncertainty and Time*. Oxford: Wiley-Blackwell, 1995, 268 s. ISBN 978-0-631-19972-4.

BROŽOVÁ, Jana. V Židlochovicích na Brněnsku vyroste ukázková čtvrť budoucnosti. *Bydlet.cz* [online]. 2020 [cit. 15. 7. 2020]. Dostupné z: https://www.bydlet.cz/551306-v-zidlochovicich-na-brnensku-vyroste-ukazkova-ctvrt-budoucnosti/

BUGEJA, Joseph, Désirée JÖNSSON a Andreas JACOBSSON. An Investigation of Vulnerabilities in Smart Connected Cameras. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* [online]. 2018, s. 537–542. DOI: https://doi.org/10.1109/PERCOMW.2018.8480184

BUCHERER, Eva a Dieter UCKELMANN. Business Models for the Internet of Things. In: UCKELMANN, Dieter, Mark HARRISON a Florian MICHAHELLES (eds.). *Architecting the Internet of Things* [online]. Berlin, Heidelberg: Springer, 2011, s. 253–277 [cit. 16. 7. 2020]. ISBN 978-3-642-19157-2. DOI: https://doi.org/10.1007/978-3-642-19157-2_10

BURIAN, David a Zuzana RADIČOVÁ. K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR). *Právní prostor* [online]. 2016 [cit. 13. 7. 2020]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr

BURTON, Cédric. Article 32. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 630–639. ISBN 978-0-19-882649-1. DOI https://doi.org/10.1093/oso/9780198826491.003.0068

BUSINESSWIRE. Navigant Research's Smart City Tracker 2Q19 Highlights 443 Projects Spanning 286 Cities Around the World. *Businesswire* [online]. 2019 [cit. 15. 7. 2020]. Dostupné z: https://www.businesswire.com/news/home/20190620005092/en/Navigant-Research%E2%80%99s-Smart-City-Tracker-2Q19-Highlights

BYGRAVE, Lee A. Legal Scholarship on Data Protection: Future Challenges and Directions. In: *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde Liber Amicorum Yves Poullet*. 1. vyd. Brussels: Larcier, 2018, s. 493–504. ISBN 978-2-8079-0346-3.

BYGRAVE, Lee A. a Luca TOSONI. Article 4(1). In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 103–115. ISBN 978-0-19-882649-1. DOI https://doi.org/10.1093/oso/9780198826491.003.0007

CALIFORNIA OFFICE OF PRIVACY PROTECTION. Recommended Practices on Notice of Security Breach Involving Personal Information. *California Office of Privacy Protection* [online]. 2012 [cit. 24. 5. 2021]. Dostupné z: https://bcourses.berkeley.edu/courses/1463120/files/71435731/download?verifier=b6heYnAye5G7U34dAxoiRw7iSzcRwYOv6lWK-fxC5&wrap=1

CENTRUM KYBERNETICKÉ BEZPEČNOSTI. Kybernetické útoky míří na strategická odvětví, aktuálně na těžební společnost OKD. *Centrum kybernetické bezpečnosti* [online]. 2019 [cit. 13. 7. 2020]. Dostupné z: https://centrumkyberbezpecnosti.cz/kyberneticke-utoky-miri-na-strategicka-odvetvi-aktualne-na-tezebni-spolecnost-okd/

CICHONSKI, Paul et al. *Computer Security Incident Handling Guide* [online]. NIST Special Publication (SP) 800-61 Rev. 2. Gaithersburg, MA: National Institute of Standards and Technology 2012 [cit. 12. 7. 2020]. DOI: https://doi.org/https://doi.org/10.6028/NIST.SP.800-61r2

CILFONE, Antonio et al. Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies. *Future Internet* [online]. 2019, roč. 11, č. 4, s. 99–133. ISSN 1999-5903. DOI: https://doi.org/doi:10.3390/fi11040099

CIMPANU, Catalin. New IoT Botnet Rises Feeding on Vulnerable Security Cameras. *BleepingComputer* [online]. 2017 [cit. 15. 7. 2020]. Dostupné z: https://www.bleepingcomputer.com/news/security/new-iot-botnet-rises-feeding-on-vulnerable-security-cameras/

CISCO. Cisco Annual Internet Report (2018–2023). *Cisco* [online]. 2020 [cit. 19. 5. 2020]. Dostupné z: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

CISOMAG. Darknet Markets Make Malware Buying Easy: Research. *Cyber Security Magazine* [online]. 2020 [cit. 22. 5. 2020]. Dostupné z: https://www.cisomag.com/darknet-markets-make-malware-buying-easy-research/

CLAESSON, Andreas a Tor E. BJØRSTAD. *"Out of Control"– A Review of Data Sharing by Popular Mobile Apps* [online]. 1.0. Oslo: Norwegian Consumer Council, 2020 [cit. 15. 7. 2020]. Dostupné z: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf

CLARKE, Roger. The prospects of easier security for small organisations and consumers. *Computer Law & Security Review* [online]. 2015, roč. 31, č. 4, s. 538–552. ISSN 0267-3649. DOI: https://doi.org/10.1016/j.clsr.2015.05.004

CLOUDFLARE. What is the Mirai Botnet? *Cloudflare* [online]. 2020 [cit. 22. 5. 2020]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Code of Federal Regulations. 12 CFR Appendix F to Part 225 – Interagency Guidelines Establishing Information Security Standards. *Gov.info* [online]. 2012 [cit. 24. 5. 2021]. Dostupné z: https://www.govinfo.gov/app/details/CFR-2012-title12-vol3/CFR-2012-title12-vol3-part225-appF/summary

COFFMAN, Kerry a Andrew M. ODLYZKO. Internet Growth: Is There a "Moore's Law" for Data Traffic? *Handbook of Massive Data Sets* [online]. 2002, roč. 4. DOI: https://doi.org/10.1007/978-1-4615-0005-6_3

COGLIANESE, Cary. Performance-based regulation: concepts and challenges. In: BIGNAMI, Francesca a David ZARING (eds.). *Comparative Law and Regulation.Understanding the Global Regulatory Process.* Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2016, Comparative Law and Regulation. ISBN 978-1-78254-561-3.

COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michingan Journal of Law Reform,* 2017, roč. 50, č. 3, s. 525–563.

COGLIANESE, Cary, Jennifer NASH a Todd OLMSTEAD. Performance-based regulation: Prospects and limitations in health, safety and environmental protection. *Administrative Law Review*, 2003, American Bar Association, roč. 55, č. 4, s. 705–729. ISSN 0001-8368.

COLLELA, Paolo. 5G and IoT: Ushering in a new era. *Ericsson* [online]. 2017 [cit. 16. 9. 2021]. Dostupné z: https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/5g-and-iot-ushering-in-a-new-era

COLUMBUS, Louis. 2018 Roundup of Internet of Things Forecasts and Market Estimates. *Forbes* [online]. 2018, roč. 2018, č. 13.12 [cit. 16. 4. 2020]. Dostupné z: https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and--market-estimates/

COMPUTERS, PRIVACY & DATA PROTECTION. Previous editions of CPDP. *Archive CPDP Conferences* [online]. 2020 [cit. 12. 7. 2020]. Dostupné z: https://www.cpdpconferences.org/archive

COSTA, Luiz. *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*. Cham: Springer International Publishing, 2016. ISBN 978-3-319-39197-7. DOI https://doi.org/10.1007/978-3-319-39198-4_1

COVINGTON & BURLING LLP. Analysis of White House Data Breach Notification Bill. *The National Law Review* [online]. 2015 [cit. 14. 7. 2020]. Dostupné z: https://www.natlawreview.com/article/analysis-white-house-data-breach-notification-bill

CSIRT.CZ. O nás. *CZ.NIC* [online]. 2019 [cit. 26. 2. 2020]. Dostupné z: https://csirt.cz/cs/o-nas/

CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ (národní CSIRT ČR) za rok 2020* [online]. Praha: CSIRT.CZ, 2021, s. 4 [cit. 20. 10. 2021]. Dostupné z: https://docplayer.cz/211881339-Zprava-o-cinnosti-csirt-cz-narodniho-csirt-cr-za-rok-2020.html

CU, Tung. Artificial Intelligence for Cybersecurity: A Review. *Faculty Research and Creative Activities Symposium* [online]. 2019. Dostupné z: https://neiudc.neiu.edu/frcas/2019/schedule/49

CUSTERS, Bart a Helena URŠIČ. Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection. *International Data Privacy Law* [online]. 2016 [cit. 15. 7. 2020]. DOI https://doi.org/10.1093/idpl/ipv028. Dostupné z: http://data-reuse.eu/wp-content/uploads/2016/01/International-Data-Privacy-Law-2016-Custers.pdf

CUTHBERTSON, Anthony. Alexa needs to be banned from the bedroom, privacy expert says. *The Independent* [online]. 2019 [cit. 16. 7. 2020]. Dostupné z: https://www.independent.co.uk/life-style/gadgets-and-tech/news/alexa-privacy-amazon-echo-delete-recordings-a9249951.html

ČTK. Provoz benešovské nemocnice ochromil počítačový virus. *ČTK České noviny* [online]. 2019 [cit. 13. 7. 2020]. Dostupné z: https://www.ceskenoviny.cz/zpravy/provoz-benesovske-nemocnice-ochromil-pocitacovy-virus/1831202

DE BRUYNE, M. F. Data breach notification and the risk of over-notification under the GDPR. A comparative analysis of US and EU experiences in practice. Master's Thesis. Tilburg: Tilburg University, 2016. Dostupné z: http://arno.uvt.nl/show.cgi?fid=140479 [cit. 19. 3. 2021].

DE GROOT, Juliana. The History of Data Breaches. *Digital Guardian* [online]. 2018 [cit. 12. 7. 2020]. Dostupné z: https://digitalguardian.com/blog/history-data-breaches

DEPARTMENT OF HEALTH AND HUMAN SERVICES. *45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule* [online]. 2009 [cit. 24. 5. 2021]. Dostupné z: https://www.govinfo.gov/content/pkg/FR-2009-08-24/pdf/E9-20169.pdf

DEVINNEY, Fran. Bringing the power of AI to the Internet of Things. *Wired* [online]. 2018 [cit. 15. 7. 2020]. ISSN 1059-1028. Dostupné z: https://www.wired.com/brandlab/2018/05/bringing-power-ai-internet-things/

Digital Transformation of European Micro Enterprises. *DITEM* [online]. Blog & Case Studies, 2019 [cit. 16. 7. 2020]. Dostupné z: https://www.ditem.eu/blog

DIGITAL TRANSFORMATION MONITOR. Germany: Industrie 4.0. *Evropská komise* [online]. 2017 [cit. 5. 8. 2021]. Dostupné z: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf

DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. EU Data Protection Reform: What benefits for businesses in Europe? Fact sheet. *European Commission* [online]. 2016 [cit. 29. 9. 2021]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/factsheets_2016/data-protection-factsheet_01a_en.pdf

DRENNAN, Matthew. Economies: Diminishing Marginal Utility. *Challenge*, Taylor & Francis, Ltd., 2006, roč. 49, č. 5, s. 71–91. ISSN 0577-5132. DOI https://doi.org/10.2753/0577-5132490505

DROZDIAK, Natalia a Helene FOUQUET. Creepy Technologies Invade European Workplaces. *Bloomberg.com* [online]. 2020 [cit. 15. 7. 2020]. Dostupné z: https://www.bloomberg.com/news/articles/2020-05-20/creepy-technologies-invade-european-post-pandemic-workplaces

EDWARDS, Ward. Behavioral Decision Theory. *Annual Review of Psychology* [online]. 1961, roč. 12, č. 1, s. 473–498. DOI: https://doi.org/10.1146/annurev.ps.12.020161.002353

EHMANN, Eugen. *Lexikon für das IT-Recht 2017/2018. Spezialausgabe für Behörden*. 5. vyd. Heidelberg: Jehle, 2017. ISBN 978-3-7825-0606-9.

EIP-SCC. About Smart City Lighthouse Projects. *EIP-SCC* [online]. 2020 [cit. 15. 7. 2020]. Dostupné z: https://eu-smartcities.eu/projects/1972/description

EL-RAZEK, Mohamed Abd, M. B. ABDELHALIM a Hanady H. ISSA. Dynamic power reduction of microprocessors for IoT applications. In: *2016 28th International Conference on Microelectronics (ICM)*: *2016 28th International Conference on Microelectronics (ICM)* [online]. 2016, s. 297–300. DOI: https://doi.org/10.1109/ICM.2016.7847874

ENISA. Incentives and Challenges for Information Sharing in the Context of Network and Information Security. *ENISA* [online]. Report/Study, 2010 [cit. 18. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing

ENISA. Reference Incident Classification Taxonomy. *ENISA* [online]. 2018 [cit. 21. 10. 2021]. Dostupné z https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches. *ENISA* [online]. 2013 [cit. 7. 2. 2021]. Dostupné z: https://www.enisa.europa.eu/publications/dbn-severity

ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches. *ENISA* [online]. 2013 [cit. 25. 10. 2021]. Dostupné z: https://www.enisa.europa.eu/publications/dbn-severity

ENISA. *Guidelines for SMEs on the security of personal data processing*. 2016. ISBN 978-92-9204-209-7.

ENISA. Baseline Security Recommendations for IoT. *ENISA* [online]. Report/Study, 2017 [cit. 16. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ENISA. Information Sharing and Analysis Center (ISACs). Cooperative models. *ENISA* [online]. Report/Study, 2017 [cit. 18. 7. 2020]. ISBN 978-92-9204-239-4. Dostupné z: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

ENISA. Methodology for a Sectoral Cybersecurity Assessment. EU Cybersecurity Certification Framework. *ENISA* [online]. 2021 [cit. 20. 10. 2021]. Dostupné z: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment

ENISA. Public Private Partnerships (PPP). Cooperative models. *ENISA* [online]. 2017 [cit. 17. 7. 2020]. ISBN 978-92-9204-241-7. Dostupné z: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/

ENISA. Reference Incident Classification Taxonomy. *ENISA* [online]. 2018 [cit. 12. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

ENISA. Incident Reporting. European Union Agency for Cybersecurity. *ENISA* [online]. 2020 [cit. 13. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/topics/incident-reporting

ERAYDIN, Ayda a Tuna TASAN-KOK. *Resilience Thinking in Urban Planning.* Springer Science & Business Media, 2012, 256 s. ISBN 978-94-007-5476-8.

ETSI. *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements* [online]. ETSI EN 303 645 V2.1.1 (2020-06) [cit. 17. 7. 2020]. Dostupné z: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

EUROPEAN COMMISSION. *Communication from the Commission* [online]. COM/2010/0609 final. Brussels: European Commission, 2010 [cit. 24. 5. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0609&from=GA

EUROPEAN COMMISSION. Frequently asked questions on languages in Europe. *European Commission* [online]. 2013 [cit. 13. 7. 2020]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_825

EUROPEAN COMMISSION. Press release. Commission proposal on new data protection rules to boost EU Digital Single Market supported by Justice Ministers. *European Commission* [online]. 2015. [cit. 13. 7. 2020]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5176

EUROPEAN COMMISSION. *Fact Sheet of the European Commission. IoT Privacy, Data Protection, Information Security* [online]. Brussels: European Commission, 2016 [cit. 12. 7. 2020]. Dostupné z: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

EUROPEAN COMMISSION. Integration of Digital Technology. In: *European Digital Services Report* [online]. 2017 [cit. 12. 7. 2020]. Dostupné z: https://ec.europa.eu/digital-single-market/en/news/europes-digital-progress-report-2017

EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock* [online]. COM(2019) 374 final. Brussels: EU, 2019 [cit. 3. 3. 2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0374

EUROPEAN CYBER SECURITY ORGANISATION. *Position Paper. European Sector-Specific ISACs* [online]. WG 3 Sectoral demand. Brussels: European Cyber Security Organisation, 2018 [cit. 17. 7. 2020]. Dostupné z: https://ecs-org.eu/documents/publications/5c0a6a3aac673.pdf

EUROPEAN DATA PORTAL. Building apps with Open Data. *European Data Portal* [online]. 2017 [cit. 15. 7. 2020]. Dostupné z: https://www.europeandataportal.eu/en/news/building-apps-open-data

EUROPEAN DATA PROTECTION SUPERVISOR. *Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations* [online]. Brussels: European Data Protection Supervisor, 2015 [cit. 24. 5. 2021]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_annex_en_1.pdf

EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 3/2015 (with addendum) Europe's big opportunity* [online]. Brussels: European Data Protection Supervisor, 2015 [cit. 24. 5. 2021]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf

EUROPEAN DATA PROTECTION SUPERVISOR. The History of the General Data Protection Regulation. Timeline. *European Data Protection Supervisor* [online]. 2016 [cit. 24. 5. 2021]. Dostupné z: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

EUROPEAN PARLIAMENT. *Position of the European Parliament* [online]. EP-PE_TC2-COD(2007)0248. Strasbourg: European Parliament, 2009 [cit. 24. 5. 2021]. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TC+P6-TC2-COD-2007-0248+0+DOC+PDF+V0//EN

EUROPEAN POLICE OFFICE. *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. The Hague: European Police Office, 2016. ISBN 978-92-95200-75-3.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Access to data protection remedies in EU Member States* [online]. Vienna: European Union Agency for Fundamental Rights, 2013 [cit. 18. 7. 2020]. ISBN 978-92-9239-309-0. Dostupné z: https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

EVROPSKÁ KOMISE. *Návrh 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]. COM(2012) 11 final 2012/0011 (COD). Brusel: Evropská komise, 2012 [cit. 29. 4. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/PDF/?uri=CELEX:52012PC0011&from=EN

EVROPSKÝ PARLAMENT. *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]. COM(2012)0011-C7-0025/2012-2012/0011(COD). Štrasburk: Evropský parlament, 2014 [cit. 29. 4. 2021]. Dostupné z: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0212+0+DOC+PDF+V0//CS

EVROPSKÝ SBOR PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Pokyny 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679* [online]. 1/2019, verze 2.0 [cit. 17. 7. 2020]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_cs.pdf

EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES. *Accelerating innovation in Europe: Horizon 2020 SME Instrument impact report* [online]. 2017 Edition. Brussels: European Commission, 2017 [cit. 1. 10. 2021]. Dostupné z: https://ec.europa.eu/easme/sites/easme-site/files/accelerating_innovation_in_europe_horizon_2020_smei_impact_report.pdf

EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES. *Evaluation of support services for would-be entrepreneurs and newly established businesses : final report*. [online]. EASME/COSME/2018/017. Brussels: European Commission, 2019 [cit. 16. 7. 2020]. Dostupné z: http://op.europa.eu/en/publication-detail/-/publication/c396caad-e977-11e9-9c4e-01aa75ed71a1/language-en/format-PDF

EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES (EASME). *Annual Report on European SMEs 2018/2019, Research & Development and Innovation by SMEs* [online]. EASME/COSME/2017/031. Brusel: Evropská komise, 2019 [cit. 21. květen 2020]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/cadb8188-35b4-11ea-ba6e-01aa75ed71a1/language-en

FAHEEM et al. A Survey of Intelligent Car Parking System. *Journal of Applied Research and Technology* [online]. 2013, roč. 11, č. 5, s. 714–726. ISSN 1665-6423. DOI: https://doi.org/10.1016/S1665-6423(13)71580-3

FANG, Junbin et al. Position Paper on Recent Cybersecurity Trends: Legal Issues, AI and IoT. In: AU, Man Ho et al. (eds.). *Network and System Security*. New York: Springer International Publishing, 2018, s. 484–490, Lecture Notes in Computer Science. ISBN 978-3-030-02744-5. DOI https://doi.org/10.1007/978-3-030-02744-5_36

FANG, X. et al. Smart Grid – The New and Improved Power Grid: A Survey. *IEEE Communications Surveys Tutorials* [online]. 2011, roč. 14, č. 4, s. 944–980. ISSN 1553-877X. DOI: https://doi.org/10.1109/SURV.2011.101911.00087

FEDERAL TRADE COMMISSION. *16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule* [online]. 2002 [cit. 24. 5. 2021]. Dostupné z: https://www.govinfo.gov/content/pkg/FR-2002-05-23/pdf/02-12952.pdf#page=11

FEDERAL TRADE COMMISSION. *16 CFR Part 318 Health Breach Notification Rule; Final Rule* [online]. 2009 [cit. 24. 5. 2021]. Dostupné z: https://www.govinfo.gov/content/pkg/FR-2009-08-25/pdf/E9-20142.pdf

FEDERAL TRADE COMMISSION. *FTC Staff Report*: *Internet of Things. Privacy & Security in a Connected World* [online]. Washington D.C.: Federal Trade Commission 2015 [cit. 14. 7. 2020]. Dostupné z: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

FERDOUSI, Sifat. Network Slicing in Smart Cities. *University of California* [online]. 2018 [cit. 17. 10. 2021]. Dostupné z: http://networks.cs.ucdavis.edu/presentation2018/Sifat-08-17-2018.pdf

FERNANDES, Earlence et al. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? *IEEE Security Privacy* [online]. 2017, roč. 15, č. 4, s. 79–84. ISSN 1558-4046. DOI: https://doi.org/10.1109/MSP.2017.3151346

FINANCIAL AND BUSINESS TERMS. just-in-time. *Academic Dictionaries and Encyclopedias* [online]. 2012 [cit. 15. 7. 2020]. Dostupné z: https://business_finance.enacademic.com/21205/just-in-time

FINANCIAL AND BUSINESS TERMS. median. *Academic Dictionaries and Encyclopedias* [online]. 2012 [cit. 16. 7. 2020]. Dostupné z: https://business_finance.enacademic.com/21867/median

FINLEY, Klint. Nest's Hub Shutdown Proves You're Crazy to Buy Into the Internet of Things. *Wired* [online]. 2016 [cit. 15. 7. 2020]. ISSN 1059-1028. Dostupné z: https://www.wired.com/2016/04/nests-hub-shutdown-proves-youre-crazy-buy-internet-things/

FISCHHOFF, Baruch a John KADVANY. *Risk. A Very Short Introduction*. Oxford: Oxford University Press, 2011, 162 s., Very Short Introductions. ISBN 978-0-19-957620-3. DOI https://doi.org/10.1093/actrade/9780199576203.003.0001

FLORIDI, Luciano. *Information. A Very Short Introduction*. Oxford: Oxford University Press, 2010, 130 s. ISBN 978-0-19-955137-8.

FLORIDI, Luciano (ed.). The Onlife Manifesto. In: FLORIDI, Luciano (ed.). *The Onlife Manifesto: Being Human in a Hyperconnected Era* [online]. Cham: Springer International Publishing, 2015, s. 7–13 [cit. 15. 7. 2020]. ISBN 978-3-319-04093-6. DOI: https://doi.org/10.1007/978-3-319-04093-6_2

FRANCE 24. The global fallout of the Ashley Madison hack. *France 24* [online]. 2015 [cit. 24. 5. 2021]. Dostupné z: https://www.france24.com/en/20150820-global-fall-out-ashley-madison-hack

FREITAS, Alex A. Data Mining Tasks and Concepts. In: FREITAS, Alex A. (ed.). *Data Mining and Knowledge Discovery with Evolutionary Algorithms* [online]. Berlin, Heidelberg: Springer, 2002, Natural Computing Series, s. 13–43 [cit. 15. 7. 2020]. ISBN 978-3-662-04923-5. DOI: https://doi.org/10.1007/978-3-662-04923-5_2

FREITAS, Maria da Conceição a Miguel Mira da SILVA. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering and Management* [online]. Modestum, 2018, roč. 3, č. 4, s. 30. ISSN 2468-4376. DOI: https://doi.org/10.20897/jisem/3941

FRÖHLICH, Radek. Odůvodnění legislativních aktů Evropské unie. In: ŽATECKÁ, Eva et al. (eds.). *COFOLA 2011*: *Cofola 2011 The Conference Proceedings* [online]. Brno: Masarykova univerzita, 2011, s. 388–394 [cit. 12. 7. 2020]. Dostupné z: https://www.law.muni.cz/sborniky/cofola2011/files/sbornik.pdf

FRUHLINGER, Josh. The Mirai botnet explained: How IoT devices almost brought down the internet. *CSO Online* [online]. 2018 [cit. 22. 5. 2020]. Dostupné z: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

GAL-OR, Esther a Anindya GHOSE. The Economic Incentives for Sharing Security Information. *Information Systems Research* [online]. INFORMS, 2005, roč. 16, č. 2, s. 186–208. ISSN 1047-7047. DOI: https://doi.org/10.1287/isre.1050.0053

GARCIA, Michael E. *The Economics of Data Breach: Asymmetric Information and Policy Interventions*. Disertační práce. Columbus: The Ohio State University, 2013. Dostupné z: https://etd.ohiolink.edu/ap/10?0:NO:10:P10_ACCESSION_NUM:osu1365784884 [cit. 3. 4. 2021].

GARTNER. Press release: Gartner Predicts Outdoor Surveillance Cameras Will Be Largest Market for 5G Internet of Things Solutions Over Next Three Years. *Newsroom* [online]. 2019 [cit. 15. 7. 2020]. Dostupné z: https://www.gartner.com/en/newsroom/press-releases/2019-10-17-gartner--predicts-outdoor-surveillance-cameras-will-be

GARVIN, Alexander. *Urban Planning Today* [online]. NED-New edition. Minneapolis: University of Minnesota Press, 2006, A Harvard Design Magazine Reader [cit. 29. 3. 2021]. ISBN 978-0-8166-4756-9. Dostupné z: http://www.jstor.org/stable/10.5749/j.cttttw4v

GONZÁLEZ FUSTER, Gloria. Article 80. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1142–1152. ISBN 978-0-19-882649-1.

GORBENKO, Anna a Vladimir POPOV. Self-Learning Algorithm for Visual Recognition and Object Categorization for Autonomous Mobile Robots. In: HE, Xingui et al. (eds.). *Computer, Informatics, Cybernetics and Applications* [online]. Dordrecht: Springer Netherlands, 2012, s. 1289–1295, Lecture Notes in Electrical Engineering. ISBN 978-94-007-1839-5. DOI: https://doi.org/10.1007/978-94-007-1839-5_139

GORDON, Lawrence A. et al. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security* [online]. 2014, roč. 6, č. 1, s. 24–30. DOI: https://doi.org/10.4236/jis.2015.61003

GORDON, Lawrence A. a Martin P. LOEB. The economics of information security investment. *ACM Transactions on Information and System Security* [online]. 2002, roč. 5, č. 4, s. 438–457. ISSN 1094-9224. DOI: https://doi.org/10.1145/581271.581274

GORDON, Lawrence A., Martin P. LOEB a William LUCYSHYN. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* [online]. 2003, roč. 22, č. 6, s. 461–485. ISSN 0278-4254. DOI: https://doi.org/10.1016/j.jaccpubpol.2003.09.001

GREENBERG, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired* [online]. 2015 [cit. 5. 8. 2021]. ISSN 1059-1028. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired* [online]. 2018 [cit. 22. 5. 2020]. ISSN 1059-1028. Dostupné z: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

GROGAN, A. Driverless trains: It's the automatic choice. *Engineering & Technology* [online]. 2012, roč. 7, č. 5, s. 54–57. ISSN 1750-9645. DOI: https://doi.org/10.1049/et.2012.0514

GROMOVA, Ekaterina, Dmitriy TIMOKHIN a Galina POPOVA. The role of digitalisation in the economy development of small innovative enterprises. *Procedia Computer Science* [online]. 2020, roč. 169, Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA, 2019 (Tenth Annual Meeting of the BICA Society), held August 15-19, 2019 in Seattle, Washington, USA, s. 461–467. ISSN 1877-0509. DOI: https://doi.org/10.1016/j.procs.2020.02.224

GSA. More than 175 5G Commercial Networks Launched in 72 Countries/Territories. *totaltelecom* [online]. 23. 8. 2021 [cit. 18. 10. 2021]. Dostupné z: https://www.totaltele.com/510680/GSA-More-than-175-5G-Commercial-Networks-Launched-in-72-CountriesTerritories

GSMA. *LTE-M Commercialisation Case Study: How AT & T and Telstra Connect Million More IoT Devices* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.gsma.com/iot/wp-content/uploads/2019/02/201901_GSMA_LTE-M_Commercial_Case_Study-ATT_Telstra.pdf

GSMA. *NB-IoT Commercialisation Case Study: How China Mobile, China Telecom and China Unicom Enable Million More IoT Devices* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.gsma.com/iot/wp-content/uploads/2019/08/201902_GSMA_NB-IoT_Commercialisation_CaseStudy.pdf

GUCCIONE, Darren. What is the dark web? How to access it and what you'll find. *CSO Online* [online]. 2020 [cit. 15. 7. 2020]. Dostupné z: https://www.csoonline.com/article/3249765/what-is-the-dark-web--how-to-access-it-and-what-youll-find.html

Guidelines 01/2021 on Examples regarding Data Breach Notification. *EDPB* [online]. 2021 [cit. 10. 10. 2021]. Dostupné z: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en

HADNAGY, Christopher. *Social engineering The Art of Human Hacking*. Indianapolis: Wiley Publishing, 2011. ISBN 978-0-470-63953-5.

HALPERIN, Jean-Louis. Law in Books and Law in Action: The Problem of Legal Change. *Maine Law Review,* 2017, roč. 64, č. 1, s. 45. ISSN 0025-0651.

HANDTE, M. et al. An Internet-of-Things Enabled Connected Navigation System for Urban Bus Riders. *IEEE Internet of Things Journal* [online]. 2016, roč. 3, č. 5, s. 735–744. ISSN 2327-4662. DOI: https://doi.org/10.1109/JIOT.2016.2554146

HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti*. Disertační práce. Brno: Masarykova univerzita, Právnická fakulta, 2018. Dostupné z: https://is.muni.cz/auth/th/agnuc/ [cit. 12. 7. 2020].

HAY, Peter. *Law of the United States*. 2. vyd. München: C. H. Beck, 2005, 407 s. ISBN 3-406-53429-5.

HAYDEN, Ernie. Data breach protection requires new barriers. *SearchSecurity* [online]. 2013. [cit. 12. 7. 2020]. Dostupné z: https://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers

HAYES, Adam. Adverse Selection Definition. *Investopedia* [online]. 2020 [cit. 17. 7. 2020]. Dostupné z: https://www.investopedia.com/terms/a/adverseselection.asp

HISCOX. *The Hiscox Cyber Readiness Report 2017* [online]. Bermunda: Hiscox 2017 [cit. 16. 7. 2020]. Dostupné z: https://www.hiscox.com/documents/brokers/cyber-readiness-report.pdf

HOFMANN, Erik a Marco RÜSCH. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry* [online]. 2017, roč. 89, s. 23–34. ISSN 0166-3615. DOI: https://doi.org/10.1016/j.compind.2017.04.002

HOSSAIN, Anwar M., Pradeep K. ATREY a Abdulmotaleb El SADDIK. Smart mirror for ambient home environment. *IET Digital Library* [online]. 2007, s. 589–596. DOI: https://doi.org/10.1049/cp:20070431

HUANG, Derrick C., Qing HU a Ravi S. BEHARA. Economics of information security investment in the case of simultaneous attacks. 2006.

HUGHES, Thomas P. Technological Momentum. In: *SMITH, Merritt Roe a Leo MARX (eds.). Does Technology Drive History?: The Dilemma of Technological Determinism*. Cambridge, Massachusetts: MIT Press, 1994, s. 101–114. ISBN 978-0-262-69167-3.

HUSTINX, Peter. *Opinion of the European Data Protection Supervisor on the Communication from the Commission* [online]. Brussels: European Data Protection Supervisor, 2011 [cit. 24. 5. 2021]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf

CHAN, Mike. Why Cloud Computing is the Foundation of the Internet of Things. *Thorn Technologies* [online]. 2017 [cit. 15. 7. 2020]. Dostupné z: https://www.thorntech.com/2017/02/cloud-computing-foundation-internet-things/

CHAPPELOW, Jim. What Is the Free Rider Problem? *Investopedia* [online]. [cit. 17. 7. 2020]. Dostupné z: https://www.investopedia.com/terms/f/free_rider_problem.asp

CHEE, Foo Yun. Amazon's Alexa comes under scrutiny of Luxembourg privacy watchdog. *Reuters* [online]. 2019 [cit. 15. 7. 2020]. Dostupné z: https://uk.reuters.com/article/us-amazon-com-privacy-luxembourg-idUKKCN1UY27H

CHEN, James. What Is a Special Purpose Vehicle (SPV)? *Investopedia* [online]. 2020 [cit. 16. 7. 2020]. Dostupné z: https://www.investopedia.com/terms/s/spv.asp

CHERTOFF, Michael. A public policy perspective of the Dark Web. *Journal of Cyber Policy* [online]. 2017, roč. 2, č. 1, s. 26–38. ISSN 2373-8871. DOI: https://doi.org/10.1080/23738871.2017.1298643

IBM. Artificial Intelligence for Smarter Cybersecurity. *IBM Security* [online]. 2020 [cit. 16. 7. 2020]. Dostupné z: https://www.ibm.com/security/artificial-intelligence

IBM X-FORCE INCIDENT RESPONSE AND INTELLIGENCE SERVICES. *X-Force Threat Intelligence Index 2020* [online]. Armonk, NY: IBM, 2020 [cit. 3. 3. 2020]. Dostupné z: https://www.ibm.com/downloads/cas/DEDOLR3W

IDC. *The Changing Face of Data Security 2020 Thales Data Threat Report Global Edition* [online]. Paris: Thales, 2020 [cit. 3. 3. 2020]. Dostupné z: https://www.thalesesecurity.com/sites/default/files/2020-02/2020-data-threat--report-global-edition-report.pdf

IEEE. 3 Key Benefits of 5G. *IEEE Innovation at Work* [online]. 2018 [cit. 16. 9. 2021]. Dostupné z: https://innovationatwork.ieee.org/3-key-benefits-of-5g/

IEEE. The Potential of Blockchain for IoT. *IEEE Innovation at Work* [online]. 2019 [cit. 15. 7. 2020]. Dostupné z: https://innovationatwork.ieee.org/the-potential-of-blockchain-for-iot/

INFORMATION IS BEAUTIFUL. World's Biggest Data Breaches & Hacks. *Information is Beautiful* [online]. 2019 [cit. 19. 2. 2021]. Dostupné z: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

IOT SOLUTIONS WORLD CONGRESS. Advantages of 5G and how will benefit IoT. *Digitalizing Industries* [online]. 2019 [cit. 17. 10. 2021]. Dostupné z: https://www.iotsworldcongress.com/advantatges-of-5g-and-how-will-benefit-iot/

(ISC)2. Strategies for Building and Growing Strong Cybersecurity Teams. *(ISC)2*. [online]. Clearwater: (ISC)2 2019 [cit. 18. 7. 2020]. Dostupné z: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

ISO/IEC JTC 1/SC 27; INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION. ISO/IEC 30111:2019. *ISO* [online]. 2019 [cit. 18. 7. 2020]. Dostupné z: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/97/69725.html

ISO/IEC JTC 1/SC 27; INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION; ISO. ISO/IEC 29147:2018. *ISO* [online]. 2018 [cit. 18. 7. 2020]. Dostupné z: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/23/72311.html

JEVONS, William Stanley. The Mathematical Theory of Political Economy. *Journal of the Statistical Society of London* [online]. Royal Statistical Society, Wiley, 1874, roč. 37, č. 4, s. 478–488. ISSN 0959-5341. DOI: https://doi.org/10.2307/2338697

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti* [online]. Brno: Národní centrum kybernetické bezpečnosti 2015 [cit. 10. 1. 2021]. Dostupné z: https://www.govcert.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

JOERLING, Jill. Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data. *Washington University Journal of Law & Policy,* 2010, č. 32, s. 467–488.

KALOR, Anders et al. Network Slicing in Industry 4.0 Applications: Abstraction Methods and End-to-End Analysis. *IEEE Transactions on Industrial Informatics* [online]. 2018, roč. 14, č. 12, s. 5419–5427. DOI: https://doi.org/10.1109/TII.2018.2839721

KAMARA, Irene. Article 40. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 716–724. ISBN 978-0-19-882649-1. DOI https://doi.org/10.1093/oso/9780198826491.003.0079

KAMIYA, Shinichi et al. What is the Impact of Successful Cyberattacks on Target Firms? *National Bureau of Economic Research: Working Papers* [online]. 2018, roč. 2018, č. 24409 [cit. 25. 5. 2021]. Dostupné z: https://www.nber.org/papers/w24409

KAPOOR, Keshav, Karen RENAUD a Jacqueline ARCHIBALD. Preparing for GDPR: helping EU SMEs to manage data breaches. In: *2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security* [online]. Liverpool: Society for the Study of Artificial Intelligence and Simulation for Behaviour (AISB), 2018, s. 13–20 [cit. 16. 7. 2020]. Dostupné z: https://rke.abertay.ac.uk/en/publications/preparing-for-gdpr-helping-eu-smes-to-manage-data-breaches

KASL, František. Internet of Things – Assessment of Incentives of Businesses to Fullfil the Personal Data Breach Obligation under the proposed General Data Protection Regulation. In: *The 33rd Annual Conference of the European Association of Law and Economics (EALE)*: *EALE* [online]. Bologna: EALE, 2016 [cit. 12. 7. 2020]. Dostupné z: https://eale.org/content/uploads/2016/08/160804-kasl-eale2016bologna-data-breach-and-gdpr-final.pdf

KASL, František. Internet věcí a ochrana dat v evropském kontextu. *Revue pro právo a technologie*, Brno: Masarykova univerzita, 2016, roč. 7, č. 13, s. 111–146. ISSN 1804-5383.

KASL, František. Towards identification of cybersecurity principles for smart city cyber-physical environment. In: *Cyberspace Conference 2017.* 2017.

KASL, František. 9 Osobnost, soukromí a osobní údaje v moderní společnosti. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 391–486. ISBN 978-80-7598-045-8.

KASL, František. Cybersecurity of Small and Medium Enterprises in the Era of Internet of Things. *The Lawyer Quarterly* [online]. Institute of State and Law of the Academy of Sciences of the Czech Republic, 2018, roč. 8, č. 2 [cit. 12. 7. 2020]. ISSN 1805-8396. Dostupné z: https://tlq.ilaw.cas.cz/index.php/tlq/article/view/281

KASL, František. Personal Data Breach in the Era of Internet of Things. In: *Internationales Rechtsinformatik Symposion IRIS 2018* [online]. 2018 [cit. 12. 7. 2020]. Dostupné z: https://is.muni.cz/auth/publication/1409546/cs/Personal-Data-Breach-in-the-Era-of-Internet-of-Things/Kasl

KASL, František. K pojmové nejednotnosti porušení zabezpečení/bezpečnosti osobních údajů v českém právu. *AUC IURIDICA* [online]. 2019, roč. 2019, č. 3, s. 117–131. ISSN 2336-6478, 0323-0619. DOI: https://doi.org/10.14712/23366478.2019.34

KASL, František. Towards Functioning Personal Data Breach Notification in the Age of Internet of Things. *Jusletter IT. Die Zeitschrift für IT und Recht.* [online]. Weblaw, 2019 [cit. 12. 7. 2020]. ISSN 1664-848X. Dostupné z: http://jusletter-it.weblaw.ch/issues/2019/IRIS/towards-functioning-_8a85876a8d.html

KASL, František. *Tvorba YouTuberů prizmatem práva na ochranu osobnosti dětí a mladistvých*. Rigorózní práce. Brno: Masarykova univerzita, Právnická fakulta, 2019. Dostupné z: https://is.muni.cz/th/d4stp/ [cit. 16. 7. 2020].

KASPERSKY. What is WannaCry ransomware? *Kaspersy* [online]. 2019 [cit. 22. 5. 2020]. Dostupné z: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

KASSNER, Michael. Anatomy of the Target data breach: Missed opportunities and lessons learned. *ZDNet* [online]. 2015 [cit. 16. 7. 2020]. Dostupné z: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

KENTON, Will. Moral Hazard Definition. *Investopedia* [online]. 2019 [cit. 17. 7. 2020]. Dostupné z: https://www.investopedia.com/terms/m/moralhazard.asp

KENWORTHY, Randal. The 5G And IoT Revolution Is Coming: Here's What To Expect. *Forbes* [online]. 2019 [cit. 17. 10. 2021]. Dostupné z: https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/

KHARRAZ, Amin et al. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: ALMGREN, Magnus, Vincenzo GULISANO a Federico MAGGI (eds.). *Detection of Intrusions and Malware, and Vulnerability Assessment* [online]. Cham: Springer International Publishing, 2015, s. 3–24, Lecture Notes in Computer Science. ISBN 978-3-319-20550-2. DOI: https://doi.org/10.1007/978-3-319-20550-2_1

KHATOUN, Rida a Sherali ZEADALLY. Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Communications Magazine* [online]. 2017, roč. 55, č. 3, s. 51–59. ISSN 1558-1896. DOI: https://doi.org/10.1109/MCOM.2017.1600297CM

KHEKARE, Ganesh S. a Apeksha V. SAKHARE. A smart city framework for intelligent traffic system using VANET. In: *2013 International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)* [online]. 2013, s. 302–305. DOI: https://doi.org/10.1109/iMac4s.2013.6526427

KHOUZANI, Arman, Viet PHAM a Carlos CID. Incentive Engineering for Outsourced Computation in the Face of Collusion. In: *Workshop on the Economics of Information Security (WEIS)* [online]. PA, US: Pennsylvania State University, 2014 [cit. 16. 7. 2020]. Dostupné z: https://www.econinfosec.org/archive/weis2014/papers/KhouzaniPhamCid-WEIS2014.pdf

KLAHR, Rebecca et al. *Cyber Security Breaches Survey 2017* [online]. London: UK Department for Culture, Media & Sport, 2017. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

KLEIN, Naomi. Naomi Klein: How big tech plans to profit from the pandemic. *The Guardian* [online]. 2020 [cit. 15. 7. 2020]. ISSN 0261-3077. Dostupné z: https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-from-coronavirus-pandemic

KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.

KOUKAL, Pavel et al. Právo duševního vlastnictví. *IS MU* [online]. Brno: Elportál MU, 2020 [cit. 18. 7. 2020]. ISSN 1802-128X. Dostupné z: https://is.muni.cz/do/rect/el/estud/praf/2019podzim/dusevni_vlastnictvi/web/index.html

KOZLOV, Denis, Jari VEIJALAINEN a Yasir ALI. Security and privacy threats in IoT architectures. In: *Proceedings of the 7th International Conference on Body Area Networks*. Oslo, Norway: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, s. 256–262, BodyNets '12. ISBN 978-1-936968-60-2. DOI https://doi.org/10.4108/icst.bodynets.2012.250550

KREBS, Brian. New Mirai Worm Knocks 900K Germans Offline. *Krebs on Security* [online]. 2016 [cit. 20. 3. 2021]. Dostupné z: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

KREBS, Brian. Equifax breach. *Krebs on Security* [online]. 2017 [cit. 24. 5. 2021]. DOI https://doi.org/10.1016/S1361-3723(17)30080-5. Dostupné z: https://krebsonsecurity.com/tag/equifax-breach/page/2/

KROES, Neelie. Ethical implications of tomorrow's digital society. In: SMITH, Ian. *Internet of Things 2012 New Horizons*. Halifax: IERC – Internet of Things European Research Cluster, 2012. ISBN 978-0-9553707-9-3.

LAI, Fujun, Dahui LI a Chang-Tseh HSIEH. Fighting identity theft: The coping perspective. *Decision Support Systems* [online]. 2012, roč. 52, č. 2, s. 353–363. ISSN 0167-9236. DOI: https://doi.org/10.1016/j.dss.2011.09.002

LAMPROPOULOS, Georgios, Kerstin SIAKAS a Theofylaktos ANASTASIADIS. Internet of Things in the Context of Industry 4.0: An Overview. *International Journal of Entrepreneurial Knowledge* [online]. 2019, roč. 7, s. 4–19. DOI: https://doi.org/10.2478/ijek-2019-0001

LANGEVIN, Jim. Langevin Reintroduces the Personal Data Notification and Protection Act. *Congressman Jim Langevin* [online]. [cit. 24. 5. 2021]. Dostupné z: https://langevin.house.gov/press-release/langevin-reintroduces-personal-data-notification-and-protection-act

LAPOWSKY, Issie. Get Ready for a Privacy Law Showdown in 2019. *Wired* [online]. 2018 [cit. 24. 5. 2021]. ISSN 1059-1028. Dostupné z: https://www.wired.com/story/privacy-law-showdown-congress-2019/

LASZKA, Aron et al. The Rules of Engagement forBug Bounty Programs. In: *22nd International Conference on Financial Cryptography and Data Security (FC 2018)* [online]. 2018, s. 1–20 [cit. 17. 7. 2020]. Dostupné z: http://aronlaszka.com/papers/laszka2018rules.pdf

LAUBE, Stefan a Rainer BÖHME. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* [online]. 2016, Oxford Academic, roč. 2, č. 1, s. 29–41. ISSN 2057-2085. DOI: https://doi.org/10.1093/cybsec/tyw002

LEENES, Ronald. Article 42. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 732–744. ISBN 978-0-19-882649-1. DOI https://doi.org/10.1093/oso/9780198826491.003.0081

LEVERETT, Eireann, Richard CLAYTON a Ross ANDERSON. *JRC Technical Reports*: *Standardisation and certification of safety, security and privacy in the 'Internet of Things'* [online]. ISBN 978-92-79-77863-6. Brussels: European Commission, 2018 [cit. 18. 7. 2020]. Dostupné z: http://op.europa.eu/en/publication-detail/-/publication/80bb1618-16bb-11e8-9253-01aa75ed71a1/language-en/format-PDF

LÉVY-BENCHETON, Cédric et al. Cyber Security for Smart Cities – an Architecture Model for Public Transport. *ENISA* [online]. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research, 2015 [cit. 20. 3. 2021]. ISBN 978-92-9204-162-5. Dostupné z: https://www.enisa.europa.eu/publications/smart-cities-architecture-model

LIGERO, Raquel. Differences between NB-IOT and LTE-M. *Accent Systems* [online]. 2018 [cit. 16. 9. 2021]. Dostupné z: https://accent-systems.com/blog/differences-nb-iot-lte-m/

LIMON DE JESUS, Gianluca. *Enhancing Vulnerability Management for IoT Devices with Bug Bounty Programs and Responsible Disclosure*. Master's Thesis. Delft: Technical University Delft, 2019. Dostupné z: https://repository.tudelft.nl/islandora/object/uuid%3A2a479391-1431-4df5-be27-f27fb7dc5d35 [cit. 19. 7. 2020].

LING, Sea, Maria INDRAWAN-SANTIAGO a Seng LOKE. RFID-based user profiling of fashion preferences: Blueprint for a smart wardrobe. *IJIPT* [online]. 2007, roč. 2, s. 153–164. DOI: https://doi.org/10.1504/IJIPT.2007.016217

LIPPMANN, Richard et al. The 1999 DARPA off-line intrusion detection evaluation. *Computer Networks: The International Journal of Computer and Telecommunications Networking* [online]. 2000, roč. 34, č. 4, s. 579–595. ISSN 1389-1286. DOI: https://doi.org/10.1016/S1389-1286(00)00139-0

LIU, Dengpan, Yonghua JI a Vijay MOOKERJEE. Knowledge sharing and investment decisions in information security. *Decision Support Systems* [online]. 2011, roč. 52, č. 1, s. 95–107. ISSN 0167-9236. DOI: https://doi.org/10.1016/j.dss.2011.05.007

LOHRMANN, Dan. Why Offering Bug Bounties Will Be Widespread, Even in Government. *Government Technology* [online]. 2017 [cit. 19. 7. 2020]. Dostupné z: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/why-offering-bug-bounties-will-be-widespread-even-in-government.html

LOOZEN, Tom a Adrian BASCHNONGA. In the next wave of telecoms, are bold decisions your safest bet? *EY* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: https://www.ey.com/en_gl/tmt/in-the-next-wave-of-telecoms-are-bold-decisions-your-safest-bet

LOUTOCKÝ, Pavel a Kamil MALINKA. Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců. *Revue pro právo a technologie,* 2016, roč. 7, č. 14, s. 45–64. ISSN 1805-2797.

LUCAS, Greg. Hackers accessed state computer but took no data / Payroll information was at risk. *SFGate* [online]. 2002 [cit. 12. 7. 2020]. Dostupné z: https://www.sfgate.com/bayarea/article/Hackers-accessed-state-computer-but-took-no-data-2830442.php

LUKÁČ, Petr. Prvním „chytrým" městem v Česku se stane Písek. Firma Schneider Electric bude řídit dopravu i vytápění. *Hospodářské noviny (iHNed.cz)* [online]. 9. 1. 2016 [cit. 15. 7. 2020]. Dostupné z: https://ihned.cz/c1-65066210-prvnim-chytrym-mestem-v-cesku-bude-pisek-rika-sef-tuzemske-pobocky-schneider-electric

LUNDIN, Nannan. COVID-19 and digital transformation – What do we see now and what will we see soon? *Offices of Science and Innovation* [online]. 2020 [cit. 16. 7. 2020]. Dostupné z: https://sweden-science-innovation.blog/beijing/COVID-19-and-digital-transformation-what-do-we-see-now-and-what-will-we-see-soon/

MALATRAS, Apostolos et al. Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review* [online]. 2017, roč. 33, č. 4, s. 458–469. ISSN 0267-3649. DOI: https://doi.org/10.1016/j.clsr.2017.03.013

MANSFIELD-DEVINE, Steve. The Ashley Madison affair. *Network Security* [online]. 2015, roč. 2015, č. 9, s. 8–16. ISSN 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(15)30080-5

MANVILLE, Catriona et al. Mapping Smart cities in the EU. *European Parliament* [online]. Brusel: Directorate-General for Internal Policies, 2014 [cit. 20. 5. 2020]. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf

MANWARING, Kayleen a Roger CLARKE. Surfing the Third Wave of Computing: A Framework for Research into eObjects. *Computer Law & Security Review: The International Journal of Technology Law and Practice* [online]. 2015, roč. 31, č. 5, s. 586–603. ISSN 0267-3649. DOI: https://doi.org/10.1016/j.clsr.2015.07.001

MARAS, Marie-Helen. Tomorrow's Privacy. Internet of Things: security and privacy implications. *International Data Privacy Law*, 2015, roč. 5, č. 2, s. 99–104. ISSN 2044-4001.DOI https://doi.org/10.1093/idpl/ipv004

MARCHANT, Gary E., Braden R. ALLENBY a Joseph R. HERKERT (eds.). *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*. Dordrecht: Springer, 2011, 212 s., The International Library of Ethics, Law and Technology, 7. ISBN 978-94-007-1356-7.

MARINOS, Louis, Adrian BELMONTE a Evangelos REKLEITIS. ENISA Threat Landscape 2015. *ENISA* [online]. 2015 [cit. 12. 7. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/etl2015

MARTIMORT, David (ed.). *The Economic Theory of Incentives* [online]. Cheltenham: Edward Elgar Publishing, 2017, 1880 s., The International Library of Critical Writings in Economics series [cit. 16. 7. 2020]. ISBN 978-1-78536-443-3. Dostupné z: https://www.e-elgar.com/shop/gbp/the-economic-theory-of-incentives-9781785364433.html

MARVÃO, Catarina a Giancarlo SPAGNOLO. *What Do We Know about the Effectiveness of Leniency Policies? A Survey of the Empirical and Experimental Evidence* [online]. SITE Working Paper, 2014, č. 28 [cit. 18. 7. 2020]. Dostupné z: https://www.econstor.eu/handle/10419/204739

MASSÉ, Estelle. *Two Years under the EU GDPR. An Implementation Progress Report. State of Play, Analysis and Recommendations* [online]. New York: Access Now, 2020 [cit. 12. 7. 2020]. Dostupné z: https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf

MATES, Pavel. Právo na digitální služby. *Revue pro právo a technologie* [online]. 2020, roč. 11, č. 21, s. 73–89. ISSN 1805-2797. DOI: https://doi.org/10.5817/RPT2020-1-4

MATTHEWS, Kayla. The Internet of Robotic Things: How IoT and Robotics Tech Are Evolving Together. *IoT Times* [online]. 2019 [cit. 15. 7. 2020]. Dostupné z: https://iot.eetimes.com/the-internet-of-robotic-things-how-iot-and-robotics-tech-are-evolving-together/

MATTONI, Benedetta, Franco GUGLIERMETTI a Fabio BISEGNA. A multilevel method to assess and design the renovation and integration of Smart Cities. *Sustainable Cities and Society* [online]. 2015, roč. 15, s. 105–119. ISSN 2210-6707. DOI: https://doi.org/10.1016/j.scs.2014.12.002

MATZLER, Kurt et al. Open innovation in small and micro enterprises. *Problems and Perspectives in Management*, 2013, roč. 11, s. 12.

MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*, 2003, roč. 25, č. 4, s. 381–401. ISSN 0265-8240. DOI https://doi.org/10.1111/j.0265-8240.2003.00155.x

MCAFEE, Andrew a Erik BRYNJOLFSSON. Big Data: The Management Revolution. *Harvard Business Review* [online]. October 2012 [cit. 15. 7. 2020]. ISSN 0017-8012. Dostupné z: https://hbr.org/2012/10/big-data-the-management-revolution

MCKEAN, Ross, Ewa KUROWSKA-TOBER a Heidi WAEM. DLA Piper GDPR data breach survey: January 2021. *DLA Piper* [online]. 19. 1. 2021 [cit. 20. 10. 2020]. Dostupné z: https://www.dlapiper.com/en/uk/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/

MELL, Peter a Timothy GRANCE. *The NIST Definition of Cloud Computing* [online]. Special Publication 800-145. Gaithersburg, MA: National Institute of Standards and Technology, 2011 [cit. 15. 7. 2020]. Dostupné z: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

MILL, John Stuart. *Utilitarianism*. Revidované vyd. Oxford; New York: Oxford University Press, 1998, 168 s. ISBN 978-0-19-875163-2.

MINERVA, Roberto, Abyi BIRU a Domenico ROTONDI. *Towards a definition of the Internet of Things (IoT)* [online]. Torino: IEEE, 2015 [cit. 1. 6. 2020]. Dostupné z: http://iot.ieee.org/definition.html

MINISTERIO DE JUSTICIA. *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* [online]. 19. 4. 2008 [cit. 12. 7. 2020]. Dostupné z: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

MINISTERSTVO SPRAVEDLNOSTI. *Návrh zákona o hromadném řízení* [online]. Praha: Portál ODok, 2019 [cit. 18. 7. 2020]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBA9EXSST

MÍŠEK, Jakub. Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing). In: SVANTESSON, Dan a Dariusz KLOZA (eds.). *Trans-atlantic Data Privacy Relations as a Challenge for Democracy*. Cambridge: Intersentia, 2017, European Integration and Democracy Series. ISBN 978-1-78068-434-5.

MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. 1. vyd. Brno: Masarykova univerzita, 2020, 279 s., Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia, sv. 694. ISBN 978-80-210-9736-0 (brož.), 978-80-210-9737-7 (online)

MITTELSTADT, Brent. Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology* [online]. 2017, roč. 19, č. 3, s. 157–175. ISSN 1572-8439. DOI: https://doi.org/10.1007/s10676-017-9426-4

Mobility, performance and engagement. *Economist Intelligence Unit* [online]. London: The Economist, 2016 [cit. 27. 10. 2021]. Dostupné z: https://www.eiuperspectives.economist.com/technology-innovation/mobility-performance-and-engagement/white-paper/mobility-performance-and-engagement

MOHANAPRIYA, R. et al. Driverless Intelligent Vehicle for Future Public Transport Based on GPS. *International Journal of Advanced Research in Electrical, Electronic and Instrumentation Engineering*, 2014, roč. 3, č. 3, s. 378–384. ISSN 2278-8875.

MOORE, Martin a Damian TAMBINI. *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*. Oxford: Oxford University Press, 2018, 441 s. ISBN 978-0-19-084513-1.

MOUTON, Francois, Louise LEENEN a Hein S. VENTER. Social engineering attack examples, templates and scenarios. *Computers & Security* [online]. 2016, roč. 59, s. 186–209. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2016.03.004

MURRAY, Tanya. How to Slay the Hydra: Adopting Charles Ann Wright's the Law of Remedies as a Social Institution as a Framework for Preventing Data Breaches. *University of Detroit Mercyla Review*, 2017, č. 94, s. 127–159.

MYRSTAD, Finn. Connected toys violate European consumer law. *Forbrukerrådet* [online]. 2016 [cit. 15. 7. 2020]. Dostupné z: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

M2M Sector Map. *Beecham Research Shaping the IoT Future* [online]. 2011 [cit. 1. 6. 2020]. Dostupné z: http://www.beechamresearch.com/download.aspx?id=18

NAGHIZADEH, Parinaz a Mingyan LIU. Inter-Temporal Incentives in Security Information Sharing Agreements. In: *AAAI workshop on Artificial Intelligence for Cyber Security (AICS)* [online]. Phoenix: AAAI, 2016 [cit. 12. 7. 2020]. Dostupné z: https://www.aaai.org/ocs/index.php/WS/AAAIW16/paper/view/12610

NCKB. Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *Národní bezpečnostní úřad* [online]. 2015 [cit. 12. 7. 2020]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

NASH, John. Non-Cooperative Games. *Annals of Mathematics* [online]. Annals of Mathematics, 1951, roč. 54, č. 2, s. 286–295. ISSN 0003-486X. DOI: https://doi.org/10.2307/1969529

NATARAJAN, Mangai. *Crime Opportunity Theories: Routine Activity, Rational Choice and their Variants*. Abingdon: Routledge, 2017, 616 s. ISBN 978-1-351-57070-1. DOI https://doi.org/10.4324/9781315095301

NEMEC, Matus et al. ROCA: Vulnerable RSA generation (CVE-2017-15361). *CRoCS wiki* [online]. 2017 [cit. 19. 7. 2020]. Dostupné z: https://crocs.fi.muni.cz/public/papers/rsa_ccs17

NEUBURGER, Jeffrey D. *Trends in Privacy and Data Security* [online]. Toronto: Thomson Reuters, 2019 [cit. 4. 3. 2020]. Dostupné z: https://store.legal.thomsonreuters.com/law-products/news-views/corporate-counsel/trends-in-privacy-and-data-security

NEUMANN, John von a Oskar MORGENSTERN. *Theory of Games and Economic Behavior. 60th Anniversary Commemorative Edition*. 2007, 776 s. ISBN 978-0-691-13061-3.

New Arizona Law to Protect Data Breach Victims. *Arizona Attorney General Mark Brnovich* [online]. 2019 [cit. 24. 5. 2021]. Dostupné z: https://www.azag.gov/press-release/new-arizona-law-protect-data-breach-victims

NEWMAN, Brett V. Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation. *Journal of Law, Technology and Policy*, 2015, roč. 2015, s. 437–460.

NEWMAN, Lily Hay. Medical Devices Are the Next Security Nightmare. *Wired* [online]. 2017 [cit. 15. 7. 2020]. ISSN 1059-1028. Dostupné z: https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

NISSENBAUM, Helen. Privacy As Contextual Integrity. *Washington Law Review*, 2004, roč. 79, s. 101–139.

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. 1. vyd. Praha: Wolters Kluwer, 2014, 484 s. ISBN 978-80-7478-665-5.

NUAIMI, Eiman Al et al. Applications of big data to smart cities. *Journal of Internet Services and Applications* [online]. 2015, roč. 6, č. 1, s. 25. ISSN 1867-4828, 1869-0238. DOI: https://doi.org/10.1186/s13174-015-0041-5

NÚKIB. Co je NCKB. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 26. 2. 2020]. Dostupné z: https://www.govcert.cz/cs/

NÚKIB. GovCERT.CZ. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 26. 2. 2020]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/

ODBOR HLAVNÍHO ARCHITEKTA EGOVERNMENTU. Digitální Česko. Informační koncepce České republiky. Navazující dokument č. 1: Metody řízení ICT veřejné správy ČR. *Ministerstvo vnitra* [online]. 2019, verze 1.0 [cit. 18. 7. 2020]. Dostupné z: https://www.mvcr.cz/soubor/navazujici-dokument-c-1-metody-rizeni-ict-verejne-spravy-cr.aspx

OFFICE OF PUBLIC AFFAIRS. Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk. *Federal Trade Commission* [online]. 2015 [cit. 4. 3. 2020]. Dostupné z: https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment

OFFICE OF PUBLIC AFFAIRS. Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information. *Federal Trade Commission* [online]. 2016 [cit. 4. 3. 2020]. Dostupné z: https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting

OFFICE OF PUBLIC AFFAIRS. FTC Gives Final Approval to Settlement with Auto Dealer Software Company That Allegedly Failed to Protect Consumers' Data. *Federal Trade Commission* [online]. 2019 [cit. 4. 3. 2020]. Dostupné z:https://www.ftc.gov/news-events/press-releases/2019/09/ftc-gives-final-approval-settlement-auto-dealer-software-company

OFFICE OF THE ATTORNEY GENERAL. Privacy Enforcement and Protection. *State of California Department of Justice* [online]. 2012 [cit. 24. 5. 2021]. Dostupné z: https://www.oag.ca.gov/privacy

OGUT, Hulisi, Nirup MENON a Srinivasan RAGHUNATHAN. Cyber Insurance and IT Security Investment: Impact of Interdependence Risk. In: *WEIS* [online]. 2005 [cit. 16. 7. 2020]. Dostupné z: https://pdfs.semanticscholar.org/7780/a75c68604ca979d0fe8896ebc998ae6a02fc.pdf

OKS, Sascha Julian, Albrecht FRITZSCHE a Claudia LEHMANN. The digitalisation of industry from a strategic perspective. In: *R & D Management Conference*. 2016.

OORSCHOT, Paul C. van a Sean W. SMITH. The Internet of Things: Security Challenges. *IEEE Security Privacy* [online]. 2019, roč. 17, č. 5, s. 7–9. ISSN 1558-4046. DOI: https://doi.org/10.1109/MSEC.2019.2925918

Opinion 03/2013 on purpose limitation. *Article 29 Data Protection Working Party* [online]. 2. 4. 2013, wp 203, 00569/13/EN [cit. 12. 7. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

PAAL, Boris P. a Daniel PAULY. *Datenschutz-Grundverordnung: DS-GVO*. München: C. H. Beck, 2017, 891 s., Beck'sche Kompakt-Kommentare. ISBN 978-3-406-69570-4.

PANDZA, Jasper. Details of "REN/CYBER-0048" Work Item. *ETSI* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=57991

PARETO, Vilfredo. The New Theories of Economics. *Journal of Political Economy*. University of Chicago Press, 1897, roč. 5, č. 4, s. 485–502. ISSN 0022-3808. DOI https://doi.org/10.1086/250454

PARK, Yong Tae, Pranesh STHAPIT a Jae-Young PYUN. Smart digital door lock for the home automation. In: *TENCON 2009 – 2009 IEEE Region 10 Conference*: *TENCON 2009 – 2009 IEEE Region 10 Conference* [online]. 2009, s. 1–6. DOI: https://doi.org/10.1109/TENCON.2009.5396038

PATO, Alexia. The Collective Private Enforcement of Data Protection Rights in the EU. In: *Privatizing Dispute Resolution* [online]. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2019, s. 129–154. ISBN 978-3-8487-5908-8. DOI: https://doi.org/10.5771/9783748900351-129

PAUL, Kari. "Tossed my Fitbit in the trash": users fear for privacy after Google buys company. *The Guardian* [online]. 2019 [cit. 15. 7. 2020]. ISSN 0261-3077. Dostupné z: https://www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data

PIZZUTI, Stefano, Mauto ANNUNZIATO a Fabio MORETTI. Smart street lighting management. *Energy Efficiency* [online]. 2013, roč. 6, č. 3, s. 607–616. ISSN 1570-6478. DOI: https://doi.org/10.1007/s12053-013-9195-9

POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3.

POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*, 2016, roč. 7, č. 13, s. 67–91. ISSN 1805-2797.

POLČÁK, Radim. 1 Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-045-8.

POLČÁK, Radim. 12 Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 587–627. ISBN 978-80-7598-045-8.

POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 86–98. ISSN 0231-6625.

POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, Právnická fakulta, 2016. ISBN 978-80-210-8426-1. Dostupné z: https://science.law.muni.cz/knihy/monografie/Polcak_Kyberneticka_bezpecnost.pdf

POLICY DEPARTMENT A ECONOMIC AND SCIENTIFIC POLICY. Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts. *Evropský parlament* [online]. IP/A/ITRE/NT/2013-5 PE 507.476. Brussels: Directorate-General for Internal Policies, 2013 [cit. 12. 7. 2020]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf

PONEMON INSTITUTE. Cost of a Data Breach Report 2019. *IBM Security* [online]. Traverse City, 2019 [cit. 22. 5. 2020]. DOI https://doi.org/10.1016/S1361-3723(19)30081-8. Dostupné z: https://www.ibm.com/security/data-breach

POULLET, Yves. About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In: GUTWIRTH, Serge, Yves POULLET a Paul de HERT (eds.). *Data Protection in a Profiled World* [online]. Dordrecht: Springer Netherlands, 2010 [cit. 13. 7. 2020]. ISBN 978-90-481-8864-2. DOI: https://doi.org/10.1007/978-90-481-8865-9

POUND, Roscoe. Law in Books and Law in Action. *44 American law Review,* 1910, s. 12–36.

POWLES, Julia a Jat SINGH. Why the internet of things favours dominance. *The Guardian* [online]. 2015 [cit. 20. 5. 2020]. ISSN 0261-3077. Dostupné z: https://www.theguardian.com/technology/2015/jul/24/internet-of-things-centralisation-dominance

PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 8/2014 k nejnovějšímu vývoji v oblasti internetu věcí* [online]. wp223_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29 2014 [cit. 12. 7. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_cs.pdf

PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 03/2014 k oznámení o narušení bezpečnosti osobních údajů* [online]. 693/14/CS WP 213. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29 2014 [cit. 12. 7. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_cs.pdf

PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679* [online]. wp248rev.01_cs. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29 2017 [cit. 29. květen 2021]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [online]. 18/CS WP250rev.01. Brusel: Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29 2018 [cit. 28. únor 2020]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

PREMNATH, Sriram N. a Zygmunt J. HAAS. Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model. *IEEE Wireless Communications Letters* [online]. 2015, roč. 4, č. 3, s. 277–280. ISSN 2162-2345. DOI: https://doi.org/10.1109/LWC.2015.2408609

PRESS OFFICE. AG Shapiro Secures $ 600 Million from Equifax in Largest Data Breach Settlement in History. *Pennsylvania Office of Attorney General* [online]. 2019 [cit. 4. 3. 2020]. Dostupné z: https://www.attorneygeneral.gov/taking-action/press-releases/ag-shapiro-secures-600-million-from-equifax-in-largest-data-breach-settlement-in-history/

PRESS ROOM. First EU collective redress mechanism to protect consumers. *European Parliament News* [online]. 2018 [cit. 25. 5. 2021]. Dostupné z: http://www.europarl.europa.eu/news/en/press-room/20181205IPR21088/first-eu-collective-redress-mechanism-to-protect-consumers

PRCHAL, Lukáš. Brněnská nemocnice po kyberútoku ruší operace, testování koronaviru ohrožené není. *Deník N* [online]. 2020 [cit. 14. 9. 2020]. Dostupné z: https://denikn.cz/314303/brnenska-nemocnice-po-kyberutoku-rusi-operace-testovani-koronaviru-ohrozene-neni/

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). *Council of European Union* [online]. 2020, 6543/20 [cit. 18. 7. 2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=CS

PROUST, Olivier. Unravelling the mysteries of the GDPR trilogues. *Fieldfisher* [online]. 2015 [cit. 13. 7. 2020]. Dostupné z: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/unravelling-the-mysteries-of-the-gdpr-trilogues

PURKOVIC, Dalibor, Marian HÖNSCH a Tobias Raphael Maria Karl MEYER. An Energy Efficient Communication Protocol for Low Power, Energy Harvesting Sensor Modules. *IEEE Sensors Journal* [online]. 2019, roč. 19, č. 2, s. 701–714. ISSN 2379-9153. DOI: https://doi.org/10.1109/JSEN.2018.2876746

QUALCOMM TECHNOLOGIES. Accelerating the mobile ecosystem expansion in the 5G Era with LTE Advanced Pro. *Qualcomm Technologies* [online]. 2018 [cit. 17. 10. 2021]. Dostupné z: https://www.qualcomm.com/media/documents/files/accelerating-the-mobile-ecosystem-expansion-in-the-5g-era-with-lte-advanced-pro.pdf

QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation* [online]. 2018, Cambridge University Press, roč. 9, č. 3, s. 502–526. ISSN 1867-299X, 2190-8249. DOI: https://doi.org/10.1017/err.2018.47

RADA EU. 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) – příprava obecného přístupu. *Rada EU* [online]. 2012/0011 (COD). Brusel, 2015 [cit. 24. 5. 2021]. Dostupné z: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/cs/pdf

RAGGETT, Dave et al. *Cross Fertilisation through Alignment, Synchronisation and Exchanges for IoT: Final report on IoT standardisation activities* [online]. Deliverable 06.06. CREATE IoT, 2020 [cit. 17. 7. 2020]. Dostupné z: https://european-iot-pilots.eu/wp-content/uploads/2020/06/D06_06_WP06_H2020_CREATE-IoT_Final.pdf

RAM, Aliya. Reports from whistleblowers on data breaches almost triple. *Financial Times* [online]. 2018 [cit. 25. 5. 2021]. Dostupné z: https://www.ft.com/content/2bec495a-014e-11e9-9d01-cd4d49afbbe3

RAMIREZ, Edith. Prepared Statement of the Federal Trade Commission On Privacy In the Digital Age: Preventing Data Breaches and Combating Cybercrime. *United States Senate* [online]. Washington D.C.: United States Senate, 2014 [cit. 24. 5. 2021]. Dostupné z: https://www.ftc.gov/public-statements/2014/02/prepared-statement-federal-trade-commission--privacy-digital-age-preventing

RAUL, Charles Alan a Sidley AUSTIN (eds.). *Chambers Global Practice Guide: Data Protection & Cyber Security 2019*. Glasgow: Chambers & Partners, 2018, 384 s. ISBN 978-0-85514-746-4.

RESEARCH AND MARKETS. Big Data Analytics Industry Report 2020. *GlobeNewswireNewsRoom* [online]. 2020 [cit. 14. 9. 2020]. Dostupné z: http://www.globenewswire.com/news-release/2020/03/02/1993369/0/en/Big-Data-Analytics-Industry-Report-2020-Rapidly-Increasing-Volume-Complexity-of-Data-Cloud-Computing-Traffic-and-Adoption-of-IoT-AI-are-Driving-Growth.html

RISK BASED SECURITY. Data Breach QuickView Report 2019 Q3 Trends. *Risk Based Security* [online]. Richmond, VA, 2019 [cit. 6. duben 2020]. Dostupné z: https://pages.riskbasedsecurity.com/data-breach-quickview-report-2019-q3-trends

ROBINSON, Dallin. Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Things with Class Action Litigation. *Richmond Journal of Law & Technology*, 2020, roč. 26, č. 1, s. 1–83. ISSN 1091-7322.

RODRIGUES, Rodolfo R. et al. An IoT-based Automated Shower System for Smart Homes. In: *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* [online]. 2018, s. 254–258. DOI: https://doi.org/10.1109/ICACCI.2018.8554793

RODRIGUEZ, Salvador. Facebook hack affected 3 million in Europe, creating the first big test for privacy regulation there. *CNBC* [online]. 2018 [cit. 25. 5. 2021]. Dostupné z: https://www.cnbc.com/2018/10/16/facebook-hack-affected-3-million-in-europe-first-big-test-for-gdpr.html

ROMAN, Rodrigo, Jianying ZHOU a Javier LOPEZ. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* [online]. 2013, roč. 57, č. 10, Towards a Science of Cyber Security, s. 2266–2279. ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2012.12.018

ROMANOSKY, Sasha, David HOFFMAN a Alessandro ACQUISTI. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, 2014, roč. 11, č. 1, s. 74–104. DOI https://doi.org/10.1111/jels.12035

RUBINSTEIN, Ira S. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* [online]. 2013, Oxford Academic, roč. 3, č. 2, s. 74–87. ISSN 2044-3994. DOI: https://doi.org/10.1093/idpl/ips036

RYCHLÝ, Tomáš. Posudek oponenta disertační práce „Právní a ekonomické aspekty porušení bezpečnosti osobních údajů v kontextu internetu věcí". 2021. Dostupné z: https://is.muni.cz/th/lu3ny/

SADEGHI, Ahmad-Reza, Christian WACHSMANN a Michael WAIDNER. Security and privacy challenges in industrial Internet of Things. In: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* [online]. 2015, s. 1–6. DOI: https://doi.org/10.1145/2744769.2747942

SAIDAMOVÁ, Suzan. Zákon o hromadných žalobách po prudké kritice opět přepracován. *epravo.cz* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.epravo.cz/top/clanky/zakon-o-hromadnych-zalobach-po-prudke-kritice-opet-prepracovan-110572.html

SAMSUNG. Family Hub Refrigerator – Overvierw. *Samsung* [online]. [cit. 19. 5. 2020]. Dostupné z: https://www.samsung.com/us/explore/family-hub-refrigerator/overview/

SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC. Security Breach Notification Laws: Views from Chief Security Officers. *University of California-Berkeley School of Law* [online]. 2007 [cit. 12. 7. 2020]. Dostupné z: https://www.law.berkeley.edu/files/cso_study.pdf

SAMUELSON, Paul A. a William D. NORDHAUS. *Microeconomics*. 17. vyd. New York: McGraw-Hill Education, 2001, 454 s. ISBN 978-0-07-118066-5.

SASSO, Brendan. Business groups call for data breach law. *The Hill* [online]. 2013 [cit. 24. 5. 2021]. Dostupné z: https://thehill.com/policy/technology/312163-overnight-tech-business-groups-call-for-data-breach-law

SCIENCEDIRECT. Behavioral Decision-Making – an overview. *ScienceDirect Topics* [online]. 2020 [cit. 16. 7. 2020]. Dostupné z: https://www.sciencedirect.com/topics/psychology/behavioral-decision-making

SCIS. Smart Cities and Communities Lighthouse projects. *EU Smart Cities Information System* [online]. 2020 [cit. 15. 7. 2020]. Dostupné z: https://smartcities-infosystem.eu/scc-lighthouse-projects

SEHNÁLEK, David. *Specifika výkladu práva Evropské unie a jeho vnitrostátní důsledky*. Praha: C. H. Beck, 2019, 208 s. ISBN 978-80-7400-741-5.

SEN, Ravi a Sharad BORLE. Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems* [online]. 2015, Routledge, roč. 32, č. 2, s. 314–341. ISSN 0742-1222. DOI: https://doi.org/10.1080/07421222.2015.1063315

SHACKLEFORD, Dave. *Combatting Cyber Risks in the Supply Chain* [online]. Bethesda, MA: SANS Institute 2017 [cit. 3. 10. 2021]. Dostupné z: https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

SHAMELI-SENDI, Alireza, Rouzbeh AGHABABAEI-BARZEGAR a Mohamed CHERIET. Taxonomy of information security risk assessment (ISRA). *Computers & Security* [online]. 2016, roč. 57, s. 14–30. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2015.11.001

Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities: Accelerating the Impact of IoT Technologies. *World economic forum* [online]. Cologny: World Economic Forum, 2018 [cit. 17. 10. 2021]. Dostupné z: https://www.weforum.org/projects/accelerating-the-impact-of-iot-technologies/

SHARETECHNOTE. NB-IoT. *LTE Quick Reference* [online]. 2019 [cit. 16. 9. 2021]. Dostupné z: http://www.sharetechnote.com/html/Handbook_LTE_NB_LTE.html

SHEAR, Michael D. a Natasha SINGER. Obama to Call for Laws Covering Data Hacking and Student Privacy. *The New York Times* [online]. 2017 [cit. 24. 5. 2021]. ISSN 0362-4331. Dostupné z: https://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html

SCHNEIER, Bruce. The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters. *Schneier on Security* [online]. 2016 [cit. 15. 7. 2020]. Dostupné z: https://www.schneier.com/essays/archives/2016/07/the_internet_of_thin_3.html

SCHNEIER, Bruce. California Passes New Privacy Law. *Schneier on Security* [online]. 2018 [cit. 24. 5. 2021]. Dostupné z: https://www.schneier.com/blog/archives/2018/07/california_pass.html

SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018.

SCHNEIER, Bruce. Facebook and Cambridge Analytica. *Schneier on Security* [online]. 2018 [cit. 24. 5. 2021]. Dostupné z: https://www.schneier.com/blog/archives/2018/03/facebook_and_ca.html

SCHOLL, Hans Jochen a Suha AL AWADHI. Creating Smart Governance: The key to radical ICT overhaul at the City of Munich. *Information Polity: The International Journal of Government & Democracy in the Information Age* [online]. 2016, roč. 21, č. 1, s. 21–42. ISSN 15701255. DOI: https://doi.org/10.3233/IP-150369

SCHWARTZ, Paul M. a Karl-Nikolaus PEIFER. Transatlantic Data Privacy Law. *The Georgetown Law Journal*, 2017, č. 106, s. 115–179.

SIMON, Herbert A. Rational Decision Making in Business Organizations. *The American Economic Review,* 1979, American Economic Association, roč. 69, č. 4, s. 493–513. ISSN 0002-8282.

SIMON, Herbert S. Rational Decision-Making in Business Organizations. Nobel Memorial Lecture, 8. 12. 1977. In: LINDBECK, Assar (ed.). *Economic Sciences, 1969-1980: The Sveriges Riksbank (Bank of Sweden) Prize in Economic Sciences in Memory of Alfred Nobel*. Singapore, New Jersey, London, Hong Kong: World Scientific, 1992. ISBN 978-981-02-0834-9.

SKROUPA, Christopher P. GDPR Priorities: Public Companies Must Urgently Handle Data Breaches. *Forbes* [online]. 2018 [cit. 25. 5. 2021]. Dostupné z: https://www.forbes.com/sites/christopherskroupa/2018/07/20/gdpr-priorities-public-companies-must-urgently-handle-data-breaches/

SMART CITIES WORLD. COVID-19 accelerates the adoption of smart city tech to build resilience. *Smart Cities World* [online]. 2020 [cit. 15. 7. 2020]. Dostupné z: https://www.smartcitiesworld.net/news/news/COVID-19-accelerates-the-adoption-of-smart-city-tech-to-build-resilience--5259

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. aktualizované a rozšířené vyd. Praha: Grada, 2013, 488 s. ISBN 978-80-247-4644-9.

SOCIAL SECURITY ADMINISTRATION. Social Security Number and Card. *Social Security* [online]. 2020 [cit. 14. 7. 2020]. Dostupné z: https://www.ssa.gov/ssnumber/

SOLIMAN, Moataz et al. Smart Home: Integrating Internet of Things with Web Services and Cloud Computing. In: *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*: *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* [online]. 2013, s. 317–320. DOI: https://doi.org/10.1109/CloudCom.2013.155

SOLOVE, Daniel J. a Danielle Keats CITRON. Risk and Anxiety: A Theory of Data Breach Harms. *Texas Law Review*, 2016, roč. 2018, č. 96, s. 737–786. DOI https://doi.org/10.2139/ssrn.2885638

SPIEKERMANN, Sarah et al. The challenges of personal data markets and privacy. *Electronic Markets* [online]. 2015, roč. 25, č. 2, s. 161–167. ISSN 1422-8890. DOI: https://doi.org/10.1007/s12525-015-0191-0

STANLEY, Tim. Free US Case Law from Google! – US Federal + 50 State Case Law. *Justia Law Blog* [online]. 2009 [cit. 3. 3. 2020]. Dostupné z: https://lawblog.justia.com/2009/11/17/free-us-case-law-from-google-us-federal-50-state-case-law/

STEELE, Katie a H. Orri STEFÁNSSON. Decision Theory. In: ZALTA, Edward N. (ed.). *The Stanford Encyclopedia of Philosophy* [online]. Winter 2016. Stanford: Metaphysics Research Lab, Stanford University, 2016 [cit. 16. 7. 2020]. Dostupné z: https://plato.stanford.edu/archives/win2016/entries/decision-theory/

STEINBERG, Scott. Cyberattacks now cost companies $ 200,000 on average, putting many out of business. *CNBC* [online]. 2019 [cit. 16. 7. 2020]. Dostupné z: https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

STEPTOE & JOHNSON LLP. Comparison of US State and Federal Security Breach Notification Laws [online]. 2016 [cit. 30. 5. 2021]. Dostupné z: https://www.steptoe.com/images/content/6/5/v1/6571/SteptoeDataBreachNotificationChart.pdf

STERGIOU, Christos et al. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems* [online]. 2018, roč. 78, s. 964–975. ISSN 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.11.031

SUCIU, George et al. Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things. In: *2013 19th International Conference on Control Systems and Computer Science* [online]. 2013, s. 513–518. DOI: https://doi.org/10.1109/CSCS.2013.58

Summary of U.S. State Data Breach Notification Statutes. *Davis Wright Tremaine LLP* [online]. 2019 [cit. 4. 6. 2021]. Dostupné z: https://www.dwt.com/gcp/state-data-breach-statutes

SUNDAR, Rajeshwari, Santhoshs HEBBAR a Varaprasad GOLLA. Implementing Intelligent Traffic Control System for Congestion Control, Ambulance Clearance, and Stolen Vehicle Detection. *IEEE Sensors Journal* [online]. 2015, roč. 15, č. 2, s. 1109–1113. ISSN 1530-437X. DOI: https://doi.org/10.1109/JSEN.2014.2360288

SWANSON, Kristofer, Thomas L. KIRSCH II a Ryan M. DUNIGAN. Data Breaches in a Whistleblower's World:What You Should Know, Why You Should Know It. *ABA Criminal Justice Section Newsletter*. 2013, s. 7–11.

SWINHOE, Dan. The 15 biggest data breaches of the 21st century. *CSO Online* [online]. 2020 [cit. 12. 7. 2020]. Dostupné z: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

SYMANTEC. Internet Security Threat Report 2017 Volume 22. *Symantec* [online]. 2017 [cit. 12. 7. 2020]. Dostupné z: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

ŠKOP, Martin. Interpretace práva jako literární interpretace. In: *Dny práva*: *Dny práva – 2010 – Days of Law* [online]. Brno: Masarykova univerzita, 2010, s. 2980–2993 [cit. 12. 7. 2020]. Dostupné z: https://www.law.muni.cz/sborniky/dny_prava_2010/files/prispevky/obsah.pdf

TAKAHASHI, Dean. Smarter's FridgeCam can guess when your food expires. *VentureBeat* [online]. 2017 [cit. 19. 5. 2020]. Dostupné z: https://venturebeat.com/2017/01/03/smarters-fridgecam-tells-you-when-your-food-will-expire/

TEMKIN, Larry S. *Rethinking the Good: Moral Ideals and the Nature of Practical Reasoning*. Oxford: Oxford University Press, 2012. ISBN 978-0-19-993221-4.

TERWANGNE, Cécile de. Article 5. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 309–320. ISBN 978-0-19-882649-1. DOI https://doi.org/10.1093/oso/9780198826491.003.0034

THE ECONOMIST. Things are looking app. *The Economist* [online]. 2016 [cit. 19. 5. 2020]. ISSN 0013-0613. Dostupné z: https://www.economist.com/business/2016/03/10/things-are-looking-app

THE ECONOMIST. The joys of data hygiene – Europe's tough new data-protection law. *The Economist* [online]. 5. 4. 2018 [cit. 13. 7. 2020]. ISSN 0013-0613. Dostupné z: https://www.economist.com/business/2018/04/05/europes-tough-new-data-protection-law

THE ECONOMIST. A connected world will be a playground for hackers. *The Economist* [online]. 2019 [cit. 17. 10. 2021]. ISSN 0013-0613. Dostupné z: https://www.economist.com/technology-quarterly/2019/09/12/a-connected-world-will-be-a-playground-for-hackers

THE ECONOMIST. The Internet of Things will bring the internet's business model into the rest of the world. *The Economist* [online]. 2019 [cit. 17. 10. 2021]. ISSN 0013-0613. Dostupné z: https://www.economist.com/technology-quarterly/2019/09/12/the-internet-of-things-will--bring-the-internets-business-model-into-the-rest-of-the-world

THE ECONOMIST. The Splinternet of Things threatens 5G's potential. *The Economist* [online]. 2019 [cit. 15. 7. 2020]. ISSN 0013-0613. Dostupné z: https://www.economist.com/the-world-in/2019/12/25/the-splinternet-of-things-threatens-5gs-potential

THE ECONOMIST. Ubiquitous computing – Drastic falls in cost are powering another computer revolution. *The Economist* [online]. 2019 [cit. 15. 7. 2020]. Dostupné z: https://www.economist.com/technology-quarterly/2019/09/12/drastic-falls-in-cost-are-powering-another-computer-revolution

THE HAGUE CENTRE FOR STRATEGIC STUDIES. Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. *The European Economic and Social Committee* [online]. QE-01-18-515-EN-N. The Hague: EESC, 2018 [cit. 15. 7. 2020]. Dostupné z: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf

TOMER, John F. Rational organizational decision making in the human firm: A socio-economic model. *The Journal of Socio-Economics* [online]. 1992, roč. 21, č. 2, s. 85–107. ISSN 1053-5357. DOI: https://doi.org/10.1016/1053-5357(92)90015-Y

TORRE, Ilaria et al. A framework for personal data protection in the IoT. In: *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* [online]. 2016, s. 384–391. DOI: https://doi.org/10.1109/ICITST.2016.7856735

TOSONI, Luca. Article 4(6). In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 138–144. ISBN 978-0-19-882649-1. DOI https://doi.org/10.1093/oso/9780198826491.003.0012

UK DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT. *Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security* [online]. London: Department for Digital, Culture, Media and Sport 2018 [cit. 17. 7. 2020]. Dostupné z: https://aioti.eu/wp-content/uploads/2019/06/DCMS_Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. *INFORMATION RESELLERS: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace* [online]. 2013 [cit. 23. 4. 2021]. Dostupné z: https://www.gao.gov/assets/660/658151.pdf

ÚŘAD PRO OCHRANU HOSPODÁŘSKÉ SOUTĚŽE. Oznámení Úřadu pro ochranu hospodářské soutěže ze dne 4. listopadu 2013 o aplikaci § 22ba odst. 1 zákona o ochraně hospodářské soutěže (program leniency). *UOHS* [online]. Brno: Úřad pro ochranu hospodářské soutěže 2013 [cit. 17. 7. 2020]. Dostupné z: http://www.uohs.cz/download/Legislativa/HS/SoftLaw/Program-leniency-2013.pdf

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. K provozování kamerových systémů. *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 15. 7. 2020]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Návrh závěrečného účtu kapitoly 343 – Úřad pro ochranu osobních údajů za rok 2018. Průvodní zpráva. *Úřad pro ochranu osobních údajů* [online]. 2019 [cit. 26. 2. 2020]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33707

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Výroční zpráva 2020. *UOHS* [online]. Praha: Úřad pro ochranu osobních údajů 2021 [cit. 18. 10. 2021]. ISBN 978-80-210-9836-7. Dostupné z: https://www.uoou.cz/vyrocni%2Dzprava%2Dza%2Drok%2D2020/ds-6593/archiv=0&p1=2089

VÁLOVÁ, Irena. Hromadné žaloby: Ministerstvo navrhuje povinné zastoupení advokátem i investorské financování. *Česká justice* [online]. 2019 [cit. 18. 7. 2020]. Dostupné z: https://www.ceska-justice.cz/2019/04/hromadne-zaloby-ministerstvo-navrhuje-povinne-zastoupeni-advokatem-i-investorske-financovani/

VAN CANNEYT, Tim; PROVOOST, Soo Mee. Belgian DPA publishes recommendation on GDPR record keeping obligation. *fieldfisher* [online]. 2017 [cit. 3. 10. 2021]. Dostupné z: http://privacylawblog.fieldfisher.com/2017/belgian-dpa-publishes-recommendation-on-gdpr-record-keeping-obligation/

VARGA, Pal et al. Security threats and issues in automation IoT. In: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)* [online]. 2017, s. 1–6. DOI: https://doi.org/10.1109/WFCS.2017.7991968

VERIZON. 2019 Data Breach Investigations Report: Executive Summary. *Verizon* [online]. New York, 2019 [cit. 24. 5. 2021]. Dostupné z: https://enterprise.verizon.com/resources/executivebriefs/2019/2019-dbir-executive-brief.pdf

VERIZON. 2019 Data Breach Investigations Report. *Verizon* [online]. New York, 2019 [cit. 24. 5. 2021]. DOI https://doi.org/10.1016/S1361-3723(19)30060-0. Dostupné z: https://enterprise.verizon.com/resources/reports/dbir/

VICTOR, Daniel, Sheera FRENKEL a Isabel KERSHNER. Personal Data of All 6.5 Million Israeli Voters Is Exposed. *The New York Times* [online]. 2020 [cit. 13. 7. 2020]. ISSN 0362-4331. Dostupné z: https://www.nytimes.com/2020/02/10/world/middleeast/israeli-voters-leak.html

VILLARI, Massimo et al. Osmotic Computing: A New Paradigm for Edge/Cloud Integration. *IEEE Cloud Computing* [online]. 2016, roč. 3, č. 6, s. 76–83. ISSN 2325-6095. DOI: https://doi.org/10.1109/MCC.2016.124

VINOCUR, Nicholas. 'We have a huge problem': European regulator despairs over lack of enforcement. *POLITICO* [online]. 2019 [cit. 12. 7. 2020]. Dostupné z: https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/

VOSTOUPAL, Jakub. Certifikace kyberbezpečnostních technologií. *Revue pro právo a technologie* [online]. 2019, roč. 10, č. 20, s. 147–268. ISSN 1805-2797. DOI: https://doi.org/10.5817/RPT2019-2-5

WANG, Hongwei a Wenbo HE. A Reservation-based Smart Parking System. In: *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* [online]. 2011, s. 690–695. DOI: https://doi.org/10.1109/INFCOMW.2011.5928901

WEBER, Rolf H. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, 2016, roč. 2016, č. 32, s. 715–728. ISSN 0267-3649. DOI https://doi.org/10.1016/j.clsr.2016.07.002

WEISER, Mark. The computer in the 21st century. *Scientific American*, 1991, roč. 1991. ISSN 0036-8733. DOI https://doi.org/10.1038/scientificamerican0991-94

What Is Petya and NotPetya Ransomware? *McAfee* [online]. 2020 [cit. 22. 5. 2020]. Dostupné z: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html

WHITTAKER, Zack. Two years after WannaCry, a million computers remain at risk. *TechCrunch* [online]. 2019 [cit. 22. 5. 2020]. Dostupné z: https://social.techcrunch.com/2019/05/12/wannacry-two-years-on/

WHITWELL, Joe. Small businesses should invest in cyber security. *The Telegraph* [online]. 2017 [cit. 10. 10. 2021]. ISSN 0307-1235. Dostupné z: http://www.telegraph.co.uk/business/open-economy/small-businesses-should-invest-in-cyber-security/

WIKIMEDIA FOUNDATION. Jurisdiction shopping. *Academic Dictionaries and Encyclopedias* [online]. 2010 [cit. 15. 7. 2020]. Dostupné z: https://enacademic.com/dic.nsf/enwiki/1323290

WILHELM, Ernst-Olivier. A brief history of the General Data Protection Regulation. *IAPP* [online]. 2016 [cit. 13. 7. 2020]. Dostupné z: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

WORLD ECONOMIC FORUM. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. *World Economic Forum* [online]. REF 020315. Cologny, 2015 [cit. 10. 10. 2021]. Dostupné z: http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

Worldwide Infrastructure Security Report. *Arbor networks* [online]. Burlington, MA: NETSCOUT, 2016 [cit. 12. 7. 2020]. Dostupné z: https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf

WU, Xindong et al. Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering* [online]. 2014, roč. 26, č. 1, s. 97–107. ISSN 1558-2191. DOI: https://doi.org/10.1109/TKDE.2013.109

YANG, Xue et al. A Multi-layer Security Model for Internet of Things. In: WANG, Yongheng a Xiaoming ZHANG (eds.). *Internet of Things*. Berlin/Heidelberg: Springer, 2012, s. 388–393, Communications in Computer and Information Science. ISBN 978-3-642-32427-7. DOI https://doi.org/10.1007/978-3-642-32427-7_54

YOUSEF, Khalil M., Jamal N. AL-KARAKI a Ali M. SHATNAWI. Intelligent Traffic Light Flow Control System Using Wireless Sensors Networks. *Journal of Information Science and Engineering*, 2010, roč. 26, s. 753–768.

YU LIU et al. Wireless Mesh Networks in IoT networks. In: *2017 International Workshop on Electromagnetics: Applications and Student Innovation Competition* [online]. 2017, s. 183–185. DOI: https://doi.org/10.1109/iWEM.2017.7968828

YUE, Wei T. et al. Network externalities, layered protection and IT security risk management. *Decision Support Systems* [online]. 2007, roč. 44, č. 1, s. 1–16. ISSN 0167-9236. DOI: https://doi.org/10.1016/j.dss.2006.08.009

ZAHADAT, Nima et al. BYOD security engineering: A framework and its analysis. *Computers & Security* [online]. 2015, roč. 55, s. 81–99. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2015.06.011

ZANFIR-FORTUNA, Gabriela. Article 82. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 1160–1179. ISBN 978-0-19-882649-1. DOI https://doi.org/10.1093/oso/9780198826491.003.0128

ZEESHAN, Afzaal Ahmad. What Code Reuse is and Why We Use It. *C#Corner* [online]. 2015 [cit. 15. 7. 2020]. Dostupné z: https://www.c-sharpcorner.com/uploadfile/201fc1/what-is-code-reuse-and-why-we-use-it/

ZHANG, Haijun et al. Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. *IEEE Communications Magazine* [online]. 2017, roč. 55. DOI: https://doi.org/10.1109/MCOM.2017.1600940

ZHANG, Shunliang. An Overview of Network Slicing for 5G. *IEEE Wireless Communications* [online]. 2019, roč. 26, č. 3, s. 111–117. ISSN 1558-0687. DOI: https://doi.org/10.1109/MWC.2019.1800234

ZHAO, Mingyi et al. Crowdsourced Security Vulnerability Discovery: Modeling and Organizing Bug-Bounty Programs. In: *HCOMP Workshop on Mathematical Foundations of Human Computation* [online]. 2016 [cit. 18. 7. 2020]. Dostupné z: https://pdfs.semanticscholar.org/7b58/fe274f41d1b37795d1a13e73d263787975d0.pdf

ZIMBA, Aaron; CHISHIMBA, Mumbi. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research* [online]. 2019, roč. 4, č. 1, s. 3–31. ISSN 2365-1695. DOI: https://doi.org/10.1007/s41125-019-00039-8

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020. *NÚKIB* [online]. 2021, s. 13 [cit. 20. 10. 2021]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/publikace/

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* [online]. 2015, roč. 30, č. 1, s. 75–89. ISSN 0268-3962, 1466-4437. DOI: https://doi.org/10.1057/jit.2015.5

Industry Backs Attorney General's Call for Federal Data-Breach Law. *AdAge* [online]. 2014. [cit. 24. 5. 2021]. Dostupné z: https://adage.com/article/privacy-and-regulation/industry-backs-ag-s-call-federal-data-breach-law/291865

Diskontování. *Wikipedia* [online]. 2017 [cit. 16. 7. 2020]. Dostupné z: https://cs.wikipedia.org/wiki/Diskontov%C3%A1n%C3%AD

Kardinální číslo. *Wikipedia* [online]. 2017 [cit. 16. 7. 2020]. Dostupné z: https://cs.wikipedia.org/wiki/Kardin%C3%A1ln%C3%AD_%C4%8D%C3%ADslo

As GDPR nears, Google searches for privacy are at a 12-year high. *The Economist* [online]. 2018 [cit. 24. 5. 2021]. ISSN 0013-0613. Dostupné z: https://www.economist.com/graphic-detail/2018/05/21/as-gdpr-nears-google-searches-for-privacy-are-at-a-12-year-high

Report from the Commisson on the implementation of the Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union law (2013/396/EU) [online]. COM/2018/040 final, 2018 [cit. 25. 5. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:40:FIN

Analýza nákladů a přínosů. *Wikipedia* [online]. 2019 [cit. 16. 7. 2020]. Dostupné z: https://cs.wikipedia.org/wiki/Anal%C3%BDza_n%C3%A1klad%C5%AF_a_p%C5%99%C3%ADnos%C5%AF

Technice Report [TR-e-IoT-SCS-Part-2] Generic Protection Profile Pilot v1.2 RELEASE [online]. [e-IoT-SCS-Part-2] GPP v1.2. Brussels: Eurosmart 2019 [cit. 17. 7. 2020]. Dostupné z: https://www.eurosmart.com/wp-content/uploads/2019/11/Part-2-Eurosmart_IoTsCS-GPP_v1.2_RELEASE.pdf

Teorie her. *Wikipedia* [online]. 2019 [cit. 16. 7. 2020]. Dostupné z: https://cs.wikipedia.org/wiki/Teorie_her

About AEI. *AEI Ciberseguridad y Tecnologías Avanzadas* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.aeiciberseguridad.es/index.php/About_AEI_1

About SECURITYMADEIN.LU. *SECURITYMADEIN.LU* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://securitymadein.lu//contact/about/

Agentura Evropské unie pro základní práva (FRA). *Evropská unie* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://europa.eu/european-union/about-eu/agencies/fra_cs

Common Criteria. *CC Portal* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.commoncriteriaportal.org/

Eulerovo číslo. *Wikipedia* [online]. 2020 [cit. 16. 7. 2020]. Dostupné z: https://cs.wikipedia.org/wiki/Eulerovo_%C4%8D%C3%ADslo

Eurosmart IoT Certification Scheme. *Eurosmart IoT Certification Scheme* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.eurosmart.com/eurosmart-iot-certification-scheme/

Framework. *IoT Security Foundation* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.iotsecurityfoundation.org/tag/framework/

Home. *European Energy Information Sharing & Analysis Centre* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.ee-isac.eu/

Home. *Riigi Infosüsteemi Amet* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.ria.ee/en

Kontrolní plán ÚOOÚ pro rok 2021. *Úřad pro ochranu osobních údajů* [online]. 2021 [cit. 18. 10. 2021]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=52202

Member ISACs. *National Council of ISACs* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.nationalisacs.org/member-isacs

O RCB. *Rządowe Centrum Bezpieczeństwa* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://rcb.gov.pl/

Open security knowledge. *IoT Security Initiative* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.iotsi.org

Product and Service Privacy Certification. *European Privacy Seal* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.european-privacy-seal.eu/EPS-en/Product-and-Service-Privacy-Certification

Schválený pořad a stav projednávání 49. schůze. *Poslanecká sněmovna Parlamentu ČR* [online] 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.psp.cz/sqw/ischuze.sqw?o=8&s=49

Síť evropských spotřebitelských center – síť ESC. *Evropská komise* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://ec.europa.eu/info/live-work-travel-eu/consumers/resolve-your-consumer-complaint/european-consumer-centres-network-ecc-net_en

Startseite. *Kuratorium Sicheres Österreich* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://kuratorium-sicheres-oesterreich.at/

Startseite. *Schutz Kritischer Infrastrukturen* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html

Sůl (kryptografie). *Wikipedia* [online]. 2020 [cit. 16. 7. 2020]. Dostupné z: https://cs.wikipedia.org/wiki/S%C5%AFl_(kryptografie)

Technical & White Papers. *Industrial Internet Consortium* [online]. 2020 [cit. 18. 7. 2020]. Dostupné z: https://www.iiconsortium.org/white-papers.htm

Vězňovo dilema. *Wikipedia* [online]. 2020 [cit. 17. 7. 2020]. Dostupné z: https://cs.wikipedia.org/wiki/V%C4%9Bz%C5%88ovo_dilema

Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. *Breach Portal* [online]. [cit. 25. 5. 2021]. Dostupné z: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

PORUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ V KONTEXTU INTERNETU VĚCÍ

JUDr. Ing. František Kasl, Ph.D.

Vydala Masarykova univerzita
Žerotínovo nám. 617/9, 601 77 Brno
v roce 2021

Spisy Právnické fakulty Masarykovy univerzity
Edice Scientia, sv. č. 717

1. elektronické vydání, 2021

ISBN 978-80-210-9986-9 (online ; pdf)
https://doi.org/10.5817/CZ.MUNI.M210-9986-2021
www.law.muni.cz

ISBN 978-80-210-9986-9

MUNI PRESS

MUNI LAW