Kybernetický bezpečnostní incident a jeho ohlašování v rámci zabezpečení osobních údajů v kontextu internetu věcí*

Cyber Security Incident and its Reporting as Part of Personal Data Protection in the Context of the Internet of Things

František Kasl**

Abstrakt

Příspěvek je věnován premise, že v moderní, stále propojenější společnosti dochází k rostoucímu obsahovému překryvu ohlašovacích povinností na základě právních rámců ochrany osobních údajů a kybernetické bezpečnosti. V obou případech jde o odraz chytré regulace, kdy stát využívá možností nabízených informačními a komunikačními technologiemi pro shromažďování aktuálních informací o situacích, které mohou vyžadovat reakci ze strany dozorových orgánů. V případě povinnosti ohlašovat porušení zabezpečení osobních údajů dle článku 33 obecného nařízení č. 2016/679, o ochraně osobních údajů, vůči Úřadu pro ochranu osobních údajů je směrodatný zásah do zpracovávaných osobních údajů. Povinnost hlášení kybernetického bezpečnostního incidentu dle § 8 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, vůči příslušnému bezpečnostnímu týmu CERT pak vzniká při zásahu do prvků informační infrastruktury povinných subjektů. Vzhledem k postupné digitalizaci přibývajícího množství činností a souvisejícím všudypřítomným zpracováváním osobních údajů dochází k rostoucímu prolínání těchto perspektiv. Autor tento vývoj vnímá jako příležitost pro úpravu de lege ferenda, kterou lze zvýšit přínos z takto sdělovaných informací pro dozorové orgány, chráněné fyzické osoby i povinností vázané subjekty.

Klíčová slova

Ochrana osobních údajů; kybernetická bezpečnost; ohlašování porušení zabezpečení osobních údajů; hlášení kybernetického bezpečnostního incidentu; internet věcí.

Abstract

The contribution is focused on the premise that in the modern, increasingly interconnected society, there is a growing content overlap of notification obligations following from the legal frameworks of personal data protection and cyber security. In both cases, this is a reflection of smart regulation, where the state uses the possibilities offered by information and communication technologies to gather up-to-date information on situations that may require a response from supervisory authorities. In the case of the obligation to notify personal data breaches pursuant to Article 33 of General Regulation No. 2016/679, on the protection of personal data,

* Zpracováno v rámci specifického výzkumu Masarykovy univerzity, projekt *Právo a technologie VIII* (MUNI/A/0989/2019). Příspěvek představuje část disertační práce autora na téma *Právní a ekonomické aspekty porušení bezpečnosti osobních údajů v kontextu internetu věcí* (2020), a byl představen odbornému publiku na národní konferenci *České právo a informační technologie* v září 2019.

** Ing. Mgr. František Kasl, Ústav práva a technologií, Právnická fakulta, Masarykova univerzita, Brno / Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic / E-mail: frantisek.kasl@mail.muni.cz / ORCID: 0000-0001-6675-9528

towards the Office for Personal Data Protection, the interference with the processed personal data is decisive. The obligation to report a cyber security incident pursuant to Section 8 of Act No. 181/2014 Sb., On cyber security, to the relevant CERT, arises upon interference with the information infrastructure elements of the obliged entities. Due to the gradual digitization of an increasing number of activities and the associated ubiquitous processing of personal data, these perspectives are increasingly overlapping. The author perceives this development as an opportunity to modify the future legal framework in a way, which can increase the benefit from the information communicated to supervisory authorities for all concerned.

Keywords

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

Úvod

Virtualizované prostředí digitálních aktiv a datových toků představuje specifickou dimenzi dnešní reality, která se prolíná řadou činností napříč společností. Informační a komunikační technologie tvoří základ nejrůznějších aktivit a umožňují fungování klíčových služeb a vztahů. Společně s jejich všudypřítomností roste též význam spolehlivosti a důvěryhodnosti zapojených prvků informační infrastruktury, ať již jde o sítě, systémy či jednotlivá zařízení. Tyto prvky však slouží různým účelům, jsou spravovány různými poskytovateli, provozovateli či správci a lze rozlišovat různé stupně jejich kritické důležitosti pro fungování dané sítě či služby. Tento stupeň významnosti se odráží v rozsahu právem uložených požadavků na přiměřené zajištění ochrany fungování těchto prvků a jimi přenášených či uchovávaných dat.

Jelikož se jedná o technické prvky, které procházejí dynamickým vývojem, není snadné regulatorně zachytit přiměřenou míru požadavků aplikovatelnou napříč tímto různorodým spektrem situačních řešení. Uplatnění zde proto často nacházejí tzv. performativní pravidla. Jak tento pojem vymezuje *Radim Polčák*, jde o normativní anomálii, která pragmaticky využívá relativně vyšší obeznámenosti regulovaného subjektu s jeho specifickou situací ve srovnání s regulující autoritou a přenechává mu proto konkretizaci uložených pravidel z obecně formulované povinnosti dle požadavků situace.[1] Právní norma tudíž nepředepisuje, jaká opatření má povinný subjekt přijmout, pouze zakládá účel, kterého má být dosaženo a kritéria, která mají zvláštní význam při hodnocení vhodnosti a přiměřenosti. Tím je ostatně také zachovávána technologická neutralita dané právní úpravy.

Rozsah povinností jednotlivého správce, poskytovatele či provozovatele na zajištění ochrany prvků informační infrastruktury tudíž závisí na jeho vyhodnocení vazby na chráněný zájem a míru ohrožení tohoto zájmu v konkrétních předvídatelných scénářích. V rámci tohoto příspěvku bude věnována pozornost dvěma významným normativním rámcům, které vymezují soubor takovýchto povinností. Jedním je právo kybernetické bezpečnosti, upravené

1 Srov. POLČÁK, Radim. 1 – Pojem a metoda práva informačních technologií. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 14. ISBN 978-80-7598-045-8.

především zákonem č. 181/2014 Sb. o kybernetické bezpečnosti (dále jen „ZoKB"). Druhým je pak úprava ochrany osobních údajů, významně sjednocená napříč EU skrze obecné nařízení č. 2016/679, o ochraně osobních údajů (dále jen „Obecné nařízení") a doplněná v českém právu zákonem č. 110/2019 Sb., o zpracování osobních údajů.

Pohled práva kybernetické bezpečnosti lze přitom zjednodušeně označit za více komunitní, kdy potřebnost ochrany daného prvku je odvozena od relativního významu jeho fungování pro zajišťování klíčových služeb a funkcí informační infrastruktury v rámci společnosti.[2] Tímto právním rámcem jsou tak vymezovány a upravovány povinnosti vážící se k ochraně provozu prvků kritické informační infrastruktury, významných informačních systémů veřejné správy, sítí elektronických komunikací či celospolečensky důležitých informačních systémů základních služeb na poli energetiky, vodohospodářství, dopravy, bankovnictví či zdravotnictví.[3]

Oproti tomu pohled právního rámce ochrany osobních údajů akcentuje individuální hledisko dotčených zájmů, stavíce do popředí kvalitu přenášených a uchovávaných dat v daném prvku informační infrastruktury. S přijetím jisté míry zjednodušení je tedy rozhodující pro přiměřenou míru potřebných opatření rozsah, citlivost a zneužitelnost dat s informacemi vážícími se k jednotlivci, definovaných pro tyto potřeby jako osobní údaje,[4] nikoliv toliko služba, kterou prvek informační infrastruktury umožňuje či poskytuje.[5]

Jde přitom zpravidla o dva pohledy na klasifikaci obdobných či stejných prvků informační infrastruktury. Servery uchovávající databázi záznamů o pacientech zdravotnického zařízení mohou být jak prostředkem pro významné zpracování osobních údajů zvláštních kategorií, tak prvkem informační infrastruktury základní služby. Je namístě připustit, že vzhledem k odlišnému účelu obou právních úprav není tento překryv zdaleka úplný. Právní rámec ochrany osobních údajů je ze své podstaty vysoké ochrany práv a svobod subjektů údajů při nejrůznějších činnostech vztažen na mnohem širší spektrum situací a podléhá mu mnohem rozsáhlejší okruh povinných subjektů, ať již jako primárně odpovědní správci či sekundárně odpovědní zpracovatelé. Povinnosti na základě ZoKB oproti tomu dopadají pouze na vymezené skupiny subjektů provozujících či spravujících významné prvky informační infrastruktury, přičemž i mezi těmito skupinami zákon činí rozdíly a nepodřizuje všechny stejnému rozsahu povinností.[6] Výsledně tak lze vnímat částečný překryv, který však má výjimky v obou směrech. Na jedné straně nalézáme vysoký počet podnikových sítí malých a středních podniků, které sice zpracovávají významná množství osobních údajů, nepodléhají však úpravě dle ZoKB. Oproti tomu

2 Viz KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 132–133. ISBN 978-80-88168-31-7.

3 Srov. § 3 ZoKB.

4 Srov. čl. 4 bod 1 Obecného nařízení.

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

6 Srov. Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Dz„ s. 64. Dostupné z: *Beck-online* [online].

např. informační systém základní služby v oblasti vodohospodářství z převážné části neoperuje s daty, která by naplňovala kvalifikaci osobních údajů.

V rámci tohoto příspěvku přitom budeme argumentovat, že vzhledem k technologickému pokroku a narůstajícímu významu informační infrastruktury bude namístě, aby právem zakládané odlišování prvků spadajících pod režim kybernetické bezpečnosti bylo stále méně ostré. V kontextu stále užšího propojování jednotlivých sítí, interakce systémů a dynamické komunikace dílčích prvků bude narůstat provázanost méně a více významných prvků informační infrastruktury. Při postupné realizaci vizí průmyslu 4.0,[7] chytrých měst,[8] či chytré distribuční sítě[9] tak bude přibývat prvků, které nelze při úsilí o zajištění vysoké míry kybernetické bezpečnosti do budoucna opomíjet. Nedávnou reakci na tento trend vnímáme v novelizacích ZoKB[10] souvisejících s transpozicí směrnice NIS.[11,12] Ty přinesly nejen rozšíření okruhu regulovaných kategorií prvků informační infrastruktury, ale také obohacení spektra uložených povinností, jelikož nově zahrnuté subjekty v řadě ohledů podléhají mírnějším či omezenějším povinnostem než stávající kategorie. Pokud je toto stupňovité rozšíření odrazem rostoucího významu dalších a širších kategorií prvků informační infrastruktury, lze s ohledem na předpokládaný pokračující rozvoj datově orientované ekonomiky EU[13] do budoucna dle našeho názoru očekávat nezbytné zahrnutí ještě výrazně početnějšího okruhu prvků.

Cílem tohoto příspěvku je poukázat na možnost, jak lze zahrnutí těchto dalších prvků do značné míry dosáhnout již jen účelným využitím informací dostupných orgánům veřejné moci skrze existující blízký rámec ochrany osobních údajů. V tomto ohledu je soustředěna pozornost na kontinuální informovanost příslušných orgánů o podobě a intenzitě hrozeb pro informační infrastrukturu, která je předpokladem včasné a přiměřené reakce.

Vedle vlastního sběru informací skrze příslušné bezpečnostní týmy CERT k tomuto účelu slouží povinnost ohlašování kybernetických bezpečnostních incidentů založená § 8 ZoKB.

---

7 Viz MINISTERSTVO PRŮMYSLU A OBCHODU. Iniciativa Průmysl 4.0. *Ministerstvo průmyslu a obchodu* [online]. Praha, 2016 [cit. 2. 4. 2020]. Dostupné z: https://www.mpo.cz/assets/dokumenty/53723/64358/658713/priloha001.pdf

8 Viz např. DAMERI, Renata Paola a Camille ROSENTHAL-SABROUX (eds.). *Smart City: How to Create Public and Economic Value with High Technology in Urban Space* [online]. Basel: Springer International Publishing, 2014 [cit. 2. 4. 2020]. ISBN 978-3-319-06159-7. DOI: 10.1007/978-3-319-06160-3

9 Viz MINISTERSTVO PRŮMYSLU A OBCHODU. Národní akční plán pro chytré sítě (NAP SG). *Ministerstvo průmyslu a obchodu* [online]. Praha, únor 2015 [cit. 2. 4. 2020]. Dostupné z: https://www.mpo.cz/assets/cz/energetika/elektroenergetika/2016/11/Narodni-akcni-plan-pro-chytre-site.pdf

10 Změnové zákony č. 104/2017 Sb. („malá novela ZoKB“) a č. 205/2017 Sb. („velká novela ZoKB“).

11 Směrnice 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Dostupné z: *EUR-Lex*.

12 Srov. body odůvodnění 4 a 5 směrnice NIS.

13 Viz. Elements of the European data economy strategy 2018. Shaping Europe's digital future. *Evropská komise* [online]. 18. 2. 2020 [cit. 2. 4. 2020]. Dostupné z: https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy

Srovnatelný projev chytré regulace, který směruje k potřebné informovanosti o aktuálních hrozbách dozorového orgánu pak nalézáme také v úpravě ochrany osobních údajů, v podobě povinnosti ohlašování porušení zabezpečení osobních údajů dle článku 33 Obecného nařízení vůči Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“).

V rámci následujícího textu budou obě tyto povinnosti podrobněji představeny. Poté bude nastíněna předpokládaná pokračující proměna regulovaného prostředí v důsledku rozvoje nových technologií. Záměrem je zde podložit tvrzení o rostoucím významu informačních infrastruktur, datových toků a zpracování osobních údajů v celospolečenském kontextu. Pro celostní zachycení těchto vlivů je přitom zvolen široce užívaný pojem internet věcí. V diskusi pak bude poukázáno na rostoucí blízkost představených perspektiv a možná opatření pro vytvoření synergií ku prospěchu dozorujícím orgánům, chráněným fyzickým osobám i povinným subjektům předmětných ohlašovacích povinností.

1 Hlášení kybernetických bezpečnostních incidentů

Provoz systémů, sítí a zařízení informačních a komunikačních technologií s sebou nese všudypřítomné riziko[14] incidentu, který zasáhne jejich řádné fungování a negativně postihne přenášená či uchovávaná data. Jedním z důvodů nemožnosti úplného vyloučení tohoto rizika je samotné spektrum situací, ve kterých může k incidentu na prvku informační infrastruktury dojít.[15] Některé mohou být důsledkem skryté chyby programování, problematické kompatibility mezi zařízeními či mechanického selhání prvků.[16] Jiné pak jsou výsledkem působení vnitřních či vnějších aktérů, kteří buďto chybují ve svém jednání či cíleně narušují integritu či funkcionalitu daného prvku. V případě vnějších aktérů pak může jít jak o cílený útok na danou složku sítě či systému ve snaze o dosažení konkrétního účelu (příkladem je organizovaná kybernetická průmyslová špionáž či kybernetický terorismus[17]), tak o projev nahodilých plošných a zpravidla automatizovaných útoků vůči určité kategorii zařízení se známou bezpečnostní chybou či jinou zranitelností (zde je častým příkladem ransomware[18] či malware vytvářející síť botnet[19]).

14 Dle § 2 písm. h) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „VoKB“), je rizikem možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu. Dle čl. 4 odst. 9 směrnice NIS je rizikem *„jakákoli v přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů.“*

15 Srov. např. SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. vyd. Praha: Grada Publishing, 2013, s. 96. ISBN 978-80-247-4644-9.

16 Viz KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 82. ISBN 978-80-88168-31-7.

17 Srov. důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Dz., s. 1. Dostupné z: *Beck-online*.

18 Např. ZIMBA, Aaron a Mumbi CHISHIMBA. 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 [cit. 2. 4. 2020]. ISSN 2365-1695. DOI: 10.1007/s41125-019-00039-8

19 Viz např. What botnets are. *Centro nazionale antibotnet* [online]. 3. 10. 2017 [cit. 2. 4. 2020]. Dostupné z: http://www.antibot.it/en/content/what-botnets-are

S ohledem na rostoucí význam prvků informační infrastruktury je dnes zajištění kybernetické bezpečnosti státu jednou z klíčových výzev.[20] Příslušný právní rámec tudíž směřuje k zakotvení pravidel pro zajištění vysoké úrovně důvěrnosti, integrity a dostupnosti (tzv. CIA triáda) nosné informační infrastruktury a jí přenášených dat.[21] V ZoKB je pro výše nastíněné jevy vyhrazena kombinace pojmů „kybernetický bezpečnostní incident" a „kybernetická bezpečnostní událost". Konkrétněji je pak kybernetický bezpečnostní incident vymezen jako *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události"*,[22] tedy události, *„která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací."*[23] Za cyklickou obecností představené definice se skrývá především výše nastíněná mnohotvárnost situací, které je nutno tímto pojmem postihnout.

V rámci právní úpravy kybernetické bezpečnosti je povinnost bezodkladně hlásit kybernetické bezpečnostní incidenty příslušnému bezpečnostnímu týmu CERT (*computer emergency response team*), resp. CSIRT (*computer security incident response team*),[24] vnímána za jeden ze základních kamenů.[25] Tímto mechanismem jsou příslušným složkám veřejné moci v aktuálním čase poskytovány potřebné informace o bezpečnostní situaci na nejvýznamnější informační infrastruktuře.[26] Vedle vlastního řešení konkrétní situace jsou tyto informace potřebné pro sledování dlouhodobějších trendů,[27] resp. včasnou přípravu na nově vystupující hrozby. Způsob komunikace a obsah hlášení upravuje VoKB. Za podstatné náležitosti platí vedle identifikace odesílatele a uvedení okamžiku zjištění incidentu především označení postiženého prvku informační infrastruktury a vlastní popis incidentu.[28] V rámci popisu incidentu je pak příslušný bezpečnostní tým vhodné informovat též o dosud provedených opatřeních, především co do nápravy vzniklých následků zranitelnosti a prevence jejich rozšíření, a o případné kontrole účinnosti zavedených opatření.[29] Odpovídající informovanost

---

20 Srov. důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Dz. , s. 2. Dostupné z: *Beck-online*.

21 Viz POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita Právnická fakulta, 2016, s. 156. ISBN 978-80-210-8426-1. Dostupné z: https://science.law.muni.cz/knihy/monografie/Polcak_Kyberneticka_bezpecnost.pdf

22 Srov. § 7 odst. 2 ZoKB.

23 Srov. § 7 odst. 1 ZoKB.

24 Ke vztahu obou pojmů viz blíže POLČÁK, Radim. 12 – Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 614–615. ISBN 978-80-7598-045-8.

25 Ibid., s. 593.

26 Srov. POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 92. ISSN 0231-6625.

27 Viz KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 492. ISBN 978-80-88168-31-7.

28 Viz § 4 VoKB.

29 Viz KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 493. ISBN 978-80-88168-31-7.

bezpečnostních týmů a dozorového orgánu je předpokladem vhodného nasazení reaktivních a ochranných opatření[30] účinně reagujících na vzniklé ohrožení regulované informační infrastruktury.[31] V tomto lze vnímat příklad chytré regulace, realizované skrze normativní tlak na bezodkladnou transparentnost vůči příslušné složce veřejné moci.[32]

Jelikož zmíněná právní úprava směřuje na zajištění funkcionality významnější informační infrastruktury, je okruh subjektů povinných k hlášení kybernetických bezpečnostních incidentů dle § 8 ZoKB relativně úzký. Lze přitom sledovat dvě variace této povinnosti. Striktnímu režimu hlášení všech kybernetických bezpečnostních incidentů podléhají správci (případně provozovatelé[33]) informačních a komunikačních systémů kritické informační infrastruktury,[34] významných informačních systémů,[35] informačního systému základní služby[36] a orgány nebo osoby zajišťující významnou síť.[37] 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 pouze oni jsou schopni posoudit reálné dopady incidentu.[38] Mírnější režim se pak vztahuje na samotné poskytovatele digitálních služeb,[39] kteří mají povinnost hlásit pouze kybernetické bezpečnostní incidenty, které mají významný dopad na poskytování digitální služby, a o nichž mají k dispozici informace, které jim umožní posoudit závažnost dopadu incidentu.[40] 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 namístě ohlášení konkrétního incidentu.[41] Na poskytovatele služby

30 Srov. § 13–15a ZoKB.

31 Srov. důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 181/2014 Dz., s. 53. Dostupné z: *Beck-online*.

32 Viz POLČÁK, Radim. 12 – Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 593. ISBN 978-80-7598-045-8.

33 Srov. § 8 odst. 5 ZoKB.

34 Srov. § 8 odst. 1 v kombinaci s § 3 písm. c) a d) ZoKB.

35 Srov. § 8 odst. 1 v kombinaci s § 3 písm. e) ZoKB.

36 Srov. § 8 odst. 1 v kombinaci s § 3 písm. f) ZoKB.

37 Srov. § 8 odst. 1 v kombinaci s § 3 písm. b) ZoKB.

38 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. Dostupné z: *Beck-online*.

39 Pojem digitální služby je přitom pro účely zákona omezen na vybrané kategorie, konkrétně na poskytovatele on-line tržiště, internetového vyhledávače či cloud computingu. Srov. § 2 písm. l) ZoKB.

40 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. Dostupné z: *Beck-online*.

41 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.

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 bezpečnostnímu týmu CERT, kterým je CSIRT.CZ[42] zajišťovaný sdružením CZ.NIC.[43] Ostatní povinné subjekty hlásí incidenty vládnímu bezpečnostnímu týmu CERT (GovCERT.CZ[44]), jehož činnost je zajišťována Národním centrem kybernetické bezpečnosti (NCKB), které je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).[45]

Na základě dostupných informací za rok 2018 bylo bezpečnostnímu týmu CSIRT.CZ, tedy ze strany poskytovatelů digitálních služeb a orgánů nebo osob zajišťujících významnou síť, ohlášeno celkem 1079 kybernetických bezpečnostních incidentů.[46] V letech 2016 a 2017 pak bylo CSIRT.CZ nahlášeno 1121, resp. 1008 incidentů.[47] Zde je však namístě dodat, že incidenty reportované CSIRT.CZ ze strany příslušných subjektů jsou charakterizovány buďto jako přetrvávající problémy, které subjekt nebyl vlastním úsilím schopen vyřešit; problémy, u kterých není jednoduché identifikovat původce či subjekt příslušný k jejich řešení; nebo incidenty se závažným dopadem na informační infrastrukturu v ČR.[48] Jde tedy zpravidla o komplexnější incidenty s rozsáhlejšími důsledky. Bezpečnostnímu týmu GovCERT.CZ bylo v roce 2018 podáno 164 hlášení incidentů,[49] v roce 2017 pak 248.[50] Mezi monitorovanými hrozbami byl například malware Triton/Trisis cílící na průmyslové bezpečnostní systémy kritické informační infrastruktury či útoky na průmyslové řídící systémy v energetickém sektoru.[51]

Trvalým trendem je narůstající sofistikovanost a četnost kybernetických bezpečnostních incidentů, zvláště v podobě spear-phishingu s cílem získání přístupu do významných sítí

---

42 Blíže viz O nás. *CSIRT.CZ* [online]. 2019 [cit. 2. 4. 2020]. Dostupné z: https://csirt.cz/cs/o-nas/

43 Srov. § 8 odst. 3 ZoKB.

44 Blíže viz Národní centrum kybernetické bezpečnosti. *NÚKIB* [online]. [cit. 2. 4. 2020]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/

45 Srov. § 8 odst. 4 ZoKB. Dále také Co je NCKB. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 2. 4. 2020]. Dostupné z: https://www.govcert.cz/cs/

46 Viz CSIRT.CZ. Zpráva o činnosti CSIRT.CZ (národní CSIRT ČR) za rok 2018. *CSIRT.CZ* [online]. Praha, 2019, s. 4 [cit. 2. 4. 2020]. Dostupné z: https://csirt.cz/media/filer_public/4e/dc/4edc3bff-5750-4527-82dc-3f155f578158/csirt_zprava_2018.pdf

47 Ibid.

48 Ibid., s. 3–4.

49 Srov. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018. *NÚKIB* [online]. Brno, 2019, s. 6 [cit. 2. 4. 2020]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/publikace/

50 Viz Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2017. *NÚKIB* [online]. Brno, 2018, s. 36 [cit. 2. 4. 2020]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/publikace/

51 Viz Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018. *NÚKIB* [online]. Brno, 2019, s. 29 a 31 [cit. 2. 4. 2020]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/publikace/

a systémů či k důvěrným databázím dat a osobních údajů.[52] 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.[53] I proto je snaha bezpečnostních týmů efektivně pracovat s maximálním okruhem dostupných a relevantních informacích o aktuálním stavu napříč informační infrastrukturou.[54] K tomuto v posledních letech směřují aktivity CSIRT.CZ na výzkumném projektu Predikce a Ochrana Před Kybernetickými Incidenty (PROKI), který shromažďuje informace o incidentech z řady zdrojů a dává je k dispozici dotčeným subjektům.[55] 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 NIS.[56] Nalézání nových zdrojů relevantních informací o incidentech je tedy přetrvávající a aktuální výzvou. Za zvláště hodnotné lze pak dle našeho názoru považovat ty, které jsou již dnes dostupné jiné složce veřejné správy. Tak je tomu v případě druhé diskutované roviny z oblasti ochrany osobních údajů.

2 Ohlašování porušení zabezpečení osobních údajů

Koncem května 2018 byla s použitelností Obecného nařízení zavedena plošná ohlašovací povinnost pro všechny správce osobních údajů v případě porušení zabezpečení zpracovávaných osobních údajů. Pojem se vztahuje na incidenty, které vedou k *„náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.“*[57] Linka ke kybernetickým bezpečnostním incidentům je zde poměrně zřejmá, zvláště pokud je zohledněna další související terminologie. Srovnatelná je např. kvalifikace, že porušení zabezpečení se může dotýkat rovin důvěrnosti, dostupnosti či integrity osobních údajů.[58] Srovnatelné je taktéž užití regulatorních mechanismů performativních pravidel, ať již v kontextu technických a organizačních opatření, která mají být provedena pro minimalizaci rizika vzniku porušení zabezpečení zpracovávaných osobních údajů,[59] tak ve vlastní kvalifikaci

52 Ibid., s. 25 a 54.

53 Ibid., s. 13 a 15.

54 Srov. KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 497. ISBN 978-80-88168-31-7.

55 Viz Zpráva o činnosti CSIRT.CZ (národní CSIRT ČR) za rok 2018. *CSIRT.CZ* [online]. Praha, 2019, s. 6 [cit. 2. 4. 2020]. Dostupné z: https://csirt.cz/media/filer_public/4e/dc/4edc3bff-5750-4527-82dc-3f155f578158/csirt_zprava_2018.pdf

56 Čl. 20 směrnice NIS, blíže také bod odůvodnění 67 směrnice.

57 Srov. čl. 4 bod 12 Obecného nařízení.

58 Srov. WP29. Guidelines on Personal data breach notification under Regulation 2016/679. *Evropská komise* [online]. 18/EN WP250rev.01. Brusel, 2018, s. 6 [cit. 2. 4. 2020]. Dostupné z: https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827

59 Srov. čl. 32 Obecného nařízení.

naplnění podmínek vzniku povinnosti notifikovat dozorový úřad o určitém incidentu jako o porušení zabezpečení osobních údajů.[60] Na druhou stranu je namístě zohlednit, že případy porušení zabezpečení se neomezují pouze na elektronicky uchovávané osobní údaje, ale i např. na ztrátu tištěných dokumentů. Přesto je v dnešní digitalizované společnosti elektronická forma uchovávání a komunikace těchto dat dominantní a neoprávněné přístupy k nim ve významnějším rozsahu jsou v zásadě limitovány na snadno kopírovatelné či pozměnitelné digitální záznamy.

Je namístě zmínit, že se jedná o povinnost, která nemá v kontinentálním právu ochrany osobních údajů rozsáhlou tradici. Již deset let sice existuje dílčí sektorová úprava pro poskytovatele veřejně dostupných služeb elektronických komunikací na základě směrnice 2009/136/ES, kterou se měnila směrnice o soukromí a elektronických komunikacích,[61] její význam však vzhledem k omezenému záběru nelze přeceňovat. Pojetí povinnosti v Obecném nařízení však na tuto úpravu přímo a úzce navazuje.[62]

Jelikož jsou k ohlašování případů porušení zabezpečení vůči dozorovému úřadu povinováni všichni správci,[63] má tato úprava dle článku 33 Obecného nařízení potenciál být podkladem pro širší sběr informací o stavu kybernetické bezpečnosti napříč prvky informační infrastruktury, než které postihuje výše nastíněná povinnost hlášení incidentů. Předpokládanou četnost hlášení dále zvyšuje nízko nastavený práh pro založení povinnosti, který se váže k pouhé pravděpodobnosti rizika pro práva a svobody dotčených fyzických osob.[64] Toto je ze své podstaty velmi hrubé síto, které vede povinné subjekty k ohlašování většiny incidentů,[65] 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 musejí být touto cestou hlášeny.[66] Zjištěná porušení zabezpečení mají být nadto hlášena bez zbytečného odkladu, pokud možno v rámci 72 hodin,[67] což dále zvyšuje jak informační hodnotu, tak tlak na dozorový úřad pro rychlé vyhodnocení a včasnou reakci.

---

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

61 Směrnice 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Dostupné z: *EUR-Lex*.

62 Viz návrh obecné nařízení o ochraně údajů. COM/2012/011 final – 2012/0011 (COD), s. 10. Dostupné z: *EUR-Lex*.

63 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.

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

65 Viz BURTON, Cédric. Article 33. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 646. ISBN 978-0-19-882649-1.

66 Ibid., s. 645.

67 Srov. čl. 33 odst. 1 Obecného nařízení. Blíže také bod odůvodnění 85.

Dozorovému úřadu jsou mimo kontaktních údajů pověřence pro ochranu osobních údajů hlášeny dostupné informace popisující povahu případu porušení; množství dotčených údajů a jejich kategorizace; množství dotčených subjektů údajů; pravděpodobné důsledky; a přijatá či plánovaná opatření.[68] Základní dělení případů porušení přitom odpovídá tzv. CIA triádě kybernetické bezpečnosti,[69] tedy na porušení důvěrnosti, integrity či dostupnosti osobních údajů.[70]

Příslušným dozorovým úřadem v českém prostředí je ÚOOÚ.[71] ÚOOÚ sice v případě úpravy ochrany osobních údajů nedisponuje srovnatelným arzenálem reaktivních a ochranných opatření, jaké se nabízejí pro řešení kybernetického bezpečnostního incidentu, přesto mu přísluší značné pravomoci založené přímo Obecným nařízením, umožňující adekvátní reakci. Vedle vyšetřovacích pravomocí dle čl. 58 odst. 1 Obecného nařízení jde především o nápravné pravomoci dle odst. 2, zvláště pak: možnost udělit správci napomenutí; nařídit správci, aby uvedl operace zpracování do souladu předepsaným způsobem a ve stanovené lhůtě; nařídit správci, aby případ porušení oznámil subjektu údajů; uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu; či uložit správní pokutu dle čl. 83 Obecného nařízení až do výše 10 000 000 € (resp. až 2 % posledního celkového celosvětového ročního obratu). U dozorových úřadů v ostatních členských státech přitom již můžeme shledávat první případy významných sankcí za nesplnění ohlašovací povinnosti. Vedle sankce 600 000 € společnosti Uber z konce roku 2018 za rok opožděné ohlášení rozsáhlého případu porušení zabezpečení, která však byla uložena na základě nizozemské národní úpravy zavádějící srovnatelnou povinnost před vlastní použitelností Obecného nařízení,[72] lze uvést sankci o hodnotě ekvivalentu 61 500 € udělenou v Litvě, ekvivalentu 34 375 € v Maďarsku, či ekvivalentu 20 000 € v Rumunsku i Německu.[73]

Tyto nápravné pravomoci by přitom měly sloužit naplnění hlavního účelu této právní úpravy, tedy zajištění ochrany základních práv a svobod dotčených fyzických osob.[74] To lze vnímat ve dvou rovinách. V rovině *ex post* se jedná o zamezení či snížení hrozící majetkové či nemajetkové újmy dotčených subjektů údajů v důsledku daného případu

---

68 Srov. čl 33 odst. 3 Obecného nařízení.

69 Viz KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 45. ISBN 978-80-88168-31-7.

70 Srov. WP29. Guidelines on Personal data breach notification under Regulation 2016/679. *Evropská komise* [online]. 18/EN WP250rev.01. Brusel, 2018, s. 7 [cit. 2. 4. 2020]. Dostupné z: https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827

71 Blíže viz Úřad. *Úřad pro ochranu osobních údajů* [online]. [cit. 2. 4. 2020]. Dostupné z: https://www.uoou.cz/urad/ds-1059/p1=1059

72 Viz např. Dutch DPA: fine for data breach Uber. *Autoriteit persoonsgegevens* [online]. 27. 11. 2018 [cit. 2. 4. 2020]. Dostupné z: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber

73 Srov. CMS. Fines Database. *GDPR Enforcement Tracker* [online]. 2020 [cit. 2. 4. 2020]. Dostupné z: http://www.enforcementtracker.com

74 Viz čl. 1 odst. 2 Obecného nařízení.

porušení zabezpečení osobních údajů.[75] Dozorový úřad v tomto směru svými opatřeními poskytuje první linii ochrany těchto fyzických osob a případně koordinuje řádné sdělení situace a doporučení vhodného postupu[76] v souvislosti s navazující povinností správce oznámit významné případy porušení zabezpečení těmto osobám v souladu s čl. 34 Obecného nařízení. Neméně významná je však role vážící se k potřebě informovanosti veřejné správy o aktuálním stavu, ke kterému tento prvek chytré regulace směřuje. Na základě těchto informací totiž může dozorový úřad koordinovat své činnosti a upravit postupy v rámci poradní činnosti vůči správcům ve srovnatelné situaci jako ohlašující subjekt, případně přistoupit k auditu subjektů, u kterých je pravděpodobný nesoulad s požadavky právní úpravy. Je však namístě doplnit, že role ÚOOÚ v tomto směru nedosahuje významu, který při koordinaci odezvy na kybernetický bezpečnostní incident zastává v souladu se ZoKB příslušný bezpečnostní tým CERT.

Data za dosavadní dva roky použitelnosti této úpravy poukazují na značný rozptyl počtu ohlášených případů porušení, který však spíše než na odlišnou míru rizikovosti zpracování osobních údajů v jednotlivých členských státech či množství správců spadajících do působnosti daného dozorového úřadu poukazují na odlišnou tradici důsledného zajištění souladu s požadavky právní úpravy ochrany osobních údajů v těchto členských státech a v důsledku též odlišné pozice či kapacity jednotlivých dozorových úřadů. Konkrétně v Nizozemí, kde již před použitelností Obecného nařízení byla ohlašovací povinnost založena národní úpravou, bylo mezi 25. květnem 2018 a 27. lednem 2019 ohlášeno 15 400 případů porušení a mezi 28. lednem 2019 a 27. lednem 2020 dalších 25 247 případů porušení. V Dánsku bylo v těchto obdobích nahlášeno 3 100 a 6 706 případů porušení. Za Českou republiku je evidováno 290 a 430 ohlášených případů porušení, což je srovnatelné číslo s Maďarskem, Rumunskem či Lucemburskem.[77]

3 Rostoucí význam notifikačních nástrojů v kontextu internetu věcí

Výše představené ohlašovací povinnosti je namístě vnímat v kontextu dynamického vývoje technologické reality. Jsou ostatně do značné míry reakcí na rozšiřování informačních a komunikačních technologií a jejich rostoucí význam v procesech na všech úrovních. V případě úpravy hlášení kybernetického bezpečnostního incidentu lze projev této vazby shledávat v rozšíření okruhu postihovaných subjektů v souladu s transpozicí

75 Srov. BURTON, Cédric. Article 33. In: KUNER, Christopher et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, s. 641–642. ISBN 978-0-19-882649-1.

76 Např. změna hesla. Srov. WP29. Guidelines on Personal data breach notification under Regulation 2016/679. *Evropská komise* [online]. 18/EN WP250rev.01. Brusel, 2018, s. 20 [cit. 2. 4. 2020]. Dostupné z: https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827

77 Viz DLA Piper GDPR data breach survey: January 2020. DLA Piper [online]. Londýn: DLA Piper, 2020, s. 6 [cit. 2. 4. 2020]. Dostupné z: https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/

směrnice NIS na provozovatele základních služeb a vybrané poskytovatele digitálních služeb. Obdobně lze vnímat také výslovné zakotvení možnosti hlášení kybernetických bezpečnostních incidentů dalšími subjekty na dobrovolné bázi. Vidíme zde legislativní reflexi faktického rozšíření okruhu významných prvků informační infrastruktury, u nichž související riziko výrazně přesahuje dotčený subjekt či místní kontext. Podobný signál přitom přišel i se zavedením obecné ohlašovací povinnosti při porušení zabezpečení osobních údajů s použitelností Obecného nařízení. V této rovině je zdůrazňován především rostoucí význam datových toků a všudypřítomnost zpracování osobních údajů. Přibývá služeb a funkcionalit postavených na uživatelském profilování či vytěžování komerčně relevantních údajů o jednotlivcích. Tím roste riziko jejich ztráty či neoprávněného zpřístupnění, jakožto i újma hrozící dotčené fyzické osobě.

Tato proměna prostředí přitom neustává. Je nutné zohlednit, že legislativní úvahy, na kterých je založeno Obecné nařízení, a do značné míry i směrnice NIS, odrážejí realitu první poloviny právě končící dekády či dřívější. Pro vývoj na poli informačních a komunikačních technologií je toto poměrně dlouhá doba. Regulatorní rámec obecně, a zvláště pro dynamické prostředí technologií, čelí problému opožděné reakce na aktuální vývoj a trendy.[78] Rozmach nových technologií přitom významně posouvá výzvy spojené s kybernetickou bezpečností a ochranou zpracovávaných osobních údajů. Ty jsou přitom dále umocněny aktuálním vývojem počátku roku 2020 v důsledku celosvětové pandemie a bezprecedentními karanténními opatřeními, která činí z informačních a komunikačních technologií zcela nepostradatelný nástroj pro alespoň omezenou realizaci řady jinak dosud nedigitalizovaných činností.

Tento trend nepolevující digitalizace převážné většiny aktivit a komunikace je charakterizovaný pro účely tohoto příspěvku jako rozvoj internetu věcí. Internet věcí představuje technologický fenomén rozšiřujícího se spektra zařízení a systémů, které se řadí mezi prvky informační infrastruktury. Jde o odraz rostoucí popularity osobních předmětů, jako jsou chytré hodinky, osobní asistenti či vozidla s interaktivním rozhraním, ale jde též o prvky rozsáhlých instalací jako jsou modernizace městské infrastruktury, digitalizace průmyslové výroby či automatizace logistických operací.[79] Současný fyzický svět je tak rostoucím tempem doplňován a prolínán nově vznikající vrstvou informačních toků, která sahá daleko za současné běžné představy o kyberprostoru jako o prostředí webových stránek celosvětové sítě Internet.[80]

---

78 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. ISBN 978-94-007-1356-7.

79 Blíže viz M2M Sector Map. *Beecham Research Ltd.* [online]. 2011 [cit. 2. 4. 2020]. Dostupné z: http://www.beechamresearch.com/download.aspx?id=18

80 Blíže viz DIN, Ikram Ud et al. The Internet of Things: A Review of Enabled Technologies and Future Challenges. *IEEE Access* [online]. 2019, roč. 7, s. 7607 [cit. 2. 4. 2020]. ISSN 2169-3536. DOI: 10.1109/ACCESS.2018.2886601

4 Diskuse prolínání ohlašovacích povinností v kontextu internetu věcí

Přestože překryv vzniku představených ohlašovacích povinností u jednotlivých povinných subjektů není v současné situaci příliš velký, je možné vnímat postupné přibližování těchto rámců, zvláště na příkladu hlášení kybernetických bezpečnostních incidentů u základních či digitálních služeb. Z výše nastíněného vývoje prostředí informační infrastruktury a datových toků tudíž vyvozujeme následující předpoklady.

Zaprvé bude narůstat počet subjektů, které spravují prvky informační infrastruktury, jež jsou relevantní z hlediska kybernetické bezpečnosti. Bude tudíž zesilovat potřeba aktuálních informací o zranitelnostech v těchto prvcích a přínos ohlašování v nich odhalených bezpečnostních incidentů. Internet věcí přináší nové vektory útoků a nové způsoby pro navýšení jejich efektivity. K posílení schopností útočníků i obránců bude dále přispívat rozvoj umělé inteligence a rozšíření sítí 5G.[81] S ohledem na obecně nevalné bezpečnostní charakteristiky zařízení internetu věcí[82] vzroste pravděpodobnost hrozeb, které mají nepřímý vliv na významné prvky informační infrastruktury, ať již se jedná o rizika vyvstávající v rámci napadení článků dodavatelského řetězce, dílčích obchodních partnerů či nadstavbových služeb. Pouhé rozšiřování dopadu povinností na základě ZoKB by však vedlo k neúčelné duplicitě s použitelnou úpravou dle Obecného nařízení.

S tím se prolíná druhý předpoklad přibývající složitosti incidentů a rostoucí nezbytnosti specializovaného odborného personálu pro analýzu a vyhodnocení hlášených informací pro včasnou a účinnou reakci dozorového orgánu. V tomto ohledu je pak namístě přihlížet k nepoměru mezi množstvím povinných subjektů a rozsahem ohlašovací povinnosti dle Obecného nařízení na straně jedné a dostupnými personálními kapacitami a rozsahem dalších agend a činností ÚOOÚ na straně druhé. ÚOOÚ má celkově okolo 100 zaměstnanců,[83] z nichž však pouze několik obstarává dílčí agendu ohlašovaných případů porušení. Dle dostupných statistik bylo přitom jen v loňském roce ÚOOÚ nahlášeno 430 případů porušení a s ohledem na údaje ze srovnatelných členských států (např. 6706 ohlášených případů v Dánsku, 4833 ve Švédsku, 3938 ve Finsku, 1105 na Slovinsku, či 1064 v Rakousku) lze vycházet z předpokladu, že značná část případů porušení v České republice není ÚOOÚ hlášena.[84] Pro účelné fungování prvků chytré regulace je přitom

---

81 Viz Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018. *NÚKIB* [online]. Brno, 2019, s. 53 [cit. 2. 4. 2020]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/publikace/

82 Srov. SCHNEIER, Bruce. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018, s. 19 a násl. ISBN 978-0-393-60888-5.

83 Viz Návrh závěrečného účtu kapitoly 343 – Úřad pro ochranu osobních údajů za rok 2018. Průvodní zpráva. *Úřad pro ochranu osobních údajů* [online]. Praha, 2019, s. 10 [cit. 2. 4. 2020]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33707

84 Srov. DLA Piper GDPR data breach survey: January 2020. *DLA Piper* [online]. Londýn: DLA Piper, 2020, s. 6 [cit. 2. 4. 2020]. Dostupné z: https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/

nezbytné, aby orgány veřejné moci důsledně motivovaly povinné subjekty k plnění informační povinnosti a následně byly schopny shromážděné informace včas a účelně využít.

Hlášení kybernetického bezpečnostního incidentu a ohlašování případu 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.[85] Česká úprava kybernetické bezpečnosti přitom také stojí na ochraně distributivních práv jednotlivců skrze opatření pro udržování a zvyšování informační a síťové bezpečnosti.[86] 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.[87] Stejně jako k ohrožení zpracovávaných osobních údajů dochází zpravidla v důsledku nedostatečných opatření při zabezpečení prvků informační infrastruktury, jsou tyto prvky často ohrožovány ve snaze o zpřístupnění jimi uchovávaných či přenášených dat. 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 bezpečnostnímu týmu CERT je jádrem popis hrozby a zavedených opatření, vůči ÚOOÚ tyto informace správci doplňují také o posouzení ohrožení osobních údajů co do rozsahu a závažnosti. Lze tedy říci, že hlášení dle Obecného nařízení jsou informativní pro bezpečnostní tým CERT, ovšem hlášení dle ZoKB nepostačují ÚOOÚ, jelikož absentují akcent na perspektivu osobních údajů.

Domníváme 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. V tomto ohledu je sice namístě respektovat, že jak ÚOOÚ, tak NÚKIB, jsou nezávislé úřady,[88] v tom však nevnímáme významnou překážku pro založení této provázanosti. Tento postup by nadto měl být preferován a vyhledáván i s ohledem na zvyšující se tlak závazků veřejné správy na optimalizaci poskytování digitálních služeb a minimalizaci zatížení fyzických a právnických osob

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

86 Viz POLČÁK, Radim. 12 – Kybernetická bezpečnost. In: POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 589. ISBN 978-80-7598-045-8.

87 KOLOUCH, Jan et al. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 99–100. ISBN 978-80-88168-31-7.

88 Resp. že národní CERT je spravován soukromoprávním subjektem na základě veřejnoprávní smlouvy dle § 19 ZoKB. To jej však dle našeho 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.

požadavky, které je možné vyřešit uvnitř veřejné správy.[89] Takto lze nahlížet i na ohlašovací povinnosti, které představují administrativní zátěž pro povinný subjekt, zvláště pak vyvstanou-li vůči více dozorovým orgánům zároveň.[90] Je tedy v duchu současných priorit a tendencí k elektronizaci veřejné správy, aby dozorové úřady shromažďující srovnatelné informace nalézaly cesty k účelnému sdílení těchto informací.

Pokud lze očekávat, že pro potřebný přehled o aktuální situaci na poli kybernetické bezpečnosti bude do budoucna namístě sledovat vývoj u stále širšího okruhu subjektů, leží dle našeho názoru ve sdílení informací mezi ÚOOÚ a bezpečnostními týmy CERT řešení této potřeby, které by snížilo potřebu rozšiřování ohlašovací povinnosti dle ZoKB při současném udržení vysoké úrovně informovanosti těchto orgánů.

Tuto spolupráci lze přitom vnímat jako přínosnou i z hlediska optimalizace využití odborných kapacit veřejného sektoru. V tomto ohledu přitom NÚKIB disponuje v rámci veřejné správy nejrozsáhlejším odborným aparátem, který je zaměřen na kontinuální analýzu a monitorování kybernetických bezpečnostních hrozeb a vyhodnocování závažnosti incidentů. Dle dostupných informací zaměstnává v současné době okolo 200 zaměstnanců, lze přitom do budoucna předpokládat další rozšiřování, ač připravované navýšení stavů v loňském roce nebylo realizováno.[91]

Považujeme tedy za vhodné systematické provázání činností těchto složek veřejné správy, které přinese mnohostranné benefity. Z hlediska předávání informací o případech porušení zabezpečení z ÚOOÚ na bezpečnostní týmy CERT je sice namístě přihlížet k omezením daným požadavky na zákonné zpracování osobních údajů, nejedná se však dle našeho názoru o zásadní překážku. V prvé řadě jde o subjekty s velmi vysokou úrovní implementovaných organizačních a technických opatření na ochranu zpracovávaných osobních údajů. Dále se zde v souladu se čl. 33 odst. 3 Obecného nařízení jedná převážně o technické údaje a agregované informace (popis povahy daného případu porušení, jeho pravděpodobných důsledků a popis opatření, která správce přijal nebo navrhl k přijetí), které tudíž často ani nemají povahu osobních údajů.

Vzhledem k tomu, že na činnost obou dozorových úřadů dopadá ústavní zásada enumerativnosti veřejnoprávních pretenzí,[92] shledáváme za nezbytné zákonné zakotvení takovéhoto systematického sdílení informací. Za vhodné řešení vnímáme vytvoření platformy pro sdílení informací, které by stálo především na systematickém předávání relevantních

---

89 Jedním z nedávných zdůraznění aktuality těchto závazků je přijetí zákona č. 12/2020 Sb., o právu na digitální služby.

90 Srov. POLČÁK, Radim et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, 2019, roč. 158, č. 1, s. 92–93. ISSN 0231-6625.

91 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

92 Srov. čl. 2 odst. 3 zákona č. 1/1993 Sb., Ústava České republiky.

informací o ohlášených případech porušení ze strany ÚOOÚ a zpětné sdílení výstupů analýzy a vyhodnocení těchto situací za využití odborných a institucionálních kapacit bezpečnostních týmů zpět na ÚOOÚ. Cílem tohoto nastavení je zefektivnění využívání existujících nástrojů chytré regulace, za účelem zvýšení ochrany poskytované právům a svobodám dotčených subjektů údajů skrze oba právní rámce.

Současně by měla být posílena odborná podpora a včasná zpětná vazba na ohlášení povinných subjektů dle Obecného nařízení pro zvýšení jejich motivace k dodržování souladu s touto nedávno zavedenou povinností. Za hlavní nedostatek normativní struktury chytré regulace v rámci ochrany osobních údajů v České republice totiž dle výše nastíněných statistik zřejmě platí její nízké dodržování ze strany povinných subjektů. Nejsme si přitom vědomi významných aktivit ÚOOÚ směřujících k vynucování této povinnosti, což přikládáme složitosti odhalení subjektu, který neohlásil případ porušení bez podnětu podaného ÚOOÚ, a personálním výzvám spojeným s obsazením této agendy. Zde proto vnímáme v nastíněném řešení vhodný nástroj pro zlepšení situace. Skrze sdílení informací a využívání analytických kapacit bezpečnostních týmů CERT by mělo dojít k institucionální podpoře ÚOOÚ v rámci této agendy za současného obohacení informovanosti složek kybernetické bezpečnosti. To by mělo usnadnit prosazování dodržování ohlašovací povinnosti, a také nabídnout personálu ÚOOÚ lepší vhled do relevantních aspektů kybernetické bezpečnosti a aktuálních hrozeb, které lze vnímat za přínosné a přenositelné do poradních, vzdělávacích i nápravných činností směřujících k posilování ochrany zpracovávaných osobních údajů.

Lepší komunikace a podpora povinným subjektům dle Obecného nařízení by měla přispět k míře plnění ohlašovací povinnosti. Účelné využívání informací pro udržování a zvyšování kybernetické bezpečnosti pak posiluje společný zájem správců, subjektů údajů a dozorového úřadu na zajištění vysoké úrovně ochrany zpracovávaných osobních údajů, vhodnému nastavení bezpečnostních opatření a minimalizaci následků případů porušení skrze včasnou a adekvátní reakci všech těchto subjektů. To by mělo dále vést i ke snížení počtu případných neohlášených kybernetických bezpečnostních hrozeb skrytých v sítích či systémech obchodních partnerů, či dalších subjektů, se kterými povinný subjekt vytváří a sdílí datové toky, což lze považovat za významný zájem správců osobních údajů na fungování tohoto mechanismu chytré regulace.

Z hlediska bezpečnostních týmů CERT je využití informací získávaných ÚOOÚ v rámci plošné ohlašovací povinnosti případů porušení potenciálně hodnotným zdrojem dat o aktuální situaci kybernetické bezpečnosti napříč širším prostředím informační infrastruktury, byť značná část hlášení se může týkat incidentů v důsledku lidské chyby spíše než inovativních a plošných hrozeb. 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. Možnost systematického poskytování zpětné vazby a doporučení ÚOOÚ nadto zlepšuje informovanost o vhodných a přiměřených opatřeních u širokého spektra provozovatelů a správců prvků informační infrastruktury, která může pozitivně přispět k udržování vysoké míry kybernetické bezpečnosti státu.

Taktéž z hlediska dotčených subjektů údajů jde dle našeho názoru o přínosné nastavení datových toků v rámci veřejné správy. Vyšší informovanost bezpečnostních týmů CERT pro ně znamená posílení kybernetické bezpečnosti státu i přes rostoucí složitost a různorodost prvků informační infrastruktury. Z toho vyplývá pozitivní vliv na snížení rizik zásahů do prvků informační infrastruktury a zneužití obsažených údajů. Pro řádné využití informačního potenciálu ohlašovací povinnosti případů porušení vůči ÚOOÚ je nezbytné její plošné dodržování a adekvátní reakce dozorového úřadu na obdržené informace. Pokud sdílení informací s bezpečnostními týmy CERT přispěje k účelnému využívání těchto informací, lze předpokládat taktéž kladný přínos pro ochranu práv a svobod dotčených subjektů údajů. Sdílení údajů mezi těmito složkami veřejné správy přitom nepřináší významná nová rizika a nevytváří rozsáhlé databáze citlivých údajů, které by mohly působit jako protiváha dosahovaným přínosům pro jednotlivce, a lze tedy předpokládat výsledný pozitivní efekt tohoto řešení.

V kontextu zmíněného může také vyvstávat otázka, zda není namístě při existenci nastíněné platformy pro sdílení informací hledat cestu, jak odstranit případnou dualitu ohlašovací povinnosti pro povinné subjekty podle obou právních rámců. Tento způsob snížení zátěže povinných subjektů je však problematický z několika pohledů. Předně nejsou obsahy hlášení vůči ÚOOÚ a bezpečnostním týmům CERT shodné, jelikož lze konstatovat, že hlášení vůči ÚOOÚ obsahují nad technický popis případu porušení dále informace o rozsahu dotčených osobních údajů a vznikajících rizicích pro dotčené fyzické osoby. Hlášení vůči bezpečnostním týmům však srovnatelné informace neobsahují a nelze jimi tudíž informační hodnotu hlášení vůči ÚOOÚ zcela nahradit. Další překážku představuje normativní struktura, konkrétně skutečnost, že ohlašovací povinnost dle Obecného nařízení je založena přímo použitelným unijním nařízením, a není ji tedy přípustné derogovat speciální národní právní úpravou v ohledech, které nařízení či evropské právo nepředvídá. Stejně tak odstranění již vytvořené komunikační vazby mezi bezpečnostními týmy a subjekty povinnými hlásit kybernetické bezpečnostní incidenty není vzhledem k významu těchto informací pro zajišťování vysoké míry kybernetické bezpečnosti státu a udržování následného funkčního kontaktu s těmito subjekty[93] namístě zvažovat jako příhodné. Jak nastíněno výše, v současné době překryv ohlašovací

93 Jak uvádí CSIRT.CZ, na nahlášení incidentu zpravidla navazuje až několik desítek e-mailů v rámci bližší komunikace s daným subjektem a reakce bezpečnostního týmu na danou informaci. Srov. Zpráva o činnosti CSIRT.CZ (národní CSIRT ČR) za rok 2018. *CSIRT.CZ* [online]. Praha, 2019, s. 4 [cit. 2. 4. 2020]. Dostupné z: https://csirt.cz/media/filer_public/4e/dc/4edc3bff-5750-4527-82dc-3f155f578158/csirt_zprava_2018.pdf

povinnosti není značný, podstatné je však s přihlédnutím k technologickým a společenským trendům nalézat řešení, které umožní vyvarovat se vzniku významné duality těchto ohlašovacích povinností *de lege ferenda*.

Závěr

Tento příspěvek byl věnován premise, že v moderní, stále propojenější společnosti dochází k rostoucímu obsahovému překryvu ohlašovacích povinností na základě právních rámců ochrany osobních údajů a kybernetické bezpečnosti. Ty jsou přitom vnímány jako funkční projevy tzv. chytré regulace, díky které složky veřejné správy získávají aktuální informace o regulované oblasti, které jim umožňují včasnou a adekvátní reakci. Jak bylo poukázáno výše, přes jisté odlišnosti v perspektivě těchto úprav, obě směřují v úzké provázanosti k ochraně souboru distributivních práv jednotlivců v kontextu fungování informační infrastruktury a všudypřítomných datových toků. Po bližším vymezení povinnosti hlášení kybernetického bezpečnostního incidentu dle § 8 ZoKB a ohlašovací povinnosti při porušení zabezpečení osobních údajů dle článku 33 Obecného nařízení, byla zdůrazněna nadále narůstající provázanost s ohledem na proměnu technologického prostředí, ve kterém se tyto povinnosti uplatňují. Vzhledem k předpokládaným důsledkům rozvoje internetu věcí a souvisejícím výzvám pro zajištění kybernetické bezpečnosti a ochranu osobních údajů bylo v rámci diskuse navrženo užší systematické propojení činnosti ÚOOÚ a bezpečnostních týmů CERT v rámci optimalizace sdílení informací v elektronizované veřejné správě. Bylo poukázáno na přínosy, které toto provázání má pro informovanost bezpečnostních týmů CERT o zranitelnostech vážících se k prvkům informační infrastruktury, se kterými nejsou v přímém kontaktu, ale které musejí být v rostoucí míře brány v potaz při hodnocení situace kybernetické bezpečnosti státu. Bylo také představeno, jaký přínos by mělo toto provázání nejen pro fungování ÚOOÚ, ale i pro vlastní dodržování souladu s povinností ohlašování případů porušení zabezpečení osobních údajů ze strany povinných subjektů. V tomto směru byly naznačeny motivující prvky pro tyto subjekty a zvážen byl také přínos pro primárně chráněné subjekty na základě obou právních rámců, tedy dotčené fyzické osoby.