IP ADRESY V KYBERNETICKÉ BEZPEČNOSTI[*]

JAKUB HARAŠTA[**], JAKUB MÍŠEK[***]

ABSTRAKT

Za účelem zajištění kybernetické bezpečnosti dohledová pracoviště zpracovávají informace o bezpečnostních incidentech. Klíčovým prvkem pro vytvoření potřebných analýz je IP adresa zařízení zapojených do bezpečnostních incidentů. Článek ve své první části shrnuje a popisuje činnost dohledových pracovišť. Ve druhé části je provedena analýza pojmu osobní údaj a uzavíráme, že IP adresy je de lege lata nezbytné považovat za osobní údaje. Na dohledová pracoviště kybernetické bezpečnosti tedy dopadají povinnosti správce osobních údajů. Základní povinností je zpracovávat pouze osobní údaje, k jejichž zpracování má správce údajů zákonný důvod. Ve třetí části článku pak nabízíme možné legitimizační důvody ke zpracování osobních údajů s akcentem na zpracování za účelem ochrany práv a právem chráněných zájmů správce údajů nebo třetích osob.

KLÍČOVÁ SLOVA

Ochrana osobních údajů; kybernetická bezpečnost; zpracování osobních údajů; oprávněný zájem správce údajů; CSIRT

ABSTRACT

Cyber Security Response Teams (CSIRT/CERT) are processing information on the course of protection of information networks. IP addresses of devices in-

[*] Tento článek vznikl rámci projektu Elektronické důkazy (MUNI/A/1296/2014).

[**] Autor je asistentem na Ústavu práva technologií PrF MU, Kontaktní e-mail: jakub.harasta@law.muni.cz

[***] Autor je prezenčním doktorským studentem na Ústavu práva technologií PrF MU, Kontaktní e-mail: jkb.misek@mail.muni.cz

volved in the security incidents are the key element for traffic analysis and other techniques used for investigation of incidents. In the first part, this article summarises and briefly describes the function of CSIRT teams. An analysis of "personal data" is provided in the second part of the article. It reaches the de lege lata conclusion that IP addresses are personal data. Therefore, CSIRT teams fall within the scope of the directive 95/46/EC and have to fulfil all the duties prescribed for data controllers. The third part of this article discusses way to achieve lawful processing of personal data and further explores the possibility to use the legitimate interest of the controller or a third party for this purpose.

KEY WORDS

Personal Data Protection; Cyber Security; Personal Data Processing; Legitimate Interest of Data Controller; CSIRT

1. ÚVOD

Jak se kybernetická bezpečnost postupně dostává do středu zájmu bezpečnostních složek, národních států i mezinárodních organizací, vyplývají na povrch i otázky souladu některých doporučovaných best practices s existující legislativou. Tento text aspiruje, vzhledem k svému charakteru, na otevření odborné diskuze některých otázek – konkrétně diskuze souladu činnosti dohledových center kybernetické bezpečnosti s legislativou chránící osobní údaje. V článku nejprve vymezíme pojem dohledových pracovišť kybernetické bezpečností, včetně některých činností, které vykonávají či mohou vykonávat. Jedná se zejména o sledování provozu na vlastních sítích za účelem vyhodnocování bezpečnostních incidentů. Budeme vycházet z tvrzení o existujícím pnutí mezi bezpečností a soukromím které, jakkoli se stává kýčem, je existujícím fenoménem s přihlédnutím k některým technikám používaným dohledovými pracovišti. Ve druhé části se pak budeme věnovat rozsahu pojmu osobních údajů, který de lege lata zahrnuje i IP adresy a podobné údaje provozního charakteru. V tomto textu jsme se rozhodli s tímto názorem nepolemizovat, ale soustředit se na otázku, jak umožnit dohledovým pracovištím vykonávat jejich činnost i v případě, že údaje jimi zpracovávané (shromažďované, předávané) za účelem evidence bezpečnost-

ních incidentů je nutné považovat za údaje osobní. Klíčovou otázkou, na kterou přímo hledáme odpověď ve třetí části článku, tak je, jestli poskytuje legislativa chránící osobní údaje legitimizační faktor pro zpracování osobních údajů dohledovými pracovišti kybernetické bezpečnosti.

2. DOHLEDOVÁ PRACOVIŠTĚ KYBERNETICKÉ BEZPEČNOSTI

Funkční dohledové pracoviště představuje jeden z důležitých prvků zajištění kybernetické bezpečnosti subjektu.[1] Jakkoli je možné označovat takováto pracoviště či týmy jako CSIRT,[2] CERT[3] nebo CIRC,[4] formální označení nehraje roli. Za dohledové pracoviště kybernetické bezpečnosti je tak v širším smyslu možné označit v podstatě jakékoli obecné kapacity určené pro řešení bezpečnostních incidentů.[5] Můžeme tak rozlišovat mezi vládními pracovišti, [6] národními pracovišti, [7] dále interními týmy přidruženými ke vzdělávacím a výzkumným institucím,[8] poskytovatelům služeb informační společnosti,[9] finančním společnostem,[10] nekomerčním subjektům[11] a případnými dalšími pracovišti.[12] Tyto týmy mají, kromě odlišné povahy, i od-

---

[1] HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR. *Revue pro právo a technologie,* 2013, roč. 4, č. 8, s. 81.

[2] Angl. Computer Security Incident Response Team.

[3] Angl. Computer Emergency Response Team.

[4] Angl. Computer Incident Response Capability.

[5] V úzkém smyslu je pak nutné dosáhnout formalizace procedur, srov. ENISA. *Good Practice Guide for Incident Management* [online]. 2010 [vid. 8. říjen. 2015]. Dostupné z: https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management, srov. dohledová pracoviště zařazená na seznam, akreditovaná nebo certifikovaná jako Trusted Introducers (dostupné na https://www.trusted-introducer.org/directory/index.html).

[6] Viz ZoKB § 20. V současné době GovCERT.cz.

[7] Viz ZoKB § 17. V současné době CSIRT.CZ.

[8] Např. CESNET-CERTS nebo CSIRT-MU.

[9] Např. CDT-CERT, O2.cz CERT, SEZNAM.CZ-CSIRT.

[10] Např. CSOB-Group-CSIRT.

[11] Např. CZ.NIC-CSIRT.

[12] Např. neakreditovaný SKY-CERT (Estonsko), jehož vznik se datuje přibližně do doby, kdy byl společnost eBay získala Skype Technologies.

lišné okruhy působnosti,[13] které mohou být určené rozsahem IP adres[14], identifikací autonomního systému[15], identifikací domén[16] nebo slovním popisem.[17] Vymezené pole působnosti jednoho týmu se může překrývat s jinými týmy,[18] což samozřejmě může způsobovat problémy, které je nutné řešit na úrovni dohody mezi týmy navzájem.[19]

Společným znakem těchto pracovišť je ale ochrana definovaného okruhu působnosti před hrozbami[20] – bez ohledu na to, jestli se jedná o fyzickou či virtuální infrastrukturu nebo o kvalitu poskytovaných služeb. Za tímto účelem dohledová pracoviště vykonávají řadu analytických i jiných činností. Často dochází k logování, analyzování provozu,[21] implementaci meta-systémů pro agregační a korelační činnosti[22] apod.

V rámci struktury dohledových pracovišť mají v České republice specifické postavení vládní a národní CERT. Existence obou těchto pracovišť je předepsána zákonem č. 181/2014, o kybernetické bezpečnosti (dále jen „ZoKB“).

ZoKB v § 20 předepisuje existenci vládního CERTu jako součásti Národního bezpečnostního úřadu, jehož roli v současné době plní GovCERT.cz působící v rámci Národního centra kybernetické bezpečnosti v Brně. Vládní CERT se svými nařizovacími a kontrolními pravomocemi působí pouze na informační a komunikační systémy, jejichž funkčnost má pro Českou repub-

[13] Angl. Constituency. Srov. ENISA 2010, op. cit., s. 14-19.

[14] CSIRT-MU např. 147.251.0.0/16, tedy 147.251.0.0 až 147.251.255.255.

[15] O2.cz CERT např. AS5610, 20884, 28725, 51154.

[16] CDT-CERT např. *.cdt.cz, *.cd-t.cz, *.cd.cz.

[17] CZ.NIC např. *„Polem působnosti týmu CSIRT.CZ je celá Česká republika, tzn. všichni uživatelé a všechny sítě provozované v České republice se nachází ve sféře vlivu CSIRT.CZ“* CZ.NIC. *O nás* [online]. [vid. 8. říjen 2015]. Dostupné z: https://www.csirt.cz/page/882/o-nas/.

[18] Např. povinnosti stanovené v § 8 ZoKB, dále vztah mezi institucionálním dohledovým pracovištěm a pracovištěm poskytovatele konektivity.

[19] Srov. ENISA 2010, op. cit., s. 19. Toto samozřejmě může hrát roli při případné snaze zajistit důkazní prostředek.

[20] Za naplnění tohoto účelu se pracoviště samozřejmě mohou neformálně i formálně sdružovat, spolupracovat a předávat si poznatky (ShadowServer foundation, různá ad hoc uskupení pro pokrytí sítí senzory atp.).

[21] Nástroje typu NetFlow pro vytváření, sběr a analýzu dat.

[22] Angl. Security Information and Event Management.

liku zásadní význam – jedná se zejména o prvky kritické informační a komunikační infrastruktury a o významné informační systémy. Vládní CERT v souladu se zákonem přijímá hlášení o kybernetických bezpečnostních incidentech a postiženým subjektům poskytuje metodickou podporu a součinnost. V anonymizované podobě (tedy bez identifikace subjektu odesílajícího hlášení) přijímá údaje i od národního CERTu.

Existenci národního CERTu předepisuje ZoKB v § 17 a reflektuje tím poptávku soukromoprávních subjektů po centralizovaném řešení sběru informací o kybernetické bezpečnosti, které by bylo nemělo veřejnoprávní charakter. Úlohu národního CERTu v současné době plní CSIRT.cz. Ten poskytuje, stejně jako vládní CERT, metodiku a asistenci při řešení různých typů kybernetických bezpečnostních incidentů v rámci systémů, které nepodléhají vládní CERTu – zejména se jedná o poskytovatele služeb elektronických komunikací a osoby zajišťující významnou síť. Národní CERT nedisponuje žádnými exekutivními pravomocemi, ale funguje právě za účelem pomoci subjektům, které mají zájem o možnost kolektivní ochrany před kybernetickými hrozbami.

Český právní řád existenci žádných dalších dohledových pracovišť přímo nezakládá, ale minimálně u subjektů provozujících prvky kritické infrastruktury se dá konstatovat minimálně předpoklad. Celý režim fungování těchto pracovišť je zde výrazně odlišný od vládního nebo národního dohledového pracoviště a výrazně záleží na tom, jestli je subjekt provozující dohledové pracoviště povinným subjektem dle ZoKB. Vše se odráží od odpovědi na otázku, jestli přijmeme IP adresy za osobní údaje a budeme tím pádem muset zkoumat účel jejich zpracování.

3. IP ADRESA JAKO OSOBNÍ ÚDAJ DE LEGE LATA

3.1 VYMEZENÍ POJMU OSOBNÍHO ÚDAJE

Směrnice o ochraně osobních údajů definuje pojem „osobní údaj" velmi široce jako „*veškeré informace o identifikované nebo identifikovatelné osobě*".[23] Tato osoba je v terminologii ochrany osobních údajů označována jako „subjekt údajů". Stejný článek dále vymezuje, že identifikovatelnou osobou se rozumí „*osoba, kterou lze přímo či nepřímo identifikovat*" a následuje demonstrativní výčet prvků, které k identifikaci mohou vést včetně identifikačního čísla, nebo odkazu na zvláštní prvky její identity. Je třeba si uvědomit, že Směrnice o ochraně údajů byla přijata před dvaceti lety po několika letech legislativního procesu, a navíc vychází z Úmluvy Rady Evropy o ochraně soukromí z roku 1981[24]. Ideově je tak zakotvena na přelomu osmdesátých a devadesátých let. Uvedené příklady tak konvenují s dobovou představou o tom, co může vést k identifikaci jedince a slouží opravdu toliko jako interpretační pomůcka.

Přímou identifikací je myšlen takový proces, kdy k identifikaci subjektu údajů stačí právě daná informace, zatímco nepřímou identifikací je proces, kdy je pro určení subjektu údajů třeba spojit dohromady více informací, které třeba samy o sobě danou osobu neidentifikují.[25] Z uvedeného vyplývá, že dle směrnice je osobním údajem jakákoli informace, která vede, nebo může vést k identifikaci fyzické osoby. Tento mohutný rozsah potvrzuje i recitál 26 směrnice, který stanoví: „*pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně pou-*

[23] Čl. 2 písm. a) Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [vid. 8. 10. 2015].

[24] Srovnej *Thirty years after, The OECD privacy guidelines*. OECD, © 2011 [cit. 8. 10. 2015]. Dostupné z: http://www.oecd.org/sti/ieconomy/49710223.pdf.

[25] Pracovní skupina pro ochranu údajů zřízená podle článku 29. *Stanovisko č. 4/2007 k pojmu osobní údaj*. WP 136. Evropská komise [online]. [vid. 8. říjen 2015], s. 13 – 14. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf.

žity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby.“[26] Recitál, byť sám o sobě není normativně závazný, je vhodnou interpretační pomůckou. Výhodou takto širokého vymezení je jeho technologická neutralita. Ať se identifikující informace nachází v jakékoli formě, dopadá na ni režim zákonné úpravy ochrany osobních údajů. Nevýhodou naopak může být určitá bezbřehost, kdy je interpretačně nesmírně složité určit hranici, na jejíž jedné straně stojí prvky, u kterých je vzhledem k jejich povaze ještě smysluplné řadit je pod zákonnou ochranu, a na jejíž druhé straně stojí prvky, kdy už to smysluplné není.

Široký rozsah ustanovení je dán zejména informacemi, které vedou k identifikaci nepřímo. Jako příklad můžeme uvést notoricky známý případ Netflix.[27] Společnost Netflix poskytující službu online půjčování filmů zveřejnila statistiky toho, jak její uživatelé hodnotili sledované filmy. Byly uveřejněny následující informace: jméno filmu, hodnocení v rozsahu jedné až pěti hvězdiček a datum hodnocení. Tato data byla stále svázána na jednoho člověka, byť byly přímé identifikační údaje z datové sady odstraněny. Nedlouho poté, co ke zveřejnění došlo, bylo prokázáno, že postačuje, aby člověk znal přesné hodnocení šesti netradičních filmů, aby dokázal jedinečně identifikovat 84% uživatelů. K přesné identifikaci 99% uživatelů pak stačilo vědět přibližné datum (v rozmezí dvou týdnů) ohodnocení šesti filmů, nehledě na to zda byly netradiční, nebo obecně známé.[28] V takovém případě se všechny uvedené informace – ohodnocené filmy, hodnota a datum hodnocení – stávají osobními údaji dle Směrnice o ochraně údajů. Tak poznamenává Tikk, jde zde o jedinečnou kombinaci informací, které dohromady tvoří možnost k identifikaci jedince.[29]

---

[26] Recitál 26 Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [vid. 8. říjen 2015].

[27] Srovnej OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. 2009, roč. 57, č. 6, s. 1720.

[28] Ibid., s 1721.

[29] TIKK, Eneken. IP Addresses subject to personal data regulation. In: TIKK, Eneken; TALIHÄRM, Anna-Maria (eds.).*International Cyber Security Legal & Policy Proceedings* [online]. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010, s. 28.

Podíváme-li se do ZoOOU, konkrétně do § 4 písm. a), zjistíme, že český zákon téměř doslovně přebírá definici pojmu osobní údaj ze Směrnice o ochraně údajů a tak vše výše uvedené platí plně i pro Českou republiku. Dokládá to ostatně i stanovisko Úřadu pro ochranu osobních údajů věnované vysvětlení pojmu „osobní údaj".[30]

Při interpretaci šíře dopadu pojmu osobní údaj hovoříme o dvou přístupech k pojetí tohoto pojmu.[31] Prvním je subjektivní pojetí, při kterém je otázka identifikovatelnosti nahlížena z pozice osoby, která s informací pracuje. Pokud má informace takovou povahu, že neidentifikuje subjekt údajů přímo, a zároveň daná osoba nemá rozumnou možnost získat další informaci, která by způsobila, že by mohlo dojít k nepřímé identifikaci (byť by někde objektivně existovala), není první informace osobním údajem. Opakem je potom objektivní pojetí, dle kterého nezáleží na možnostech a schopnostech osoby disponující první informaci. Pokud někde objektivně existuje další informace, která by spojením s tou první mohla vést k identifikaci subjektu údajů, je první informace rovněž osobním údajem a je třeba k ní tak přistupovat. V této situaci není podstatné, zda a jak může druhou informaci daná osoba zjistit.

De lege lata je třeba při interpretaci vycházet z objektivního přístupu k pojmu osobního údaje. Účelem Směrnice o ochraně údajů je zajištění vysoké úrovně ochrany soukromí skrze ochranu osobních údajů.[32] To pravidelně potvrzuje ve svých rozhodnutích Soudní dvůr Evropské unie (dále „SDEU").[33] Jak vyplývá z kontextu celé Směrnice o ochraně údajů, právní úprava ochrany osobních údajů chrání soukromí na prevenčním principu, na rozdíl od občanskoprávní úpravy ochrany soukromí, která má

[30] Stanovisko Úřadu pro ochranu osobních údajů č. 3/2012 z března 2012, K pojmu osobní údaj. [vid. 8. říjen. 2015]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9187.

[31] Srovnej NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů? *Právní rozhledy*. 2015, roč. 2015, č. 12.

[32] Recitál 10 Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [vid. 8. 10. 2015].

[33] Srovnej například bod 66 rozhodnutí Google Spain (C-131/12), nebo bod 27 rozhodnutí Ryneš (C-212/13).

funkci reparační a satisfakční. Aby mohla být prevence účinná, je nezbytné pokud možno co nejvíce zabránit protizákonnému zpracování osobních údajů. Za předpokladu, že by bylo k pojmu osobní údaj přistupováno ze subjektivního hlediska, mohlo by dojít k nešetrnému nakládání s údaji[34], u kterých může v pozdější fázi jejich životního cyklu dojít ke spojení s jinými údaji, a tak způsobit zásah do soukromí subjektu údajů. Přihlédneme-li navíc opět k nedávno potvrzené ustálené rozhodovací praxi SDEU, je nezbytné při rozhodování, zda je zpracování podřízeno režimu Směrnice o ochraně údajů, interpretovat situaci tak, aby Směrnice aplikována byla.[35] Případné výjimky z povinností správce jsou pak řešeny již v rámci režimu ochrany osobních údajů. Subjektivní pojetí osobního údaje v důsledku vede k zúžení věcné působnosti Směrnice o ochraně údajů, což je v rozporu ustáleným názorem SDEU. Z těchto důvodů se domníváme, že je pojem osobní údaj nezbytné vykládat z pozice objektivního přístupu. Tuto interpretaci nakonec potvrzuje i výše uvedený recitál 26 Směrnice o ochraně údajů.

3.2 IP ADRESA JAKO OSOBNÍ ÚDAJ

Při síťovém provozu se zařízení připojují za užití IP adres a při procesu komunikace jsou zaznamenávány adresy jak odesílatele, tak recipienta. Vzhledem k tomu, že již v současné době je k internetu připojeno více zařízení, než nyní primárně používaný systém IPv4 umožňuje, je tento nedostatek vyřešen protokolem NAT („Network Address Translation“). Příkladem zařízení, kde je tento protokol užíván, jsou domácí routery, k nimž je připojeno několik samostatných zařízení. Router má jednu IP adresu, kterou užívá na komunikaci s vnějším světem, a zároveň přiděluje vlastní IP adresy zařízením k němu připojeným. Za jednu veřejnou IP adresou tak může být „ukryto“ více zařízení.

IP adresa je série číslic, sloužící k jedinečné identifikaci zařízení připojeného k síti internet. Skládá se ze dvou částí, identifikace sítě, která určuje geografickou lokalizaci sítě, a „Host ID“ přesně určující konkrétní zařízení

[34] Byť v danou chvíli nejsou osobními údaji.

[35] Viz bod 28 rozhodnutí Ryneš (C-212/13), který odkazuje na starší rozhodnutí, například na Digital Rights Ireland (C-293/12).

nebo část sítě. Na základě toho, zda je jedna IP adresa trvale přiřazena konkrétnímu zařízení, nebo zda se IP adresa zařízení mění v průběhu času, rozlišujeme ještě statické a dynamické IP adresy. V současné době, vzhledem k výše uvedenému nedostatku IP adres při využívání protokolu IPv4 převažují dynamické adresy, které jsou konkrétním zařízením přiděleny ve chvíli, kdy se připojí k internetu. Nová technologie IPv6, která je postupně zaváděna, nabízí řádově větší počet možných současně připojených zařízení, díky čemuž umožní, aby více zařízení mělo statickou IP adresu. Jak uvádí Lah, tento stav může mít za následek, že jedno konkrétní zařízení bude dle IP adresy vždy dohledatelné nehledě na to, odkud se připojuje, a bude tak snadnější sledovat pohyb konkrétních zařízení po světě.[36]

McIntyre připomíná, že je potřeba zdůraznit, že IP adresa je skutečně vázána k zařízení a nikoli člověku.[37] To je důležité z hlediska úvah, zda může jít o osobní údaj.[38] Aby byla naplněna zákonná definice, musí informace odkazovat na fyzickou osobu, nikoli na technické zařízení. IP adresa je však vzhledem k soukromí velmi specifickou informací, vzhledem k úzkému provázání zařízení, jako je osobní počítač, nebo mobilní zařízení se svým vlastníkem.[39] Je obvyklé, že osobní počítač, nebo mobilní zařízení, používá právě jedna osoba. Byť je samozřejmě možné, aby je půjčila někomu jinému, v průměru se to nestává v takové míře, aby nebylo možné pracovat s uvedenou domněnkou jako faktem. Pokud jsou ukládány klíčové údaje identifikující zařízení, jako právě jeho IP adresa, IP adresy, na které se připojuje, lokalitu, kde zařízení operuje a čas, kdy se tak děje, je díky tomu je možné poměrně snadno identifikovat, co daná osoba se zařízením dělala, jaké informace hledala a kde se pohybovala. Vezmeme-li jako výše uvedený příklad se statickou IPv6 IP adresou, je velmi snadné sledovat po-

[36] LAH, Frederick. Online and Locational Privacy: Are IP Addresses „Personally Identifiable Information"? *I/S: A Journal of Law and Policy for the Information Society*. 2009, roč. 4, s. 686.

[37] MCINTYRE, Joshua J. Balancing Expectations of Online Privacy: Why Internet Protocol (ip) Addresses Should Be Protected as Personally Identifiable Information. *DePaul Law Review*. 2011, roč. 60, s. 8.

[38] A hraje roli např. i v rámci dokazování provozními a lokalizačními údaji.

[39] Toto konstatuje například WP 29 ve stanovisku č. 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení, s. 7.

hyb osob po celé planetě. Ovšem i v případě dynamických IP adres je možné snadno dojít ke konkrétnímu zařízení a tím i fyzické osobě. Litvinov k tomu říká: „*Internet service providers can determine which subscriber received a particular address and the time at which the address was assigned. Such information has been used to identify individuals for the purposes of imposing criminal liability.*“[40] IP adresa je tak klíčovou nepřímo identifikující informací, esenciální složkou množiny data, které vedou k identifikaci konkrétního člověka. Proto je třeba považovat ji za osobní údaj.

Litvinov se dotýká institutu povinného uchovávání provozních a lokalizačních údajů, známého spíše jako „data retention“.Do evropského práva byla zavedena směrnicí 2006/24/ES, posléze zneplatnělou SDEU v rozhodnutí Digital Rights Ireland. I přes to v současné době v řadě členských států, včetně České republiky, je zavedena povinnost poskytovatelů služeb elektronických komunikací plošně uchovávat po určitou dobu[41] provozní a lokalizační údaje uživatelů služeb pro účely trestního vyšetřování a dalších zákonem uvedených případů.[42] Uchovávána jsou metadata popisující provoz sítě, tedy kdo koho kontaktoval, kdy tomu tak bylo a geolokalizační údaje, kde komunikace probíhala. Tyto údaje, mezi kterými je rovněž IP adresa, jsou přiřaditelné konkrétnímu uživateli služeb, kterého je na jejich základě možné identifikovat. Jedná se proto o osobní údaje.

Vraťme se k otázce subjektivního a objektivního pojetí osobních údajů. Pokud bychom vycházeli ze subjektivního pojetí, bylo by rozhodování, zda je IP adresa osobním údajem komplikovanější. Záleželo by totiž na osobě správce. Jako příklad můžeme vzít společnost A, poskytovatele služeb informační společnosti, který loguje IP adresy svých klientů a na základě dalších informací vytváří profily pro cílenou reklamu. Při subjektivním pojetí

[40] LITVINOV, Aleksandr V. The Data Protection Directive as Applied to Internet Protocol (IP) Addresses: Uniting the Perspective of the European Commission with the Jurisprudence of Member States. *The George Washington international law review*. 2013, roč. 45, č. 3, s. 584.

[41] V České republice je to šest měsíců dle § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

[42] Tato povinnost je evropským právem umožněna díky znění čl. 15 směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

osobního údaje by se o osobní údaj jednat nemuselo, protože společnost A nemá zákonnou možnost, jak se dostat k doplňující informaci, která by z IP adresy osobní údaj udělala. Přístup k údajům uchovávaným poskytovateli elektronických komunikací, mají jen taxativně určené instituce. V České republice jsou to Policie ČR a další orgány činné v trestním řízení, zpravodajské služby a Česká národní banka.[43] Lundevall s Tanvikem ve svém článku vycházejí z tohoto předpokladu a navrhují dvoustupňový test pro určení, zda je IP adresa osobním údajem. Prvním stupněm je test legality[44], který je splněn jen, pokud správce údajů má možnost legální cestou získat doplňující informace, které by napomohly k identifikaci subjektu údajů. Vzhledem k tomu, že v příkladné situaci tato možnost není,[45] nejednalo by se dle subjektivního pojetí o osobní údaje.

Dle našeho názoru je však s touto interpretací nutné nesouhlasit. Jak bylo uvedeno výše, vzhledem k prevenčnímu principu zákonné úpravy ochrany osobních údajů je třeba zaujmout objektivní přístup. Pokud někde existuje informace, která může IP adresu doplnit tak, aby identifikovala konkrétní zařízení a tím jedince, je IP adresa osobním údajem. Tím spíš, že v tomto případě s jistotou víme, že takové informace existují. Přistoupit na uvedený test legality by znamenalo snížit úroveň ochrany subjektů údajů. Pokud je chráněno nakládání s informacemi, ke kterým má osoba legální přístup, tím spíš je třeba chránit nakládání s informacemi, k nimž je přistupováno nelegálně. Výklad, že je možné volně nakládat s IP adresami (tedy například je bez dalšího zveřejnit na internetu) a vystavit je tak riziku spojení s jinými údaji, je dle našeho názoru v rozporu se Směrnicí o ochraně údajů.

Interpretace IP adresy jako osobního údaje vede krom pozitivních dopadů, jako je zvýšení ochrany soukromí jedince, i k praktickým problémům

[43] § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

[44] LUNDEVALL-UNGER, Patrick; TRANVIK, Tommy. IP Addresses – Just a Number? *International Journal of Law and Information Technology* [online]. 2011, roč. 19, č. 1, s. 57 [vid. 8. říjen 2015].

[45] Oficiální cestou společnost A informace držené v rámci data retention nezíská a pokud by se je pokusila získat například hackováním databáze poskytovatele elektronických komunikací, narazí trestněprávní ochranu.

na straně správců údajů, kteří s IP adresami pracují. Z toho důvodu můžeme sledovat snahu interpretací nějakým způsobem zmírnit přísnost zákonného režimu. Například Tikk navrhuje, aby IP adresa byla chápána a hodnocena, že je osobní údaj nikoli dle své povahy, ale dle účelu, k jakému slouží. „*IP addresses can be personal data when used in investigation, but for the purpose of managing the networks and possibly also monitoring traffic and exchanging information about anomalies, the important factor is that the purpose of such processing is not to identify the individual (which is the core concern of the Directive) but detecting threats, vulnerabilities and potential defences.*“ [46] Tato interpretace však dle našeho názoru, bohužel, není použitelná. Jde opět o vnášení subjektivního prvku do objektivní otázky působnosti Směrnice o ochraně údajů. Analogicky argumentoval František Ryneš, což bylo odmítnuto jak Generálním advokátem[47], tak následně Nejvyšším správním soudem[48].

V neposlední řadě je třeba připomenout rozhodnutí SDEU, které IP adresy za osobní údaje přímo označuje, minimálně pro potřeby daného případu.[49] Na rozhodnutí ve věci Breyer[50], které do této otázky opět může přinést trochu světla, však stále čekáme. V českém prostředí IP adresu jako osobní údaj označuje Úřad pro ochranu osobních údajů ve svém stanovisku adresovaném Národnímu bezpečnostnímu úřadu.[51]

Závěrem této části je třeba upozornit na situace, kdy IP adresa za žádných okolností nemůže být osobním údajem. Jedním příkladem je situace, kdy, jak uvádí Prokeš „*dostupnými nástroji nelze identifikaci provést, zej-*

---

[46] TIKK, Eneken. IP Addresses subject to personal data regulation. In: TIKK, Eneken; TALIHÄRM, Anna-Maria (eds.). *International Cyber Security Legal & Policy Proceedings* [online]. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010, s. 38.

[47] Bod 20 Stanoviska generálního advokáta Niila Jääsikenena k věci C-212/13 František Ryneš proti Úřadu pro ochranu osobních údajů.

[48] Bod 71 rozhodnutí rozsudku Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 113/2012 – 133. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 8. 10. 2015].

[49] Body 26 a 51 rozhodnutí Scarlet Extended (C-70/10).

[50] Věc C-582/14.Předběžná otázka byla podána 17. prosince 2014.

[51] Stanovisko Úřadu pro ochranu osobních údajů adresované Národnímu bezpečnostnímu úřadu. *Povinnost Národního bezpečnostního úřadu evidovat kybernetické bezpečnostní incidenty z pohledu právní úpravy ochrany osobních údajů.*

ména pokud jsou údaje uchovávány krátce.“[52] Další možností je fenomén Internet of Things. Jeho principem je připojení velkého množství zařízení, které však nejsou provázány s konkrétním člověkem. Jedná se například o různá čidla monitorující své okolí, elektronické spotřebiče, systémy řídící klimatizaci a podobně. V takovém případě není možné vytvořit podobnou vazbu mezi zařízením a člověkem jako například v případě mobilních telefonů, nebo osobních počítačů a nemůže se proto jedna o osobní údaje. Protože však není technicky možné na úrovni osoby logující internetový provoz dodatečně odfiltrovat IP adresy zařízení Internet of Things od IP adres mobilních zařízení a osobních počítačů, je třeba ke všem IP adresám přistupovat tak, jako by osobními údaji byly.

4. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ DOHLEDOVÝMI PRACOVIŠTI KYBERNETICKÉ BEZPEČNOSTI

Jak bylo výše uvedeno, dochází ze strany dohledových pracovišť kybernetické bezpečnosti při jejich činnosti často ke zpracování údajů, které jsou de lege lata údaji osobními. Při hodnocení souladu předmětné činnosti s legislativou chránící osobní údaje je nutné věnovat náležitou pozornost účelu zpracování. Zpracování může probíhat zejména na základě souhlasu,[53] kde je účel specifikován, ale ani v nejmenším se nejedná o jediný mód zpracování, který můžeme pozorovat. V případě činnosti dohledových center se sice dá předpokládat existence souhlasu v případě zpracovávání bezpečnostních informací o vlastních uživatelích v rámci vlastní infrastruktury, často ale bude docházet i k nutnosti zpracovávat údaje uživatelů, kteří se nacházejí vně dané sítě. V tomto případě nebude možné získat platný souhlas a je tak nutné zkoumat, jakým jiným způsobem je možné legitimizovat zpracování osobních údajů dohledovými pracovišti. V úvahu připadá, v případě vládního a národního dohledového pracoviště, zejména plnění právní povinnosti správce, tedy zpracování podle § 5 odst. 2 písm. a)

[52] PROKEŠ, Josef. IP adresa v ochraně osobních údajů. *Data Security Management*. 2014, roč. 2014, č. 4, s. 31.

[53] Více k institutu souhlasu viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů internetu. *Revue pro právo a technologie.* 2014, roč. 5, č. 9, s. 3-74.

ZOOÚ, kdy zpracováváním osobních údajů dochází k plnění povinnosti zpracovávat oznámení o bezpečnostních incidentech. Stejné platí i pro dohledová pracoviště subjektů povinných podle ZoKB, tedy pro dohledová pracoviště, která zpracovávají hlášení o incidentech a postupují je národnímu a vládnímu dohledovému pracovišti – zde se jedná zejména o subjekty provozující prvky kritické infrastruktury.

Pokud není dohledové pracoviště provozováno v rámci plnění zákonné povinnosti subjekty povinnými podle ZoKB, je nutné zvažovat další faktory umožňující zpracování osobních údajů – je možné diskutovat zejména o ochraně životně důležitých zájmů subjektu údajů (§ 5 odst. 2 písm. d) nebo o ochraně práv a právem chráněných zájmů správce (§ 5 odst. 2 písm. e). Domníváme se, že nejjednodušší argumentační pozici má dohledové pracoviště (resp. jeho provozovatel) v případě zpracovávání osobních údajů, které směřuje k ochraně práv nebo právem chráněných zájmů správce – zde je možné hovořit o obecném zájmu na fungování informačních systémů a argumentovat o realizaci tohoto zájmu na konkrétní infrastruktuře ve formě činnosti dohledového pracoviště. Přesto ani legitimizace zpracování tímto účelem není zcela bez problémů, zejména ve vztahu k neurčitému pojmu oprávněného zájmu v ustanovení obsaženém.

4.1 OPRÁVNĚNÝ ZÁJEM

Paragraf 5 odst. 2 písm. e) ZOOÚ je v české legislativě přítomen jako národní podoba článku 7 písm. f) Směrnice 95/46/ES.[54] Zásadní otázkou tak je, k ochraně jakých práv a právem chráněných zájmů (v jazyce směrnice „oprávněné zájmy“) musí jednání směřovat, aby bylo možné zpracování osobních údajů legitimizovat právě tímto způsobem. V prvé řadě tedy takové zpracování musí být nezbytné pro ochranu práv správce údajů nebo jiné dotčené osoby a dále nesmí zasahovat nepřiměřeným způsobem do práv subjektu údajů. Je tedy nutné provést posuzování chráněného práva a míry zásahu do práv subjektu.

[54] Zajímavostí je, že se nejedná o přímý ekvivalent, ale nejbližší obsahovou podobu. Srov. KUČEROVÁ, Alena et al. Zákon o ochraně osobních údajů. Komentář. Praha: Nakladatelství C.H. Beck, 2012, s. 145.

Jakkoli je otázka vymezení chráněného zájmu především otázkou národních provedení směrnice 95/46/ES, pokusila se WP29 v rámci svého stanoviska[55] vymezit některé situace, ve kterých by měl mít správce osobních údajů možnost pokrýt zpracování právě výše uvedenou výjimkou.

Oprávněný zájem musí být zákonný, tedy v souladu s aplikovatelným právem EU i s národními předpisy, dostatečně explicitně formulovaný, aby umožnil prozkoumání proporcionality ve vztahu k právům subjektu údajů, a nesmí být spekulativní.[56] Momenty, které je nutné při posuzování oprávněnosti zájmu pečlivě zvažovat, jsou mimo jiné i dodatečné záruky, které mají mitigovat dopad opatření na subjekt údajů.[57]

4.1.1 POSOUZENÍ OPRÁVNĚNOSTI ZÁJMU

V případě dohledových pracovišť kybernetické bezpečnosti je možné v nejobecnější rovině uvažovat o zájmu informační společnosti na ochraně distributivních práv právě za pomoci nedistributivní[58] kybernetické bezpečnosti. V úvahu připadá i argumentace ochranou vlastní infrastruktury, případně dodržení právních povinností (zejména prevenční povinnosti) plynoucí z provozu této infrastruktury. Jakkoli výše zmíněné stanovisko zmiňuje otázku bezpečnosti jenom v rovině obecného příkladu,[59] nejčastěji se argumentace v rovině oprávněného zájmu objevuje právě v případech individuální nebo firemní bezpečnosti, např. v případě implementace kamerových systémů v bytových domech či školských zařízeních.[60] Obecně lze říci, že je tímto způsobem možné chránit základní právo (v případě dohledových pracovišť např. právo vlastnit majetek nebo svobodně podnikat), zájem veřejnosti nebo širší komunity (tedy zájem na funkci informačních systémů, poskytování služeb, které jsou součástí standardu života a jsou pro

[55] Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, dostupné z http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[56] Tamtéž, s. 25.

[57] Tamtéž, s. 33.

[58] K pojmu srov. POLČÁK, Radim. Internet a proměny práva. S. 341-371.

[59] 6/2014, s. 25.

[60] Viz KUČEROVÁ, Alena et al. Zákon o ochraně osobních údajů. Komentář. Praha: Nakladatelství C. H. Beck, 2012, s. 148.

jednotlivce prostředkem k výkonu některých základních práv) nebo další zájmy. Problémem, kterým se WP29 ve svém stanovisku zabývá, může být společenské nebo právní uznání oprávněnosti tohoto zájmu.[61] Zejména v oblasti kybernetické bezpečnosti, jakkoli existuje v zásadě celospolečenská poptávka po jejím zajištění, je možné pozorovat značně rozdílné názory ve chvíli, kdy začínáme hovořit o konkrétních oprávněních jednotlivých subjektů. Obecný společenský zájem na zajištění určitého stupně kybernetické bezpečnosti můžeme převést na diskuzi o konkrétních oprávněních pro dohledová pracoviště, která nekontrolují pouze prvky kritické infrastruktury, ale účastní se běžného provozu (jedná se např. o poskytovatele internetové konektivity). V tu chvíli se ale existující společenský konsenzus tříští a diskuze o povaze konkrétních oprávnění se stává méně jasnou. Tento element hodnocení oprávněnosti zájmu tak může být, vzhledem k novosti dohledových pracovišť v českém právu, problematický.

4.1.2 DOPAD NA SUBJEKT ÚDAJŮ

V rámci hodnocení dopadu realizace oprávněného zájmu na subjekt údajů je nutné vzít v potaz jak benefity, které může subjektu údajů zpracování osobních údajů přinést, ale i případná rizika, která mu přináší. V případě zpracovávání IP adres a jejich uchovávání pro pozdější analýzu připadá v úvahu riziko profilování. V tuto chvíli totiž nemusí docházet ke zpracování údajů ve smyslu identifikace konkrétní osoby, ale může dojít k vytvoření profilu uživatele ve smyslu entity, která je odlišitelná od jiných entit skrze své chování nebo některé znaky – může tedy být identifikována jako jedna a tatáž v průběhu času.[62] Ostatní rizika, která zmiňuje stanovisko, tedy zejména vytvoření nebo zvýšení rizika následné diskriminace nebo ovlivnění jinak chráněného chování (svoboda projevu, svoboda výzkumu),[63] jsou v případě IP adres nejspíše jen obtížně realizovatelná – resp. jsou realizovatelná právě s přihlédnutím k profilování.

---

[61] 6/2014, s. 36.

[62] Distinkce mezi L-identifikátory a R-identifikátory. Viz KOOPS, Bert-Jaap. The Trouble with European Data Protection Law. International Data Privacy law, 2014, vol. 4, no. 4, s. 250-261. S. 257.

[63] 6/2014, s. 37.

Povaha zpracovávaných údajů bude v rámci vyvažování fungovat ve prospěch oprávněného zájmu – jak je výše uvedené, de lege lata se v případě IP adres jedná o osobní údaje, ale jejich povaha je problematická[64] a v rámci neostrých linií vyvažování zásahu do práv subjektu údajů nepůsobí právě IP adresa jako výrazný destabilizační element. Domníváme se tak zejména ve chvíli, kdy obecně je zpracování biometrických údajů za účelem zajištění fyzické bezpečnosti exponovaných pracovišť považováno za oprávněný zájem,[65] bude tomu tak i v případě řádově menšího zásahu do informačního sebeurčení subjektu údajů v případě zpracování IP adres.

Dopad na subjekt údajů může být ovlivněn i zvolenými prostředky zpracování – v případě zpracování zdánlivě nepodstatných dat (kterými IP adresy mohou být) na úrovni dostatečné pro plošný monitoring a v případě jejich kombinace s dalšími údaji může dojít ke zpracování, které nebude možné diskutovanou výjimkou pokrýt (může se jednat např. o metody deep packet inspection v případě implementace specifických bezpečnostních opatření[66]). Obecně je tedy nezbytné, v případě formulace oprávněného zájmu, věnovat pozornost formulaci opatření, která budou ke zpracování údajů poskytnuta. V případě existujících alternativ je nutné zvolit tu nejméně invazivní ve vztahu k právům subjektu údajů a v případě zpracovávání údajů je nutné volit pouze takové metody, které umožňují předvídat výstupy a nemohou delegitimizovat oprávněný zájem právě skrze nejistotu o průběhu zpracování.

Roli při posuzování vlivu na subjekt údajů hraje rovněž oprávněné očekávání subjektu – zde se domníváme, že se situace může do budoucna výrazně zlepšit se vzděláváním subjektů údajů o probíhajících opatření a o obecných činnostech dohledových pracovišť. V případě jasné komunikace uplatňovaných opatření veřejnosti se stanou některé bezpečnostní opatření implementovaná dohledovými pracovišti a jejich provozovateli součástí obecného povědomí o bezpečnosti provozu na internetu.

---

[64] Stanovisko např. hovoří o citlivosti zúčastněných údajů. Tamtéž, s. 39.

[65] Tamtéž, s. 38-39.

[66] Tamtéž, s. 39-40.

4.1.3 DODATEČNÉ ZÁRUKY

V oblasti dodatečných záruk, jejich naformulování a jejich institucionální realizace, spatřujeme nejdůležitější aspekt zpracování osobních údajů, které se spoléhá na oprávněný zájem. V současné době je z technického hlediska poměrně jednoduché implementovat opatření, která budou výrazně invazivní ve vztahu k právům subjektů údajů. Zároveň bude, vzhledem ke specifickému postavení dohledových pracovišť (nebo obecně provozovatelů komunikační infrastruktury), problematické tato opatření zjistit a ze strany uživatelů (byť odborně často velmi zdatných) přesně definovat jejich rozsah. Dohledová pracoviště tak zejména při formulaci existujících dostatečných záruk musejí být velice konkrétní, aby bylo možné dovodit existenci oprávněného zájmu, který nebude neproporcionálně zasahovat do práv subjektů údajů.

Za taková opatření je možné považovat obecně nastavení užívaných nástrojů v souladu s principy *privacy by design*, nebo formulaci specifických procedur pro přístup ke shromažďovaným údajům nebo obecně minimalizaci manuálního zpracování. V případě, že bude analýza sebraných údajů probíhat automaticky a bude v rámci dohledového pracoviště existovat přesně specifikovaný postup pro přístup k těmto údajům ze strany zaměstnanců pracoviště, vytváří se dodatečná záruka, která může podpořit sílu oprávněného zájmu a umožní realizaci některých bezpečnostních opatření. Několikastupňová autorizace v rámci hierarchie dohledového pracoviště, přizvání externího subjektu pro zajištění nestrannosti nebo vymezení specifických situací, kdy je přístup možný, konkretizuje cíle opatření a přispívá tím k předvídatelnosti zpracování a větší jistotě dohledového pracoviště nebo jeho provozovatele. Dalším způsobem zvýšení dodatečných záruk je pak zkrácení doby uchovávání údajů.

5. ZÁVĚR

V rámci tohoto textu jsme se zabývali možností dohledových pracovišť kybernetické bezpečnosti zpracovávat údaje, které jsou de lege lata pova-

žované za osobní.[67] Dospěli jsme k názoru, že při konkretizaci postupů, kterými budou tyto údaje zpracovávány, při vhodném vyvážení možného zásahu do práv subjektů údajů a jeho minimalizaci a při formulaci dodatečných záruk, je možné toto zpracování legitimizovat za pomocí výjimek v existující legislativě i ve chvíli, kdy příslušné dohledové pracoviště nepředstavuje povinný subjekt podle ZoKB. Součástí dalšího výzkumu aplikovatelnosti legislativy na ochranu osobních údajů na činnost dohledových pracovišť kybernetické bezpečnosti by mělo být zahrnutí těchto údajů do formalizovaných i neformálních modů spolupráce mezi dohledovými pracovišti a případné vyhodnocení praxe při zpracování údajů pro bezpečnostní výzkum.[68] V tu chvíli by totiž docházelo ke zpřístupňování shromážděných osobních údajů dalším subjektům. Hranice toho, co je možné považovat za realizaci oprávněného zájmu dohledového pracoviště, by se tak opět posunula.[69] Tato oblast si tak zaslouží další systematickou pozornost.

6. POUŽITÁ LITERATURA

[1] HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR. *Revue pro právo a technologie,* 2013, roč. 4, č. 8, s. 66-93. ISSN 1804-5383.

[2] KOOPS, Bert-Jaap. The trouble with European data protection law. *International Data Privacy Law* [online]. 2014, roč. 4, č. 4, s. 250–261 [vid. 11. listopad 2015]. ISSN 2044-3994, 2044-4001. Dostupné z: doi:10.1093/idpl/ipu023

[3] KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů : komentář*. Beckova edice komentované zákony. Praha: C.H. Beck, 2012, 516 s. ISBN 978-80-7179-226-0.

[4] LAH, Frederick. Online and Locational Privacy: Are IP Addresses „Personally Identifiable Information"? *I/S: A Journal of Law and Policy for the Information Society*. 2009, roč. 4, s. 681.

[5] LITVINOV, Aleksandr V. The Data Protection Directive as Applied to Internet Protocol (IP) Addresses: Uniting the Perspective of the European Commission with the Jurisprudence of Member States. *The George Washington international law review*. 2013, roč. 45, č. 3, s. 579–610. ISSN 1534-9977.

[67] Jakkoli se o správnosti tohoto přístupu dá dlouze diskutovat.

[68] Srov. OHM, Paul, SICKER, Douglas and Dirk GRUNWALD. Legal Issues Surrounding Monitoring During Network Research (Invited Paper). *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* [online]. 2007. Dostupné z: http://conferences.sigcomm.org/imc/2007/papers/imc152.pdf.

[69] Srov. např. některé zajímavé závěry v CORMACK, Andrew. Incident Response and Data Protection. 2011. Dostupné z: https://www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf.

[6] LUNDEVALL-UNGER, Patrick; TRANVIK, Tommy. IP Addresses – Just a Number? *International Journal of Law and Information Technology* [online]. 2011, roč. 19, č. 1, s. 53–73 [vid. 8. říjen 2015]. ISSN 0967-0769, 1464-3693. Dostupné z: doi:10.1093/ijlit/eaq013

[7] MCINTYRE, Joshua J. Balancing Expectations of Online Privacy: Why Internet Protocol (ip) Addresses Should Be Protected as Personally Identifiable Information. *DePaul Law Review*. 2011, roč. 60, s. 895 – 948. ISSN 0011-7188.

[8] MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů internetu. *Revue pro právo a technologie*, Masarykova univerzita, 2014, roč. 5, č. 9, s. 3-74. ISSN 1804-5383.

[9] NONNEMANN, František. Objektivní, či subjektivní pojetí osobních údajů? *Právní rozhledy*. 2015, roč. 2015, č. 12, s. 425 – 431. ISSN 1210-6410.

[10] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. 2009, roč. 57, č. 6, s. 1701–1777. ISSN 0041-5650.

[11] OHM, Paul, SICKER, Douglas and Dirk GRUNWALD. Legal Issues Surrounding Monitoring During Network Research (Invited Paper). *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* [online]. 2007. Dostupné z: http://conferences.sigcomm.org/imc/2007/papers/imc152.

[12] POLČÁK, Radim. *Internet a proměny práva*. Téma. Praha: Auditorium, 2012, 388 s. ISBN 9788087284223.

[13] PROKEŠ, Josef. IP adresa v ochraně osobních údajů. *Data Security Management*. 2014, roč. 2014, č. 4, s. 31 – 33. ISSN 1211-8737.

[14] TIKK, Eneken. IP Addresses subject to personal data regulation. In: TIKK, Eneken; TALIHÄRM, Anna-Maria (eds.). *International Cyber Security Legal & Policy Proceedings* [online]. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010, s. 24 – 39. ISBN 978-9949-9040-4-4. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/LP_Proceedings_2010.pdf

[15] Pracovní skupina pro ochranu údajů zřízená podle článku 29. *Stanovisko č. 4/2007 k pojmu osobní údaj*. WP 136. Evropská komise [online]. [vid. 8. říjen 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf.

[16] Pracovní skupina pro ochranu údajů zřízená podle článku 29. *Stanovisko č. 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení*. WP 185. Evropská komise [online]. [vid. 8. říjen 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_cs.pdf.

[17] Stanovisko Úřadu pro ochranu osobních údajů č. 3/2012 z března 2012, K pojmu osobní údaj. [cit. 8. říjen 2015]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9187.

[18] Stanoviska generálního advokáta Niila Jääsikenena k věci C-212/13 František Ryneš proti Úřadu pro ochranu osobních údajů [online]. [cit. 8. říjen 2015]. Dostupné z: http://curia.europa.eu/juris/document/document_print.jsf?
doclang = CS&text = &pageIndex = 0&part = 1&mode = lst&docid = 154842&occ = first&dir = &cid = 629379.

[19] CZ.NIC. *O nás* [online]. [vid. 8. říjen 2015]. Dostupné z: https://www.csirt.cz/page/882/o-nas/.

[20] ENISA. *Good Practice Guide for Incident Management* [online]. 2010 [vid. 8. říjen 2015]. Dostupné z: https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management

---
