K POJMOVÉ NEJEDNOTNOSTI PORUŠENÍ ZABEZPEČENÍ/BEZPEČNOSTI OSOBNÍCH ÚDAJŮ V ČESKÉM PRÁVU

FRANTIŠEK KASL*

Abstract: **The Terminological Inconsistency of Personal Data Breach in the Czech Law**
The contribution compares the terminology of current and previous Czech and European personal data protection law from the perspective of the use of two possible Czech terms for the personal data breach. Firstly, the pattern of the use of these legal terms is analysed with regard to the relevant legal framework and the difference or overlay of their normative content is assessed. The identified disparities within or between the core laws are assessed on the European level first based on the comparison of the language versions and then also in broader context. The conclusion of the contribution is a structured argumentation in favour of one of the terms.

Klíčová slova: porušení zabezpečení osobních údajů; porušení bezpečnosti osobních údajů; narušení bezpečnosti osobních údajů; obecné nařízení o ochraně osobních údajů

Keywords: personal data breach; GDPR

DOI: 10.14712/23366478.2019.34

1. ÚVOD[1]

Nový jednotný evropský právní rámec ochrany osobních údajů přinesl řadu změn a nových právních institutů. V rámci této komplexní novelizace nosných norem oboru lze však nalézt jisté změny, které se zdají býti neodůvodněné. Příkladem je užití pojmu *zabezpečení* osobních údajů na úkor předchozího termínu *bezpečnost* osobních údajů, preferovaného evropskou právní úpravou. Cílem tohoto příspěvku je podrobněji nahlédnout na tuto terminologickou proměnu a zhodnotit, jaké možné praktické důsledky s sebou přináší a zda jde o změnu konzistentní z hlediska právně teoretického.

* Mgr. Ing. František Kasl je prezenčním doktorským studentem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity.

[1] Tento článek byl zpracován za podpory Technologické agentury ČR v rámci projektu „*Právní a technické prostředky pro ochranu soukromí v kyberprostoru* (TL02000398)“. Závěry příspěvku byly prezentovány před odborným publikem na XIII. ročníku konference pro doktorandy a mladé právní vědce COFOLA 2019 uspořádané Právnickou fakultou Masarykovy univerzity dne 5. dubna 2019 v Telči.

2. INTERPRETACE PRÁVA

Předpokladem řádného poznávání či aplikace obsahu právní normy je vhodné užití metod právní interpretace. Výkladové metody a přípustné argumentační postupy pro propojování textového znění právní normy s jejím právním významem jsou jádrem arzenálu právních profesí. Přes jisté dělení či systemizaci těchto metod není pevně stanovena jejich hierarchie, ale je zpravidla zdůrazňována potřeba jejich využití v kombinaci a jejich bilancování s ohledem na konkrétní situaci.[2]

Přímočará metoda výkladu právního textu je založena na nalézání jeho jazykového a gramatického významu. Je jí tedy předvídáno, že zákonodárce užívá slov s ohledem na jejich význam a užívá text normy co nejbližší jejímu významovému obsahu z právního hlediska.[3] Tento předpoklad je doplňován o očekávání systematického a logického formulování právních norem, kdy lze následně při výkladu či poznávání obsahu referovat na ustálená systematická pravidla struktury právního předpisu a dovozovat záměr zákonodárce z postavení, řazení či kategorizace jednotlivých prvků v předpisu obsažených.[4] Logický výklad následně odkazuje na předpoklad obecné racionality jednání a projevu zákonodárce, kdy lze při nejednoznačném či nevysloveném obsahovém komponentu normy využít standardních logických postupů k výkladu, který je v souladu se záměrem zákonodárce.[5] Na základě této trojice metod, některými autory označovaných jako standardní výkladové metody práva,[6] je zpravidla možné učinit jednoznačné soudy týkající se hlavních obsahových kontur právní normy.

Vzhledem k abstraktnosti právně-normativní úpravy a neúměrné složitosti a různorodosti životních situací, na které je aplikována, je možné shledat potřebu pro využití dalších, doplňujících metod výkladu obsahu právní normy. Jde především o situace jazykové nejednotnosti, zjevné nesystematičnosti či logické neucelenosti určitých ustanovení v rámci normy či ve vztahu k normám ostatním. Právní teorie přijímá poznání, že jazyk není optimální nástroj pro vyjádření právních norem v jejich úplnosti. Je tedy nutné nalézat účel a smysl právní normy stojící za daným jazykovým vyjádřením, ač tím může docházet k překonání závěrů na základě jazykového výkladu.[7] Souvisejícím argumentem ve prospěch jisté nadřazenosti teleologického výkladu je pak překonání mýtu racionálního a neomylného zákonodárce a pragmatická akceptace často značně tristní reality soudobého legislativního procesu. Často je tedy nutné prohlédnout za vlastní text a systematiku právního předpisu a za pomoci doktrinální, historické či komparativní analýzy nalézat skutečný obsah, který je právní normou a měl by být textem vyjádřen, ač není.

---

2 MELZER, F. *Metodologie nalézání práva; Úvod do právní argumentace*. Praha: C. H. Beck, 2010, s. 78.
3 BOGUSZAK, J. – ČAPEK, J. – GERLOCH, A. *Teorie práva*. Praha: ASPI, 2003, s. 151.
4 MELZER, c. d., s. 130.
5 KNAPP, V. *Teorie práva*. Praha: C. H. Beck, 1995, s. 171.
6 BOGUSZAK – ČAPEK – GERLOCH, c. d., s. 156.
7 MELZER, c. d., s. 159.

3. PRÁVNÍ NORMY OCHRANY OSOBNÍCH ÚDAJŮ A JEJICH VÝKLAD

Obecný úvod k interpretaci práva v předchozích odstavcích nepřináší nové poznatky právně znalým čtenářům, je však pokladem pro následující proces poznávání práva ve vztahu ke konkrétní právní skutečnosti (*porušení zabezpečení* osobních údajů či *narušení/porušení bezpečnosti* osobních údajů), resp. právem chráněné hodnoty (*zabezpečení* zpracování osobních údajů či *bezpečnost* zpracování osobních údajů).

Problematika ochrany osobních údajů představuje z hlediska normotvorby značně dynamickou oblast, která postihuje velmi široké spektrum dílčích situací z pohledu značně abstraktních právních norem. Projevují se zde konflikty mezi veřejnoprávní a soukromoprávní povahou jednotlivých ustanovení příslušných právních předpisů. Současně jde o oblast, pro kterou potřeba právní úpravy vychází z tlaku v důsledku změny společenské reality působené technologických pokrokem a digitalizací interakcí v moderní společnosti. Právní úprava zde tedy čelí neustálé potřebě „dohánět" společenskou realitu.[8] To činí text právních norem často nepřiléhavým a vede k potřebě extenzivního či analogického výkladu za účelem zachování funkce dané právní normy.[9]

V neposlední řadě pak jde o jeden z předních segmentů právní úpravy, ve kterých se prosadila sjednocující iniciativa legislativního projektu Evropské unie. Dochází zde tudíž v současné době ke střetu právních norem národního a nadnárodního zákonodárce. Ten přináší dodatečný metodologický prvek do výkladu obsahu právní normy, totiž požadavek eurokonformního výkladu.[10] Je jím doplňován obecný požadavek na teleologický soulad s ústavní normou, může však mít i mnohem konkrétnější a výraznější dopad.[11]

4. KDYŽ SE ŘEKNE „PERSONAL DATA BREACH"

Předmětem tohoto pojednání je interpretační analýza jazykové nejednotnosti právních norem vztahujících se k jednomu z nosných prvků systematiky práva ochrany osobních údajů. Lze totiž dovozovat, že primárním účelem pravidel založených touto právní oblastí je vymezení přípustného postupu pro nakládání s osobními údaji, který adekvátně respektuje práva a svobody dotčené fyzické osoby.[12] Zásadní roli tudíž hrají požadavky a povinnosti vedoucí k zabránění či zmírnění důsledků situací, kdy dojde k porušení těchto mantinelů, ať již subjektem, který jinak údaje nabyl a zpracovával v souladu s právní úpravou, či skrze nahodilý či cílený incident, který údaje zpřístupnil třetí osobě, která k jejich zpracování nemá potřebné oprávnění.

---

[8] BENNETT MOSES, L. Recurring Dilemmas: The Law's Race to Keep Up with Technological Change. *UNSW Law Research Paper*. Sydney: UNSW, 2007, vol. 2007, no. 21.

[9] BOGUSZAK – ČAPEK – GERLOCH, c. d., s. 156.

[10] MELZER, c. d., s. 174.

[11] GERLOCH, A. et al. *Teorie a praxe tvorby práva*. Praha: ASPI, 2008, s. 354–355.

[12] MATOUŠOVÁ, M. – HEJLÍK, L. *Osobní údaje a jejich ochrana*. Praha: ASPI, 2003, s. 10; NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014, s. 222.

Správce či zpracovatel tedy odpovídá za přiměřené zajištění ochrany zpracovávaných osobních údajů, respektive za zajištění jejich bezpečnosti, tedy vlastně za zabránění porušení jejich zabezpečení. Jak naznačuje předchozí věta, jedná se z právně terminologického hlediska o hodnotu či skutečnost, která v současné právní úpravě nemá zcela ustálené označení.

Je však otázkou, zda tato pojmová nejednotnost uvnitř a napříč příslušných právních předpisů z oblasti ochrany osobních údajů značí záměr zákonodárce, tedy je na místě jí věnovat pozornost při výkladu a aplikaci příslušné právní normy, či zda se jedná o jeden z projevů nedokonalosti zákonodárce, a je tedy na místě odlišnost pojmů překonat výkladem. Pro zodpovězení této otázky je předně nutné analyzovat vývoj institutu a užití předmětných termínů v čase.

5. PŘEHLED TERMINOLOGIE V RELEVANTNÍCH PRÁVNÍCH PŘEDPISECH

5.1 ÚMLUVA Č. 108 A ZÁKON Č. 256/1992 SB.

Za první inspirativní podklad české úpravy ochrany osobních údajů lze právem pokládat Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat přijatou Radou Evropy v roce 1981[13] a vstoupivší v platnost ratifikací pěti státy roku 1985. Ačkoliv k přijetí této mezinárodní smlouvy do českého právního řádu nedošlo před rokem 2001, obsažené principy a pravidla se odrazila v prvním českém zákoně vztahujícím se k problematice ochrany osobních údajů, zákoně č. 256/1992 Sb., o ochraně údajů v informačních systémech. Z hlediska zde analyzovaných termínů je relevantní článek 7 úmluvy, který se vztahuje v závazném anglickém znění k *data* ***security***, resp. v závazném francouzském znění k ***sécurité*** *des données*. V českém znění přijatém do Sbírky mezinárodních smluv v roce 2001 nese pak článek označení ***zabezpečení*** *údajů*.[14] V zákoně č. 256/1992 Sb. je pak namísto termínů bezpečnost či zabezpečení upřednostněno v § 17 písm. i) i § 19 odst. 1 písm. d) spojení ***zajištění ochrany*** *informací*. Pojmu *zabezpečit* je užito pouze ve významu *zajistit* či *obstarat*.[15]

5.2 SMĚRNICE 95/46/ES A ZÁKON Č. 101/2000 SB.

Za nosnou normu pro etablování ochrany osobních údajů nejen v českém právu, ale napříč Evropskou unií je pak na místě považovat směrnici 95/46/ES o ochraně osobních údajů.[16] Tento evropský právní předpis bez přímé aplikovatelnosti sice

---

[13] COUNCIL OF EUROPE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [online]. 28. 1. 1981 [cit. 29. 4. 2019]. Dostupné na: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[14] Sdělení Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat vyšlo ve Sbírce mezinárodních smluv dne 15. 11. 2001 v částce 52 pod bodem 115.

[15] Viz § 11 odst. 1 zákona 256/1992 Sb.

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

harmonizoval postoj zákonodárců tehdejšího okruhu členských států k problematice ochrany osobních údajů, vyžadoval však transpozici do národního práva.

Proces transpozice směrnice jako takový přestavuje z hlediska právní teorie poměrně složitou proceduru, jelikož dochází k eurokonformnímu přenesení obsahu harmonizovaného evropského předpisu do národního právního řádu, nelze však vyloučit dílčí terminologické či obsahové diskrepance způsobené změnou formulace či rozvedením textu ustanovení na základě diskrece, která je národnímu zákonodárci v rámci systematiky evropského práva v tomto směru poskytnuta.[17] Pro Českou republiku se směrnice stala právně relevantní v důsledku aproximace českého práva v rámci procesu přistoupení k Evropské unii, přičemž důsledkem tohoto procesu byl mimo jiné zákon č. 101/2000 Sb.[18]

Samotná směrnice nabyla dodatečně závazného znění v českém jazyce, jakožto jazyce nového členského státu. V tomto českém znění směrnice nalézáme plné pojmové spektrum naznačené v předchozí sekci příspěvku. Oddíl VIII a článek 17 směrnice užívají pojmu ***bezpečnost*** *zpracování* (německá verze: ***Sicherheit*** *der Verarbeitung*, anglická verze: ***Security*** *of processing*, francouzská verze: ***Sécurité*** *des traitements*). Obsah pojmu je následně přiblížen v prvním odstavci, kde druhá věta zní: „*Tato opatření mají zajistit, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň* ***bezpečnosti*** *odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny*.“

Z hlediska výkladu jsou následně relevantní, ač bez srovnatelné právní závaznosti, recitály směrnice. V recitálu 37 je pojednáváno o *opatřeních pro* ***zajištění bezpečnosti*** *zpracování*, podobně v recitálu 46 je kladen důraz na *přijetí příslušných technických a organizačních opatření s cílem zajistit především* ***bezpečnost*** *a tím také zabránit jakémukoli neoprávněnému zpracování*. Směrnice oproti tomu až na výjimku recitálu 25 neužívá pojmu *zabezpečení*. Ten je pak užit jen ve významu technického opatření, jak vyplývá z výňatku: „[…] *zásady ochrany se musí odrazit jednak v povinnostech jednotlivců, orgánů veřejné moci, podniků, agentur nebo jiných subjektů odpovědných za zpracování údajů týkajících se zejména kvality údajů,* ***technického zabezpečení****, oznamování okolností, za jakých může být zpracování provedeno* […]“.

Třetím pojmem, který se ve směrnici objevuje a lze pokládat za související, je ***ochrana***. Ta se zde však vzhledem k článku 1 odst. 1 a řadě recitálů obsahově projevuje na abstraktnější právní rovině ochrany práv a svobod dotčených fyzických osob, spíše než ve smyslu souboru opatření na ochranu zpracování osobních údajů. Přesto je v článku 6 odst. 1 písm. b a e pojednáváno o povinnosti členských států stanovit *vhodná* ***ochranná opatření***, stejně jako je tomu v článku 8 odst. 4 či v recitálu 29.

Pokud pro srovnání nahlédneme do textu zákona č. 101/2000 Sb., který je transpozicí směrnice 95/46/ES českým zákonodárcem, je poměrně překvapující nalézt v označení § 13, který je obsahovou transpozicí výše zmíněného článku 17, pojednání o *povinnostech osob při* ***zabezpečení*** *osobních údajů*. Také v § 6 a § 15 je opakován pojem ***zabezpečení*** *osobních údajů,* resp. ***zabezpečení ochrany*** *osobních údajů*. Oproti tomu

[17] GERLOCH et al., c. d., s. 332.
[18] Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů.

§ 44 odst. 2 písm. h a § 45 odst. 1 písm. h referují nikoliv k zabezpečení osobních údajů, ale k *opatřením pro **zajištění bezpečnosti** zpracování osobních údajů*.

V zákoně dochází i k pojednání o ***bezpečnostních opatřeních*** v § 15 odst. 1 a znovu pak v § 27 odst. 3 písm. b. Za zmínku pak stojí, že v důvodové zprávě zákona jsou jako subsidiární právní předpisy pro stanovení a aplikaci bezpečnostních opatření ve smyslu § 13 zákona uvedeny předně vyhlášky NBÚ č. 12/1999 Sb. o zajištění **technické bezpečnosti** utajovaných skutečností a certifikaci technických prostředků; č. 56/1999 Sb. o **zajištění bezpečnosti** informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátů; a č. 339/1999 Sb. o **objektové bezpečnosti**.

5.3 SMĚRNICE 2002/58/ES A ZÁKON Č. 127/2005 SB.

Směrnice 95/46/ES však není jediným evropským právním předpisem, který upravuje tuto problematiku. Je zde také speciální úprava pro oblast elektronických komunikací. Tato úprava je významná ze dvou momentů.

Zaprvé jde o mnohem techničtěji koncipovanou normu, jelikož směřuje vůči sektorově omezenému okruhu povinných subjektů. Ochrana sítě a přenášených dat pak nabývá v tomto kontextu širších a složitějších rozměrů, než je pouhá ochrana osobních údajů, jelikož se zde jedná o prvky významné z hlediska kybernetické bezpečnosti. I proto hlavní předpis v této oblasti, směrnice 2002/58/ES,[19] již v původním znění obsahovala článek 4 týkající se ***bezpečnosti***. V něm je uložena povinnost *přijmout vhodná technická a organizační opatření pro **zajištění bezpečnosti** služeb s ohledem na **bezpečnost sítě***. Je zde tedy pojednáváno o ochraně před kybernetickým bezpečnostním incidentem, což je pojem, který je v současném českém právním řádu jednoznačně definován a zakotven v § 7 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti[20] jakožto: „[…] *narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události*“.

Zde je pak podstatný druhý moment evropské úpravy elektronických komunikací, a to pozměňovací směrnice 2009/136/ES.[21] Tato směrnice vnesla do textu směrnice 2002/58/ES malou, avšak z hlediska zde analyzovaného pojmu významnou změnu, skrze inkorporaci nových odstavců 3 až 5 do zmíněného článku 4 týkajícího se ***bezpečnosti zpracování***. Tímto byl do evropského práva vnesen právní instrument ohlašovací povinnosti pro případ ***narušení bezpečnosti*** *osobních údajů*. Směrnice nadto v článku 2 odst. 2 písm. c doplnila konkrétní definici tohoto pojmu. Pro oblast elektronických komunikací tedy platí, že „***narušením bezpečnosti*** *osobních údajů' se rozumí narušení*

---

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

[20] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů.

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

bezpečnosti, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně či neoprávněnému vyzrazení nebo zpřístupnění osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných v souvislosti s poskytováním veřejně dostupné služby elektronických komunikací ve Společenství". Tato terminologie je ve zmíněném segmentu evropského práva vysoce konzistentní, jak potvrzuje i navazující nařízení 611/2013 o opatřeních vztahujících se na oznámení o **narušení bezpečnosti** osobních údajů.[22]

Pokud česká verze užívá pojmů **bezpečnost zpracování** a **narušení bezpečnosti** osobních údajů, je vhodné upozornit na dalších jazykové verze, především na německou, která užívá pojmy ***Sicherheit*** *der Verarbeitung* a ***Verletzung des Schutzes*** *personenbezogener Daten*, anglickou s pojmy ***Security*** *of processing* a *personal* ***data breach***, či francouzská s pojmy ***Sécurité*** *du traitement* a ***violation de données à caractère*** *personnel*. Je zde tedy možné ve všech verzích nalézat konzistenci se směrnicí 95/46/ES ve směru užití českého pojmu **bezpečnost zpracování**.

Srovnatelnou konzistenci však nenalézáme v transpozici těchto právních norem provedené českým zákonodárcem. Směrnice 2002/58/ES byla do českého práva transponována v podobě, v mezidobí silně novelizovaného, zákona č. 127/2005 Sb., o elektronických komunikacích.[23] Z hlediska řešeného pojmu je však příslušný předpis temporálně vysoce konzistentní, v § 88 zde nalezneme namísto bezpečnosti ***zabezpečení ochrany*** *osobních, provozních a lokalizačních údajů a důvěrnosti komunikací*. Pokud pak nahlédneme do definic v § 2, směrnicí vymezené narušení bezpečnosti osobních údajů český zákonodárce pod písm. y transponoval jako ***porušení ochrany*** *osobních údajů*, které je ovšem vymezeno jako „***porušení bezpečnosti****, které vede k neoprávněnému přístupu nebo k neoprávněné nebo nahodilé změně, zničení, vyzrazení či ztrátě osobních údajů zpracovávaných v souvislosti s poskytováním veřejně dostupné služby elektronických komunikací*".

5.4 OBECNÉ NAŘÍZENÍ 2016/679, SMĚRNICE 2016/680 A ZÁKON Č. 110/2019 SB.

Třetím a v současné době nejvýznamnějším souborem právních norem týkajících se diskutované problematiky je od 25. května 2018 přímo účinné obecné nařízení 2016/679,[24] které nahradilo právní rámec směrnice 95/46 ES, a paralelně přijatá směrnice 2016/680.[25]

Na rozdíl od výše představené konzistentní terminologie na evropské úrovni v podobě směrnice 95/46/ES a směrnice 2002/58/ES užívá obecné nařízení 2016/679 v české verzi pro článek 32 označení ***zabezpečení zpracování***. Články 33 a 34 tudíž upravují ohlašování a oznamování případů ***porušení zabezpečení*** *osobních údajů* a v článku 4

---

22 Nařízení Komise (EU) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích.

23 Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů.

24 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

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

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

Pokud však nahlédneme do cizojazyčných verzí nařízení, nalézáme stále v německé verzi pojmy ***Sicherheit*** *der Verarbeitung* a ***Verletzung des Schutzes*** *personenbezogener Daten*, v anglické verzi pojmy ***Security*** *of processing* a *personal* ***data breach***, a ve francouzské verzi pojmy ***Sécurité*** *du traitement* a ***violation de données à caractère*** *personnel*. Ve všech třech zmíněných cizojazyčných verzích je tedy na rozdíl od české verze plná konzistence s výše popsanou evropskou terminologií směrnice 95/46/ES a směrnice 2002/58/ES.

Při snaze o rozklíčování původu této pojmové proměny v českém znění obecného nařízení je vhodné přihlédnout ke zněním v rámci dlouhého a komplikovaného legislativního procesu přijímání nařízení. Pokud nahlédneme do českého znění původního návrhu obecného nařízení předloženého Evropskou komisí a schváleného Evropským parlamentem v roce 2014, zjistíme, že zde bylo předvídatelně užito pro výše popsané články pojmu **narušení bezpečnosti** osobních údajů.[26] Je zde tedy soulad s terminologií novelizované směrnice 2002/58/ES, která byla výslovně uvedena za podklad instrumentu přeneseného do obecného nařízení.[27] I ve verzi obecného nařízení přijaté Radou v roce 2015 sice dochází k modifikaci textu ustanovení, stále je však pro celý Oddíl 2 i článek 30 (budoucí článek 32) voleno označení **bezpečnost** zpracování a článek 31 (budoucí článek 33) se váže k **porušení ochrany** osobních údajů.[28] Cizojazyčné verze předmětných článků přitom zůstávají pojmově konzistentní po celý legislativní proces.

Z uvedeného je tedy zjevné, že ke změně české terminologie pro tuto část obecného nařízení dochází až v pozdní části legislativního procesu v rámci trialogu Evropské komise, Evropského parlamentu a Rady, přičemž nic nenaznačuje tomu, že by změna pojmů reflektovala změnu v obsahu daných pojmů či předmětného právního instrumentu oproti směrnici 95/46/ES a směrnici 2002/58/ES.

Ostatně nekonzistence terminologie české verze se projevuje i ve vlastním obsahu článku 32, který přestože pojednává o zabezpečení zpracování, obsahuje v odst. 1 písm. d požadavek na zajištění odpovídající úrovně zabezpečení včetně „*procesu pra-*

---

[26] EVROPSKÝ PARLAMENT. *Legislativní usnesení Evropského parlamentu ze dne 12. března 2014 o návrhu nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) (COM(2012)0011 – C7-0025/2012–2012/0011(COD))* [online]. 12. 3. 2014 [cit. 29. 4. 2019]. Dostupné na: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0212+0+DOC+PDF+V0//CS.

[27] EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) COM(2012) 11 final* [online]. 25. 1. 2012 [cit. 29. 4. 2019]. Dostupné na: https://eur-lex.europa.eu/legal-content/cs/TXT/PDF/?uri=CELEX:52012PC0011&from=EN, s. 10.

[28] RADA EU. *Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) – příprava obecného přístupu 2012/0011 (COD)* [online]. 11. 6. 2015 [cit. 29. 4. 2019]. Dostupné na: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/cs/pdf.

*videlného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro **zajištění bezpečnosti** zpracování*“. Odst. 2 pak pokračuje v této terminologické odchylce a stanoví: „*Při posuzování vhodné úrovně **bezpečnosti** se zohlední zejména rizika* […].“ Termín je také užit v článku 35 týkajícím se posouzení vlivu na ochranu osobních údajů, kde je zmínka o ***bezpečnostních opatřeních** a mechanismech k **zajištění ochrany** osobních údajů* a o ***bezpečnosti** operací zpracování*.

Nejvýznamnější projev vnitřní rozporuplnosti terminologie obecného nařízení 2016/679 je pak obsažen v článku 40 odst. 2 písm. h, kde je namísto o zabezpečení zpracování na článek 32 odkazováno textem: „[…] *opatření k **zajištění bezpečnosti** zpracování podle článku 32*.“ Jinak je pojem *bezpečnosti zpracování* v obecném nařízení 2016/679 zmíněn pouze v recitálu 81.

Pokud nahlédneme do směrnice 2016/680, přijaté společně s obecným nařízením 2016/679, nalézáme v zásadě shodnou terminologii jako v nařízení. Článek 3 bod 11 definuje souladně s nařízením 2016/679 ***porušení zabezpečení** osobních údajů*. Pojmů ***zabezpečení** osobních údajů* či ***zabezpečení** zpracování* je pak užito v článku 4 odst. 1 písm. f, článku 25 odst. 2, článku 29, 30, 31, či článku 51 odst. 1 písm. d a e. Pouze recitál 28 obsahuje v jednom souvětí oba pojmy, když uvádí: „*Aby byla zachována **bezpečnost** zpracování a zabránilo se zpracování v rozporu s touto směrnicí, měly by být osobní údaje zpracovávány způsobem, který zajistí náležitou úroveň **zabezpečení** a mlčenlivosti* […]“ Zbývající recitály konzistentně operují s pojmem *zabezpečení zpracování*.

Dne 24. dubna 2019 nabyl účinnosti zákon č. 110/2019 Sb., o zpracování osobních údajů, který nahrazuje výše zmíněný zákon č. 101/2000 Sb. a zajišťuje adaptaci národní právní úpravy v důsledku přímé účinnosti obecného nařízení 2016/679 a transpozici směrnice 2016/680 (společně se změnovým zákonem č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů). Tento zákon v § 12 užívá termínu ***porušení zabezpečení** osobních údajů*. Obdobně v § 19 odst. 4, § 32 odst. 4 písm. i, § 34 odst. 4 písm. d, § 36 odst. 3, §§ 40, 41, 42, 46, § 59 odst. 1 a § 63 zákona.

Avšak v § 16 o zpracování osobních údajů za účelem vědeckého nebo historického výzkumu nebo pro statistické účely odst. 1 písm. j poměrně překvapivě pojednává o posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění ***bezpečnosti** zpracování*. Stejně tak v § 44 zákon uvádí „[…] *záruky zpracovatele o přijetí a dodržování technických a organizačních opatření k zajištění **bezpečnosti** a **ochrany** osobních údajů*“. Nakonec pak i § 47 zmiňuje „[…] *zachovávat mlčenlivost o osobních údajích a o organizačních a technických opatřeních, jejichž zveřejnění by ohrozilo **bezpečnost** osobních údajů*“.

6. DISKUSE

Předcházející kapitola příspěvku analyzovala terminologii relevantních právních předpisů týkajících se problematiky, která je v anglické terminologii označována v evropském právu jako *personal data breach*. Jak bylo výše poukázáno, napříč

evropskými předpisy lze vnímat konzistenci užitých termínů k této problematice jak v anglickém jazyce, tak v jazykových verzích německých a francouzských.

6.1 K OBSAHOVÉ KONTINUITĚ POJMŮ V ČESKÉM PRÁVU OCHRANY OSOBNÍCH ÚDAJŮ

Při studiu českých verzí těchto předpisů je však zjevná odlišnost terminologie u nejnovějších předpisů, tedy u obecného nařízení 2016/679 a směrnice 2016/680, která byla přenesena do nového zákona č. 110/2019 Sb. Dosud konzistentně užívané termíny ***bezpečnost*** *zpracování* a ***narušení bezpečnosti*** *osobních údajů* jsou zde v zásadě napříč předpisem nahrazeny termíny ***zabezpečení*** *zpracování* a ***porušení zabezpečení*** *osobních údajů.*

Současně je v tomto směru navázáno na terminologii zákona č. 101/2000 Sb., který představoval transpozici směrnice 95/46/ES. Český zákonodárce se již zde odchýlil od zmíněné evropské terminologie a zavedl pojem ***zabezpečení*** *zpracování*. V tomto směru lze tedy vnímat jistou konzistenci terminologie české právní úpravy.

S tímto argumentem konzistence se však nelze ve světle eurokonformního výkladu spokojit. Na jeho metodologickou rovnocennost s ústavněkonformním výkladem upozorňuje *Melzer*[29] s odkazem na rozhodnutí velkého senátu Soudního dvora Evropské unie (tehdy stále ještě Evropského soudního dvora) ve věci *Bernhard Pfeiffer a další*, spojené věci C-397/01 až C-403/01 ze dne 5. října 2004.[30] Bod 113 rozhodnutí přímo uvádí: „*Vnitrostátní soud je tak při použití vnitrostátního práva a zejména ustanovení právní úpravy specificky přijaté za účelem provedení požadavků směrnice povinen vykládat vnitrostátní právo v co možná největším rozsahu ve světle znění a účelu příslušné směrnice, aby tak dosáhl výsledku jí zamýšleného, a dosáhl tak souladu s třetím pododstavcem článku 249 ES (viz v tomto smyslu zejména výše uvedené rozsudky Von Colson a Kamann, bod 26; Marleasing, bod 8, a Faccini Dori, bod 26; viz rovněž rozsudky ze dne 23. února 1999, BMW, C63/97, Recueil, s. I905, bod 22; ze dne 27. června 2000, Océano Grupo Editorial a Salvat Editores, C240/98 až C244/98, Recueil, s. I4941, bod 30, a ze dne 23. října 2003, AdidasSalomon a Adidas Benelux, C408/01, Recueil, s. I12537, bod 21).*“

Mnohojazyčnost evropského práva je obecně unikátní situací, která vytváří řadu specifických výzev a problémů. Je ovšem nežádoucí stav, aby studium odlišných jazykových verzí vedlo k rozdílným výkladovým závěrům.[31]

Pro argument, že se jedná o nevhodný terminologický odklon, nikoliv o účelné odlišení institutů, hovoří též podrobnější studium dostupné odborné a komentářové literatury vážící se k zákonu č. 101/2000 Sb.

---

[29] MELZER, c. d., s. 178.

[30] Rozsudek Soudního dvora (velkého senátu) ze dne 5. října 2004 ve spojených věcech *Bernhard Pfeiffer* (C-397/01), *Wilhelm Roith* (C-398/01), *Albert Süß* (C-399/01), *Michael Winter* (C-400/01), *Klaus Nestvogel* (C-401/01), *Roswitha Zeller* (C-402/01) a *Matthias Döbele* (C-403/01) *proti Deutsches Rotes Kreuz, Kreisverband Waldshut eV*.

[31] KŘEPELKA, F. *Mnohojazyčnost Evropské unie a její důsledky pro českou právní praxi*. Brno: Masarykova Univerzita, 2007, s. 67.

Komentář k zákonu z pera *Kučerové, Bartíka, Peci, Neuwirtha* a *Nejedlého* z roku 2003 při diskusi klíčového § 13 zákona již v úvodním odstavci takto jednoznačně odkazuje na terminologii směrnice: „*Tímto ustanovením je stanovena obecná povinnost správců a zpracovatelů osobních údajů tyto údaje chránit. Jedná se o další ze základních povinností (viz komentář k § 5), jejímž obsahem je povinnost ze strany správců a zpracovatelů zajistit tzv. ‚**bezpečnost** dat'* […].“[32] Autoři následně užívají terminologii zákona při diskusi „*výčtu situací, na které musí reagovat **zabezpečení** osobních údajů*“ [33] a „*naplnění povinností stanovených k **zabezpečení (ochraně)** osobních údajů*“. [34]

Prakticky koncipovaná monografie *Matoušové* a *Hejlíka Osobní údaje a jejich ochrana,* taktéž z roku 2003, v teoretickém úvodu vykládá rovinu **zabezpečení** osobních údajů před únikem a zneužitím jako pojímající nejen informační bezpečnost, ale též „[…] *formalistický mikrosvět byrokratických a technokratických omezení ochranářů a strážců různých tajemství majetku a případně jinak vymezovaných hodnot*“.[35] V kapitole týkající se výkladu povinnosti přijmout **bezpečnostní opatření** dle § 13 zákona však autoři zdůrazňují případnost pojmu **bezpečnost** nejen s odkazem na recitál 46 směrnice,[36] ale též při argumentaci ve prospěch podpůrného využití právních úprav pro bezpečnostní opatření pro jiné formy **bezpečnosti**.[37]

To, že se pojem zabezpečení na úkor pojmu bezpečnost v českém akademickém diskursu pevně neustálil, pak dokazují monografie vydané s výrazným časovým odstupem od účinnosti zákona č. 101/2000 Sb.

V komentáři k zákonu č. 101/2000 Sb. *Bartíka* a *Janečkové* z roku 2010 začíná výklad k § 13 odst. 1 větou: „*Tímto ustanovením je určena obecná povinnost správců a zpracovatelů osobních údajů chránit osobní údaje. Jedná se o další ze základních povinností, jejímž obsahem je povinnost zajistit tzv. ‚**bezpečnost** zpracovávaných osobních údajů'* […].“[38] Lze také citovat z úvodu komentáře pro odst. 3 daného paragrafu: „*S ohledem na velmi obecnou formulaci povinnosti zajistit **bezpečnost** osobních údajů, byl Úřad od samého počátku své existence žádán o vymezení základních bezpečnostních podmínek nějakým zvláštním opatřením Úřadu nebo právním předpisem*.“[39]

U monografie *Matese, Janečkové* a *Bartíka* z roku 2012 lze pro zajímavost zmínit, že ačkoliv výše zmíněné české znění Úmluvy č. 108 publikované ve Sbírce mezinárodních smluv překládá článek 7 jako *Zabezpečení údajů*, autoři na něj odkazují za užití sousloví *Zásada **bezpečnosti***.[40]

Komentář k zákonu č. 101/2000 Sb. autorského kolektivu pod vedením *Kučerové* z roku 2012 v poznámkách k § 13 zákona silně inklinuje k preferování pojmu bezpečnost před pojmem zabezpečení. Příkladem následující krátké úryvky: „[…] *správce je povinen zvolit si pouze takové zpracovatele, kteří garantují potřebnou míru **bez-***

---

32 KUČEROVÁ, A. et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2003, s. 136.
33 Tamtéž.
34 Tamtéž.
35 MATOUŠOVÁ – HEJLÍK, c. d., s. 18.
36 Tamtéž, s. 253.
37 Tamtéž, s. 255.
38 BARTÍK, V. – JANEČKOVÁ, E. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: Anag, 2010, s. 158.
39 Tamtéž, s. 163.
40 MATES, P. – JANEČKOVÁ, E. – BARTÍK, V. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 18.

***pečnosti** zpracování*“;[41] „*Správce osobních údajů uzavřením takové smlouvy zajišťuje, že také zpracování prováděné zpracovatelem osobních údajů bude probíhat v souladu s požadavky na **bezpečnost** zpracovávaných dat*“;[42] „[…] *§ 13 OchOsÚ nemůže obsahovat detailní nebo přímo taxativní výčet opatření potřebných k zajištění **bezpečnosti** zpracovávaných dat*“;[43] „*Další kategorií opatření ve smyslu § 13 odst. 1 OchOsÚ jsou vnitřní organizační opatření, tj. závazné interní normy či pokyny stanovící odpovědnost konkrétních osob za **bezpečnost** zpracovávaných osobních údajů* […]“;[44] „*Rizika pro **bezpečnost** osobních údajů vznikají také v souvislosti s využíváním elektronické pošty* […]“;[45] „*Kromě povinnosti podniknout konkrétní kroky k zajištění **bezpečnosti** zpracovávaných osobních údajů může správce postupem podle § 6 OchOsÚ pověřit zpracovatele také zpracováním dokumentace opatření* […]“;[46] či „*Podle citovaných sankčních ustanovení je totiž v rozporu se zákonem o ochraně osobních údajů pouze nepřijetí či neprovedení opatření pro zajištění **bezpečnosti** zpracování osobních údajů*.“[47]

Novák ve svém podrobném komentáři k zákonu č. 101/2000 Sb. z roku 2014 taktéž uvádí svůj rozbor § 13 v podobném duchu: „*Problematiku **bezpečnosti** osobních údajů upravuje článek 17 směrnice 95/46/ES, konkretizující jeden ze základních principů ochrany osobních údajů*.“[48] Na to následně navazuje jak slovy: „[Ustanovení § 13 odst. 1] *Nedefinuje ani jednotlivé prostředky zajišťující **bezpečnost** osobních údajů; blíže se k této otázce vyjadřují odst. 3 a 4*“;[49] tak komentářem: „*Byť v § 13 odst. 1 zák. o ochraně os. údajů nediferencuje mezi jednotlivými kategoriemi správců údajů, je nabíledni, že pojem **bezpečnosti** bude mít rozdílný obsah v závislosti na rizicích, kterým správce údajů, resp. subjekty údajů, čelí*.“[50] Přestože se pak *Novák* při diskuzi konkrétních rozhodnutí Úřadu pro ochranu osobních údajů přidržuje terminologie zákona,[51] svou inklinaci k užití pojmu bezpečnost dává najevo v následujících pasážích komentáře, kde uvádí např.: „*Lze zdůraznit, že porušení § 13 odst. 1 zakládá též delikt ohrožovací, který je dokonán již tehdy, pokud je **bezpečnost** osobních údajů jednáním správce údajů ohrožena*“;[52] „*Tím spíše správce údajů není oprávněn činit odpovědným za **bezpečnost** subjekt údajů, vystupující kupř. v pozici příjemce služby*“;[53] či: „*Citované ustanovení ukládá správci osobních údajů povinnost přijmout technická i organizační opatření k zajištění **bezpečnosti** zpracovávaných osobních údajů, přičemž porušením této povinnosti je již situace, kdy vznikne riziko neoprávněného přístupu k osobním údajům*.“[54]

---

41 KUČEROVÁ, A. et al. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 228.
42 Tamtéž, s. 228.
43 Tamtéž, s. 229.
44 Tamtéž, s. 231.
45 Tamtéž, s. 233.
46 Tamtéž, s. 235.
47 Tamtéž, s. 236.
48 NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014, s. 222.
49 Tamtéž.
50 Tamtéž, s. 223.
51 Tamtéž, s. 225–226.
52 Tamtéž, s. 228.
53 Tamtéž, s. 230.
54 Tamtéž, s. 232.

Lze tedy uzavřít, že při výkladu obsahu termínů užitých zákonem č. 101/2000 Sb. bylo přes jejich terminologický odklon stále na místě co možná nejvíce vycházet z jejich zachycení ve směrnici 95/46/ES. S ohledem na proklamovanou kontinuitu obsahu pojmů, i absenci změn v jiných jazykových verzích, lze pak dojít k závěru, že pojmy **zabezpečení** a **bezpečnost** (zpracování) osobních údajů, jakož i **narušení bezpečnosti** a **porušení zabezpečení** by měly být vnímány co do obsahu a právní teorie za totožné a provázané.

6.2 K TERMINOLOGICKÉ PREFERENCI POJMU BEZPEČNOST

Upřednostnění pojmu **zabezpečení** před pojem **bezpečnost** pro české právo ochrany osobních údajů při současném přímém dopadu obecného nařízení je tudíž zřetelně zavádějící. Ostatně výše nastíněný vývoj jazykových verzí v legislativním procesu přijetí obecného nařízení i zmíněné vnitřní nekonzistence, jako odkaz ve článku 40 odst. 2 písm. h obecného nařízení, silně indikují, že zavedení pojmu **zabezpečení** na úkor pojmu **bezpečnost** do české jazykové verze obecného nařízení je důsledkem nedopatření překladatele, nikoliv záměrem zákonodárce.

Za přijetí této premisy je však na místě položit si otázku, jaký má tento objevený terminologický nedostatek význam, tedy zda lze obecně nalézat obsahový rozdíl mezi pojmy **bezpečnost** a **zabezpečení**. Proto je na místě nahlédnout blíže na význam užití těchto termínů v právu i v souvisejících oborech relevantních pro problematiku zajištění ochrany osobních údajů v moderní společnosti.

Pojem **bezpečnost** má zakořeněný a konzistentně aplikovaný význam v úzké souvislosti s technickými, ale i společenskovědními rovinami zde diskutovaného problému. Významným oborem jsou v tomto směru bezpečnostní studia, která řeší mezinárodní, společenské a politické roviny problematiky bezpečnostních hrozeb a bezpečnostních opatření.[55] Bezpečnost v tomto kontextu nabývá řadu významů, které se mohou dotýkat ochrany osobních údajů, ale také ji výrazně přesahovat.[56] V právní terminologii je pojem *bezpečnosti* etablován především v blízkém překryvu pro oblast kybernetické bezpečnosti. Kybernetická bezpečnost představuje souhrnný zastřešující koncept pro soubor právních, organizačních, technických a dalších prostředků a opatření, které směřují k zajištění důvěrnosti, integrity a dostupnosti dat, sítí a systémů v rámci kyberprostoru.[57] Nepominutelnou rovinou je pak také technická perspektiva zajištění bezpečnosti ICT sítí a systémů. Pro závaznou terminologii je v tomto ohledu na místě upozornit na přijaté technické normy ČSN, především normu *ČSN ISO/IEC 27000 Systémy řízení bezpečnosti informací – Přehled a slovník*,[58] či pak příkladem normu *ČSN ISO/IEC 27017 Soubor postupů pro opatření bezpečnosti informací pro cloudové služby* zalo-

---

55 Viz např. Charakteristika oboru Bezpečnostní studia FSV MUNI [online]. [cit. 17. 3. 2019]. Dostupné na: https://fsv.cuni.cz/uchazeci/magisterske-studium/bezpecnostni-studia.

56 Viz např. studijní materiál Bezpečnost (Miroslav Mareš) [online]. [cit. 17. 3. 2019]. Dostupné na: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511.

57 Srov. JIRÁSEK, P. – NOVÁK, L. – POŽÁR, J. *Výkladový slovník Kybernetické bezpečnosti* [online]. Brno: Národní centrum kybernetické bezpečnosti, 2015 [cit. 10. 1. 2019]. Dostupné na: https://www.govcert.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf, s. 69.

58 Náhled normy dostupný na: https://shop.normy.biz/detail/501452#nahled [cit. 17. 3. 2019].

žený na ISO/IEC 27002 (v anglickém znění: *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*).[59]

Pojem **zabezpečení** oproti tomu nemá srovnatelnou terminologickou bázi, která by odůvodňovala jeho záměnu s pojmem *bezpečnost*. Nejedná se ani o pojem široce či běžně užívaný, jelikož jde v převážné míře o zpodstatněné sloveso zabezpečit, které se významově blíží slovesům zajistit či zaručit.[60] Tomu odpovídá i v podstatě jediný běžný význam slova v právní terminologii, tedy problematika sociálního zabezpečení, která vytváří rámec záruk a podpory pro zajištění základních potřeb občanů v rámci společenské solidarity. Ovšem i v teorii práva sociálního zabezpečení zaznívají hlasy, které upozorňují na původ termínu v nepřesném překladu a větší přiléhavosti pojmu sociální bezpečnost.[61] Jiní autoři doplňují, že termín *zabezpečení* odpovídal dynamické činnosti přerozdělování důchodů v komunistickém pojetí, zatímco pojem *bezpečnost* je blíže současnému stavovému zajištění odpovídajících práv v demokratické společnosti.[62] Vzhledem k tomuto lze pojem *zabezpečení* v právní terminologii ochrany osobních údajů považovat za nepřípadný a neodpovídající obsahu, ke kterému je v českém znění obecného nařízení 2016/679 a směrnice 2016/680 užit.

Z tohoto důvodu lze v užití pojmu **zabezpečení** vnímat z hlediska právní teorie nevhodný terminologický odklon, který je na újmu českému právu ochrany osobních údajů. Nebezpečí z toho plynoucí je především zbytečné oddálení právní a technické roviny této problematiky, jelikož, jak bylo zmíněno výše, české technické normy pro tuto oblast pracují s pojmy *bezpečnost* a *narušení bezpečnosti*. V situaci, kdy je ze strany všech úrovní recipientů právního rámce ochrany osobních údajů voláno po vyšší srozumitelnosti a provázanosti s konkrétními technickými a organizačními požadavky, je pak tento jev značně nešťastný.

7. ZÁVĚR

Jádrem příspěvku byla analýza terminologie národních i evropských právních předpisů ochrany osobních údajů ve vztahu k problematice narušení bezpečnosti, resp. porušení zabezpečení zpracování. Je představen přístup k pojmu v relevantních normách zahrnujících Úmluvu č. 108 Rady Evropy, zákon č. 256/1992 Sb., směrnici 95/46/ES, zákon č. 101/2000 Sb., směrnici 2002/58/ES novelizovanou směrnicí 2009/136/ES, zákon č. 127/2005 Sb., obecné nařízení 2016/679, směrnici 2016/680 i nedávno přijatý zákon č. 110/2019 Sb. Hlavním poznatkem je odklon pojmů užitých ve finální české jazykové verzi obecného nařízení 2016/679 od konzistentní terminologie předcházejících evropských právních předpisů bez zjevného důvodu či odrazu v jiných jazykových verzích obecného nařízení.

---

[59] Náhled normy dostupný na: http://csnonlinefirmy.unmz.cz/html_nahledy/36/502319/502319_nahled.htm [cit. 17. 3. 2019].

[60] Srovnání viz *ABZ slovník českých synonym* [online]. 2019 [cit. 17. 3. 2019]. Dostupné na: http://www.slovnik-synonym.cz/web.php/slovo/zabezpecit.

[61] GALVAS, M. – GREGOROVÁ, Z. *Sociální zabezpečení*. Brno: Masarykova univerzita, Právnická fakulta, 2000, s. 22.

[62] TOMEŠ, I. et al. *Právo sociálního zabezpečení*. Praha: Všehrd, 1993, s. 11.

V rámci diskuse jsou představeny dva závěry, které má příspěvek za cíl podpořit v rámci akademického diskurzu ve snaze o překonání tohoto nedostatku účinné právní úpravy.

Zaprvé je na základě rozboru terminologie užívané českou odbornou veřejností ke zmíněné problematice i vzhledem k požadavku na jednotný eurokonformní výklad dovozeno, že předmětná normativní úprava obecného nařízení 2016/679 a směrnice 2016/680 plně navazuje na úpravu dle směrnici 95/46/ES a směrnici 2002/58/ES a není zde na místě nalézat obsahové odlišnosti v důsledku odlišnosti užitých pojmů.

Zadruhé je argumentováno, že pojmy **zabezpečení** zpracování a **porušení zabezpečení** (zpracování) osobních údajů jsou z hlediska teorie nepřípadné a v zájmu zdůraznění provázanosti jak eurokonformní, tak mezioborové, je na místě upřednostňovat v rámci odborného diskurzu pojmů **bezpečnost** zpracování, resp. **narušení/porušení bezpečnosti** (zpracování) osobních údajů.

Závěr příspěvku nelze jistě přeceňovat co do významu, především ve srovnání s klíčovými obsahovými změnami, které přinesla reforma ochrany osobních údajů, jako je například již vlastní zakotvení obecné povinnosti ohlašování a oznamování porušení bezpečnosti (zabezpečení) osobních údajů vůči všem správcům osobních údajů. Přesto je na místě upozornit na tuto neopodstatněnou nekonzistenci v české verzi daného evropského předpisu a prosazovat reflektování vhodného pojmosloví přinejmenším v rovině odborného diskurzu.

Mgr. Ing. František Kasl
Právnická fakulta Masarykovy univerzity
frantisek.kasl@mail.muni.cz