11

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 6 / Rok 2015 / Číslo 11

Revue.law.muni.cz

Ústav práva a technologií Právnické fakulty Masarykovy univerzity
si Vás dovoluje pozvat na VII. národní konferenci

České právo a informační technologie 2015

Plenární diskuse se zaměří na následující témata

Novelizace českého autorského zákona

Nařízení eIDAS

Abstrakty Vašich příspěvků do sekcí

Elektronické důkazy (vedoucí: Jakub Harašta)
Témata: elektronické důkazy a dokazování při autoritativní aplikaci práva, elektronické stopy

Právní ochrana výzkumných dat (vedoucí: Michal Koščík)
Témata: ochrana PDV, ochrana osobních údajů, právní ochrana dat, mezinárodní, evropské a národní politiky ochrany dat, open science data

Evropské právo on-line a v PIS (vedoucí: Danuše Spáčilová)
Témata: rešerše evropského práva a judikatury, evropský identifikátor judikatury ECLI

Síťová neutralita (vedoucí: Zdeněk Kučera)
Témata: síťová neutralita, omezování přístupu ke službám ISP, soutěžně-právní aspekty omezování služeb na internetu

lze odevzdávat prostřednictvím konferenčního webu do **30. 8. 2015**. Písemná vyhotovení příspěvků, která budou nabídnuta k publikaci v časopisu Revue pro právo a technologie, je třeba odevzdat do redakčního systému do **31. 10. 2015**. Pokyny ke zpracování příspěvků, jakož i detailní informace o konferenci jsou dostupné na konferenčním webu. Bezplatná registrace na konferenci je otevřena do **2. 9. 2015** včetně.

Datum a čas konání	24. 9. – 25. 9. 2015
Místo konání	Právnická fakulta MU, Veveří 70, Brno
Konferenční web	http://cpit.law.muni.cz

call for papers

CYBERSPACE 15
www.cyberspace.muni.cz

Brno, Czech Republic
27 – 28 November 2015

12th internatonal conference organized by the Institute of Law and Technology, Faculty of Law in cooperation with the Faculty of Social Studies, Masaryk university and the European Academy of ICT Law

Papers are solicited to the following streams:

- Cybersecurity, Cybercrime
- eCommerce, eFinance
- Government 2.0, eJustice
- Intellectual Property On-Line
- International Internet Law
- Privacy and Surveillance
- New Media and Politics
- New Media and Society
- Psychology of Cyberspace
- Religion in Cyberspace
- Video Games and Society
- Ideas for Cyberspace

Accepted papers will be, depending on their topic, published upon peer review in one of the following scientific journals:

Masaryk University Journal of Law and Technology
mujlt.law.muni.cz

Cyberpsychology
cyberpsychology.eu

Important dates

Abstract submissions
31 July 2015

Notice on acceptance
31 August 2015

Conference dates
27 – 28 November 2015

Papers for publication
11 January 2016

Conference fees

full pass – speakers: 1390 CZK (approx. 50 EUR), full pass – delegates: 1790 CZK (approx. 65 EUR),
full pass – VIPs: FREE, student pass light (programme only): FREE, student pass full: 490 CZK (approx. 18 EUR),
last minute (on-site) registration: 2100 CZK (approx. 77 EUR)

Dinner fee (Saturday conference dinner with free complementary drinks: 590 CZK (approx. 22 EUR),
Last minute (on-site): 690 CZK (approx. 25 EUR)

The registration will be carried out on-line through the conference web at www.cyberspace.muni.cz. The registration opens 1 June 2015 and closes 12 November 2015 (after that, it will be possible to register on-site).

all info at: www.cyberspace.muni.cz

REVUE PRO PRÁVO A TECHNOLOGIE

Ročník 6 | Rok 2015 | Číslo 11

DISKUZE

RECENZE

ANOTACE

TÉMA

Revue pro právo a technologie
odborný recenzovaný časopis pro technologické obory práva a právní vědy zařazený na Seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice a v databázi ERIH PLUS.
Recenzovány jsou příspěvky v sekci Diskuze a Téma.
Vychází dvakrát ročně. Toto číslo vyšlo 30. 6. 2015.
ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. č. MK ČR E 19707.
Vydává Masarykova univerzita, Žerotínovo nám. 9, 601 77 Brno, ČR, IČ 00216224.
Šéfredaktor: doc. JUDr. Radim Polčák, Ph.D.
Zástupce šéfredaktora a kontaktní osoba: JUDr. Matěj Myška, Ph.D., Ústav práva a technologií Právnické fakulty MU, Veveří 70, 611 80 Brno, ČR, tel: +420 549 494 751, fax: +420 541 210 604, e-mail: revue@law.muni.cz | https://journals.muni.cz/revue, www.revue.law.muni.cz.
Redakce: Mgr. Michal Koščík, Ph.D., Mgr. Václav Stupka, JUDr. Bc. Jaromír Šavelka, Mgr. Jakub Harašta.
Tajemník redakce: Martin Loučka.
Redakční rada: JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., Mgr. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., Mgr. Antonín Panák, LL.M., doc. JUDr. Radim Polčák, Ph.D., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Grafická úprava: Martin Loučka, JUDr. Matěj Myška, Ph.D.
Tisk: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno.
Vydání časopisu Revue pro právo a technologie bylo financováno z projektu „Právo a technologie III“, MUNI/A/1320/2014.
© 2015 Masarykova univerzita.

POKYNY PRO AUTORY

Revue pro právo a technologie je recenzovaný vědecký časopis. Recenzovány jsou příspěvky v sekci Téma a Diskuze. Rukopisy jsou anonymně posuzovány nezávislými recenzenty a konečné rozhodnutí o publikaci je v kompetenci redakční rady. Bližší informace podá na požádání redakce na e-mailu revue@law.muni.cz.

V příspěvku by měly být použity nejvýše dvě úrovně nadpisů.

DOPORUČENÝ ROZSAH PŘÍSPĚVKŮ:

Sekce Téma:	30 – 80 normostran
Sekce Diskuze:	5 – 20 normostran
Anotace judikatury:	2 – 10 normostran
Recenze knihy:	1 – 5 normostran

Pro další informace ohledně struktury a formálních náležitostí příspěvků prosím navštivte stránku „Pokyny pro autory“ na webu www.revue.law.muni.cz.

FORMÁT CITACÍ

Citace se řídí primárně Směrnicí děkana PrF MU č. 4/2013 (dostupná z http://is.muni.cz/do/law/ud/predp/smer/S-04-2013_O_citacich_dokumentu.pdf), podpůrně pak normou ISO 690 standard, 3. vydání publikované v březnu 2011. Na jednotlivé prameny se odkazuje v textu číslem poznámky psané horním indexem. Samotná citace pramene se uvádí v poznámce pod čarou.

STRUKTURACE CITACE

PRIMÁRNÍ AUTORSKÉ ÚDAJE. *Název: podnázev informačního pramene*. Sekundární autorské údaje. Vydání. Místo vydání: Nakladatelství, rok. Fyzický popis.

Pro další informace ohledně citací a jejich příkladů prosím navštivte stránku „Pokyny pro autory“ na webu https://journals.muni.cz/revue/about/submissions.

TERMÍNY PRO DODÁNÍ PŘÍSPĚVKŮ

Do letního čísla: 31. března

Do zimního čísla: 30. září

Autor zasláním příspěvku uděluje souhlas k užití svého příspěvku v elektronických databázích společností Wolters Kluwer, a. s., Nakladatelství C.H. BECK, s. r. o. a ATLAS consulting spol. s r. o., potažmo v jimi provozovaných právních informačních systémech ASPI, Beck-online a CODEXIS.

Časopis je též volně dostupný na webových stránkách https://journals.muni.cz/revue a http://revue.law.muni.cz pod licencí Creative Commons BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0/).

LICENCOVÁNÍ PSI A HOSPODÁŘSKÁ SOUTĚŽ[*]

TOMÁŠ KUBEŠA[**]

ANOTACE

Ve svém příspěvku se budu věnovat problematice licencování informací veřejného sektoru ve světle ochrany hospodářské soutěže. Rozeberu, které typy porušení hospodářské soutěže lze v souvislosti s licencováním PSI detekovat. Úzce se zaměřím na zneužití dominantního postavení podnikem, který nabude dominantního postavení v souvislosti s nabytím licence k informacím veřejného sektoru. Rozeberu kritéria, která je nutné zohlednit při posouzení, zdali došlo ke vzniku dominantního postavení. Pozastavím se u možných způsobů zneužití takového dominantního postavení. Dále navrhnu praktická opatření pro užití licencovaných PSI, která nebudou zakládat podezření ze zneužívacích praktik. Ve svém příspěvku se budu opírat o teoretický i právní základ „LAPSI" a zneužití dominantního postavení. Své závěry poměřím i s judikaturou k tématu, zejména s případem Chaps.

KLÍČOVÁ SLOVA

PSI; zneužití dominantního postavení; informace veřejného sektoru; licencování

ABSTRACT

In this article, I focus on licensing of public sector information in competition law perspective. I will list the possible breaches of competition law that can occur in PSI licensing. I will analyze an abusive behaviour of a dominant undertaking, whose dominance is based on the control of licensed PSI. The article also contains a list of criteria, that need to be met when establishing a dominant position of such undertaking. Then, possible breaches of competition

[*] Publikace tohoto článku byla podpořena z projektu specifického výzkumu PrF MU MUNI/A/0918/2013.

[**] Doktorand katedry občanského práva, Právnická fakulta MU. Kontaktní e-mail: tomas.kubesa@seznam.cz.

regulation by such a dominant will be presented. I will conclude with a list of practical measures that should clear any suspision of abusive behaviour. The article is based on the theoretical and legal foundations of LAPSI and abuse of dominance. In the final part of the article, the conclusions are applied to existing case law and the Chaps case

KEYWORDS

PSI, abuse of dominance, public sector information, licensing

1. ÚVOD DO LAPSI

Základní právní rámec pro přístup a opakované užití informací veřejného sektoru (LAPSI) je stanoven v nedávno revidované směrnici 2003/98/EC („směrnice LAPSI“), do českého právního řádu pak byl zaveden zákonem o svobodném přístupu k informacím[1]. Základem LAPSI je úvaha o prospěšnosti přístupu veřejnosti k nejširšímu spektru informací, generovaných orgány veřejné moci s možností jejich následného širokého využití, včetně komerčního. Takové využití informací veřejného sektoru („PSI“) má být omezeno jen na základě jasně vymezených důvodů, mezi něž patří ochrana soukromí, obchodního tajemství či autorských práv třetích osob. Následné využití PSI včetně komerčních způsobů skýtá potenciál jejich plného využití samostatně či v kombinaci s jinými informacemi, v surové či zpracované podobě. Vede k rozvoji podnikání, tvorbě pracovních míst a dalším prospěšným důsledkům. To vše přitom platí pro informace, které by bez LAPSI nemusely být takto efektivním způsobem využity.

Pro LAPSI platí, že informace mají být poskytovány pokud možno bezúplatně, v odůvodněných případech za úplatu odpovídající skutečně vynaloženým nákladům na poskytnutí PSI. Takové náklady zahrnují například zachycení na hmotný nosič či vyhledávání příslušných informací v širším souboru a musí být předem sdělovány. Oproti tomu obecně nelze stanovit úhradu, která by vedla ke generování zisku na straně povinného subjektu. Dále lze říci, že ani pro problematiku LAPSI nelze zavádět diskriminující kritéria pro poskytování PSI.

[1] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím.

PSI lze poskytovat s využitím licenční smlouvy. Doporučováno[2] je využití veřejných licencí, a to pokud možno co nejméně restriktivních. Směrnice LAPSI se v zásadě nestaví ani proti poskytování PSI za úplatu na základě úplatné licenční smlouvy[3], opět však pouze na nediskriminačním základě. Směrnice PSI se staví proti výhradním licenčním smlouvám, umožňuje je pouze v případě, kdy není možné zajistit správu PSI jiným způsobem[4].

Pro formát poskytovaných údajů platí jednoznačně vyjádřená preference elektronické formy[5] kdekoli je to možné či účelné. V souladu se zásadami Open Government Partnership[6]mají být PSI poskytovány v otevřených, strojově zpracovatelných formátech tak, aby další zpracování PSI bylo zjednodušeno.

Česká úprava problematiky LAPSI za evropským vzorem poněkud zaostává. ČR sice přistoupila k Open Government Partnership[7] a zavázala se tak dodržovat jeho standardy, praxe však nevykazuje příliš velkou míru souladu s těmito závazky[8]. Z poměrně obsáhlé české judikatury však již víme[9], že povinnost sdělovat informace v režimu zákona o svobodném přístupu k informacím, které mohou odpovídat PSI, svědčí i soukromým osobám, na které byl přenesen výkon veřejnoprávní pravomoci.

2. LAPSI A TRH

Z výše uvedených základních údajů o LAPSI se může zdát, že tato problematika vede pouze k pozitivním tržním dopadům. Jak si ukážeme dále, není tomu tak vždy.

---

[2] Guidelines on recommended standard licenses, datasets and charging for reuse of documents (2014/C 240/01) ze dne 24. 7. 2014. Evropská komise.

[3] Čl. 6, revidovaná směrnice 2003/98/EC o opakovaném použití informací veřejného sektoru

[4] Rec.. 20, revidovaná směrnice 2003/98/EC o opakovaném použití informací veřejného sektoru.

[5] Čl. 4, revidovaná směrnice 2003/98/EC o opakovaném použití informací veřejného sektoru

[6] Open Government Declaration, dostupná na http://www.opengovpartnership.org/about/open-government-declaration, cit. dne 16. 9. 2014.

[7] Usnesení Vlády České republiky ze dne 14. 9. 2011 č. 691 o přistoupení k mezinárodní inicicativě Open Governemnt Partnership.

[8] Zhodnocení plnění Akčního plánu České republiky „Partnerství pro otevřené vládnutí" v roce 2012 a jeho aktualizace, dostupné na http://www.korupce.cz/assets/partnerstvi-pro-otevrene-vladnuti/Zhodnoceni-AP-OGP-2012.pdf, cit. dne 16. 9. 2014.

[9] Např. Usnesení Nejvyššího správního soudu ze dne 27. 9. 2013, sp. zn. 5 As 57/2013 ve věci „*Chaps*".

V současné době lze konstatovat, že využití LAPSI v čisté podobě nezpůsobuje žádné zásadní negativní ekonomické jevy. Vzhledem k nízkým či nulovým nákladům na získání PSI, širokým možnostem jejich následného využití a pouze nepatrně omezenému okruhu subjektů, které mohou usilovat o získání a využití PSI je zajištěna vysoká míra konkurence mezi jednotlivými soutěžiteli, kteří jsou silně motivováni k vývoji produktů, postavených na využití PSI. Zásada zákazu diskriminace, jakožto i tlak na použití elektronických, otevřených a strojově zpracovatelných formátů dat dále působí jako podpora výrazně tržního prostředí a vede k optimální alokaci zdrojů.

Drobný konflikt představuje pouze vzájemný vztah zákazu diskriminace a zároveň možnosti orgánu veřejné správy účtovat za přípravu a vyhledání PSI úhradu vynaložených nákladů, spočívajících zejména v tzv. mimořádně rozsáhlém vyhledání informací[10]. Tuto úhradu lze totiž požadovat pouze po prvním žadateli totožné informace, neboť pro další žadatele již není žádné vyhledávání nutné – stačí užít jednou již vyhledaných informací. Vzniká však nerovné postavení, kdy první žadatel je povinen náklady hradit, další v pořadí však již nikoli. Dikce zákona však situaci řeší v dostatečném rozsahu.

Z pohledu hospodářské soutěže LAPSI v čisté podobě nevede ke vzniku zásadních hrozeb pro hospodářskou soutěž.

Poněkud problematická je však kombinace LAPSI s dalším ze známých institutů spolupráce veřejného a soukromého sektoru. Tímto institutem je přenos výkonu vymezené veřejnoprávní pravomoci spojené se vznikem PSI na soukromou osobu, obvykle na smluvním základě. Součástí takové dohody orgánu veřejné moci a soukromé osoby je pak obvykle i úprava problematiky přístupu ke vznikajícím PSI a jejich možného využití. Obvyklým způsobem úpravy těchto otázek je výhradní zpracování PSI soukromým subjektem spojené s jejich komerčním využitím. Taková situace již přináší z pohledu ochrany hospodářské soutěže jisté problematické momenty, nejčastěji obavy ze zneužití dominantního postavení.

[10] § 17 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

3. DOMINANTNÍ POSTAVENÍ

Tento příspěvek si neklade za cíl vyčerpávajícím způsobem rozebírat problematiku dominantního postavení a jeho zneužití. Postačí pouze stručný vhled do problematiky s tím, že zájemci mají k dispozici dostatek specializovaných kvalitních zdrojů[11].

Dominantní postavení se presumuje u soutěžitelů, disponujících určitým tržním podílem, popřípadě splňujícím další stanovená kritéria[12]. Platí přitom předpoklad, že dominantní soutěžitel disponuje tržní silou, která mu umožní chovat se do značné míry nezávisle na svých konkurentech i zákaznících[13]. Takové dominantní postavení lze přitom zneužít řadou různých způsobů, mezi jinými účtováním podnákladových cen, uzavíráním trhu a dalšími[14].

Pro dominantního soutěžitele platí jistá omezení chování na relevantním trhu, která se neužijí u ostatních, nedominantních soutěžitelů.

Pro vymezení dominantního postavení je nezbytné určení tržního podílu soutěžitele na definovaném relevantním trhu s relevantním produktem[15]. Pro správné soutěžněprávní posouzení konkrétní tržní situace je tak definice relevantního trhu a produktu zcela klíčová. Řada používaných nástrojů pro vymezení relevantního trhu pracuje s cenou relevantního produktu a jejími změnami a následnými změnami nabídky a poptávky po relevantním produktu. V případě bezúplatného plnění tyto nástroje mnohdy negenerují dostatečně spolehlivé důsledky, lze se však stále spolehnout na posouzení zastupitelnosti plnění na funkčním základě.

4. LAPSI A DOMINANTNÍ POSTAVENÍ

Jak bylo naznačeno výše, z povahy samotného LAPSI lze dovodit, že ve své čisté podobě je nepravděpodobný vznik dominantního postavení s PSI. Žádný soutěžitel se nemůže chovat nezávisle na ostatních soutěžitelích či zákaznících, neboť ti mají taktéž přístup k PSI, a to na základě totožných či

[11] Např. PETR, Michal. Zakázané dohody a zneužívání dominantního postavení v ČR, MUNKOVÁ, Jindřiška. Soutěžní právo. Praha: C.H.Beck. 2. Vyd. 2012, ISBN 978-80-7400-424-7 a další.

[12] § 10 odst. 2 zákona č. 143/2001 Sb., o ochraně hospodářské soutěže.

[13] § 10 odst. 1 zákona č. 143/2001 Sb., o ochraně hospodářské soutěže.

[14] § 11 zákona č. 143/2001 Sb., o ochraně hospodářské soutěže.

[15] § 2 odst. 2 zákona č. 143/2001 Sb., o ochraně hospodářské soutěže.

mírně výhodnějších podmínek[16]. Případné pokusy o zneužití by byly rychle korigovány přesunem poptávky k jinému soutěžiteli, případně samostatnou žádostí o PSI. Situace je samozřejmě odlišná v případě, kdy dominantní soutěžitel užívá PSI ve spojení s dalšími informacemi či službami, pak však nelze vznik dominantního postavení přičítat pouze PSI.

Dominantní postavení však může soutěžiteli vzniknout v situaci, kdy dojde k uzavření výhradní dohody o zpracování PSI. Toto postavení je posíleno, pokud je tato dohoda součástí smlouvy o výkonu specifikované veřejnoprávní pravomoci, v jejímž rámci PSI vznikají.

V obecné rovině přitom nelze přesvědčivě potvrdit závěr o tom, že dominantní postavení nevzniká pro neexistenci trhu jako takového, a to i při úzkém vymezení relevantního trhu a relevantního produktu jako informací odpovídajících rozsahem i obsahem předmětným PSI. Další soutěžitelé mnohdy mají možnost PSI či srovnatelné informace získávat sami, byť pracněji, s vynaložením větších prostředků a menší měrou spolehlivosti. Soutěž tak je, byť v čistě potenciální rovině, zachována. Výše popsané komplikace však ztěžují postavení soutěžitelů a ve svém důsledku způsobí vznik dominantního postavení subjektu, kterému PSI vznikají jako součást výkonu veřejnoprávní pravomoci.

Dominant, určený výše, se přitom nachází v komplikovaném postavení. Orgánem veřejné moci byl pověřen výkonem specifikované veřejnoprávní pravomoci, tedy činností, se kterou jsou v každém případě spojeny náklady. Při takovém výkonu přitom vznikají PSI. Častou součástí takových dohod je také ustanovení o výhradnosti použití PSI, které má generovat dostatečný příjem pro úhradu nákladů, spojených s výkonem veřejnoprávní pravomoci. Orgán veřejné moci tak ušetří veřejné prostředky a o využití PSI se stará soukromá osoba motivovaná vlastním ziskem. Taková soukromá osoba však je povinným subjektem ve smyslu zákona o svobodném přístupu k informacím, svědčí jí tedy povinnost PSI na žádost poskytnout. Vedle toho se ještě nachází v dominantním postavení, což dále omezuje možné způsoby jejího chování.

Tato situace nabízí několik řešení s tím, že žádné z nich není zcela bezproblémové. Tato řešení se pokusím popsat, představit jejich silné

[16] Jak bylo uvedeno výše, pokud povinný subjekt PSI již poskytl, byť za úhradu, tuto úhradu si nesmí nárokovat znovu. Další žadatelé v pořadí tak jsou v mírné výhodě.

i slabé stránky a následně doporučit jedno z nich jako nejméně nevhodné řešení problému.

První řešení spočívá v preferenci LAPSI a hospodářské soutěže. Soukromá osoba v tomto modelu začne na žádost poskytovat v plném rozsahu bezúplatně PSI. Jednotliví žadatelé, potenciální konkurenti na totožném relevantním trhu se tak ocitnou ve výhodě, když nebudou nuceni nést náklady, spojené se vznikem PSI výše popsaným způsobem. Soukromá osoba přijde nejen o své dominantní postavení, ale bude ekonomicky nucena odejít z trhu. Nedokáže tedy již nadále vykonávat specifikovanou veřejnoprávní pravomoc. Její výkon se vrátí orgánu veřejné moci, který po období fungování popsaného modelu již nedisponuje zdroji pro její výkon. Lze důvodně očekávat i zhoršení kvality poskytovaných PSI a zvýšení veřejných výdajů.

Druhé řešení spočívá v ignoraci LAPSI i hospodářské soutěže. Soukromá osoba bude v tomto případě odmítat poskytování PSI a vystaví se tím taktéž riziku sankcí za zneužití dominantního postavení ze strany soutěžního úřadu. Soutěžní úřad následně s využitím své pravomoci vynutí ukončení zneužívací praktiky a uloží sankce. Další vývoj již kopíruje popis první varianty. Taktéž končí odchodem soukromé osoby z trhu a návrat výkonu veřejnoprávní pravomoci orgánu veřejné moci.

5. OPATŘENÍ PROTI ZNEUŽÍVACÍM PRAKTIKÁM

Z výše uvedeného je patrné, že popsaná situace neměla v první řadě vůbec vzniknout. Z pohledu LAPSI i soutěže by bylo vhodnější, kdyby si stát ponechal výkon veřejnoprávní pravomoci a umožnil pouze široký přístup k PSI. Takový přístup lze snadno odsoudit s poukazem na nutnost vydání veřejných prostředků s tím, že výše rozebraný model takovou nutnost sice přináší, avšak až v delším časovém horizontu. Nelze však zapomenout na to, že dominant není motivován k efektivnímu fungování právě kvůli své nezávislosti na ostatních. Při výsledném porovnání obou variant je možné, že situace, kdy stát vykonává specifikovanou pravomoc a pouze poskytuje PSI, bude z celospolečenského hlediska výhodnější.

Předpokládejme však, že taková situace již vznikla[17] a pokusme se najít přijatelné řešení. Na první pohled by takovým řešením mohla být aplikace

[17] A to proto, že skutečně vznikla, v českém právním prostředí např. případ Chaps – viz dále.

tzv. essential facility doctrine[18]. Jako essential facility jsou poměrně přesvědčivě určeny například železniční koleje či produktovody[19], stále se však vedou diskuse o vhodnosti aplikace této doktríny i na nehmotné statky, například na standard-essential patents[20]. Na příkladmo uvedených trzích se osvědčilo oddělení subjektu, spravujícího onu essential facility a soutěžitelů, kteří ji následně skutečně užívají a poskytují služby na ní závislé[21].

Pro účely LAPSI by tak byl představitelný vznik další osoby, která by vykonávala specifikovanou veřejnoprávní pravomoc, vznikalo u ní PSI a byla povinným subjektem ve smyslu zákona o svobodném přístupu k informacím. Vznikající PSI by připravovala pro předání soutěžitelům na daném relevantním trhu, se kterými by uzavírala úplatné licenční smlouvy. Jejich výnos by potom pokrýval náklady na výkon veřejnoprávní pravomoci i přípravu PSI. Problém však představuje konstrukce úhrad za poskytování informací, ať už dle PSI směrnice, tak dle zákona o svobodném přístupu k informacím. Úhrada dle těchto předpisů smí být pouze ve výši marginálních či přesně vyčíslených nákladů na samotné poskytnutí informací, nikoli na jejich vznik, správu či získání. Neexistuje zde tak dostatečný prostor pro úhradu nákladů, spojených s činností tohoto samostatného podniku. Nelze tak předpokládat, že by takový podnik mohl dlouhodobě fungovat. Tato varianta řešení není z uvedených důvodů použitelná.

Nabízí se další řešení, které se zdá být použitelné za současného právního stavu, byť klade na povinný subjekt značné nároky. Řeší však vzniklou situaci bez nutnosti zásadních změn legislativy i judikatury ve věci. Toto řešení předpokládá, že povinný subjekt bude dále plnit úkoly, spojené s aplikací veřejné moci a spravovat přitom vznikající PSI. Bude

[18] Pojem essential facility je obvykle užíván bez překladu, lze však narazit na českou variantu *podstatná zařízení*. Tento koncept je kvalitně, včetně komparativního pohledu, vysvětlen např. v The Essential Facility Concept. OECD. 1996. Dostupný na http://www.oecd.org/competition/abuse/1920021.pdf, cit. dne 16. 9. 2014.

[19] The Essential Facilities Concept. Policy Roundtables. OECD. Paříž 1996. Dostupný na http://www.oecd.org/competition/abuse/1920021.pdf, cit. dne 23. 9. 2014.

[20] Pojem taktéž bývá používán převážně v originálním anglickém znění, lze však narazit na českou variantu standardní esenciální patent. Standard-essential Patents. Competition policy brief. Evropská komise. Červen 2014. 8. vydání. Dostupný na http://ec.europa.eu/competition/publications/cpb/2014/008_en.pdf, cit. dne 23. 9. 2014.

[21] Příkladem je vyčlenění Správy železniční a dopravní cest, státní organizace jako správce essential facility v podobě železniční sítě a ji využívajících dopravců.

zároveň i povinným subjektem dle zákona o svobodném přístupu k informacím a vznikající PSI bude na základě tohoto zákona poskytovat. Výše zmíněné komplikace jeho fungování, spočívající v nutnosti vynakládat zvýšené výdaje v souvislosti s výkonem veřejné moci přitom bude možné překonat, a to z následujících důvodů.

Povinný subjekt jakožto inkumbent[22] již má vybudovánu potřebnou infrastrukturu pro získávání, správu, údržbu, zpracování i komerční využití PSI. Nebude tedy nucen do této oblasti vkládat vysoké počáteční výdaje tak, jako nově vstupující subjekty, entranti[23]. Nejméně z krátkodobého pohledu tak entranti nebudou schopni nabídnout nižší ceny či lepší obchodní podmínky při využití PSI, neboť budou muset splácet náklady na vstup na trh.

Inkumbent již má vyvinutý funkční obchodní model, stabilní zákaznický kmen s jemu známými potřebami a fungující vztahy s obchodními partnery. Nemusí na tyto aspekty podnikání vynakládat další investice, opět na rozdíl od entrantů.

Inkumbentovi svědčí setrvačnost trhu a zvyk jeho zákazníků, která i po vstupu entrantů udrží značnou část jeho zákazníků, bude bránit jejich odchodu a tím inkumbentovi udrží značnou část příjmů, a to nejméně krátkodobě i za situace, kdy entranti přijdou s lepším produktem, využívajícím PSI.

I inkumbentovi svědčí zákonné lhůty pro poskytování PSI, takto poměrně dlouhé. PSI tak má k dispozici dříve než entranti, a to aniž by jejich vydání zdržoval.

Z výše uvedených důvodů má inkumbent dostatečné možnosti a zdroje k tomu, aby úspěšně zvládl otevření PSI entrantům, byť na něj budou kladeny nové nároky. Je třeba si připomenout, že pokud inkumbent není schopen nabídnout ani za těchto podmínek dostatečně kvalitní produkt, který by dokázal entrantům úspěšně konkurovat, nelze jeho postavení chránit před konkurenčními tlaky, a to ani prostředky práva hospodářské soutěže, ani LAPSI. Toto platí obzvláště na tzv. dvoustranných trzích, kde jedné straně trhu je produkt poskytován zdarma, zatímco příjmy jsou generovány na druhé straně trhu, a to v závislosti na počtu či charakteru

[22] Tedy soutěžitel, který na daném relevantním trhu již působí.
[23] Tedy soutěžitelé, kteří se pokouší o vstup na daný relevantní trh.

uživatelů na opačné straně trhu. Lze tedy říci, že na první straně trhu je konkurence spíše necenová, například kvalitativní, zatímco cenová konkurence panuje až na druhé straně trhu.

6. PŘÍPAD CHAPS

V České republice je typickým případem, kde se projevují výše obecně popsané jevy, případ *Chaps*. Jádrem případu je situace, kdy Ministerstvo dopravy pověřilo na základě zákonného zmocnění[24] smluvně[25] společnost Chaps vedením a správou CIS JŘ[26]. Existuje veřejnoprávní povinnost provozovatelům veřejné linkové dopravy zasílat správci CIS JŘ, tedy společnosti Chaps, aktuální jízdní řády provozovaných linek, a to ve formátu, specifikovaném správcem CIS JŘ[27]. Dle příslušné smlouvy je činnost společnosti Chaps pro Ministerstvo dopravy vykonávána bezplatně, pouze výměnou za právo výhradně užívat vzniklé informace. Společnost Chaps na těchto informacích vystavěla vyhledavač spojení IDOS[28], v současné době součást portálu idnes.cz[29], generující velmi vysokou návštěvnost a následně také příjmy ze zobrazované reklamy[30]. Činnost vyhledávače IDOS je pro jeho uživatele zdarma, obsahuje také propojení na prodej autobusových a vlakových jízdenek či na mapový server. Vyhledávání IDOSu přitom neprobíhá pouze nad daty Chapsu, získanými v jeho veřejnoprávní roli, ale i nad daty, získanými v rámci jeho obchodní činnosti[31].

---

[24] § 17 odst. 2 zákona č. 111/1994 Sb., o silniční dopravě.

[25] Příslušný text smlouvy je dostupný např. na http://www.mdcr.cz/NR/rdonlyres/78D0A36B-683B-49B4-83B0-2107D8C88BFB/0/KopieUlozeneSmlouvyCISsDodatky.PDF, cit. Dne 23. 9. 2014.

[26] Celostátní informační systém o jízdních řádech.

[27] Metodický pokyn č. 4 k organizaci celostátního informačního systému o jízdních řádech, č.j. 56/2012-190-IDS/1. Ministerstvo dopravy. Dostupný na http://www.mdcr.cz/NR/rdonlyres/C35BBFAE-E315-48F0-9040-A3339F482F48/0/MetodickyPokyn4schvaleny.PDF, cit. dne 23. 9. 2014.

[28] Vyhledávač je dostupný na http://jizdnirady.idnes.cz, cit. dne 23. 9. 2014.

[29] http://www.idnes.cz/.

[30] DOČEKAL, D., iDnes je prý jednička mezi zpravodajskými servery. Skutečně? Lupa.cz. Dostupný na http://www.lupa.cz/clanky/idnes-je-pry-jednicka-mezi-zpravodajskymi-servery-skutecne/, cit. dne 23. 9. 2014.

[31] VYLEŤAL, M., Tomáš Chlebničan (CHAPS): Data, která má Bileto a Seznam, pocházejí od nás. Lupa.cz. Dostupný na http://www.lupa.cz/clanky/tomas-chlebnican-chaps-data-ktera-ma-bileto-a-seznam-pochazeji-od-nas/, cit. dne 23. 9. 2014.

Nejvyšší správní soud rozhodl[32], že informace, vznikající Chapsu při správě CIS JŘ je nutné podřídit režimu zákona o svobodném přístupu k informacím a označil je tedy za PSI. Společnost Chaps na základě tohoto usnesení sice poskytuje požadované informace, avšak nikoli ve formátu, jak je poskytují sami dopravci, ale v jiném formátu, a to v *.xls[33]. Tento formát sice je strojově zpracovatelný, ale již nikoli otevřený a k jeho vytvoření byla nezbytná další činnost Chapsu. Pro další zpracování je přitom formát *.xls méně vhodný než původní formát *.csv, neboť formát *.xls vyžaduje poněkud náročnější zpracování a kontrolu dat. Takové jednání spol. Chaps přitom postrádá racionální právní vysvětlení. Chaps má k dispozici požadovaná data ve vhodném otevřeném zaručeném a strojově zpracovatelném formátu, neboť je v něm dostává od samotných dopravců. Oprávněným však poskytuje data zpracovaná, přičemž při takovém zpracování může dojít ke zhoršení jejich kvality. Chaps tak vynakládá značné úsilí a prostředky k tomu, aby svým konkurentům poskytovat požadované PSI v potenciálně horší kvalitě, než v jaké je sám dostává, aniž by pro takové jednání existoval právní důvod. Takové jednání lze stěží zařadit do legitimního rámce s pro poskytování PSI popsaného výše, když dochází k faktickému omezování dodávek.

Z představených okolností případu je zřejmé, že jedinými schůdnými, resp. nejlepšími možnými, jsou řešení představené ve výše uvedeném teoretickém modelu. Prvním řešením je stav, kdy inkumbent poskytuje PSI entrantům a čelí jejich konkurenci s tím, že konkurenční nevýhoda spočívající v nutnosti nést náklady na zpracování PSI je vyvážena nejrychlejším přístupem k těmto PSI a dalšími výhodami, popsanými výše. Druhým možným řešením je ukončení smluvního vztahu mezi Ministerstvem dopravy a Chapsem a návrat výkonu příslušné veřejnoprávní pravomoci ministerstvu[34].

[32] Usnesení Nejvyššího správního soudu sp. zn. 5 As 57/2013 ze dne 27. 9. 2013.

[33] VYLEŤAL, M., Tomáš Chlebničan (CHAPS): Data, která má Bileto a Seznam, pocházejí od nás. Lupa.cz. Dostupný na http://www.lupa.cz/clanky/tomas-chlebnican-chaps-data-ktera-ma-bileto-a-seznam-pochazeji-od-nas/, cit. dne 23. 9. 2014.

[34] Tento přístup zvolily např. holandské orgány ve věci PostNL, viz. například http://www.epsiplatform.eu/content/dutch-postcodes-case cit. dne 23. 9. 2014.

7. ZÁVĚR

V tomto příspěvku jsem popsal velmi specifickou situaci, reálně vznikající v oblasti nakládání s informacemi orgány veřejné správy. Tato situace vzniká v rámci snah o úsporu veřejných prostředků, avšak může vést k omezením hospodářské soutěže i práva na svobodný přístup k informacím. Základním závěrem tohoto příspěvku je, že k popisované situaci nemělo primárně vůbec dojít. Z uvedených závěrů vyplývá, že tato situace nenabízí dobrých řešení, pouze méně špatných. Tato řešení ve svém důsledku vedou ke značnému zvýšení konkurenčního tlaku na subjekt, kterému PSI vznikají. Takový subjekt je přitom při soutěži znevýhodněn, neboť nese náklady na vznik a zpracování PSI, má však řadu předpokladů proto, aby tento tlak ustál a na daném trhu se udržel. Alternativou je navrácení výkonu činností, směřujících ke vzniku PSI orgánu veřejné správy.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

NEJEDNOZNAČNOST ODKAZŮ K SOUDNÍM ROZHODNUTÍM A MOŽNOSTI ŘEŠENÍ

JAKUB HARAŠTA[*]

ABSTRAKT

Článek je úvahou na téma nejednoznačné citace judikatury. Nejednoznačná citace může v zsáadě způsobit dva problémy - problém faktické nedohledatelnosti kvůli použití neurčitého identifikátoru a problém nejednoznačnosti použité verze. Článek prokazuje, že mezi jednotlivými vyjádřeními téhož rozhodnutí je možné najít za pomoci nástrojů jazykové analýzy rozdíly, a na jednoznačné identifikaci verze je tak nutné trvat. Článek dále představuje dva možné přístupy k řešení těchto problémů. Problém s dohledatelností by mohl být vyřešen centralizovaně za pomoci identifikátoru ECLI a naplnění související databáze. Problém s nejednoznačností verze je pak možné řešit decentralizovaně korektní citací, která často jde nad rámec citačních předpisů.

KLÍČOVÁ SLOVA

judikatura; citace; ECLI; nejednoznačné identifikátory

ABSTRACT

This article reflects the theme of ambiguous citation of the case law. The ambiguous citations may cause two problems - the problem of factual untraceability due to the use of uncertain identificator and the problem of ambiguity of the used version. As the article shows, there are differences between different expressions of the same decision. Therefore, it is necessary to insist on the unambiguous identification of the decision. The article further presents two

[*] Mgr. Jakub Harašta je asistentem na Ústavu práva a technologií PrF MU a externím doktorandem tamtéž. Kontaktní e-mail: jakub.harasta@law.muni.cz.

possible approaches that could solve these issues. The issue of untraceability can be solved by the ECLI identifier and the related database. The issue of the ambiguity of the used version can be solved by the proper citation of the case law, often going beyond the standard of citation.

KEYWORDS

case law; citation; ECLI; ambiguous identifiers

ÚVOD

Citace judikatury je neoddělitelnou složkou práce mnoha právních povolání, ať už jde o soudce, advokáty anebo akademické pracovníky. Současnou praxi odkazování na judikaturu je však možné považovat za problematickou. Autoři často zapomínají na primární účel citace, kterým je zajistit dohledatelnost odkazovaného dokumentu. Neadekvátní citace soudního rozhodnutí má zpravidla za následek jednu z následujících situací: Závažnější je situace, kdy citované rozhodnutí nelze dohledat. Méně závažnou je pak situace, kdy není zřejmé, jakou verzi rozhodnutí měl autor na mysli. Nedohledatelnost může být způsobena například odkazem na vzácný zdroj či použitím nesrozumitelné citace. Nejednoznačnost verze může vzniknout v případě mnohostí zdrojů dokumentu nebo v případě násobného výskytu rozhodnutí v rámci jednoho zdroje (např. právního informačního systému). Tento text analyzuje závažnost předestřeného problému a dále diskutuje jeho možná řešení.

1. VÝZNAM JUDIKATURY

Viktor Knapp ve své knize Teorie práva poznamenává, že v rámci kontinentálního práva má právo soudcovské menší roli než v rámci systému common law.[1] Za materializaci tohoto přístupu Knapp označuje článek 5 francouzského Code Civil z roku 1804 i pozdější § 12 rakouského Allgemeines bürgerliches Gesetzbuch. Obě tato ustanovení zapovídají soudům rozhodovat způsobem obecným a normativním. Rozhodování soudů se musí dít pouze v intencích daného případu a nesmí přesáhnout jeho hranice. Soudce nesmí aspirovat na roli svěřenou zákonodárci. Ač tedy

[1] KNAPP, Viktor. *Teorie práva*. 1. vyd. Praha: C.H. Beck, 1995, xvi, 247 s. ISBN 8071790281. s. 133 odst. 328.

soudci ve Francii před rokem 1789[2] dominovali a de facto se účastnili právotvorby, po roce 1804 svá rozhodnutí téměř neodůvodňovali – zřejmě právě z důvodu nemožnosti odvozovat z nich aplikovatelná pravidla. Knapp svůj výklad uzavírá konstatováním, že *„současná literatura většinou připouští, že soudní rozhodování, a to zejména tzv. konstantní judikatura vyšších soudů, která zpravidla bývá ať už oficiálně nebo neoficiálně publikována, působí, jako by byla pramenem práva.“*[3]

To v praxi znamená, že by judikatura měla být citována jak ve chvíli, kdy s ní soudce souhlasí, tak ve chvíli, kdy se vůči ní vymezuje. Soudce totiž musí svůj odlišný názor náležitým způsobem odůvodnit. Stejně, jako jsme mohli za materializaci předchozího přístupu považovat příslušná ustanovení Code Civil nebo Allgemeines bürgerliches Gesetzbuch, můžeme dnes za materializaci aktuálního přístupu považovat v českém prostředí § 13 zákona č. 89/2012, občanského zákoníku. Ochraňovanou hodnotou je v pojmosloví občanského zákoníku „důvodné očekávání“ neboli právní jistota a náležitá odůvodněnost soudního rozhodování ve vztahu k typovým věcem. Docházíme tak ke konstatování, že *„statický pohled na právo jako sumu norem vyjádřenou v textech zákonů je v soudobém kontinentálním právním diskursu již dávno překonán.“*[4]

Akceptujeme-li tedy, že s judikaturou je třeba pracovat při odůvodňování právního názoru, musíme zároveň přisvědčit tomu, že judikatura musí být náležitě publikována. Publikace je jedním z faktorů, který ovlivňuje použitelnost judikatury pro další argumentaci. Smejkalová konstatuje, že tato podmínka je vytvářena samotnou existencí právního státu, který musí dát účastníkům šanci se s rozhodovací praxí seznámit.[5] Soudy totiž svojí interpretací dotvářejí obsah právních norem. Stát má tedy, v zájmu zajištění právní jistoty, pozitivní povinnost sdělit tento

[2] KÜHN, Zdeněk, Michal BOBEK a Radim POLČÁK. *Judikatura a právní argumentace: teoretické a praktické aspekty práce s judikaturou*. Vyd. 1. Praha: Auditorium, 2006, xxii, 234 s. ISBN 8090378609. S. 1.

[3] Knapp 1995, op. cit., s. 133 odst. 329. Shodně KÜHN, Zdeněk a Hynek BAŇOUCH. O publikaci a citaci judikatury aneb proč je někdy judikatura jako císařovy nové šaty. *Právní rozhledy* [online]. 2005, č. 15, s. 484. In: Beck-online [právní informační systém]. *C. H. Beck* [cit. 26. 3. 2015]. Dostupné z: https://www.beck-online.cz/bo/document-view.seam?documentId=nrptembqgvpxa4s7gezv643uojptiobu&groupIndex=0&rowIndex=0.

[4] Kühn 2005, op. cit.

[5] SMEJKALOVÁ, Terezie. *Soudnictví, jeho povaha a role v právním systému ČR*. Disertační práce [online]. IS MUNI [cit. 26. 3. 2015]. Dostupné z: https://is.muni.cz/auth/th/77065/pravf_d/Smejkalova_Soudnictvi.pdf. S. 179.

interpretovaný obsah subjektům práva. Polčák k tomu uvádí, že *„judikát, který je sice pravomocný, avšak není běžnými prostředky dostupný veřejnosti, […] lze jen stěží považovat za součást argumentačně závazné judikatury a jeho vývody bez dalšího autoritativně aplikovat.“*[6] Při odkazování na takto publikované rozhodnutí je však navíc nutné zajistit jeho dohledatelnost tak, aby bylo možné si ověřit deklarované vlastnosti rozhodnutí, na které je odkazováno.[7]

Samotná publikace v současné době probíhá ve třech rovinách – zákonné, oficiální a soukromé. Zákonnou publikací je publikace přímo předpokládaná zákonnými ustanoveními. Například v případě Ústavního soudu zákon zakotvuje povinnost vydávat Sbírku nálezů a stanovisek Ústavního soudu.[8] Oficiální publikační platformy nejsou explicitně předpokládány ustanoveními zákona. Jejich existence[9] však usnadňuje přístup veřejnosti k právu. K přístupu do oficiálních databází totiž není nutné vynakládat žádné prostředky, vyjma zajištění přístupu k internetu. Zákonné sbírky je oproti tomu nutné fyzicky zakoupit.[10] Oficiální publikační platformy tedy, dle názoru autora, lépe naplňují maxima svobodného přístupu k právu. Ostatně jsou často vytvářeny právě s poukazem na zákon č. 106/1999 Sb., o svobodném přístupu k informacím. Soukromými publikačními platformami má autor na mysli jakýkoli způsob publikace judikatury prostřednictvím soukromých subjektů. Jejich vydávání negarantuje žádná oficiální autorita a jejich existence není předepisována zákonem. Jakýkoli právní informační systém, který v sobě zahrnuje judikaturu, tak představuje soukromou publikační platformu. Soukromé publikační platformy nejsou omezeny pouze na publikaci prostřednictvím právních informačních systémů, ale v širším

---

[6] POLČÁK, Radim. Internet a proměny práva. Praha: Auditorium, 2012, 388 s. ISBN 9788087284223. S. 234.

[7] Shodně Kühn 2005, op. cit., kdy v intencích pojmu „ustálená judikatura“ autoři konstatují, že citace musí být přesná, aby bylo možné ověřit, nakolik je judikatura opravdu konstantní a kvalitně argumentovaná.

[8] § 59 zákona č. 182/1993 Sb., o ústavním soudu, ve znění k 26. 3. 2015.

[9] Databáze Ústavního soudu na http://nalus.usoud.cz/, databáze Nejvyššího soudu na http://http://www.nsoud.cz/JudikaturaNS_new/ns_web.nsf/WebSpreadSearch, databáze Nejvyššího správního soudu na http://www.nssoud.cz/main0col.aspx?cls=JudikaturaBasicSearch&pageSource=0 a Evidence soudních rozhodnutí vrchních a krajských soudů na http://www.nsoud.cz/Judikaturans_new/judikatura_vks.nsf/uvod.

[10] Elektronické verze se nezveřejňují. Nejvyšší správní soud zveřejňuje *ex post* seznam rozhodnutí do sbírky zařazených.

slova smyslu zahrnují též periodika, ve kterých je judikatura v té či oné formě zahrnuta.

Právě soukromou publikaci judikatury je v současné době možno považovat za nejméně průhlednou – ať už z hlediska publikace textů rozhodnutí nebo z hlediska použitých identifikátorů. Šavelka v minulosti kritizoval praxi několikanásobného zařazování rozhodnutí publikovaných ve více zdrojích do právních informačních systémů[11] a nedá se říci, že by se situace výrazným způsobem posunula k lepšímu. Publikace tak zůstává do značné míry nepřehledná a vícekolejnost publikace přináší problémy v použití konkrétních rozhodnutí.

Při zmíněné mnohosti publikačních platforem a často násobném zařazování téhož rozhodnutí do informačních systémů je vhodné brát v potaz i ontologickou úroveň rozhodnutí, na které odkazujeme. Při použití standardního referenčního rámce, který používá IFLA[12] a dále i Opijnen,[13] můžeme identifikovat čtyři ontologické úrovně[14] každého rozhodnutí:

1. Dílo[15]
2. Vyjádření[16]
3. Manifestace[17]
4. Předmět[18]

Dílo je individuální intelektuální výtvor autora a na ontologickou úroveň díla odkazujeme například ve chvíli, kdy v textu uvádíme názor soudu. Citace, kterou náš argument doprovázíme v podobě poznámky pod čarou nebo v závorce, odkazuje na konkrétní vyjádření rozhodnutí – to jsme mohli získat například ze zákonné sbírky, z oficiálních stránek soudu atp. Manifestace představuje PDF nebo DOC verzi, která je k dispozici ke

[11] ŠAVELKA, Jaromír. Jak zlepšit zpřístupňování judikatury? *Jiné Právo* [online]. 2012 [cit. 26. 3. 2014]. Dostupné z: http://jinepravo.blogspot.cz/2012/04/jaromir-savelka-jak-zlepsit.html.

[12] IFLA Study Group on the Functional Requirements for Bibliographic Records. *Functional Requirements for Bibliographic Records* [online]. IFLA Section on Cataloguing: Mnichov [cit. 26. 3. 2015]. Dostupné z: http://www.ifla.org/files/assets/cataloguing/frbr/frbr.pdf. S. 12.

[13] OPIJNEN, Marc van. *Finding Case Law on a European Scale – Current Practice and Future Work* [online]. SSRN, 2008 [cit. 26. 3. 2015]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046266. Kap. 3.2.

[14] Úrovně abstrakce.

[15] Angl. work.

[16] Angl. expression.

[17] Angl. manifestation.

[18] Angl. item.

stažení. Po stažení na paměťové médium pak hovoříme o ontologické úrovni předmětu.[19]

Například ve chvíli, kdy je dále v textu uváděno rozhodnutí Nejvyššího správního soudu ve věci sp. zn. 6 Ads 94/2007 ze dne 11. září 2008, je odkázáno na existenci tohoto rozhodnutí na ontologické úrovni díla. Poznámka pod čarou, kterou je tato zmínka doprovázena, představuje identifikaci konkrétního vyjádření, v tomto případě vyjádření, které je k dispozici na oficiálních stránkách Nejvyššího správního soudu. Anonymizovaná PDF verze tohoto rozhodnutí[20] představuje manifestaci a po stažení na paměťové médium se jedná o předmět. Abychom mohli hovořit o dohledatelnosti a jednoznačnosti citovaného rozhodnutí, je nutné výše nastíněné rozdíly brát v potaz.

2. ŘEŠENÍ PROBLÉMU DOHLEDATELNOSTI

Ve svém komentáři k trestnímu řádu,[21] a to konkrétně v části věnované § 88a tohoto zákona, odkazuje Šámal na související rozhodnutí, které označuje jako „TP 796/2011“.[22] Dále následuje pouze právní věta rozhodnutí. Pokud se čtenář s touto informací nehodlá spokojit a chce si rozhodnutí přečíst celé, musí ho nalézt. Výše uvedený identifikátor však o samotném rozhodnutí nesděluje žádné další informace. Při vynaložení jisté míry úsilí je možné dospět k významu identifikátoru „TP“ jako náležejícímu časopisu Trestní právo. Toto rozhodnutí bylo uveřejněno v čísle 2/2011 jako „č. 796/2011“ a jedná se o Usnesení Vrchního soudu v Olomouci ze dne 15. 6. 2010, sp. zn. 5 To 42/2010. Je však otázkou, zda by například laik byl schopen rozhodnutí za pomoci poskytnutého identifikátoru dohledat. Používání nejednoznačných identifikátorů, které jsou přiřazovány v rámci konkrétní publikační platformy a které nesdělují žádné informace o rozhodnutí samotném, není v České republice ani mimo ni nikterak výjimečné. Rovněž Nejvyšší správní soud tento problém

[19] Jedná se tedy o jeden konkrétní exemplář manifestace.

[20] Dostupné z: http://www.nssoud.cz/files/SOUDNI_VYKON/2007/0094_6Ads_0700073A_prevedeno.pdf [cit. 26. 3. 2015].

[21] ŠÁMAL, Pavel a kol.: *Trestní řád. Komentář*. 7. vydání. Praha: C. H. Beck, 2013, 4700 s. In: Beck-online [právní informační systém]. *C. H. Beck* [cit. 26. 3. 2015].Dostupné z: https://www.beck-online.cz/bo/document-view.seam?documentId=nnptembrgnpwk5tlge3a&groupIndex=3&rowIndex=0.

[22] Tamtéž, s. 1236.

kritizoval ve svém rozhodnutí sp. zn. 6 Ads 94/2007 ze dne 11. září 2008,[23] kdy vytknul soudu nižší instance použití interních identifikátorů Ejk 99/2006 či Ej 308/2006 jako nedostatečné.

Jedním ze základních způsobů identifikace judikatury by tak mělo být používání identifikátorů, které na první pohled sdělují dostatečné množství informací o rozhodnutí samotném. Standardním způsobem identifikace je použití tří atributů: identifikace soudu, čísla věci a dne rozhodnutí. Právě tyto tři údaje se běžně používají na přímou identifikaci rozhodnutí českých soudů – zajišťují jednoznačnou identifikaci rozhodnutí, ale samy o sobě nás neinformují o místě, na kterém můžeme dané rozhodnutí najít.

V případě použití tří atributů (Usnesení Vrchního soudu v Olomouci ze dne 15. 6. 2010, sp. zn. 5 To 42/2010) i neurčitého identifikátoru (TP 796/2011) je odkazováno na toto rozhodnutí v ontologické úrovni díla. Jedná se o jednoznačnou identifikaci, ta ale automaticky neznamená dohledatelnost. Dohledatelnosti je dosaženo až v případě recepce tohoto identifikátoru čtenářem, který je dostatečně zkušený na to, aby věděl, kde za pomoci tohoto identifikátoru text rozhodnutí hledat. Při identifikaci výše zmíněnou trojicí atributů je, dle mého názoru, potřebná míra zkušeností a znalostí výrazně nižší než v případě použití identifikátoru specifického pro publikační platformu. Trojice atributů je technologicky neutrální a informuje nás o specifických vlastnostech rozhodnutí – i z toho důvodu ji považuji za vhodnou.

Používání neurčitých identifikátorů opakovaně kritizuje i Opijnen,[24] který je duchovním otcem European Case Law Identifier (dále jen „ECLI“). ECLI představuje jeden z projektů směřujících ke zjednodušené identifikaci konkrétních soudních rozhodnutí na celoevropské úrovni. Má pevnou syntax a stejně jako výše uvedená trojice atributů má i schopnost informovat nás o konkrétních vlastnostech rozhodnutí. Identifikátor se skládá z prefixu ECLI, který jednoznačně určuje druh identifikátoru a tím do jisté míry snižuje znalostní práh potřebný k jeho pochopení. Dále následuje kód korespondující s příslušným členským státem EU, rok vydání rozhodnutí a alfanumerický identifikátor ve formátu, který určí členský

[23] Rozsudek Nejvyššího správního soudu ze dne 11. 9. 2008, č. j. 6 Ads 94/2007-73. *Nejvyšší správní soud* [online]. Nejvyšší správní soud, 2003 – 2010 [cit. 26. 3. 2015]. Dostupné z: http://www.nssoud.cz/.

[24] Opijnen 2008, op. cit., kap. 3.3.

stát. Tento alfanumerický formát může mít maximálně 25 znaků a v případě českých rozhodnutí umožní velice snadnou identifikovatelnost ze strany českých právníků, protože se skládá ze spisové značky věci, ve které bylo rozhodnutí vydáno, a je doplněný o pořadí rozhodnutí v daném spise. Kompletní identifikátor pro rozhodnutí českého Nejvyššího soudu tak může vypadat následujícím způsobem: ECLI:CZ:NS:2013:21.Cdo.1934.2012.1. Tento identifikátor nám tedy postupně (odděleno dvojtečkami) sděluje, že se jedná o identifikátor ECLI, rozhodnutí je vydané soudem České republiky, jedná se o Nejvyšší soud, rozhodnutí vydané roku 2013 ve věci sp. zn. 21 Cdo 1934/2012. Identifikátor zcela na konci za tečkou pak informuje o faktu, že se jedná o první rozhodnutí v dané spisové značce. Tento identifikátor, jakkoli vypadá složitě, je díky své pevné struktuře ideálním způsobem, jak identifikovat každé jednotlivé rozhodnutí v Evropské unii. Přesněji řečeno ve státech, které se projektu v současné době účastní.

Identifikátor je samozřejmě pro laického čtenáře stejně nesrozumitelný jako výše kritizovaný odkaz na rozhodnutí publikované v časopise Trestní právo. Zásadní rozdíl však spočívá v předpokládané existenci online platformy, která by měla zajistit dostupnost rozhodnutí pod daným identifikátorem. Testovací provoz této platformy v současné době probíhá. Vyhledávač má fungovat jako rozcestník – při zadání ECLI má fungovat jako sbírka jednotlivých vyjádření daného rozhodnutí. Při zadání shora uvedeného ECLI:CZ:NS:2013:21.Cdo.1934.2012.1 tak bude vyhledávač obsahovat odkaz na plné znění rozhodnutí v rámci databáze na stránkách Nejvyššího soudu a v případě plné naplněnosti i odkazy na jeho další vyjádření, např. v komerčních právních informačních systémech.[25] Celá iniciativa je totiž otevřená jak národním soudům, tak i provozovatelům soukromých publikačních platforem a dalším subjektům.[26] V praxi by pak existence platformy mohla mj. znamenat, že při použití ECLI identifikátoru jako hledaného výrazu v běžném vyhledávači by byl čtenáři nabídnut odkaz na záznam o rozhodnutí v rámci této online platformy.

[25] Zřejmě s příznakem „subscription needed“ nebo s podobným označením.

[26] V rámci zkušebního provozu je do vyhledávače zařazována i judikatura vydavatelem ACA-Europe (provozuje databáze Dec.Nat a JURIFAST).

Zásadní slabinou celého systému je ve výše nastíněném kontextu jeho dobrovolnost. V jejím důsledku totiž není garantováno, že hledané rozhodnutí je v systému skutečně zařazeno.

Systému se v současné době účastní Česká republika,[27] Bulharsko, Dánsko, Německo, Irsko, Španělsko, Francie, Litva, Malta, Nizozemsko, Slovinsko, Slovensko a Finsko.[28] Jestli vůbec kdy k plné naplněnosti ECLI platformy dojde či nikoli, zůstává otázkou. Samotná existence projektu je větší části odborné veřejnosti spíše neznámá a skepse je, vzhledem k naplněnosti databází Dec.Nat a JURIFAST a jejich výrazným nedokonalostem, zcela na místě.

ECLI tedy má fungovat jako jednoznačná identifikace rozhodnutí na ontologické úrovni díla obsahující nezbytné informace o rozhodnutí samém. Ve chvíli, kdy bude vyhledávač zprovozněn a naplněn, což je, jak bylo výše uvedeno, poměrně problematické, bude s jeho pomocí možné identifikovat všechna vyjádření daného rozhodnutí,[29] čímž dojde k zajištění dohledatelnosti i při identifikaci na ontologické úrovni díla. Jedná se tak o systém, který by při plné naplněnosti představoval řešení problému dohledatelnosti.

3. ŘEŠENÍ PROBLÉMU NEJEDNOZNAČNOSTI VERZE

Kompletní citace, která obsahuje vedle určení ontologické úrovně rozhodnutí i zdroj, je identifikací ontologické úrovně vyjádření. Směrnice děkana č. 4/2013, o citacích dokumentů užívaných v pracích podávaných na Právnické fakultě Masarykovy univerzity,[30] předpokládá úplnou bibliografickou citaci ve tvaru: druh soudního rozhodnutí, soud, který rozhodnutí vydal, datum vydání, spisová značka (nebo podobné označení).[31] Za tuto bibliografickou citaci, která rozhodnutí identifikuje na ontologické úrovni díla, je nutné připojit bibliografickou citaci zdroje, ze

[27] Identifikátorem ECLI označuje svá rozhodnutí Nejvyšší soud a Ústavní soud.

[28] V rámci zkušebního provozu systému, který bude zmíněn dále v textu, jsou ale pouze rozhodnutí z České republiky, Nizozemska, Slovinska, Francie, Německa, Finska a Španělska.

[29] A to bez ohledu na publikační platformu, použité médium a přístupnost.

[30] Směrnice děkana č. 4/2013, o citacích dokumentů užívaných v pracích podávaných na Právnické fakultě Masarykovy univerzity [online]. [cit. 26. 3. 2015]. Dostupné z: http://is.muni.cz/do/law/ud/predp/smer/S-04-2013_O_citacich_dokumentu.pdf.

[31] Tamtéž, čl. 7 odst. 1.

kterého byl text rozhodnutí čerpán,[32] která by ho měla identifikovat na ontologické úrovni vyjádření. V takovém případě je rozhodnutí dohledatelné. Problém však může nastat v případě, že je v příslušném zdroji zařazeno více verzí téhož rozhodnutí.

Například výše uvedené rozhodnutí Nejvyššího soudu (sp. zn. 21 Cdo 1934/2012) jsme schopni dohledat hned v několika vyjádřeních. Beck-online obsahuje tři různá vyjádření tohoto rozhodnutí, ASPI potom dvě. V rámci oficiální databáze Nejvyššího soudu pak lze nalézt další vyjádření téhož rozhodnutí.

Jednotlivá vyjádření rozhodnutí 21 Cdo 1934/2012:

1. Beck-online, C 12845[33]
2. Beck-online, AN 1/2014 str. 29[34]
3. Beck-online, Výběr NS 4377/2013[35]
4. ASPI, Původní nebo upravené texty[36]
5. ASPI, SoJ 12/2014 str. 961[37]
6. Nejvyšší soud[38]

V případě korektní citace v souladu s výše uvedenou citační směrnicí Právnické fakulty Masarykovy univerzity je možné jednoznačně určit verzi rozhodnutí v rámci systému Beck-online, protože je nutné citaci doprovázet URL dokumentu. I v případě násobné publikace v systému je tak možné vyhnout se problému s nejednoznačností citované verze. Problém nastává

---

[32] Tamtéž, čl. 7 odst. 3.

[33] Usnesení Nejvyššího soudu ČR ze dne 25. 9. 2013, sp. zn. 21 Cdo 1934/2012. *Beck-online* [právní informační systém]. C. H. Beck [cit. 26. 3. 2015]. Dostupné z: https://www.beck-online.cz/bo/document-view.seam?documentId=njptembrgnpwgxzrgi4dini&groupIndex=0&rowIndex=0.

[34] Usnesení Nejvyššího soudu ČR ze dne 25. 9. 2013, sp. zn. 21 Cdo 1934/2012. *Beck-online* [právní informační systém]. C. H. Beck [cit. 26. 3. 2015]. Dostupné z: https://www.beck-online.cz/bo/document-view.seam?documentId=njptembrgrpwc3s7gfpxg5dsl4zds&groupIndex=1&rowIndex=0.

[35] Usnesení Nejvyššího soudu ČR ze dne 25. 9. 2013, sp. zn. 21 Cdo 1934/2012. *Beck-online* [právní informační systém]. C. H. Beck [cit. 26. 3. 2015]. Dostupné z: https://www.beck-online.cz/bo/document-view.seam?documentId=njptembrgnpxm6lcmvzf63ttl42dgnzx&groupIndex=2&rowIndex=0.

[36] Usnesení Nejvyššího soudu ČR ze dne 25. 9. 2013, sp. zn. 21 Cdo 1934/2012. *ASPI* [právní informační systém]. Wolters Kluwer [cit. 26. 3. 2015]. ASPI ID JUD242186CZ.

[37] Usnesení Nejvyššího soudu ČR ze dne 25. 9. 2013, sp. zn. 21 Cdo 1934/2012. *ASPI* [právní informační systém]. Wolters Kluwer [cit. 26. 3. 2015]. ASPI ID JUD277354CZ.

[38] Usnesení Nejvyššího soudu ČR ze dne 25. 9. 2013, sp. zn. 21 Cdo 1934/2012. *Nejvyšší soud* [online]. Nejvyšší soud, © 2010 [cit. 25. 4. 2013]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/53EF4A8D02706D95C1257C08002E7693?openDocument&Highlight=0.

např. v případě systému ASPI, který sice obsahuje unikátní identifikátor ASPI ID, ten ale není obligatorní součástí citace v souladu se směrnicí.

Logicky se nabízí otázka, nakolik jsou vlastně vyjádření téhož rozhodnutí odlišná. V rámci ověření, zda se jednotlivá vyjádření tohoto rozhodnutí liší, je třeba je očistit od hlaviček a podobných výsledků redakčního procesu. Výsledek tohoto procesu je dále v textu označován jako „očištěná struktura". Nad těmito strukturami a nad právními větami jednotlivých vyjádření byla provedena volně dostupnými nástroji jazyková analýza směřující k porovnání podobnosti jednotlivých vyjádření.

TAB. Č. 1: POČTY ZNAKŮ V OČIŠTĚNÉ STRUKTUŘE[39]

Vyjádření	**Počet znaků v očištěné struktuře**
1 Beck, C 12845	22850
2 Beck, AN 1/2014, s. 29	22938
3 Beck, Výběr NS 4377/2013	22541
4 ASPI, PnU	22815
5 ASPI, SoJ 12/2014, s. 961	22001
6 Nejvyšší soud	22820

TAB. Č. 2: POČTY ZNAKŮ V PRÁVNÍ VĚTĚ

Vyjádření	**Počet znaků**
1 Beck, C 12845	253
2 Beck, AN 1/2014, s. 29	852
3 Beck, Výběr NS 4377/2013	860
4 ASPI, PnU	353
5 ASPI, SoJ 12/2014, s. 961	290
6 Nejvyšší soud	X

[39] Tedy pouze samotný text odůvodnění – došlo k odstranění hlaviček, podpisů apod.

TAB. Č. 3: PODOBNOSTI OČIŠTĚNÉ STRUKTURY ZÍSKANÉ POROVNÁNÍM ŘETĚZCŮ[40]

Očištěná struktura	**1 Beck, C 12845**	**2 Beck, AN 1/2014, s. 29**	**3 Beck, Výběr NS 4377/2013**	**4 ASPI, PnU**	**5 ASPI, SoJ 12/2014, s. 961**	**6 Usnesení Nejvyššího soudu**
1 Beck, C 12845	1	0,9964	0,9851	0,9905	0,9527	0,9912
2 Beck, AN 1/2014, s. 29	0,9964	1	0,9825	0,9873	0,9555	0,988
3 Beck, Výběr NS 4377/2013	0,9852	0,9825	1	0,9932	0,8991	0,994
4 ASPI, PnU	0,9905	0,9873	0,9933	1	0,9443	0,9993
5 ASPI, SoJ 12/2014, s. 961	0,9523	0,9558	0,8999	0,9444	1	0,9441
6 Nejvyšší soud	0,9912	0,988	0,994	0,9993	0,9437	1

[40] *String similarity test* [online]. Tools 4 noobs, 20072015 [cit. 26. 3. 2015]. Dostupné z: http://www.tools4noobs.com/online_tools/string_similarity/.

TAB. Č. 4: PODOBNOSTI PRÁVNÍCH VĚT ZÍSKANÉ POROVNÁNÍM ŘETĚZCŮ[41]

Právní věta	**1 Beck, C 12845**	**2 Beck, AN 1/2014, s. 29**	**3 Beck, Výběr NS 4377/2013**	**4 ASPI, PnU**	**5 ASPI, SoJ 12/2014, s. 961**	**6 Usnesení Nejvyššího soudu**
1 Beck, C 12845	1	0,4531	0,3365	0,4861	0,9195	X
2 Beck, AN 1/2014, s. 29	0,4531	1	0,4339	0,3953	0,509	X
3 Beck, Výběr NS 4377/2013	0,3365	0,3967	1	0,4573	0,3629	X
4 ASPI, PnU	0,4861	0,317	0,4573	1	0,5525	X
5 ASPI, SoJ 12/2014, s. 961	0,9195	0,509	0,3272	0,5525	1	X
6 Nejvyšší soud	x	x	x	x	x	X

Na základě Tab. č. 1 a Tab. č. 3 je možné uzavřít, že jednotlivá vyjádření získaná z právních informačních systémů se liší. Na základě porovnávání řetězců textu však nedosahuje podobnost jakékoli dvojice získaných vyjádření hodnoty nižší, než je 89,91%. Této nejnižší míry podobnosti, kterou je možné považovat za poměrně nízkou s ohledem na fakt, že se jedná o různá vyjádření téhož rozhodnutí, bylo dosaženo např. rozdílnou praxí v označování soudů nebo redakční prací při odkazování na související ustanovení zákonných předpisů. Z toho je možno uzavřít, že co do obsahu se jednotlivé verze neliší.

Na základě Tab. č. 2 a Tab. č. 4 je naopak možné konstatovat, že mezi právními větami je výrazně menší podobnost než mezi očištěnými strukturami jednotlivých vyjádření téhož rozhodnutí. Skutečný rozdíl mezi jednotlivými vyjádřeními pak tkví v přítomnosti[42] a podobě právních vět, které přitom nejsou součástí rozhodnutí samotného. Jedná se o výsledek,

[41] Tamtéž.
[42] Nebo absenci.

který bylo do značné míry možné očekávat. Vzhledem k častému (a dle mého názoru nesprávnému) používání právních vět pro argumentaci není možné akceptovat nedostatečné určení konkrétní použité verze. Jako prostředek k řešení tohoto problému je nutné doporučit přesnou citaci, která by měla jít i nad rámec některých používaných citačních předpisů.

4. ZÁVĚR

Současná praxe odkazování k judikatuře trpí závažnými nedostatky. K odstranění těchto nedostatků by mohlo přispět zavedení jednotného identifikátoru a vytvoření obecně známého vyhledávače. Citace běžným způsobem, tedy na úrovni vyjádření, je pak žádoucí vzhledem k existujícím citačním standardům na úrovni ČSN nebo předpisům jednotlivých institucí. Ani ta nicméně není bez problémů. Nejednoznačná identifikace ve zdroji s násobnou přítomností (tedy např. identifikace v rámci ASPI bez uvedení ASPI ID) neodkazuje na ontologickou úroveň vyjádření a ve své podstatě je nekompletní. I přesto, že lze na základě výše uvedené analýzy konstatovat velmi malé rozdíly mezi jednotlivými vyjádřeními téhož rozhodnutí, je nutné trvat na jednoznačné identifikaci rozhodnutí. Jsem si vědom, že náhodně vybrané rozhodnutí není možné považovat za reprezentativní vzorek. Empirické ověření závěrů na větším vzorku rozhodnutí a/nebo při zařazení většího množství jednotlivých vyjádření bude předmětem dalšího výzkumu.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

ZAISTENIE ELEKTRONICKÉHO DÔKAZU VO SVETLE REKODIFIKÁCIE TRESTNÉHO PORIADKU

TOMÁŠ ABELOVSKÝ[*]

ANOTACE

Predmetom tejto krátkej úvahy je zamyslenie sa nad inštitútom elektronického dôkazného prostriedku, jeho úskaliami a súčasnými tendenciami, ktoré by nemali ostať opomenuté v pripravovanom trestnom procesnom kódexe. Zaujímavým a často diskutovaným spôsobom získavania dôkazov je zvláštna ediční povinnosť na uchovávanie a vydanie inkriminovaných počítačových údajov, resp. dát. Táto povinnosť je zakotvená v § 90 TP SR. Môže sa zdať, že tento procesný inštitút môže slúžiť ako vhodná inšpirácia pre súčasné legislatívne práce v ČR. V úvahe bude poukázané aj na jeho nedostatky a možné spôsoby nápravy.

KLÍČOVÁ SLOVA

elektronický dôkazný prostriedok, dátový nosič, dokazovanie, zaistenie dôkazu

ABSTRACT

The subject of this short paper is the reflection on institute of electronic evidence, on its difficulties and present tendencies, which should not be forgotten in the upcoming Code of Criminal Procedure. An interesting and often discussed way of collection of evidence is special obligation to safeguarding and surrendering incriminating computer stored information (resp., data). The obligation is based in the Section 90 of Slovak Code of Criminal Procedure. It may seem that this procedural institute can serve as an appropriate inspiration

[*] Autor je doktorským studentem Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: tomas@abelovsky.com

for the current legislative works in Czech Republic. Also, the discussion shall highlight its deficiencies and possible means of redress.

KEYWORDS

electronic evidence, data storage, evidencing, seizing of evidence

1. ÚVODNÉ POZNÁMKY

Elektronický, resp. digitálny dôkazný prostriedok[1] v súčasnom trestnom konaní predstavuje jeden z kľúčových nástrojov získavania dôkazov.[2] V dobe rozmachu kyberkriminality a sofistikovaného organizovaného zločinu sa vyťažovanie počítačových systémov pre účely ďalšieho forenzného skúmania stalo dennou rutinou orgánov činných v trestnom konaní. Tie sú konfrontované s neutíchajúcim technologickým pokrokom a sústavnou rafinovanosťou páchateľov. Avšak na druhej strane tu stojí základné právo na spravodlivý súdny proces vyšetrovanej osoby, ktorá sa v postavení účastníka konania aktívne zaujíma o spôsob, formu a účel zaistenia elektronického dôkazného prostriedku.[3] Napätie medzi týmito dvoma záujmami je riešené predovšetkým procesnou kodifikáciou trestného práva. Tá by mala predstavovať základ pre správne zbieranie (zaisťovanie), vykonávanie a hodnotenie dôkazov. Zmyslom dokazovania je overenie si určitého tvrdenia, čo predstavuje myšlienkový proces zrekonštruovania minulých dejov. Preto, nový fenomén elektronického dôkazného prostriedku posúva paradigma vnímania procesu dokazovania do úplne novej roviny. Pri každom dokazovaní po získaní požadovanej informácie, pristupuje logická operácia podradenia skutkovej (dejovej) podstaty pod zodpovedajúcu právnu normu.[4] Navyše, pre dokazovanie elektronickými dôkaznými prostriedkami bude priliehavosť voľby právnej normy súdom

[1] Anglo-americká právna úprava hovorí o *e-evidence, digital evidence* alebo *electronic stored information.*

[2] Táto skutočnosť je daná aj tým, že podiel elektronických dát v podnikovom sektore sa za posledných 15 rokov zvýšil z 20% na 90%. Viď. Forenzní služby: eDiscovery. In: PWC Česká Republika, s.r.o. [online]. [cit. 2015-06-12]. Dostupné z: http://www.pwc.com/cz/cs/forenzni-sluzby/assets/pwc-vyhledavaci-technologie.pdf

[3] Viď. napr. Rampášek, M. Ústavnoprávne garancie pri uchovaní a vydaní počítačových údajov. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 6. 2013.

[4] Podľa Knappa môžeme hovoriť, že súčasťou aplikácie práva je práve táto operácia - subsumpcia. Viď. KNAPP, Viktor. Teorie práva. Praha : C.H.Beck, 1995. ISBN 80-7179-028-1. s. 187.

okrem iného závislá aj na tom, ako dobre bude zistená samotná skutková podstata prostredníctvom vykonávania takýchto dôkazov.[5] Je preto dôležité sledovať, ako bude vyzerať úprava zaisťovania elektronických dôkazov v novom procesnom kódexe.

Pripravovaná rekodifikácia trestného poriadku v ČR si kladie za cieľ zrýchliť trestné konanie, posilniť význam štádia konania pred súdom, zvýšiť aktivitu procesných strán a stanoviť procesnú zodpovednosť štátneho zástupcu za nevykonanie dôkazu v potrebnom rozsahu (formálne dôkazné bremeno).[6] Okrem toho, že pred súdom bude zvýraznený princíp kontradiktórnosti, nový trestný poriadok počíta so samostatnou úpravou absolútne neúčinných dôkazov. Ako je vidieť, nový kódex precizuje dokazovanie a stranou neostáva ani súčasný inštitút zaistenia veci. Východiska a princípy nového trestného poriadku počítajú v nadväznosti na rozvoj používania elektronických prostriedkov s novou úpravou zaisťovania dát z počítača a iných elektronických zariadení, a to aj spôsobom na diaľku. Rozhodovacia prax ukázala, že zaisťovanie dát dostáva nový rozmer a vymaňuje sa zo zaužívaného inštitútu zaisťovania veci. Príkladom môže byť nedávne rozhodnutie Ústavného súdu ČR, kde sa okrem povahy sociálnej siete riešil aj spôsob nešťastne predloženého elektronického dôkazu – printscreenu počítačovej obrazovky (sociálnej siete Facebook) policajným vyšetrovateľom.[7] O konkrétnych detailoch rekodifikácie pracovná komisia zatiaľ mlčí, ale pre potreby tejto práce je potrebné predstaviť možnosti komparatívneho pohľadu so slovenskou procesnou úpravou.

2. ZAISTENIE DÁTOVÉHO NOSIČA ALEBO DÁT?

Súčasná právna úprava v prípade využitia zaisťovacieho prostriedku v prípravnom konaní alebo konaní pred súdom počíta so všeobecnou

---

[5] Abelovský, T. Elektronický dôkazný prostriedok vo svetle práva duševného vlastníctva. In: Cofola 2014: the conference proceedings. 1. vyd. Brno: Masaryk University, 2014. Spisy Právnické fakulty Masarykovy univerzity v Brně, sv. 483. ISBN 9788021072114. s. 185.

[6] MS ČR: Komise pro nový trestní řád. Věcný záměr trestního řádu - hlavní principy navrhované rekodifikace trestního práva procesního [online]. [cit. 2015-06-12]. Dostupné z: http://www.ceska-justice.cz/wp-content/uploads/2014/04/hlavn%C3%AD_principy_1.pdf

[7] Rozhodnutie Ústavného súdu ČR zo dňa 30.10.2014 spis.zn. III.ÚS 3844/13. [online]. [cit. 2015-06-12]. Dostupné z: http://www.usoud.cz/aktualne/?tx_ttnews%5Btt_news%5D=2746&cHash=2a4e443657acf7a2db351b9cac9264f8

edičnou povinnosťou zakotvenou v § 78 TŘ ČR.[8] V praxi sa často tento inštitút využíva spolu s domovou prehliadkou podľa § 82 až § 85b TŘ ČR. Navyše, podľa zjednocujúceho stanoviska NSZ, zaistenie aktuálneho stavu emailovej schránky (online služba umožňujúca uloženie dát prijatej, rozpísanej, odoslanej a zmazanej elektronickej komunikácie) je možné vykonávať aj v súlade s inštitútom sledovania osôb a vecí podľa § 158 odst. 1, 3 TŘ ČR.[9] Avšak, platný trestný poriadok nerobí rozdiel v otázkach zaistenia dôkazných prostriedkov medzi vecou a elektronicky uloženou informáciou, resp. dátami. Orgány činné v trestnom konaní sa k dôkazom dostávajú prostredníctvom vyťažovania zaistených elektronických nosičov (vecí) za využitia odbornej znaleckej expertízy. Táto koncepcia je však prekonaná, nakoľko už dávno nie sme svedkami toho, že by páchatelia nechávali svoje elektronické stopy len na USB kľúčoch, pevných diskoch, cédečkách alebo na už historicky znejúcich disketách (hmotných predmetoch). Kyberpriestor v súčasnosti predstavuje nový fenomén, ktorý umožňuje virtualizovanie dát do takej podoby, že tie sú fyzicky nelokalizovateľné.[10] Čo je však dôležitejšie, zaistenie dát na rozdiel od zaistenia veci (napr. celého hard disku počítača) môže priniesť omnoho šetrnejší a precíznejší zásah do práv vyšetrovaného. Ide o vyjadrenie zásady zdržanlivosti a primeranosti, resp. minimalizácie a subsidiarity, ktoré sú vlastné trestnému právu.[11]

---

[8] „Kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu; je-li ji nutno pro účely trestního řízení zajistit, je povinen věc na vyzvání těmto orgánům vydat.“ Viď. § 78 odst. 1 zákona č. 141/2014 Sb. o trestním řízení soudním (trestní řád) In: Beck-online [právní informační systém]. Nakladatelství C. H. Beck [online]. [cit. 2015-06-12]. Dostupné z: http://www.beck-online.cz/

[9] „Aktuální obsah e-mailové schránky je určován vůlí uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 trestního řádu, který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin.“ Viď. Stanovisko č.1/2015 NSZ ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek [online]. [cit. 2015-06-12]. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

[10] Napr. cloud systém, ktorý využíva serverové farmy po celom svete a ani sám správca tohto systému nevie, kde sa nachádza ten ktorý sektor disku s požadovanou informáciou, nakoľko tieto môžu byť v neustálom pohybe.

[11] Kolouch, J. Zajišťovací úkony a důkazní prostředky využitelné v rámci boje s kybernetickou trestnou činností. [online]. [cit. 2014-01-12]. Dostupné z: https://csirt.cesnet.cz/Dokumenty?
action=AttachFile&do=get&target=Zajistovaci+ukony-RTF.pdf

Budapeštiansky dohovor o počítačovej kriminalite (ďalej len ako „Dohovor“)[12] definuje počítačové údaje ako akékoľvek znázornenie faktov, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu umožňujúceho nariadiť výkon nejakej funkcie počítačovým systémom. Ďalej o prevádzkových údajoch hovorí, že ide o akékoľvek počítačové dáta, ktoré súvisia s komunikáciou prostredníctvom počítačového systému, sú generované počítačovým systémom, ktorý tvoril súčasť reťazca komunikácie, s uvedením pôvodu, cieľa, trasy, času, dátumu, objemu, trvania komunikácie alebo typu základnej služby. Počítačové údaje môžu byť súčasťou jedného alebo viacerých dátových nosičov. Môžu byť zašifrované a navonok vystupovať ako prázdne nezapísané miesto dátového nosiča. Môžu byť rovnako schované v inom dátovom formáte (napr. steganografia). Navyše nikdy nemusia byť uložené v celku a na jednom fyzickom mieste (napr. packaging). Ich vlastnosťou je potencionálna ubiquita a volatilita. Potencionálna ubiquita predstavuje pojmový znak predmetu, ktorý je v nehmotnej podobe a ktorý sa vyznačuje schopnosťou byť všadeprítomný. Môže byť kedykoľvek a kdekoľvek vnímaný (napr. webstránka s protiprávnym obsahom, pirátska kópia audiovizuálneho diela šírená sieťou P2P). Taktiež ho môže užívať (prezerať) neobmedzený počet ľudí. Čo je zásadné, toto užívanie nemusí ovplyvňovať jeho podstatu a funkciu. Na druhej strane volatilita alebo volatilnosť (z angl. volatility) je v ekonomických vedách pojem užívaný pre kolísavosť, nestálosť, prchavosť, resp. premenlivosť hodnôt. Táto vlastnosť však výstižne popisuje základnú črtu elektronických dát. Totiž každý elektronický alebo digitálny záznam sa môže pomerne jednoducho a nepozorovane (aj automaticky) modifikovať alebo zmeniť. Takáto zmena je spôsobená povahou alebo okolnosťami, za ktorých bolo s týmto záznamom nakladané. Inak povedané, už len samotným kopírovaním záznamu dát sa môže kontaminovať ich obsah. Kľúčom k elektronickému dokazovaniu je práve pochopenie tejto vlastnosti – volatility elektronického dôkazného prostriedku v počiatočnej fáze – zaisťovania počítačových údajov. Aj keď ide o pomerne náročné technické vedomosti o spôsobe zberu, nakladania a uchovávania dát výpočtovej

[12] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č.104/2013 Sb. medzinárodných smluv ČR. [online]. [cit. 2015-06-12]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=26438

techniky, už samotná vedomosť o možnej volatilite napovie o správnej voľbe postupov. Navyše, pre správne technické postupy musí existovať opora v trestnom poriadku.

3. ZAISŤOVANIE POČÍTAČOVÝCH ÚDAJOV VO SVETLE SLOVENSKÉHO TRESTNÉHO PRÁVA

3.1 ZÁKONNÉ USTANOVENIE

Slovenská právna úprava priniesla vo svojej rekodifikácii trestného poriadku (ďalej ako „TP SR“) z roku 2005 v štvrtej hlave o zaistení osôb a vecí v § 90 špeciálnu úpravu uchovania a vydania počítačových údajov:[13]

> § 90 Uchovanie a vydanie počítačových údajov
>
> *(1) Ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné uchovanie uložených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, môže predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor vydať príkaz, ktorý musí byť odôvodnený aj skutkovými okolnosťami, osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, aby*
>
> a) také údaje uchovali a udržiavali v celistvosti,
>
> b) umožnili vyhotovenie a ponechanie si kópie takých údajov,
>
> c) znemožnili prístup k takým údajom,
>
> d) také údaje odstránili z počítačového systému,
>
> e) také údaje vydali na účely trestného konania.
>
> (2) V príkaze podľa odseku 1 písm. a) alebo písm. c) musí byť ustanovený čas, po ktorý bude uchovávanie údajov vykonávané, tento čas môže byť až na 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz.
>
> (3) Ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné, vydá predseda senátu

[13] Viď. § 90 zákona č. 301/2005 Zb. Trestný poriadok In: Jednotný automatizovaný systém právnych informácií [online]. [cit. 2015-06-12]. Online. Dostupné z: http://jaspi.justice.gov.sk

> a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovávania týchto údajov.
>
> *(4) Príkaz podľa odsekov 1 až 3 sa doručí osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, ktorým sa môže uložiť povinnosť zachovať v tajnosti opatrenia uvedené v príkaze.*
>
> *(5) Osoba, v ktorej držbe alebo pod jej kontrolou sa nachádzajú počítačové údaje, vydá tieto údaje, alebo poskytovateľ služieb vydá informácie týkajúce sa týchto služieb, ktoré sú v jeho držbe alebo pod jeho kontrolou, tomu, kto vydal príkaz podľa odseku 1 alebo osobe uvedenej v príkaze podľa odseku 1.*

Podľa tohto ustanovenia ide o situáciu, kedy na objasnenie skutočností závažných pre trestné konanie je nevyhnutné uchovanie, resp. vydanie uložených počítačových údajov vrátane prevádzkových údajov. Tento zaisťovací úkon nie je podmienený výpočtom špecifických trestných činov. Navyše, použitie § 90 TP SR nie je v aplikačnej praxi jednoznačné a prináša nedorozumenia, kedy sa toto ustanovenie má využiť.[14] V nasledujúcej časti budú rozobraté jednotlivé podmienky použitia tohto ustanovenia.

3.2 POČÍTAČOVÉ A PREVÁDZKOVÉ ÚDAJE, OTÁZKA ICH VZNIKU

Tak ako Dohovor, aj zákon rozlišuje dve samostatné kategórie údajov. Zákon priamo neuvádza, či v čase vydania príkazu už musia údaje existovať a musia byť uložené prostredníctvom počítačového systému. Dôvodová správa k zákonu sa obmedzuje na konštatovanie že, „[ú]prava reaguje na dohovor Rady Európy o počítačovej kriminalite, ktorý bol prijatý členskými štátmi Rady Európy dňa 23.11.2001 v Budapešti. Toto ustanovenie umožňuje vydať príkaz na uchovanie a vydanie počítačových dát pre účely trestného konania, najviac na 90 dní. Príkaz na uchovanie a vydanie počítačových dát, ak sú potrebné na účely trestného konania je možné vydať opätovne.“[15] Súčasná odborná literatúra je veľmi skromná

[14] Rampášek, M. Uchovanie a vydanie počítačových údajov v trestnom konaní. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 5 (2013), - s. 21-26. Lit.

[15] MS SR. Dôvodová správa, Všeobecná časť, Podľa Plánu legislatívnych úloh vlády SR na rok 2003 sa predkladá do legislatívneho procesu návrh nového Trestného poriadku. Epi.sk. Elektronické právne informácie. [online]. [cit. 2015-06-12]. Dostupné z: http://www.epi.sk/dovodova-sprava/Dovodova-sprava-k-zakonu-c-301-2005-Z-z.aspx

a obmedzuje sa na konštatovanie, že „účelom tohto inštitútu je najmä odhaľovanie a vyšetrovanie trestnej činnosti páchanej prostredníctvom internetu.“[16] V praxi sa objavuje názor, že by mohlo ísť aj o údaje prenášané v reálnom čase (najmä z dôvodu možného zaistenia reálne prenášaných prevádzkových údajov). S týmto názorom sa však nie je možné stotožniť. Účel tohto ustanovenia smeruje iba k uchovaniu už prenesených (uložených) údajov (a to vrátane uložených prevádzkových údajov). Teda ide o zaistenie počítačových údajov už zapísaných na pevnom nosiči. Taktiež, gramatickým výkladom je možné dospieť k tomu, že ide o minulé údaje (t.j. tie, ktoré boli uložené prostredníctvom počítačového systému). Navyše, Dohovor rozlišuje medzi urýchleným uchovaním uloženým počítačových údajov (článok 16), urýchleným uchovaním a čiastočným sprístupnením prevádzkových údajov (článok 17), zhromažďovaním údajov v reálnom čase (článok 20) a zachytením obsahových údajov (článok 21). Predmetné zákonné ustanovenie však kopíruje povinnosti uvedené v ustanoveniach o urýchlenom uchovaní uložených počítačových údajov (článok 16)[17] a prehliadke o zaistení uložených počítačových údajov (článok 19).[18]

3.3 OPRÁVNENÝ ORGÁN A POVINNÁ OSOBA

Právomoc na vydanie tohto príkazu má pred začatím trestného stíhania alebo v prípravnom konaní prokurátor, v ostatných prípadoch predseda senátu.

Príkaz môže smerovať voči osobe, v ktorej držbe alebo pod ktorej kontrolou sa nachádzajú počítačové údaje alebo voči poskytovateľovi

[16] Minárik, Š. Trestný poriadok. Stručný komentár. 2010. Iura edtion s.r.o. str. 315 an.

[17] Čl.16 ods. 1 Dohovoru: „Každá strana prijme potrebné legislatívne a iné opatrenia, aby umožnila jej príslušným orgánom nariadiť alebo podobným spôsobom zabezpečiť urýchlené uchovanie určených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, najmä ak existujú dôvody domnievať sa, že hrozí osobitné riziko straty alebo pozmenenia týchto počítačových údajov.“

[18] Čl.19. ods. 3 Dohovoru: „Každá strana prijme potrebné legislatívne alebo iné opatrenia na udelenie oprávnenia jej príslušným orgánom zaistiť alebo podobne zabezpečiť počítačové údaje, ku ktorým získali prístup podľa odseku 1 alebo 2. Tieto opatrenia zahŕňajú oprávnenie zaistiť alebo podobne zabezpečiť počítačový systém alebo jeho časť, alebo pamäťový nosič počítačových údajov, vyhotoviť a ponechať si kópiu týchto počítačových údajov, zachovať celistvosť relevantných uložených počítačových údajov, znemožniť prístup k takým počítačovým údajom alebo ich odstrániť z počítačového systému, do ktorého sa vstúpilo.“

služieb.[19] Procesná legitimácia povinnej osoby je definovaná buď fyzickou držbou údajov alebo štatútom poskytovateľa služieb. Teda príkaz sa bude doručovať osobe, v ktorej držbe alebo pod ktorej kontrolou sa nachádzajú také údaje alebo poskytovateľovi takých služieb (napr. prevádzkovateľovi webhostingu, cloudovej služby, účtovných služieb atď.)

Je potrebné zdôrazniť, že príkaz nemusí smerovať len priamo voči osobe, ktorá je pôvodcom počítačových údajov. Z praktického hľadiska je možné rozlíšiť medzi:

- tretími osobami, t.j. operátorom (poskytovateľom telekomunikačnej služby podľa zákona č. 351/2011 Z. z. o elektronických komunikáciách), inou osobou poskytujúcou online služby (napr. služby informačnej spoločnosti podľa zákona č. 22/2004 Zb. o elektronickom obchode) alebo vôbec neregulovanou osobou, a
- podozrivým, resp. obvineným alebo obžalovaným v zmysle TP SR.

Nakoľko procesné nároky v prípravnom konaní sú nenáročné (stačí príkaz prokurátora), prax ukázala, že využitím tohto inštitútu môže dôjsť k obchádzaniu iných informačno-technických prostriedkov (napr. odpočúvanie a záznam telekomunikačnej prevádzky, sledovanie osôb a vecí), pre ktoré sú definované vyššie kontrolné mechanizmy na ich vykonanie.[20] V súčasnosti orgány činné v trestnom konaní nemôžu bez súhlasu súdu žiadať od poskytovateľa telekomunikačnej služby (operátora) obsahové údaje. Podľa zrušeného § 116 ods. 4 TP SR, ustanovenia o zaistení prevádzkových údajov o uskutočnenej telekomunikačnej prevádzke sa primerane vzťahovali aj na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému. Táto skutočnosť

[19] Slovenská platná právna úprava pozná dva základné subjekty v oblasti telekomunikačnej (internetovej) prevádzky. Ide o telekomunikačného operátora, ktorý poskytuje elektronickú komunikačnú sieť alebo službu v zmysle § 5 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách. Ďalším je poskytovateľ služieb informačnej spoločnosti podľa zákona č. 22/2004 Z.z. o elektronickom obchode. Z dostupnej odbornej literatúry (Rampášek) vyplýva, že sa poskytovateľom služby na účely príkazu podľa § 90 Trestného poriadku rozumie podnik podľa zákona o elektronických komunikáciách. Totiž rozdiel medzi uvedenými subjektmi je potrebný pre rozlíšenie medzi dvoma druhmi počítačových údajov, a to medzi obsahovými údajmi a prevádzkovými údajmi.

[20] Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky vydáva predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Viď. § 115 ods.1 zákona č.301/2005 Z. z. Trestný poriadok. In: Jednotný automatizovaný systém právnych informácií. [online]. [cit. 2015-06-12]. Dostupné z: http://jaspi.justice.gov.sk/jaspiw1/jaspiw_mini_fr0.htm

bola zmenená nedávnym rozhodnutím Ústavného súdu SR spis. zn. PL. ÚS 10/2014 zo dňa 29.4.2015, v ktorom plénum Ústavného súdu SR vyhlásilo ustanovenia § 58 ods. 5 až ods. 7 a § 63 ods. 6 zákona č. 351/2011 Z.z. o elektronických komunikáciách, ktoré doteraz prikazovali operátorom sledovať komunikáciu svojich užívateľov, ako aj § 116 zákona č. 301/2005 Z. z. Trestný poriadok a § 76a ods. 3 zákona č. 171/1993 Z. z. o Policajnom zbore, ktoré umožňovali ich sprístupňovanie, za nesúladné s ústavne garantovaným právom obyvateľov na súkromie a ochranu osobných údajov.[21]

Je možné ešte dodať, že existujú rôzne odborné názory v interpretácií ustanovení inštitútu príkazu podľa § 90 TP SR. Rampášek uvádza, že „napriek tomu, že Slovenská republika implementovala Dohovor, implementácia predovšetkým oprávnení orgánov činných v trestnom konaní pri uchovávaní a vydaní počítačových údajov bola vykonaná nesprávne, miestami až v rozpore s účelom jednotlivých ustanovení Dohovoru, pretože pripúšťa širšie, a teda neprimerané použitie implementovaných oprávnení na uchovávanie a predovšetkým vydanie počítačových údajov.“[22] Je naozaj potrebné prisvedčiť tomu, že povinnosť vydať prevádzkové údaje v zmysle § 90 TP SR nedosahuje legálny rámec nárokov už zrušeného ustanovenia § 116 TP SR.[23] Tu totiž príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydával písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť odôvodnený aj skutkovými okolnosťami. Navyše, tieto ustanovenia sa primerane vzťahovali aj na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému.

3.4 POVINNOSTI UVEDENÉ V PRÍKAZE

Príkaz musí byť v prvom rade odôvodnený skutkovými okolnosťami. Rozsah skutkových okolností síce nie je presne definovaný, avšak príkaz

[21] V súčasnosti ešte nie je k dispozícii odôvodnenie súdu. Viď. Ústavný Súd SR, Tlačová informácia č. 25/2015. [online]. [cit. 2015-06-12]. Dostupné z: http://portal.concourt.sk/plugins/servlet/get/attachment/main/ts_data/Tl_info_25_15_el_komunikacie.pdf

[22] Ibid. Rampášek, M. Uchovanie a vydanie počítačových údajov v trestnom konaní.

[23] Paradoxne, v zmysle § 90 TP SR v súčasnosti môže prokurátor vydať príkaz na vydanie prevádzkových údajov osobe, ktorá poskytuje telekomunikačné služby, ale už nemá povinnosť tieto údaje uchovávať v zmysle zákona o elektronických komunikáciách.

musí rešpektovať základné zásady trestného procesu, najmä zásadu stíhania len zo zákonných dôvodov, kedy orgány činné v trestnom konaní môžu stíhať páchateľov len spôsobom, ktorý stanoví trestný poriadok a vykonávať na to nadväzujúce úkony. Príkaz smeruje k uloženiu taxatívne určených povinností, a to aby:

a) také údaje uchovali a udržiavali v celistvosti,
b) umožnili vyhotovenie a ponechanie si kópie takých údajov,
c) znemožnili prístup k takým údajom,
d) také údaje odstránili z počítačového systému,
e) také údaje vydali na účely trestného konania.[24]

Za najzásadnejší prienik do základných práv dotknutého subjektu sa považuje posledná povinnosť, t.j. vydania počítačových údajov. Pôvodným účelom príkazu bolo v zmysle článkov 16 až 18 Dohovoru urýchlené uchovanie uložených počítačových údajov, teda zabezpečenie elektronického dôkazného prostriedku pre budúce dokazovanie. V odbornej literatúre sa objavuje názor, že toto ustanovenie slúži aj na predĺženie plynutia šesť mesačnej lehoty podľa zákona o elektronických komunikáciách, počas ktorej podnik uchováva uvedené údaje s tým, že prokurátor môže týmto príkazom zabezpečiť, aby sa tieto legálne uchovávali aj dlhšie (jedným príkazom môže prokurátor prikázať uchovanie údajov až na 90 dní).[25] Avšak táto skutočnosť bola zmenená nedávnym rozhodnutím Ústavného súdu SR.[26]

Čo sa týka časového aspektu, v príkaze podľa § 90 odseku 1 písm. a) alebo písm. c) TP SR musí byť ustanovený čas, po ktorý bude uchovanie údajov povinnou osobou vykonávané. Avšak ide už o uchovanie uložených údajov. Tento čas môže byť až 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz. Táto špecifikácia bola doplnená až novelou č. 262/2011 Z.z. účinnou od 1. 9. 2011. Dovtedy platilo, že v akomkoľvek príkaze musí byť ustanovený presný čas, po ktorý bude

[24] Podobné povinnosti sú stanovené v článku 16 a 21 Dohovoru.

[25] Rampášek, M. Uchovanie a vydanie počítačových údajov v trestnom konaní. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 5 (2013), - s. 21-26.

[26] Ústavný súd SR, Tlačová informácia č. 25/2015. [online]. [cit. 2015-06-12]. Dostupné z: http://portal.concourt.sk/plugins/servlet/get/attachment/main/ts_data/Tl_info_25_15_el_komunikacie.pdf

uchovanie údajov vykonávané, čo vyvolávalo mnohé interpretačné pochybnosti.[27]

Avšak v súčasnosti je zrejmé, že pre potreby trestného konania edičná povinnosť uvedená pod písm. b) a e) predstavuje najpoužívanejší spôsob zadováženia elektronického dôkazného prostriedku v trestnom konaní bez ohľadu na povinný subjekt (ktorá má počítačové údaje v držbe resp. pod kontrolou). Túto skutočnosť demonštruje nasledujúca staršia štatistika Generálnej prokuratúry SR:[28]

	2010	**2011**	**2012**
§ 90 ods. 1 písm. a)	7	15	26
§ 90 ods. 1 písm. b)	25	57	103
§ 90 ods. 1 písm. c)	1	1	2
§ 90 ods. 1 písm. d)	0	4	7
§ 90 ods. 1 písm. e)	15	104	88
Spolu	**48**	**181**	**226**

3.5 PROCESNÉ PODMIENKY VYDANIA PRÍKAZU

Príkaz predstavuje rozhodnutie *sui generis*, voči ktorému nie je prípustný riadny opravný prostriedok. Avšak, ústavná sťažnosť za predpokladu splnenia určitých podmienok nie je vylúčená.[29] Príkaz musí byť písomný. Na rozdiel od veci, ktorú dotknutá osoba vydáva policajtovi, prokurátorovi alebo súdu, počítačové údaje je osoba, v ktorej držbe alebo pod ktorej

[27] Nález Ústavného súdu SR sp. zn. III. ÚS 68/2010 z 25. augusta 2010 [online]. [cit. 2015-06-12]. Dostupné z: http://www.pravnelisty.sk/rozhodnutia/a87-ustavny-sud-sr-o-prehliadke-advokatskej-kancelarie-a-zaisteniu-pocitacovych-udajov

[28] Novocký, J. Zaistenie majetku a vecí v trestnom konaní – aplikačné problémy, Justičná akadémia 2013. [cit. 2014-01-12]. Dostupné z: http://www.jasr.sk/files/Zaistenie_majetku_a_veci_v_trestnom_konani_aplikacne_problemy.pdf.

[29] Viď. Nález Ústavného súdu SR sp. zn. III. ÚS 68/2010 z 25. augusta 2010 [cit. 2014-01-12]. Dostupné z: http://www.pravnelisty.sk/rozhodnutia/a87-ustavny-sud-sr-o-prehliadke-advokatskej-kancelarie-a-zaisteniu-pocitacovych-udajov

kontrolou sa tieto nachádzajú povinná vydať tomu, kto vydal príkaz (predseda senátu alebo prokurátor) alebo osobe uvedenej v príkaze.[30]

Ďalej je potrebné uviesť, že použitie tohto príkazu nie je obmedzené špecifickým výpočtom trestných činov, pri ktorých je tento príkaz možné použiť (napr. ako to je pri odposluchu alebo pri inom informačno – technickom prostriedku). Ako už bolo uvedené, príkaz v prípravnom konaní nevyžaduje súhlas sudcu alebo senátu. Táto skutočnosť sa môže negatívne odraziť aj v tom, že súčasťou zaistených počítačových údajov môže byť napr. neotvorená alebo rozpísaná pošta v cloude (resp. uložená na diskovom poli servera), uložený textový rozhovor (chat), uložená streamovaná telefonická videokonferencia viacerých účastníkov atď. Je nutné poukázať na znenie Dohovoru v čl. 14 - Rozsah procesných ustanovení, ktoré sa snaží definovať hranice signatárov v prijímaní potrebných legislatívnych a iných opatrení. Dohovor nepriamo identifikuje trestné činy, voči ktorým sa rozsah procesných ustanovení uplatňuje. Totiž každá strana uplatní právomoci a postupy uvedené len na tieto trestné činy, iné trestné činy spáchané prostredníctvom počítačového systému alebo zhromažďovanie dôkazov o trestnom čine v elektronickej forme. V tomto prípade je nutné apelovať na to, aby slovenský zákonodarca v budúcnosti revidoval pôsobnosť tohto ustanovenia v zmysle Dohovoru a taktiež rozhodnutia Ústavného súdu SR ohľadom vydávania prevádzkových údajov od osôb podnikajúcich podľa ZEK.

3.6 UKONČENIE PRÍKAZU

Zákon ďalej pozná ukončenie tohto príkazu, a to pre prípad ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné. V tomto prípade vydá predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovania týchto údajov. Je potrebné dodať, že ide o vágnu formuláciu, ktorá navyše bude ťažko podliehať procesnej kontrole zo strany účastníkov alebo povinných. Tu je potrebné pripomenúť zásadu oficiality, kedy orgány činné v trestnom konaní vykonávajú úkony

[30] Hasíková, J. Počítačový údaj - zdroj dokazovania. Bulletin slovenskej advokácie. 1-2/2013. Bratislava. s. 29. Obdobne Minárik, Š. Trestný poriadok, stručný komentár. Druhé, prepracované a doplnené vydanie. Iura Edition, Bratislava. 2010. s. 315.

na základe svojej úradnej povinnosti. Čiže tie sú povinné sústavne skúmať dôvodnosť vydaného príkazu a v prípade potreby ho revidovať.

3.7 POVINNOSŤ MLČANLIVOSTI

Špeciálne je upravená povinnosť mlčanlivosti. Ako už bolo spomenuté, príkaz môže smerovať voči prevádzkovateľovi počítačového systému a nie voči pôvodcovi počítačových údajov. Preto popri tomto príkaze sa mu môže uložiť aj povinnosť zachovať v tajnosti opatrenia uvedené v príkaze. Tajnosť opatrenia smeruje k snahe zabrániť zmareniu zaistenia dôkazného prostriedku. Neuposlúchnutie príkazu je sankcionované poriadkovou pokutou v zmysle § 70 ods.1 TP SR.[31]

Pre doplnenie je možné uviesť, že povinnosť mlčanlivosti smeruje vždy do budúcnosti oproti zaisťovaniu minulých (zapísaných) údajov. Je obzvlášť potrebné si dať pozor na zle formulovaný príkaz (napr. „prikazujú sa uchovávať všetky v budúcnosti získané počítačové údaje a zachovávať o tom mlčanlivosť“). Tu môže dôjsť k tomu, že sa vykoná závažnejší zásah do práv vyšetrovaného bez procesnej kontroly súdu. Totiž takýto príkaz by *de facto* nahradil odpočúvanie (napr. streamované hovory, budúca prenášaná elektronická pošta atď.)

3.8 VÝKON PRÍKAZU

V prípade ak subjekt nevyhovie dobrovoľne príkazu, orgán činný v trestnom konaní postupuje podľa § 91 TP SR (čo je spoločný postup pre vydanie veci). Podľa tohto ustanovenia, ak vec dôležitú pre trestné konanie alebo počítačové údaje na vyzvanie nevydá ten, kto ju má pri sebe, môže mu byť na príkaz predsedu senátu a v prípravnom konaní na príkaz prokurátora alebo policajta odňatá. Policajt potrebuje na vydanie takého príkazu predchádzajúci súhlas prokurátora. Bez predchádzajúceho súhlasu ho môže vydať len vtedy, ak predchádzajúci súhlas nemožno dosiahnuť

[31] „Kto napriek predchádzajúcemu napomenutiu ruší konanie alebo kto sa voči súdu, prokurátorovi, alebo policajtovi správa urážlivo, alebo kto bez dostatočného ospravedlnenia neposlúchne príkaz, alebo nevyhovie výzve alebo predvolaniu podľa tohto zákona, toho môže sudca a v prípravnom konaní prokurátor alebo policajt potrestať poriadkovou pokutou do 1 650 eur; ak ide o právnickú osobu, až do 16 590 eur. Na možnosť uloženia poriadkovej pokuty musia byť dotknuté osoby vopred upozornené.“ § 70 ods.1 zákona č. 301/2005 Zb. Trestný poriadok In: Jednotný automatizovaný systém právnych informácií [online]. [cit. 2015-06-12]. Online. Dostupné z: http://jaspi.justice.gov.sk

a vec neznesie odklad. K odňatiu veci sa podľa možnosti priberie nezúčastnená osoba. Otázkou ostáva, čo predstavujú pojmy „pri sebe“ a „podľa možnosti“ vo svetle počítačových údajov? Taktiež je dôležité sledovať ako bude táto skutočnosť vyhodnotená súdom, resp. či bude mať vplyv na následnú zákonnosť dôkazu.[32] Problémom však ostáva, ako orgán činný v trestnom konaní vykoná príkaz na odňatie počítačových údajov, ktoré sú nelokalizovateľné alebo v sústavnom pohybe (napr. cloud, ktorého dáta sa fyzický môžu nachádzať na viacerých miestach – serverových farmách). Súdna prax o aktuálnych riešeniach týchto praktických otázok zatiaľ mlčí.

V prípade ak sa počítačové údaje nachádzajú na území SR, ich zaistenie bude predchádzať dobre zvolená kriminalistická taktika - určenie typu požadovaných údajov, určenie ich pôvodcu a najmä zistenie ich aktuálneho držiteľa. V prípade ak pôjde o údaje uložené na zahraničných serveroch (najčastejší prípad využívania služieb cloud storage akými sú DropBox, GoogleDrive, OneDrive atď.), je nutné využiť existujúci zmluvný rámec medzinárodnej spolupráce v trestných veciach a poznať *best practices v* oblasti vydávania údajov jednotlivých poskytovateľov týchto informačných služieb. Buď pôjde o vykonávanie jednotlivých úkonov právnej pomoci na základe medzinárodnej zmluvy alebo o realizáciu právnej pomoci bez zmluvného základu.[33]

---

[32] Päť kritérií zákonnosti dôkazu v trestnom konaní podľa Repíka. Viď. Repík, B. Procesní důsledky porušení předpisů o dokazování v trestním řízení. , Bulletin advokacie, 1982, s. 125-126; Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní, 2003, s. 408

[33] Príkladom môže byť spolupráca členských štátov EÚ, kde základom sú články 82 a 86 Zmluvy o fungovaní Európskej únie. Dňa 29. mája 2000 Rada ministrov EÚ schválila Dohovor o vzájomnej pomoci v trestných veciach, ktorého cieľom je podporovať spoluprácu medzi justičnými, policajnými a colnými orgánmi v rámci Únie doplňovaním ustanovení v existujúcich právnych nástrojoch z 20.4.1959. Taktiež významnú rolu zohráva aj budapeštiansky Dohovor o počítačovej kriminalite zo dňa 23.11.2001. V neposlednom rade ide o Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi EÚ, vypracovaný Radou v súlade s článkom 34 Zmluvy o EÚ. Justičná spolupráca v trestných veciach v rámci Európskej únie stojí na dvoch kľúčových princípoch: na uznávaní rozsudkov a súdnych rozhodnutí a taktiež na zbližovaní právnych predpisov členských štátov. Ide najmä o úpravu v prípade príkazu na zaistenie majetku a dôkazov v prípade zaisťovania elektronických dôkazov v pôsobnosti cudzieho prevádzkovateľa sociálnej siete. Vyjadrenie týchto princípov vo sfére dokazovania bolo zavŕšené v smernici Európskeho parlamentu a Rady č. 014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. Viď. Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. [online]. [cit. 2015-06-12]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014L0041&qid=1430677259904&from=EN

Je možné ešte spomenúť prípad riešený pred Ústavným súdom SR, kedy Protimonopolnému úradu SR vo veci „dawn raid“ bolo zakázané pokračovať ďalej v prehliadaní dátového nosiča vyšetrovaného subjektu Najvyšším súdom SR (bolo rozhodnuté o nezákonnom zásahu orgánu štátnej správy). Avšak tento skúmaný dátový nosič v zmysle ustanovenia § 89 TP SR Protimonopolný úrad následne vydal vtedajšiemu Úradu boja proti korupcii, ktorý až po jeho dôslednom prezretí vydal príkaz v zmysle § 90 TP SR na vydanie počítačových údajov. Takéto konanie vykazovalo znaky excesu orgánov činných v trestnom konaní. Napriek tomu Ústavný súd SR k námietke nezákonného dôkazu konštatoval, že „ v tomto kontexte neobstojí námietka sťažovateľov o tom, že orgán činný v trestnom konaní zadovážil dôkaz „ z otráveného stromu“. Protimonopolný úrad bol povinný na základe rozsudku Najvyššieho súdu sp. zn. 3 Sžz 1/2011 z 5. apríla 2011 a nepokračovať v prezeraní dátového nosiča, na druhej strane však týmto rozhodnutím nebola obmedzená jeho edičná povinnosť podľa § 89 TP SR a neboli ním limitované ani oprávnenia orgánov činných v trestnom konaní na postup podľa § 89 a § 90 TP SR.“[34] Aj keď ustanovenie je pokrokové a počíta s odňatím počítačových údajov, jeho faktická realizácia môže byť komplikovaná. Zdá sa, že pri odňatí je celá koncepcia prísne viazaná na dátový nosič – vec. Očakáva sa súdna interpretácia a stanovenie zákonných medzí tohto úkonu.

Zákon pre vykonanie procesných úkonov stanovuje náležitosti zápisnice. Zápisnica alebo potvrdenie o zaistení počítačového údaja často predstavuje ťažiskový dokument pre kontrolu legálnosti takéhoto zásahu. Zápisnica musí obsahovať dostatočne presný opis vydanej veci, odňatej veci, prevzatej veci (dátového nosiča) alebo počítačových údajov (napr. meno a špecifikáciu zaistených súborov, resp. partícií diskov), ktoré umožnia určiť ich totožnosť. Osobe, ktorá vec alebo počítačové údaje vydala alebo ktorej boli vec alebo počítačové údaje odňaté, alebo od ktorej boli vec alebo počítačové údaje prevzaté, vydá orgán, ktorý úkon vykonal, ihneď písomné potvrdenie o prevzatí veci alebo počítačových údajov alebo rovnopis zápisnice. Podstatné je ustanovenie ods.2 druhá veta § 93 TP SR, ktoré hovorí, že „osobu, ktorej počítačové údaje boli zaistené, o tom

[34] Viď. Uznesenie Ústavného súdu SR, spis. zn. III. ÚS 24/2012-53zo dňa 17.1.2012. [online]. [cit. 2015-06-12]. Dostupné z: http://www.concourt.sk/SearchRozhodnutiav01/rozhod.do?urlpage=dokument&id_spisu=422752

písomne vyrozumie orgán, ktorý počítačové údaje prevzal.“ Toto ustanovenie môže spôsobovať interpretačný problém, či ide o osobu, ktorá má v držbe tieto údaje alebo o osobu, ktorá je ich pôvodcom. Aj keď gramatickým výkladom sa dá vyvodiť záujem zákonodarcu chrániť procesné postavenie pôvodcu (zákonná záruka), súčasná prax orgánov činných v trestnom konaní ukazuje na to, že tie sú na akékoľvek informácie skúpe a tieto dotknuté osoby žiadnym spôsobom neinformujú v prípade, ak zaisťujú počítačové údaje v detencii tretích osôb.[35] Správny postup by mal byť ten, kedy orgán činný v trestnom konaní informuje pôvodcu údajov. Takáto informácia môže byť vykonaná ústne, elektronicky alebo písomne, avšak musí byť vierohodne zaznamená vo vyšetrovacom alebo súdnom spise.

4. ÚVAHA DE LEGA FERENDA

Aj keď súčasná judikatúra ESĽP nevyžaduje explicitnú zákonnú úpravu pre zaistenia počítačových údajov,[36] je v závere vhodné poukázať na niektoré pozitíva tohto inštitútu oproti všeobecnej edičnej povinnosti podľa § 89 TP SR (resp. § 78 TŘ ČR) alebo domovej prehliadke podľa § 99 TP SR (resp. § 82 TŘ CŘ).[37]

V prípade zaistenia počítačových údajov priamo z dátového nosiča – veci (napr. viaceré diskové polia, vysoko kapacitné úložiská), organ činný v trestnom konaní má zákonnú možnosť selektovať a citlivo vyberať tie

---

[35] Svedčí o tom prípad, kedy príkaz na uchovávanie počítačových údajov špeciálna prokuratúra adresovala samotnému vyšetrovateľovi policajného zboru: „ V súvislosti s vybavením podnetu prokurátor konštatoval, že je pravdou, že 18. mája 2011 protimonopolný úrad „zápisnične“ vydal inkriminovaný disk vyšetrovateľovi úradu boja proti korupcii, ale zároveň dodal, že pri postupe podľa § 89 ods. 1 Trestného poriadku nedochádza k vydaniu rozhodnutia. […] Okrem toho prokurátor konštatoval, že vzhľadom na to, že sa javilo, že na vydanom disku sa nachádzajú počítačové údaje a že tieto je potrebné uchovať, udržiavať v celosti, prípadne vyhotoviť a ponechať si orgánmi činnými v trestnom konaní kópie takých údajov, 27. mája 2011 vydal [prokurátor špeciálnej prokuratúry] v súlade s § 90 Trestného poriadku príkaz na uchovanie a vydanie počítačových údajov.“ Viď. Uznesenie Ústavného súdu SR, spis. zn. III. ÚS 24/2012-53zo dňa 17.1.2012. [online]. [cit. 2015-06-12]. Dostupné z: http://www.concourt.sk/SearchRozhodnutiav01/rozhod.do?urlpage=dokument&id_spisu=422752

[36] Vec Wieser a Bicos Beteiligungen GmbH proti Rakúsku. Rozhodnutie ESĽP zo dňa 16.10.2007, spis. zn. 74336/01 [online]. [cit. 2015-06-12]. Dostupné z: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-82711

[37] Výkladové stanovisko Najvyššieho štátneho zastupiteľstva por. č. 9/2001 Zb. tvrdí, že ako vec dôležitú pre trestné konanie je možné zaistiť aj výpočtovú techniku a záznamové médiá. Viď. §82 odst. 1 TŘ. Šámal, P. a kol.: Trestní řád. Komentář. 7. vydání. Praha : C. H. Beck, 2013, 4700 s. S. 1114.

údaje, ktoré sú pre trestné konanie naozaj dôležité. Je zrejmé, že odstavením celého počítačového systému môže dôjsť k závažným ekonomickým škodám na strane povinného alebo iných tretích osôb. Je pravda, že tento postup tu bolo možné dovodiť aj pred zakotvením tohto inštitútu. Avšak povinnosti akými sú uchovanie a udržiavanie v celistvosti, umožnenie vyhotovenia a ponechania si kópie údajov, znemožnenie prístupu k údajom alebo povinnosť odstránenia údajov z počítačového systému dávajú orgánom činným v trestnom konaní celú novú škálu nástrojov pre boj s počítačovou kriminalitou.

Ďalej to je otázka proporcionality zásahov. Ústavný súd SR v prípade prehliadky advokátskej kancelárie judikoval, že „záujem štátu na ochrane pred zločinnosťou zakladajúci legitímnosť zásahov do práva na súkromie pri realizácii niektorých inštitútov zaistenia osôb a vecí musí byť uvedený do rovnováhy so závažnosťou zásahu do tohto práva. Odkázal tak na princíp proporcionality.“ Podľa jeho názoru to znamená „zvoliť si pri realizácii zásahu čo najmiernejší prostriedok, ktorý je súčasne spôsobilý zabezpečiť dosiahnutie sledovaného cieľa. Je preto potrebné uprednostniť úkon uchovania a vydania počítačových údajov pred inštitútom vydania, resp. odňatia veci. V opačnom prípade znamená neproporcionálny postup konajúceho orgánu porušenie garancií práva na súkromie a spravodlivého procesu.“[38] Je možné zhrnúť, že pokiaľ existujú prostriedky, ktoré umožnia realizáciu citovaného cieľa a zároveň predstavujú menej radikálny zásah do chránených práv, je nevyhnutné použiť práve tieto prostriedky. Menej radikálny zásah do chránených práv je práve inštitút uchovania a vydania počítačových údajov oproti všeobecnej edičnej povinnosti podľa § 89 TP SR (resp. § 78 TŘ ČR). Umožňujú totiž voči tretím osobám uplatňovať miernejší prostriedok zásahu (vydanie konkrétnych počítačových údajov pred vydaním celistvého dátového nosiča, čo predstavuje krajné riešenie). Na druhú stranu je však nutné podotknúť, že praktická aplikácia princípu proporcionality v otázkach zaisťovania počítačových údajov je obzvlášť náročná v prípade osoby, ktorá je v postavení podozrivého (resp. obvineného alebo obžalovaného). Orgány činné v trestnom konaní v tomto prípade môžu čeliť obvyklému problému – rezistencii týchto osôb a musia postupovať pomocou efektívnejších zaisťovacích mechanizmov (domová

[38] Ibid. Nález Ústavného súdu SR sp. zn. III. ÚS 68/2010 z 25. augusta 2010

prehliadka, sledovanie osôb a vecí, atď.) v záujme naplnenia základného účelu trestného procesu.

V neposlednom rade je možné odporučiť, aby technická forma realizácie zaistenia počítačových údajov bola popísaná vo verejne dostupnom odporúčaní - smernici alebo vnútornom predpise policajného zboru. Každé zaistenie počítačových údajov by malo vychádzať z princípu zachovania proporcionálneho postupu, t.j. mal by byť zvolený taký postup orgánov činných v trestnom konaní, ktorý nepredstavuje väčší zásah do práv ako sú tie záujmy, ktoré sa týmto procesným postupom chránia. Taktiež by sa mala uplatňovať zásada nezmeniteľnosti otlačku počítačového údaja od jeho prvého zaistenia až po jeho vykonanie (resp. odovzdanie znalcovi). Práve táto skutočnosť by mala byť reflektovaná nielen v možnosti dotknutej osoby získať opis zápisnice alebo potvrdenia pri zaistení počítačového údaja s otlačkom (kópiou), ale aj v samotnej možnosti vyhotoviť si rovnocenný otlačok (kópiu) pre vlastnú potrebu toho, čo si odniesol orgán činný v trestnom konaní. Zaistené počítačové údaje sú súčasťou trestného spisu a osoba (najmä ak ide o osobu odlišnú od páchateľa) by mala mať postavenie zúčastnenej osoby, a teda právo do takéhoto spisu nazerať. V neposlednom rade je nevyhnutná transparentnosť v procese nakladania so zaistenými počítačovými údajmi a taktiež reálna možnosť procesnej kontroly nad spôsobom ich zaisťovania a nakladania s nimi.

5. ZÁVER

Zistenie skutkového stavu, o ktorom neexistujú dôvodné pochybnosti, a to v takom rozsahu, ktorý je nevyhnutný pre rozhodnutie, predstavuje vyjadrenie cieľu trestného práva procesného.[39] Voľba prostriedkov pre dosiahnutie tohto cieľu musí spĺňať základné požiadavky ústavnosti. Ak rekodifikačná komisia uvažuje o zavedení nového inštitútu zaistenia počítačových údajov s úmyslom zrýchliť a zjednodušiť procesné štádium zaisťovanie a vykonávania dôkazov, je možné poukázať na príklad slovenskej úpravy ako jeden z možných exemplárov. Aj keď niektoré otázky

[39] Zásada materiálnej pravdy. Viď. MS ČR: Komise pro nový trestní řád. Východiska a principy nového trestního řádu [online]. [cit. 2015-06-12]. Dostupné z: http://portal.justice.cz/Justice2/soubor.aspx?id=112883. s. 33.

slovenská súdna prax stále nevyriešila, definícia počítačových údajov sa zdá byť vhodná. Text zákona nemusí vždy za každú cenu dobiehať stav technológie (mnohé podstatné otázky sú aj tak vyriešené), ale spresnenie termínov a príkazov smerujúcich k počítačovým údajom, no najmä ich terminologické oddelenie od dátového nosiča, prispievajú lepšiemu pochopeniu procesu dokazovania. Práve jasná definícia procesných záruk dotknutej osoby pri zaisťovaní počítačových údajov predstavuje jednu z možných ciest pre budúci vývoj. Aj keď sa môže zdať, že záruky prvotne vyznievajú v prospech páchateľa, ich zakotvenie v procesnom poriadku nielenže stanoví limity špekulatívnej obhajoby, ale súčasne aj dodá sebaistotu orgánom činným v trestnom konaní vstupovať do situácií, ktoré sa predtým zdali byť nejasné.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

SMEJKAL, V. KYBERNETICKÁ KRIMINALITA

MIROSLAV UŘIČAŘ[*]

SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Nakladatelství Aleš Čeněk, 2015, 636 str. ISBN 978-80-7380-501-2.

Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. se kromě klasické právnické literatury stále více profiluje jako vydavatelství děl z oblasti kriminalistiky. Pod vedením jedné z nejuznávanějších osobností tohoto oboru, prof. JUDr. Ing. Viktora Porady, DrSc., zde vyšla díla jako Kriminalistika (teorie, metody, metodologie), Kriminalistika (výzkum, pokroky, perspektivy) nebo Kriminalistika - Kriminalistická taktika a metodiky vyšetřování, bez nichž by tento vědní obor nebyl dokonale popsán.

Obdobně významné dílo, tentokráte coby průnik trestního práva a kriminalistiky na straně jedné a informačních technologií na straně druhé nyní v nakladatelství vydal prof. Ing. Vladimír Smejkal, CSc., LL.M., jeden ze zakladatelů oboru IT právo a IT kriminalistika v České republice, dlouholetý vysokoškolský pedagog a soudní znalec.

Kniha poměrně velkého formátu (B5) o celkem 636 stránkách názorně ukazuje, co vše lze napsat o kriminalitě spojené s počítači a počítačovými sítěmi. Dnes, kdy se informační technologie nacházejí prakticky v každém předmětu nejen v zaměstnání, ale i v domácnostech, to ovšem není nikterak překvapivé. Nemluvě o tom, že bezpečnost IS/IT je dnes jedním z nejčastěji skloňovaných pojmů, a to nejen v souvislosti s útoky hackerů páchajících

[*] Mgr. Miroslav Uřičař je ředitelem úseku práva, regulace, vnějších vztahů a bezpečnosti společnosti T-Mobile Czech Republic a.s. a předsedou legislativní komise České asociace pro soutěžní právo. Je dále členem představenstva Asociace provozovatelů mobilních sítí, členem výkonné rady UNICEF ČR a působí jako rozhodce Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky.

trestnou činnost v kyberprostoru, zcela běžně se již hovoří o kyberútocích vedených teroristickými skupinami a dokonce státy.

Zejména v tomto shledávám vysokou prospěšnost a výborné načasování díla prof. Smejkala, neboť otázka kybernetické kriminality je dnes jednou ze stěžejních otázek pro celé lidstvo. Nemusí totiž nastat výpadek dodávek elektrické energie; stačí jen když kyberteroristé zaútočí na elektronická zařízení (a data v nich) pomocí systémů typu HERF (high energy radio frequency) a EMPT bomby (electromagnetic pulse transformer) a zničí elektronické obvody v nich.

Autor v díle shrnul výsledky svého dlouholetého působení (v předmluvě uvádí, že první článek na toto téma publikoval s doc. JUDr. Martinem Vlčkem, CSc. již v roce 1988) jak v oblasti trestněprávní a kriminalistické teorie, tak i vlastní obsáhlé praxe, kdy se podílel jako znalec na vyšetřování nejzávažnějších případů počítačové kriminality u nás.

O čem tedy pojednává dílo nazvané *Kybernetická kriminalita*? Měli jsme zde kriminalitu počítačovou a ve svém předchozím díle, *Právo informačních a telekomunikačních systémů* prof. Smejkal zavedl termín „informatická kriminalita“. Nutno říci, že termín „počítačová kriminalita“ odpovídá zahraničnímu „computer crime“ a dlouho se držel v čele používané terminologie. Dnes se stejně často používá označení „kybernetická kriminalita“, a to jako synonymum. Pravdou je, že Smejkalův pojem „informatická kriminalita“ se příliš neprosadil, neboť vytváří dojem, že se jedná spíše o kriminalitu informatiků, nežli spojenou s informačními systémy. Přesto zřejmě bude mít pravdu, když vnímá kriminalitu kybernetickou jako něco komplexnějšího, nežli počítačovou. Je tomu tak, že kyberprostor (autor s ním pracuje zpočátku jako s notorietou a definuje jej až na straně 93) klade větší důraz na nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů nebo chceme-li, počítačů a počítačových sítí.

Autor přistoupil ke zpracování tématu klasickým vědeckým způsobem – od obecného (definice počítačové kriminality, kyberprostoru, kyberterorismu apod.) ke zvláštnímu (zevrubný popis jednotlivých skutkových podstat včetně forem a způsobů páchání trestných činů a detailního rozboru jednotlivých částí jejich definic podle trestního zákoníku). Vždy pak následuje obsáhlá judikatura, přičemž autor na rozdíl

od obvyklého způsobu prezentace judikatury neuvádí pouze právní větu, ale vybral ve většině případů i relevantní části odůvodnění, resp. parafrázoval je coby popis případu, vysvětlující čtenáři, oč v dané věci šlo a jaká byla geneze v rámci rozhodování zúčastněných soudů všech stupňů. Užitečnost tohoto přístupu zvyšují i vlastní komentáře autora, které hodnotí, zobecňují nebo naopak rozporují soudní rozhodnutí, zejména v kontextu s jinými, obdobnými případy.

Ještě před tento výklad ale autor předřadil kapitolu první, která je jakýmsi vysvětlujícím a definičním textem terminologie z oblasti ICT. Vysvětlujícím, aby text mohli bez problémů zvládnout i ti právníci, kteří nemají příliš vřelý vztah k moderním informačním technologiím. A definičním proto, aby IT odborníci vnímali, jak se s daným pojmem pracuje prismatem právních a technických norem. Najdeme zde definice základních stavebních kamenů kyberprostoru, jako jsou počítače (HW, SW), data, informace a informační systémy, počítačové sítě, Internet a dálkový přístup. Proto nejsou čtenáři, jejichž světem není IT, ale spíše soudní síně, ponecháni na pospas nesrozumitelné terminologii.

Těžiště výkladu představuje 460 stran kapitoly druhé nazvané *Kriminalita v prostředí informačních systémů a na Internetu.* Najdeme zde takové činy jako např. sabotáže, teroristické útoky a obecné ohrožení, poškození obecně prospěšného zařízení či cizí věci, neoprávněné užívání ICT zařízení, podvody, poškození cizích práv, či vydírání. Značná pozornost je věnována trestné činnosti spočívající v získávání a šíření informací. Zde autor popisuje sociální sítě, zabývá se odpovědností za obsah, ústavními základy ochrany soukromí a osobních údajů a konkrétní ochranou obsahu v sítích elektronických komunikací a osobních údajů. V rámci jednotlivých skutkových podstat je uvedeno neoprávněné nakládání s osobními údaji, šíření pornografie a dětská pornografie, porušování tajemství dopravovaných zpráv a dokumentů uchovávaných v soukromí, ohrožení utajované informace, vyzvědačství, šíření poplašné zprávy, nebezpečné vyhrožování a pronásledování (stalking), manipulace s kurzem investičních nástrojů, nekalá soutěž) a další možné trestné činy související se šířením informací.

Následující část kapitoly je věnována nehmotným statkům a duševnímu vlastnictví – průmyslovým a autorským právům. Velmi podrobně jsou

popsány výslovně počítačové trestné činy, jak jsou definovány v ust. § 230 – *Neoprávněný přístup k počítačovému systému a nosiči informací*, § 231 – *Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a* § 232 – *Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.*

Závěr druhé kapitoly tvoří ostatní trestné činy související s počítači, kde autor uvádí neoprávněné opatření, padělání a pozměnění platebního prostředku, výrobu a držení padělatelského náčiní, padělání a pozměnění veřejné listiny, zkreslování údajů o stavu hospodaření a jmění, poškození finančních zájmů Evropské unie, vývoz zboží a technologií dvojího užití a zahraniční obchod s vojenským materiálem. Souhrnně by se dalo říci, že prof. Smejkal provedl analýzu všech trestných činů podle platného trestního zákoníku a zamýšlel se nad možným výskytem počítače jako souhrnu technického a programového vybavení včetně dat, případně většího množství počítačů propojených do počítačové sítě, a to jako předmětu nebo jako nástroje trestné činnosti. Činil tak tedy zjevně v souladu s definicí počítačové kriminality, nacházející se na str. 20 knihy.

Je nutno ocenit pozornost, kterou autor věnoval jednomu z nejvýznamnějších fenoménů dneška – kyberterorismu, který ovšem zcela správně vnímá šířeji, a to vzhledem k naplnění dalších skutkových podstat s tímto jednáním souvisejících, jako jsou poškození a ohrožení provozu obecně prospěšného zařízení a poškození cizí věci. Tuto problematiku pojal autor značně do hloubky – od darkingu a phreakingu přes hackery a crackery až po kyberteroristy. V knize je navíc stručně popsán i zákon o kybernetické bezpečnosti, který nabyl účinnost těsně před jejím vydáním.

Třetí kapitola *Odhalování a vyšetřování kybernetické kriminality* nás z oblasti trestního práva přesouvá do kriminalistiky a jejích metod. Zde se autor zabývá kriminalistickou metodikou a expertizou v oblasti počítačové kriminality, přičemž značnou pozornost věnuje důkazům, dokazování a digitálním stopám. Ještě zajímavější je ale část, v níž prof. Smejkal popisuje hlavní současné problémy při odhalování a dokazování kybernetické kriminality: jsou to podle něj problém jurisdikce, problém odhalování trestné činnosti, problém dokazování a problémy související s dalším možným vývojem kyberkriminality. Jsou zde také popsány jednotlivé fáze trestního řízení a jejich specifika v souvislosti

s kybernetickou kriminalitou: od prověřování před zahájením trestního stíhání, přes vyšetřování a dokazování v prostředí ICT. Tato kapitola obsahuje i informace o pachatelích kybernetické kriminality a jejich nejčastějších motivech.

Zatímco v předchozích kapitolách nejdeme některé myšlenky, které již autor publikoval dříve, byť v méně propracované formě, čtvrtá kapitola *Prognóza dalšího vývoje kybernetické kriminality* soustředila velké množství nových, originálních informací a úvah autora. Lze ji v zásadě rozdělit do několika tematických oblastí. Jako první zde najdeme další úvahy o možnostech postihu útoků DoS/DDoS v rámci českého právního řádu; je otázkou, zda neměly být součástí výkladu již dříve k ust. § 230, ale faktem je, že aplikace tohoto ustanovení není zcela jednoznačná a autor zde diskutuje možnost postihu napříč celým trestním zákoníkem. Recenzent se nicméně přiklání k tomu, že odpověď na otázku, zda takové jednání vůbec stíhat a pokud ano, pak zda se snažit aplikovat § 228, § 230 nebo některá jiná ustanovení – za určitých okolností např. o nekalé soutěži – se zatím ještě vyvíjí a nemá tedy finální podobu.

Druhá část kapitoly je věnována virtuálním světům a virtuální kriminalitě. Je třeba ocenit, že autor nesklouzl k často používanému, leč chybnému ztotožnění kyberprostor = virtuální svět, který definuje jako „počítačově implementovaná simulovaná prostředí, která se nacházejí v prostředí kyberprostoru“. Především je však třeba ocenit, že zde diskutuje různé aspekty virtuality, jako jsou virtuální vlastnictví a virtuální majetek a jejich interakce se světem reálným. Dochází zde k závěru, že objekty ve virtuálním světě jsou produkty, které se za určitých okolností mohou stát zbožím, majícím svou tržní a směnnou hodnotu (cenu). Proto poměrně logicky navazuje další podkapitola, zabývající se virtuálními měnami, a to zdaleka ne pouze nejznámějšími z nich, tj. bitcoiny. Nejzajímavější je to, co uvádí hned na počátku: „*Ve skutečnosti ale hodnota peněz je dána především důvěrou uživatelů v ně, přičemž současné měny jsou tzv. fiat měny, tj. peníze existují na základě rozhodnutí státu (právních předpisů) a žádný stát ani centrální banka dnes nebude peníze vyměňovat za zlato ani za žádné jiné aktivum, a to přes různá oficiální tvrzení, mnohdy surrealistického charakteru.*“. Logicky z toho vyplývá závěr, že mohou existovat soukromé peníze a že démonizace virtuálních měn, zejména pak tzv. kryptoměn, mezi které patří

i bitcoiny, není zcela na místě. A to přesto, že vzhledem k jejich vlastnostem lze předpokládat, že budou existovat pokusy, jak využít virtuální měny pro páchání nejrůznější trestné činnosti, jako např. praní špinavých peněz, daňové úniky včetně online sázek, financování terorismu, nákupy drog, možná i podvody a jiné. Autor dále krátce zmiňuje virtuální sex a popisuje vizi roku 2050, kdy se sexuální robot/robotka více či méně chová jako reálný partner/partnerka a kdy místo prostitutek budou sexuální služby poskytovat roboti – androidi pod kontrolou magistrátu. Další část je věnována virtuální a skutečné kriminalitě ve virtuálním světě, tedy klasické kriminalitě ve vztahu k virtuálnímu prostoru a naopak. Podle prof. Smejkala již můžeme hovořit o vzájemném prolínání reálného a virtuálního světa i v oblasti kriminality, resp. trestního postihu. V další části kapitoly jsou zmiňovány nové aspekty IT/IS, které se začínají promítat do reálného života, a tedy i do trestní oblasti. Patří sem 3D tisk, který, přes své nesporné přínosy, může usnadňovat porušování práv duševního vlastnictví, ale i jiné trestné činy, např. nedovolené ozbrojování. V rámci dalšího předpokládaného vývoje kybernetické kriminality uvádí autor také další možné formy jednání: útoky na technologické řídicí systémy (SCADA a ICS), útoky prostřednictvím sociálních sítí a vysoká rizika spojená s tzv. Internetem věcí a BYOD (Bring Your Own Device) neboli používání vlastních zařízení ve firemním prostředí. Poněkud nesystematicky je sem zařazena i část věnovaná odpovědnosti za škodu způsobenou provozem nezabezpečeného informačního systému; je však otázkou, kam jinam toto téma, které rovněž souvisí s trestnou činností, zařadit.

Závěrečná část čtvrté kapitoly je věnována opět vysoce aktuálnímu tématu, kterým je střet mezi anonymitou a ochranou soukromí na Internetu. Zde autor diskutuje otázku prolamování ochrany soukromí, odposlechy a monitorování služeb elektronických komunikací a lokalizačních údajů jako součást boje proti trestné činnosti, samozřejmě nikoliv toliko kybernetické. Popisuje snahy států o prolamování ústavních práv občanů spočívající v povinnosti poskytnout státním orgánům svá vlastní hesla či šifrovací klíče, což podle autora představuje porušení zákazu sebeobviňování, resp. zákazu donucování k poskytnutí důkazů proti sobě samému. Uvádí, že nejvíce byla tato ochrana prolomena překvapivě ve Spojeném království Velké Británie a Severního Irska, kde podle zákona

RIPA (Regulation of Investigatory Powers Act) je možné vynutit vydání kryptografických klíčů nebo zpřístupnění požadovaných materiálů. Poněkud překvapivé, uvědomíme-li si, že jde o zemi, která byla jednou z prvních, jež ve svém právním řádu nastavila ochranu jednotlivce (Magna charta libertatum v roce 1215). Přitom podle Evropského soudu pro lidská práva patří právo nevypovídat a právo nepřispívat k obvinění proti sobě samému k obecně uznávaným mezinárodním principům.

V závěru svého obsáhlého díla prof. Smejkal zmiňuje další technologické novinky, které se mohou dostat do rozporu s ochranou soukromí nebo dalšími zájmy chráněnými podle trestního zákoníku. Uvádí zde „chytré šaty“ a šperky, monitorující životní pochody nositelů, létající roboty – drony, mikrominiaturní roboty (velikosti až mikroorganismů) a zdůrazňuje, že čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití musíme, bohužel, počítat.

Kniha *Kybernetická kriminalita* je zpracována na vysoké odborné úrovni, současně však velice přehledně a srozumitelně. Je obdivuhodnou syntézou oborů práva, kriminalistiky a informačních technologií a lze ji tedy doporučit čtenářům působícím ve všech těchto oblastech. Zcela samozřejmě by se měla stát základním zdrojem informací právníků všeho druhu – podnikových právníků nejen v IT firmách, advokátů, zaměstnanců orgánů veřejné moci, ale i osob působících v orgánech činných v trestním řízení, jako jsou policisté, státní zástupci, soudci. Nepostradatelnou bude i pro manažery IS/IT, specialisty na bezpečnost – od správců po auditory. Vysoce užitečná je pro výuku na všech typech vysokých škol, od právnických až po manažerské a informatické.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

ROZHODNUTÍ RYANAIR A OCHRANA DATABÁZÍ

JAKUB HARAŠTA

Soud:	Soudní dvůr Evropské unie
Věc:	C-30/14
Datum:	15. 1. 2015
Dostupnost:	curia.europa.eu

1. SHRNUTÍ SKUTKOVÉHO STAVU

PR Aviation nabízí vyhledávání nízkonákladových letů různých leteckých společností, včetně možnosti porovnávání cen a rezervace. Jednou z leteckých společností, jejichž letenky je možno skrze PR Aviation vyhledávat a rezervovat, je i společnost Ryanair Ltd. Ta ale vyžaduje při přístupu na svoje stránky souhlas s obchodními podmínkami, které mimo jiné výslovně stanoví, že právo distribuce letenek náleží výhradně společnosti Ryanair. Screen scraping, který za účelem nabízení letenek (tedy za obchodními účely) PR Aviation prováděla, tak není umožněn, protože jím dochází k nabízení letenek subjektem odlišným od Ryanair. A jelikož PR Aviation neuzavřela dohodu s Ryanair o přístupu k této databázi a letenky nabízela, mělo dojít k porušení obchodních podmínek.

2. ŘÍZENÍ PŘED NÁRODNÍM SOUDEM

Nizozemský Gerechtshof te Amsterdam původně rozhodl ve propěch PR Aviation, když uzavřel, že společnost neporušila právní ochranu databáze, protože její jednání odpovídalo běžnému užívání stránek Ryanair a aplikovaly se tak výjimky ze sui generis ochrany databáze. Ryanair podalo proti tomuto rozhodnutí kasační stížnost k Hoge Raad der Nederlanden.

3. PŘEDBĚŽNÁ OTÁZKA

Hoge Raad der Nederlanden dospěl k závěru, že pro účely ochrany autorským právem nelze uplatnit jiné kritérium, než je kritérium originality. Ze spisu i z rozhodnutí nižšího stupně přitom vyplývalo, že soubor údajů, který společnost Ryanair zpřístupňovala na svých stránkách, skutečně toto kritérium nesplňoval. V této chvíli tak došlo k přerušení řízení a soud předložil SDEU předběžnou otázku na výklad směrnice 96/9/ES ve znění:

„Rozšiřuje se účinek i na online databáze, které nejsou chráněny na základě kapitoly II směrnice autorským právem, ani na základě kapitoly III zvláštním právem, a to v tom smyslu, že ani v tomto ohledu nemůže být smluvně omezena svoboda užívat takové databáze při (obdobném nebo neobdobném) použití čl. 6 odst. 1 a článku 8 ve spojení s článkem 15?“[1]

4. ÚVAHY SOUDU

Samotná podstata předběžné otázky tak vycházela z předpokladu, že soubor údajů, kterého se spor v řízení před národními soudy přímo týkal, představuje databázi ve smyslu čl. 1 odst. 2 směrnice 96/9/ES, ale tento soubor není chráněn autorským právem ani zvláštním právem. Tuto premisu SDEU žádným způsobem nezpochybnil a konstatoval, že ověření její pravdivosti náleží národnímu soudu.

SDEU dále konstatoval, v souladu s argumentací předloženou PR Aviation, že definice databáze je skutečně obsažená v čl. 1 odst. 2 směrnice a k tomuto pojmu je nutno přistupovat široce, bez ohledu na formální, technické nebo materiální aspekty.[2] Zároveň ale doplnil, že tato definice je, jak text ustanovení napovídá, „[p]ro účely této směrnice.“[3] Samotné splnění definice uvedené v čl. 1 odst. 2 tak neumožňuje vztáhnout soubor údajů pod rozsah směrnice. V případě nenaplnění dalších podmínek stanovených

[1] Žádost o rozhodnutí o předběžné otázce podaná Hoge Raad der Nederlanden (Nizozemsko) dne 22. ledna 2014 – Ryanair Ltd v. PR Aviation BV. In: *EUR-Lex* [online]. Úřad pro publikace [cit. 7. 3. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=OJ:JOC_2014_135_R_0020. Zde si dovolím podotknout, že totožný anglický text obsažený v rozhodnutí v bodě 27 a obsažený v žádosti o rozhodnutí o předběžné otázce je do češtiny přeložen jinak.

[2] Rozhodnutí Soudního dvora Evropské unie ze dne 15. ledna 2015 ve věci C-30/14. In: *EUR-Lex* [online]. Úřad pro publikace [cit. 7. 3. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0030. Bod 33.

[3] Tamtéž.

v čl. 3 odst. 1 nebo v čl. 7 odst. 1 směrnice na takový soubor údajů skutečně nedopadá.[4] Celou tuto analýzu SDEU opřel o obecnou strukturu směrnice.[5]

5. ZÁVĚR SOUDU

Soud tak celé rozhodnutí uzavřel tak, že v případě databáze, na kterou se nevztahuje směrnice 96/9/ES, není možné domáhat se výjimek směrnicí harmonizovaných.[6] Pokud tedy databáze není chráněna právem autorským (po splnění podmínek stanovených v čl. 3 odst. 1 směrnice)[7] ani zvláštním právem (po splnění podmínek stanovených v čl. 7 odst. 1 směrnice),[8] nelze na ni vztáhnout směrnici tak, aby čl. 6 odst. 1 a čl. 8[9] představoval překážku tomu, aby autor databáze smluvně omezil její používání. Za běžné situace, kdy pořizovateli databáze svědčí autorskoprávní nebo sui generis ochrana, je smluvní dispozice s touto databází přímo omezena výjimkami z těchto ochranných režimů. Jak ale uzavřel SDEU, pokud nesvědčí pořizovateli ani jeden z ochranných režimů, není možné omezovat jeho smluvní svobodu.[10]

6. DOPADY PRO PRAXI

SDEU vyložil systematiku směrnice tak, že databáze nemusí splňovat pouze pojmové znaky vymezení v čl. 1 odst. 2, ale musí kumulativně naplnit pomové znaky obsažené v čl. 1 odst. 2 a čl. 3 odst. 1 (za účelem dosažení autorskoprávní ochrany) nebo kumulativně naplnit pojmové znaky obsažené v čl. 1 odst. 2 a čl. 7 odst. 1 (za účelem dosažení ochrany právy souvisejícími). Samotné naplnění čl. 1 odst. 2 totiž ke konstatování existence ochranného režimu autorskoprávního nebo sui generis nepostačuje.

Argumentaci, která vedla k tomuto závěru, nelze než označit za mistrný litigační tah. Závěr, ke kterému SDEU v anotovaném rozhodnutí dospěl, lze

[4] Tamtéž, bod 35.
[5] Tamtéž, bod 40.
[6] Tamtéž, bod 44.
[7] V ČR § 2 odst. 2 zákona č. 121/2000 Sb., autorského zákona.
[8] V ČR § 88a odst. 1 zákona č. 121/2000 Sb., autorského zákona.
[9] Kogentnost obou těchto ustanovení je zakotvena v čl. 15 směrnice.
[10] Nepřímo z tohoto rozhodnutí také plyne, že výjimky z ochranných režimů není možné vyloučit smluvně.

z právního hlediska jen stěží označit za překvapivý, ale může mít některé poměrně překvapivé následky. Dostáváme se totiž do situace, kdy je pro držitele práv výhodnější argumentovat neexistencí ochranného režimu. SDEU v tomto rozhodnutí nepřímo potvrdil, že autorskoprávní ochrana respektuje povahu informace a jakýkoli restriktivní režim je vyvažován dohodnutou výjimkou.[11] Pokud ochranný režim s jeho dohodnutými limity chybí, nastupuje smluvní právo, které tyto výjimky dohodnuté nemá, resp. možnost využít předmět smlouvy způsobem odpovídajícím těmto výjimkám musí být ve smlouvě přímo zakotvena. Celý problém se tak přenáší z roviny existence výjimek z ochranného režimu do roviny existence smluvních podmínek, resp. jejich způsobilosti založit smluvní vztah.

Jak podotýká IPKat, resp. Eleonora Rosati,[12] důvodem může být snaha poskytovat konzistentní kvalitu služeb, ale i snaha zvýšit obrat z reklam zobrazovaných na stránkách, kde se databáze nachází, nebo skrze které je možné k ní přistupovat. Oba důvody jsou, z mého úhlu pohledu, naprosto legitimní. Tento výklad nicméně může v budoucnosti podstatným způsobem změnit některé služby fungující na podobném principu jako fungovala služba poskytovaná PR Aviation.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

[11] Za tuto myšlenku děkuji Matěji Myškovi. Srov. BLOMQUIST, Jørgen. *Primer on International Copyright and Related Rights*. Cheltenham: Edward Elgar, 2014, s. 157. Podpůrně recitál č. 31 směrnice 2001/29/ES.

[12] CJEU says that owner of an online database not protected by copyright or sui generis right may restrist its use by contract. *The IPKat* [online]. [cit. 7. 3. 2015]. Dostupné z: http://ipkitten.blogspot.cz/2015/01/breaking-cjeu-says-that-owner-of-online.html.

JURISDIKCE PŘI ZÁSAHU DO AUTORSKÝCH PRÁV

PAVEL LOUTOCKÝ

Soud:	Soudní dvůr Evropské unie
Věc:	C-441/13
Datum:	22. 1. 2015
Dostupnost:	curia.europa.eu

1. SHRNUTÍ SKUTKOVÉHO STAVU

Pez Hejduk je profesionální fotografkou, která se specializuje na fotografování architektonických děl. Autorka se zaměřuje zejména na fotografování staveb rakouského architekta Georga W. Reinberga. Tento architekt v rámci kolokvia pořádaného německou společností EnergieAgentur použil fotografie Pez Hejduk pro účely ilustrace svých staveb, a to s jejím výslovným souhlasem. Společnost EnergieAgentur poté ale bez souhlasu paní Hejduk a uvedení toho, komu náleží autorská práva, zpřístupnila uvedené fotografie k prohlížení a ke stažení na svých internetových stránkách (provozovaných na německé ccTLD doméně .de). Pez Hejduk měla za to, že společnost EnergieAgentur porušila její autorská práva a podala k rakouskému Handelsgericht Wien žalobu na náhradu škody, jakož i k povolení uveřejnit rozsudek na náklady uvedené společnosti.

2. ŘÍZENÍ PŘED NÁRODNÍM SOUDEM

Předkládající soud uvedl, že pro odůvodnění výběru uvedeného soudu se paní Hejduk dovolává článku 5 bod 3 nařízení č. 44/2001 (známého jako

nařízení Brusel I.).[1] Společnost EnergieAgentur vznesla námitku mezinárodní a územní nepříslušnosti rakouského Handelsgericht Wien, když tvrdila, že její internetové stránky nejsou primárně určené pro Rakousko a že pouhá možnost zobrazit je v členském státě nepostačuje ke vzniku místní příslušnosti rakouského soudu.

3. PŘEDBĚŽNÁ OTÁZKA

Za těchto podmínek se Handelsgericht Wien rozhodl přerušit řízení a položit Soudnímu dvoru tuto předběžnou otázku:

„Je třeba čl. 5 bod 3 nařízení [č. 44/2001] vykládat v tom smyslu, že v právním sporu o porušení práv souvisejících s autorským právem, které bylo způsobeno tím, že byla na internetových stránkách zpřístupněna fotografie, přičemž internetové stránky jsou provozovány v doméně nejvyšší úrovně jiného členského státu, než je stát, ve kterém má majitel práv bydliště, jsou příslušné pouze soudy

1. *členského státu, ve kterém má údajný porušitel sídlo, jakož i*
2. *členského státu nebo členských států, na které jsou internetové stránky vzhledem ke svému obsahu zaměřeny?“*[2]

4. ÚVAHY SOUDU

Nejprve bylo nutno, aby soud identifikoval, jaký vztah má pravidlo příslušnosti dle článku 5 bod 3 nařízení Brusel I. ke konkrétnímu sporu. Již v minulosti bylo rozhodnuto, že místo, kde došlo ke škodné události, se vztahuje k místu, kde došlo k újmě, a zároveň k místu příčinné události, v níž má tato škoda původ, takže žalovaný může být podle volby žalobce žalován u soudu jednoho nebo druhého místa. Pravidlo příslušnosti se tedy

---

[1] *„Osoba, která má bydliště na území některého členského státu, může být v jiném členském státě žalována, (3) ve věcech týkajících se protiprávního jednání či jednání, které je postaveno na roveň protiprávnímu jednání, u soudu místa, kde došlo nebo může dojít ke škodné události […].*“Článek 5 bod 3. Nařízení Rady (ES) č. 44/2001 ze dne 22. prosince 2000 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech. In: *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 13. 4. 2015]. Dostupné z: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:CS:HTML

[2] Žádost o rozhodnutí o předběžné otázce podaná Handelsgericht Wien (Rakousko) dne 5. srpna 2013 – Pez Hejduk v. EnergieAgentur.NRW GmbH (Věc C-441/13). In: *EUR-Lex* [online]. Úřad pro publikace [cit. 13. 4. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1428921362388&uri=CELEX:62013CN0441

zakládá na existenci zvláště úzké vazby mezi sporem a soudem místa, kde došlo nebo může dojít ke škodné události. Příslušným soudem tak musí být soud, který má objektivně nejlepší předpoklady pro posouzení, zda jsou skutečnosti zakládající odpovědnost žalované osoby splněny.[3] Je třeba připomenout, že přestože je třeba autorská práva chránit zejména na základě směrnice 2001/29 automaticky ve všech členských státech, podléhají zásadě teritoriality. Uvedená práva tedy mohou být porušena v každém členském státě podle použitelných hmotněprávních předpisů (viz rozsudek Pinckney[4]). Nejprve bylo třeba zkoumat příčinnou souvislost a její vznik. Za ni je třeba považovat spuštění technického postupu vedoucího ke zveřejnění fotografií na dané internetové stránce. Skutečnost vedoucí k případnému porušení autorských práv tedy spočívá v jednání majitele uvedené internetové stránky.[5] Lze tedy nepopiratelně říci, že na základě výše řečeného je příslušným soudem soud nacházející se v Německu. Bylo tedy posléze nutno zkoumat, zda může být soud příslušný i na základě místa, kde se tvrzená škoda projevila.[6] Soudní dvůr již v minulosti uvedl (rozsudek Pickney), že *„nejen že se místo, kde se projevila škoda ve smyslu uvedeného ustanovení, může lišit v závislosti na povaze práva, které bylo údajně porušeno, ale i riziko, že se škoda projeví v určitém členském státě, existuje za podmínky, že právo, které bylo údajně porušeno, je v tomto členském státě chráněno.“*[7] Z důvodu zveřejnění fotografií Pez Hejduk na internetových stránkách společnosti EnergieAgentur došlo k porušení jejích autorských práv. Upozorňujeme, že společnost EnergieAgentur během celého řízení zdůrazňovala, že její internetové stránky, na kterých byly sporné fotografie zveřejněny, jsou provozovány v německé doméně nejvyšší úrovně a taková doména není určena pro Rakousko. V důsledku toho tvrzení žalované se škoda v Rakousku nemohla projevit. Takové prohlášení je ale zcela v rozporu s předešlou rozhodovací praxí Soudního dvora, kdy rozhodnutí

[3] Rozhodnutí Soudního dvora Evropské unie ze dne 22. ledna 2015 ve věci C-441/13. In: *EUR-Lex* [online]. Úřad pro publikace [cit. 13. 4. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62013CJ0441. Bod 16-21.

[4] Rozhodnutí Soudního dvora Evropské unie ze dne 3. října 2013 ve věci C-170/12. In: *EUR-Lex* [online]. Úřad pro publikace [cit. 13. 4. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0170

[5] Rozhodnutí Soudního dvora Evropské unie ze dne 22. ledna 2015 ve věci C-441/13. In: *EUR-Lex* [online]. Úřad pro publikace [cit. 13. 4. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62013CJ0441. Bod 24.

[6] Tamtéž, bod 27.

[7] Tamtéž, bod 29.

Pickney mimo jiné zdůrazňuje, že článek 5 bod 3 nařízení Brusel I. nevyžaduje, aby byly dotčené internetové stránky „zaměřeny" na členský stát sídla soudu, jemuž byl předložen spor.[8] Není tedy důležité, že internetové stránky nejsou směřovány na členský stát, kde má sídlo soud, jemuž byl předložen spor – je podstatné, že možnost projevení škody je dána tím, že na stránkách společnosti EnergieAgentur jsou dostupné fotografie, s nimiž se pojí práva, kterých se dovolává Pez Hejduk. Je však třeba upozornit na to, že pokud se žaloba „*vztahuje pouze na území daného členského státu, je soud, kterému byla žaloba předložena na základě místa, kde se projevila tvrzená škoda, příslušný pouze k rozhodnutí o škodě způsobené na území uvedeného členského státu*".[9] Soudy jiných členských států jsou s ohledem na zásadu teritoriality příslušné k rozhodování daného sporu na území svého členského státu, neboť se očekává, že takové soudy budou mít nejlepší předpoklady k tomu, aby posoudily porušení daných práv a aby určily povahu způsobené škody.

5. ZÁVĚR SOUDU

Soud na závěr tedy konstatoval, že článek 5 bod 3 nařízení Brusel I. musí být vykládán v tom smyslu, že v případě tvrzeného porušení práv souvisejících s autorským právem zaručených členským státem, v němž má sídlo soud, k němuž byla podána žaloba, je tento soud na základě místa, kde se škoda projevila, příslušný k projednání žaloby na určení odpovědnosti za škodu způsobenou na uvedených právech zveřejněním chráněných fotografií na internetových stánkách přístupných v obvodu jeho příslušnosti. Tento soud je příslušný pouze k rozhodnutí o škodě způsobené na území členského státu, kde má sídlo.

6. DOPADY PRO PRAXI

Soudní dvůr v tomto rozhodnutí vlastně konstatoval, že žalovat porušení autorských práv (a práv s nimi souvisejících) lze prakticky kdekoli. Soudní dvůr argumentoval tím, že internetová stránka je dostupná odkudkoli (*internet je všude*). Jediným omezením je pak vyčíslení škody, o kterém rozhoduje vždy místně příslušný soud pro území konkrétního členského

[8] Tamtéž, bod 32.
[9] Tamtéž, bod 39.

státu, kde je náhrada škody požadována. Dopady rozhodnutí mohou být dalekosáhlé v tom smyslu, že poté, co bude daný spor úspěšně žalován v příslušném státě, lze požadovat náhradu škody ve všech ostatních členských státech (obrátit se na soud příslušný rozhodovat o škodě na území tohoto státu). Negativní efekt se projeví zejména ve státech, které nahrazují skutečně vzniklou škodu fikcí (paušálem), kdy žalobce v takových státech na základě původního rozhodnutí obdrží paušalizovanou náhradu škody. Pro eliminaci takového jevu se nabízí řešení v podobě upuštění od paušalizované náhrady škody a nutnosti požadovat po žalobci prokázání skutečné škody v příslušném členském státě.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

KAUZA RYNEŠ

JAKUB MÍŠEK

Soud:	Soudní dvůr Evropské unie
Věc:	C-212/13
Datum:	11. 12. 2014
Dostupnost:	curia.europa.eu

Soud:	Nejvyšší správní soud
Věc:	1 As 113/2012
Datum:	25. 2. 2015
Dostupnost:	www.nssoud.cz

František Ryneš roku 2007 po sérii vandalských útoků a výhrůžek spáchané neznámými pachateli nainstaloval na svůj rodinný dům kameru, která snímala jak jeho pozemek, tak veřejně přístupné ulice před ním, včetně vchodu do protějšího bytového domu. Kamera byla napevno zabudovaná bez možnosti otáčení a umožňovala jen obrazový záznam, který se ukládal formou nekonečné smyčky na pevný disk ke kameře připojený. Jakmile byla kapacita disku zaplněna, záznam se opětovně přemazával novým záznamem. K systému nebyl připojen monitor, takže nebylo možné sledovat v reálném čase dění na ulici a jediný, kdo měl k datům přístup, byl sám František Ryneš.

Při jednom z dalších útoků kamera zachytila dva útočníky a Ryneš podal trestní oznámení, použiv při tom videozáznam pořízený kamerou. Jeden ze dvou podezřelých, kteří byli na základě záznamu identifikování,

dal Policii ČR podnět k prověření provozu kamerového systému a Policie celý případ postoupila Úřadu pro ochranu osobních údajů (dále „UOOU"). UOOU konstatoval, že užíváním kamery docházelo ke zpracování osobních údajů a uložil Františku Rynešovi pokutu za provinění se vůči třem povinnostem, které má správce dle zákona č. 101/2000 Sb., o ochraně osobních údajů (ZOOU), a to zpracování osobních údajů bez řádného zákonného důvodu, neinformování subjektů údajů o probíhajícím zpracování a nesplnění registrační povinnosti u UOOU. Pokuta byla potvrzena i v rozkladovém řízení předsedou UOOU.

Následná správní žaloba byla Městským soudem zamítnuta ve všech bodech. Soud se ztotožnil s názorem UOOU a rozhodl, že se v daném případě opravdu jedná o zpracování osobních údajů podléhající režimu ZOOU. Soud zamítl možnost, že by se jednalo o zpracování osobních údajů výlučně pro osobní potřebu dle § 3 odst. 3 ZOOU a tudíž by leželo mimo působnost zákona. Stejně tak dle městského soudu nebylo možné aplikovat legitimizační důvod pro zpracování osobních údajů, který by umožnil údaje zpracovávat bez souhlasu subjektů údajů, jímž dle Rynešova názoru mělo být zpracování osobních údajů pro ochranu jeho práv a právem chráněných zájmů – tedy ochrana zdraví a majetku. Důvodem k tomuto rozhodnutí byl fakt, že nastavením kamery mířící na veřejně přístupnou komunikaci a na vchodové dveře protějšího domu docházelo k zásahu do soukromí třetích osob. V této části rozhodnutí František Ryneš viděl chybně aplikovaný test proporcionality, což se překvapivě odráží i v textu rozsudku Městského soudu, kde stojí *„[m]rzí nás to, ale žalobu musíme zamítnout. Soud přisvědčuje žalobci, že jeho počínání je logické a odůvodněné a chápe celou situaci, ale je třeba postupovat dle zákona.*" Po svém neúspěchu u městského soudu podal Ryneš kasační stížnost k Nejvyššímu správnímu soudu (NSS).

Vzhledem k tomu, že jádrem problému případu je interpretace ustanovené ZOOU, potažmo evropské směrnice 95/46/ES, jíž je zákon implementací, obrátil se NSS formou předběžné otázky na Soudní dvůr Evropské unie (SDEU) s dotazem, zda lze výše popsané jednání považovat za zpracování osobních údajů výlučně pro osobní účely a zda je tudíž vyňato z režimu ZOOU.

SDEU rozhodl 11. prosince 2014 nedlouhým rozsudkem, v němž stanovil, že se v daném případě o zpracování prováděné výlučně pro výkon osobních a domácích činností nejedná. Rozsudek ve své argumentaci navazuje na předchozí rozhodnutí Google Spain, IPI a Digital Rights Ireland, když tvrdí že základním principem směrnice 95/46/ES je zajištění vysoké úrovně ochrany soukromí jak ve veřejné, tak v soukromé sféře, a že výjimky z této ochrany mohou být činěný pouze v mezích toho, co je naprosto nezbytné pro dosažení účelu kolidujícího práva, jež v daném případě převážilo. Komentované rozhodnutí tak plně navazuje na sérii dřívějších judikátů. Doktrína úzké výjimky z ochrany soukromí je navíc v tomto případě, jak soud připomíná, podpořena rovněž textem Směrnice, když je specifikování, že mimo její věcnou působnost spadají toliko zpracování, která jsou prováděna výlučně pro výkon osobních a domácích činností. Jak SDEU uvádí v bodu 33 rozsudku:

> *„Jestliže takový kamerový systém, jako je systém dotčený ve věci v původním řízení, zabírá – třebaže částečně – veřejné prostranství, a je tudíž zaměřen mimo soukromou sféru osoby, která jeho prostřednictvím zpracovává údaje, nelze jeho provozování považovat za výlučně „osobní či domácí" činnost ve smyslu čl. 3 odst. 2 druhé odrážky směrnice 95/46."*

Užívání kamery, jak bylo prováděno v popsaném případě, je zpracováním osobních údajů, ustanovení Směrnice 95/46/ES na něj dopadají, a jeho provozovatel je správcem údajů se všemi povinnostmi z tohoto statusu vyplývajícími. Důvodem je právě uvedené zaměření zpracování údajů mimo soukromou sféru správce, které se projevuje snímáním veřejného prostoru. Pomocný argument UOOU, že zaměření mimo soukromou sféru můžeme v daném případě vidět i na subjektivní úrovni, jelikož původní úmysl správce byl poskytnout nahrané údaje orgánům činným v trestním řízení, je pochopitelný, leč dle SDEU není relevantní. Soud totiž dále pokračuje ve své linii striktně objektivního přístupu k osobním údajům.[1] V bodu 22 rozsudku SDEU tvrdí: „*Obraz osoby zaznamenaný prostřednictvím kamery tudíž představuje osobní údajů, …, neboť umožňuje identifikovat subjekt údajů.*" V kombinaci s výše zmíněným bodem

[1] Srovnej bod 71 zde rozebíraného rozsudku NSS.

33 tak soud vlastně tvrdí, že zcela nezáleží na úmyslech nahrávající osoby a budoucích způsobech použití zaznamenaného materiálu, ale jakmile je na video záznamu identifikovatelný člověk jedná se o zpracování osobních údajů v režimu Směrnice 95/46/ES.

Můžeme bez obav říci, že SDEU tímto rozsudkem potvrdil tendenci, v jeho rozhodování dlouhodobě sledovatelnou, jíž staví ochranu soukromí a osobních údajů mezi ty nejvýrazněji chráněná práva. Svým rozhodnutí zúžil možnost, že by se na užití CCTV kamer, byť pro soukromé použití, vůbec nevztahoval režim Směrnice 95/46/ES. Zároveň však SDEU v 35 bodu rozhodnutí připomíná, že při aplikaci Směrnice je možné zohlednit konkrétní situaci. Pro vyvážení právních povinností konkrétního správce nacházejícího se v konkrétní, pro omezení tvrdosti zákona a nadbytečného formalismu, mají být užity instituty ve směrnici obsažené. Soud jinými slovy říká: *„Je nezbytné chránit soukromí, což se děje důslednou aplikací Směrnice. Drazí domácí operátoři CCTV kamer, nedám vám bianko šek, který vás zbaví všech povinností z ochrany osobních údajů vyplývající. Směrnice však obsahuje postupy, jak vaši administrativní zátěž snížit na nezbytně nutnou míru.*“ Těmito instituty jsou například možnost zpracování osobních údajů z důvodu oprávněných zájmu správce (v tomto případě ochrana majetku, zdraví a života), výjimky z registrační a informační povinnosti atd. Aplikace těchto výjimek je na národních institucích.

Po rozhodnutí SDEU vydal UOOU tiskovou zprávu, ve které potěšeně komentoval, že SDEU dal za pravdu jeho právnímu názoru. Tisková zpráva, která vyšla po konečném rozhodnutí NSS, měla k předchozí spokojenosti vpravdě daleko.

Je třeba předeslat, že rozsudek NSS je argumentačně velmi dobře odůvodněn. Soud se v něm postupně vypořádává s řadou Rynešových kasačních námitek, kterých stěžovatel vznesl takové množství, že jeho strategie může až asociovat metodu aplikovanou americkými vojáky ve Vietnamské válce zvanou „*spray and pray*“. Jednou z nejzajímavějších námitek, kterou soud označil za nedůvodnou, byl názor, že při pořizování záznamu vůbec nebyly zpracovávány osobní údaje, jelikož Okresní soud v Třebíči v rozhodnutí v trestní věci zprostil obžalované obžaloby, jelikož je nedokázal ze záznamu dostatečně identifikovat. NSS námitku odmítl s odkazem na objektivní podstatu osobních údajů a své předchozí

rozhodování, kdy stanovil, že o osobní údaj by se nejednalo, pokud by k identifikaci subjektu údajů bylo třeba nepřiměřené množství času, úsilí či materiálních prostředků, což však nebyl tento případ. Navíc, na záznamu nebyli zachycení jen obžalovaní, ale například i sousedé Františka Ryneše, které již bylo možné určit snadno.

Na tomto místě je třeba připomenout rozdíl v potřebné jistotě identifikace fyzické osoby mezi posuzováním správně právního institutu ochrany osobních údajů a trestním řízením. V další námitce se stěžovatel bránil proti informační a registrační povinnosti, kterou jako správce údajů měl splnit. František Ryneš tvrdil, že informovat subjekty údajů by bylo nepřiměřeně složité. NSS to odmítl vzhledem k tomu, že takové informování je možné učinit prostým umístěním značky s oznámením, že je prostor monitorován. Navíc, díky preventivní funkci, kterou takové oznámení má, se jedná o prostředek, který přímo směřuje k zamýšlenému účelu užití kamerového systému, tedy ke snížení a zabránění útoků na majetek a zdraví stěžovatele (bod 105 rozhodnutí). Stejně tak NSS odmítl možnost, že by se Ryneš nemusel registrovat u UOOU, byť s povzdechnutím, že český zákon o ochraně osobních údajů je velmi strohý a na rozdíl od zahraničních úprav na kamerové systémy výslovně v tomto směru nepamatuje (bod 109 rozhodnutí).

V případě námitky, že rozhodovací správní praxe UOOU je roztříštěná, což vedlo do stavu, kdy nebylo možné objektivně spolehlivě určit účinné právo, stěžovatel mířil přesně a NSS mu po precizní a detailní analýze dal za pravdu. Situace ohledně otázky, zda je možné použití kamerového systému vykládat jako zpracování osobních údajů výhradně pro osobní potřebu, byla nejasná až do okamžiku rozhodnutí SDEU. Svědčí o tom i stanoviska členských států vyjádřených při řízení před SDEU, kdy česká, italská, polská a britská vláda měly za to, že je tato činnost vyňata ze zpracování osobních údajů dle Směrnice 95/46/ES.[2] V českém případě byla navíc situace ztížená faktem, že zákon 101/2000 Sb., o ochraně osobních údajů je velmi stručný a o kamerách zcela mlčí. NSS tuto složitou situaci komentuje: „*Čelil-li tedy stěžovatel* [František Ryneš, pozn. JM] *nejasné zákonné normě, která měla svůj předobraz v obsahově neurčité normě práva EU, na jejíž výklad panoval rozpor mezi jednotlivými členskými státy Unie, bylo*

[2] Bod 51 rozhodnutí NSS ve věci Ryneš.

důležité, aby na vnitrostátní úrovni tuto nejasnost odstranila konzistentní praxe žalovaného [UOOU, pozn. JM]. *Jak zdejší soud vysvětlí dále, správní praxe žalovaného má k jednoznačnosti velmi daleko.*“[3]

Soud v rozhodnutí uvádí čtyři dokumenty, ve kterých si UOOU protiřečí. V odpovědi na dotaz Policie ČR UOOU uvádí, že při zpracování osobních údajů pořízených kamerou za účelem ochrany majetku se jedná o osobní potřebu ve smyslu § 3 odst. 3,[4] v prvostupňovém rozhodnutí z roku 2008 naopak výslovně stojí, že o osobní potřebu nejde.[5] Ve výroční zprávě za rok 2008 UOOU toto rozhodnutí komentuje, opětovně uvádí, že se jedná o zpracování osobních údajů,[6] a naproti tomu o tři roky později tento názor znovu obrací a využívání kamerových systémů pro ochranu vlastního majetku uvádí jako typický příklad výjimky zpracování osobních údajů výlučně pro osobní potřebu dle § 3 odst. 3.[7] Na základě těchto skutečností NSS konstatoval, že rozhodování v těchto typových věcech bylo schizofrenní, nepředvídatelné a svévolné, což mělo fatální dopad na právní jistotu. František Ryneš tak nemohl dost dobře předem určit, jaké chování bylo proti právu, tedy v rozporu se zákonem v jeho materiálním smyslu, jeho předvídatelnost je, jak NSS připomíná, zcela klíčová pro udělování sankcí.[8] Z toho důvodu soud rozhodl, že jeho potrestání bylo v rozporu s čl. 7 odst. 1 Úmluvy o ochraně lidských práv a základních svobod. Za tuto argumentaci je třeba NSS pochválit. Přijmout formalisticky rozhodnutí SDEU, který jednou pro vždy tuto otázku vyjasnil na sklonku roku 2014, a poměřovat jeho optikou sedm let starý případ, by znamenalo faktickou retroaktivitu.

Po přijetí faktu, že se v daném případě jednalo o zpracování osobních údajů, se NSS zabýval otázkou, jaký zákonný důvod mohl takové zpracování legitimizovat. František Ryneš se dovolával legitimizačního důvodu zpracování z důvodu ochrany práv a oprávněných zájmů správce, zakotvené v českém zákoně o ochraně osobních údajů v § 5 odst. 2 písm. c). UOOU opakovaně tvrdil, že tento legitimizační důvod není možné

[3] Ibid, bod 53.
[4] Ibid, bod 55.
[5] Ibid, bod 57.
[6] Ibid, bod 60.
[7] Ibid, bod 62.
[8] Ibid, bod 69.

použít, protože umístění kamery způsobuje příliš velký zásah do soukromí obyvatel protějšího domu, jehož vchod je sledován. NSS tuto úvahu však odmítl z důvodu její zjevné zkratkovitosti (nebyl proveden řádný test proporcionality). Odkázal rovněž na výše zmíněnou poznámku SDEU, že mechanismy obsažené ve Směrnici, zejména pak legitimizační důvody pro zpracování bez souhlasu subjektu údajů, umožňují spravedlivé vyvážení povinností správce a míry ochrany subjektu údajů. Námitku UOOU, že SDEU nebyl plně obeznámen s okolnostmi případu, tedy že kamera zabírala protější vchod, NSS bez skrupulí konstatuje: „*Soudní dvůr i generální advokát s touto informací* [kamera snímá protější vchod, pozn. JM] *opakovaně pracují. … Zdá se tedy, že se žalovaný doposud neseznámil s celým textem rozsudku Soudního dvora ani se stanoviskem generálního advokáta.*“[9]

NSS po provedení testu proporcionality konstatoval, že použití kamery za účelem ochrany majetku bylo v daném případě vhodné a potřebné. Neopomněl sarkasticky poznamenat, že pokud UOOU radí Františku Rynešovi, že kamera neměla snímat veřejný prostor, ale měla být například sklopena a zabírat jen obvodovou zeď domu, což by nutně vedlo k tomu, že by se její funkce tak zcela míjela svým účinkem, je to jen smutný důkaz odtržení UOOU od reálií běžného světa. NSS potvrdil i v dalších krocích testu proporcionality, že řešení, které Ryneš použil, bylo adekvátní a přiměřené a proto zpracování mohlo probíhat na základě oprávnění § 5 odst. 2 písm. c) zákona č. 101/2000 Sb., o ochraně osobních údajů. Kasační námitka tak i v tomto případě byla důvodná.

Výsledky celé kauzy se dají shrnout ve dvou rovinách. Tou první je sympatické pobídnutí ke korekci chování UOOU ze strany vrcholných článků soudní soustavy. Nezbývá než doufat, že toto rozhodnutí bude adekvátně reflektováno a rozhodovací i poradní činnost UOOU bude více odpovídat realitě „běžného světa“. Kauza Ryneš ostatně není jediným takovým případem z poslední doby. Nedávno UOOU podobným způsobem narazil v případu e-Kolo.[10]

Druhou rovinou je dopad potvrzení objektivního přístupu k definici osobních údajů a působnosti Směrnice a tedy i zákona o ochraně

[9] Ibid, bod 79.

[10] Plný text rozsudku k nalezení online http://ekolo.cz/uploads/assets/files/11A_77_2012_19.pdf [cit. 10. 6. 2015].

osobních údajů. Jestliže soud rozhodl, že se za zpracování osobních údajů považuje nahrávání videozáznamu bez ohledu na jeho účel, znamená to, že žádné pořizování videozáznamu nemůže být posuzováno jako zpracování osobních údajů pro výkon výlučně osobních či domácích činností. To potvrzuje i stanovisko UOOU zabývající se kamerami v motorových vozidlech.[11] Celá situace vede k tomu, že vznik jakéhokoli video záznamu, ať už se jedná o CCTV kamery, kamery v autech, kamery na sportovních Go-Pro helmách, kamery na dronech, nebo jen prosté ruční kamery případně záznam chytrým telefonem, je zpracováním osobních údajů a pořizovatel záznamu je správcem údajů dle Směrnice. Jak UOOU uvádí ve svém stanovisku ke kamerám v autech, v případě českého práva je možné využít výjimky v podobě § 3 odst. 4 zákona o ochraně osobních údajů, který stanoví, že se zákon nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány. V případě záznamů z kamer aut je takovým dalším zpracováním zřejmě nejčastěji jejich využití pro potřeby šetření incidentu. Informační povinnost dle § 11 odst. 5 zákona o ochraně osobních údajů by v takovém případě bylo možné splnit až v okamžiku dalšího využití takových údajů.[12] Výjimka nahodilosti je však českou specialitou a ve Směrnici uvedená není. Zcela stranou teď ponechme fakt, že podobným nahodilým zaznamenáváním podoby člověka zřejmě dochází k zásahu do práva na ochranu soukromí dle Občanského zákoníku,[13] který výjimku umožňující nahodilé zaznamenání lidské podoby pro osobní potřebu neobsahuje. Je však možné, že je činnost legitimizována poměrně širokým ustanovením § 88 odst. 1, který uvádí: *„Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.“*[14]

Otázky, které nechalo rozhodnutí SDEU ve věci Ryneš otevřené tak zůstávají poněkud palčivé. Jakým způsobem by měli dle pravidel ochrany

[11] Stanovisko Úřadu pro ochranu osobních údajů č. 1/2015. Provozování kamery v motorovém vozidle se záběrem mimo toto vozidlo. Cit. 10. 6. 2015. Online: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=14864

[12] Ibid, s. 2.

[13] Zákon č. 89/2012 Sb., Občanský zákoník. In: *Beck-online* [právní informační systém]. Cit. 10. 6. 2015.

[14] Ibid, § 88 odst. 1.

osobních údajů postupovat například tvůrci videí věnovaných parkourovému běhu skrz zalidněné město? Podíváme-li se na tento příklad z Evropské perspektivy, záznam probíhajícího akrobata a obličejů lidí, kolem nichž běží, je zpracováním osobních údajů ve smyslu Směrnice. Důvodem pro zpracování osobních údajů bude zřejmě jeho nezbytnost pro uskutečnění oprávněných zájmů správce dle článku 7 písm. f). Jaké přesně však bude mít správce povinnosti, nejsme jen na základě směrnice schopní určit, protože možnost určit výjimky z povinností správce, který zpracovává údaje pro účely uměleckého projevu,[15] zanechává článek 9 Směrnice členským státům. V našem případě by se jednalo o nahodilé zpracování osobních údajů. Není však následná publikace hotového videa tím „dalším zpracováním údajů“ dle § 3 odst. 4? A pokud ano, jak má správce zaznamenané subjekty údajů informovat o zpracování, nebo dát subjektu údajů možnost protestovat? Podobná situace pak platí například i pro zpravodajství, nebo turistické pořizování soukromého záznamu pro domácí použití (sic). Dovedeme-li úvahu SDEU logicky do důsledků, získáváme absurdní a nesplnitelné závěry.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

[15] Berme pro potřeby příkladu, že záznam osoby skákající ze střechy na střechu je skutečně uměleckým projevem.

PŘEHLED AKTUÁLNÍ JUDIKATURY II/2014 A I/2015

JAKUB HARAŠTA, PAVEL LOUTOCKÝ, JAKUB MÍŠEK, MATĚJ MYŠKA

PARODIE JAKO AUTONOMNÍ POJEM EVROPSKÉHO PRÁVA

Soud: Soudní dvůr Evropské unie
Věc: C-201/13
Datum: 3. 9. 2014
Dostupnost: curia.europa.eu

V případu *Deckmyn* se SDEU vyjádřil k podstatě a chápání pojmu parodie v evropském autorském právu a možnosti členských států interpretovat harmonizované omezení autorského práva na základě směrnice 2001/29/ES („InfoSoc"). Deckmyn se domnělého zásahu do autorských práv dopustil tím, že na novoroční oslavě distribuoval kalendáře, na kterých byla otištěna kresba podobná kresbě otištěné na obálce jednoho ze sešitů seriálu Suske en Wiske. Tato kresba zachycovala starostu města Gent, jak oděn v bílé tunice sype peníze osobám tmavé pleti a osobám zahaleným v burce. Takové užití díla bylo dle žalujících dědiců neoprávněné. Deckmyn se však bránil tím, že se jedná o přípustnou politickou karikaturu (parodii). Belgický odvolací soud (Hof van beroep Brussel) se rozhodl přerušit sporné řízení a dotázal se SDEU na výklad čl. 5 odst. 3 písm. k) InfoSoc směrnice.

Předně SDEU označil parodii za autonomní pojem unijního práva, který je nutno vykládat jednotným způsobem v celé EU. Za podstatné znaky parodie pak SDEU označil schopnost evokovat existující dílo, a přitom se od něj zřetelně lišit, a přítomnost komedie či ironie. Tento prvek se ale nemusí vztahovat pouze k dílu samotnému – parodii lze využít i ke komické či ironické kritice aktuálních společenských poměrů. Parodie dále nemusí být původně osobitá, jinak než skrze zřetelné odlišnosti od parodovaného

původního díla. Stejně tak nemusí být racionálně připsatelná jinému autorovi, týkat se původního díla nebo uvádět zdroj parodovaného díla. Pokud ovšem parodie nese diskriminační poselství, může majitel autorských požadovat, aby původní dílo nebylo s takovým poselstvím asociováno.

Rozsudek má ale i zásadní obecné dopady na interpretaci výjimek a omezení autorského práva. Předně se jedná o odklon od jejich restriktivní interpretace k jejich účelovému chápání. Výjimky a omezení musí respektovat přiměřenou rovnováhu mezi zájmy a právy majitelů práv na straně jedné a svobodou projevu uživatelů chráněného díla. Konečně, rozsudek jasně stanovuje, že pokud si již členské státy vyberou z „nabídky" harmonizovaných výjimek a omezení, je nutno je interpretovat jednotně v rámci celé EU a nelze je tedy v rámci národní implementace (restriktivně) modifikovat.

DIGITALIZACE KNIHOVNÍHO FONDU A PŮJČOVÁNÍ ELEKTRONICKÝCH KNIH

Soud: Soudní dvůr Evropské unie
Věc: C-117/13
Datum: 11. 9. 2014
Dostupnost: curia.europa.eu

Technische Universität Darmstadt vytvořila v rámci univerzitní knihovny místo pro četbu elektronických knih. Veřejnosti tím umožnila přístup k dílům z knihovního fondu. V jeden okamžik mohlo být tímto způsobem užíváno pouze tolik elektronických kopií knihy, kolik měla knihovna kopií fyzických. Tento fond obsahoval i učebnici vydanou společností Ulmer. Ta v roce 2009 oslovila knihovnu s nabídkou na zakoupení příslušných děl a umožnění jejich užívání ve formě elektronických knih. Knihovna toto odmítla a zakoupila pouze fyzické exempláře. Ty posléze digitalizovala a zpřístupnila ve formě elektronických knih. Soud ve Frankfurtu nad Mohanem, který rozhodoval v prvním stupni, zamítnul návrh požadující

zákaz další digitalizace. Přikázal ale knihovně znemožnit tištění částí digitalizovaných knih či jejich odnášení na datových nosičích. Spolkový soudní dvůr, který rozhodoval o opravném prostředku, pak dospěl k několika otázkám výkladu čl. 5 odst. 3 písm. n) InfoSoc směrnice 2001/29/ES. Konkrétně se jednalo o otázku, (i) zdali se prodejní a licenční podmínky vztahují na dílo v případě, že nositel práv nabídnul uzavření licenční smlouvy za přiměřených podmínek. SDEU se také měl vyjádřit, (ii) zdali mohou členské státy poskytnout právo digitalizovat díla ze sbírek, pokud to zpřístupnění terminálem vyžaduje, a (iii) jestli mohou umožnit uživatelům takto zpřístupněná díla tisknout nebo ukládat na paměťová zařízení. SDEU odpověděl, že (i) samotná nabídka v minulosti nestačí a musí být uzavřena licenční smlouva. Dále konstatoval, že (ii) členský stát má možnost poskytnout právo digitalizovat obsah, pokud je tento úkon nezbytný pro zpřístupnění děl prostřednictvím k tomu určených zařízení umístěných v prostorách knihovny. Zároveň ale (iii) není možné vztáhnout vykládané ustanovení na tisk děl na papír nebo ukládání na média.[1]

STANOVENÍ VÝŠE ŠKODY PŘI PORUŠOVÁNÍ AUTORSKÉHO PRÁVA

Soud: Nejvyšší soud
Věc: 5 Tdo 171/2014
Datum: 8. 10. 2014
Dostupnost: nsoud.cz

Nejvyšší soud rozhodoval o dovolání obviněného R. R., který směřoval proti výroku o náhradě škody v odsuzujícím rozsudku Městského soudu v Brně, kterým byl uznán vinným zločinem porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 odst. 1, 2 písm. c), odst. 3 písm. a) zákona č. 40/2009 Sb., trestní zákoník, ve

[1] Takové úkony mohou být nicméně povoleny na základě národních právních předpisů provádějících čl. 5 odst. 2 písm. a) a/nebo b) směrnice 2001/29/ES, protože se nejedná o sdělování, ale rozmnožování. V ČR tento úkon povolen není, viz §37 odst. 1 písm. c) zákona č. 121/2000 Sb., autorského zákona.

znění pozdějších předpisů. Tento trestný čin spáchal tím, že „uploadoval" audiovizuální díla na datová úložiště a následně šířil po různých fórech odkazy umožňující jejich „stažení". Tímto jednáním měl poškozeným způsobit škodu v celkové výši 11 041 514 Kč. Nejvyšší soud ale shledal způsob určení této konkrétní finanční ztráty jako problematický neboť *„stojí na čistě hypotetickém a nijak nepodloženém základě, že každý uživatel Internetu, který si zdarma stáhl z datového úložiště konkrétní film nebo jiný audiovizuální nebo hudební záznam, by si jinak koupil jeho legální DVD nebo CD nosič."* Soud prvního stupně též neřešil otázku příčinné souvislosti mezi neoprávněným zveřejněním díla na Internetu a počtem prodaných originálních nosičů typu DVD nebo CD. Nejvyšší soud tak pro trestněprávní účely zcela odmítl konstrukci, že by bylo možno stanovit výši ušlého zisku násobkem ceny nosiče obsahujícího rozmnoženinu díla. Z těchto důvodů tak dle Nejvyššího soudu spočívají napadená rozhodnutí soudů nižších instancí na nesprávném právním posouzení. Nejvyšší soud je tak zrušil a přikázal věc obviněného R. R. v potřebném rozsahu znovu projednat a rozhodnout. Samotný mechanismus stanovování konkrétního ušlého zisku pak má být dle Nejvyššího soudu předmětem znaleckého posudku.

POŘIZOVÁNÍ KAMEROVÉHO ZÁZNAMU PRO OSOBNÍ POTŘEBU ZA ÚČELEM OCHRANY ZDRAVÍ A MAJETKU

Soud: Soudní dvůr Evropské unie
Věc: C-212/13
Datum: 11. 12. 2014
Dostupnost: curia.europa.eu

František Ryneš na podzim 2007 z důvodu ochrany před neznámými vandaly, kteří jej a jeho rodinu opakovaně ohrožovali a ničili jeho majetek, nainstaloval pod střechu svého domu bezpečnostní kameru. Kamera však krom jeho pozemku zabírala rovněž veřejně dostupnou ulici za ním a vchod do protějšího bytového domu. I přes to, že ke kamerovému systému nebyl připojen monitor a jediný, kdo měl k datům zaznamenávaným ve smyčce

na pevný disk přístup, byl František Ryneš, Úřad pro ochranu osobních údajů („ÚOOÚ“) posoudil probíhající zpracování osobních údajů jako protizákonné a udělil Rynešovi pokutu. Případ se postupně dostal až před Nejvyšší správní soud, který položil Soudnímu dvoru Evropské Unie předběžnou otázku, zda lze takovéto provozování kamerového systému považovat za zpracování osobních údajů prováděné pro výkon výlučně osobních či domácích činností ve smyslu čl. 3 odst. 2 směrnice 95/46/ES, díky čemuž by byl vyloučen z věcné působnosti směrnice pro ochranu osobních údajů. Soudní dvůr v tomto ne příliš rozsáhlém rozhodnutí nejprve zkonstatoval, že monitorováním prostřednictvím obrazového záznamu dochází k automatizovanému zpracování osobních údajů osob kamerou zachycených, a následně určil, že na případ projednávaný v původním řízení se výjimka osobního účelu zpracování dle čl. 3 odst. 2 nevztahuje. Svůj názor podepřel argumentem, že výjimky ve směrnici 95/46 uvedené je nezbytné vykládat restriktivně, vzhledem k důležitosti základního práva na ochranu soukromí. Malý rozsah výjimky je navíc rovněž vyjádřen v samotném textu směrnice, který praví, že mimo věcnou působnost směrnice, a tedy i zákona č. 101/2000 Sb., o ochraně osobních údajů, stojí toliko takové zpracování údajů, které je prováděné pro výkon výlučně osobních či domácích činností. SDEU však v bodě 34 rozsudku připomněl, že pro konkrétní případy lze zohlednit oprávněné zájmy správce spočívající například v ochraně majetku, zdraví a života tohoto správce a jeho rodiny.

VYMÁHÁNÍ BEZDŮVODNÉHO OBOHACENÍ KOLEKTIVNÍMI SPRÁVCI A „SDĚLOVÁNÍ DÍLA VEŘEJNOSTI“

Soud: Ústavní soud
Věc: II. ÚS 2186/14
Datum: 13. 1. 2015
Dostupnost: nalus.usoud.cz

Ústavní soud v tomto nálezu rozpracoval své předchozí úvahy (II. ÚS 3076/13[2]) ke sdělování díla veřejnosti provozováním televizního či rozhlasového vysílání a vymáhání bezdůvodného obohacení kolektivními správci, potažmo k zásahu do práva na spravedlivý proces dle čl. 36 Listiny.

Stěžovatel, provozovatel restauračního zařízení, odmítl uzavřít licenční smlouvy s kolektivním správcem INTERGRAM z důvodu, že přístroj byl nefunkční a nezpůsobilý přijímat signál. Neumožňoval tak užití předmětů ochrany. Kolektivní správce („KS“) pak u příslušného krajského soudu úspěšně vymáhal bezdůvodné obohacení. Jelikož se jednalo o bagatelní věc, nemohl se budoucí stěžovatel domáhat nápravy u soudu druhé instance, a proto podal ústavní stížnost. Tu shledal Ústavní soud opodstatněnou, jelikož *„skutkový stav zjištěný krajským soudem dostatečně nesvědčí jím vyřčeným právním závěrům, neboť mnohé ze skutečností, které jsou klíčové pro určení toho, zda došlo na straně stěžovatele k bezdůvodnému obohacení tkvícím v užití díla bez patřičného licenčního oprávnění, nebyly prokázány“* (bod 49). Takové zásadní pochybení krajského soudu má za následek vadu řízení, kterou je nutné považovat za zásah do práva na spravedlivý proces podle čl. 6 odst. 1 Úmluvy a do práva na soudní ochranu podle čl. 36 odst. 1 Listiny.

Při posuzování důkazního břemene, které tíží kolektivní správce v těchto sporech, pak Ústavní soud vycházel z toho, že *„povinnost uzavřít licenční smlouvu týkající se autorského vlastnictví* (sic!) *vyvstává pouze tehdy, pokud je do tohoto práva autorů předmětů ochrany ze strany dalších subjektů skutečně zasaženo.“* Při posuzování „sdělování díla veřejnosti“ lze

[2] Viz HARAŠTA, Jakub a Matěj MYŠKA. Přehled aktuální judikatury I/2014. Brno: Masarykova univerzita, 2014. S. 253-263. *Revue pro právo a technologie*. ISSN 1804-5383. S. 259-261.

akceptovat určitou míru presumpce spočívající ve faktu, že „*funkční a provozuschopné zařízení je schopné zpřístupnit užití chráněných děl, a proto jeho provozovatel musí mít (za splněných dalších podmínek (sic!)) uzavřenou platnou licenční smlouvu pro veřejnou produkci těchto předmětů ochrany*“ (bod 30). Na druhou stranu ale ÚS dále konstatuje, že požadavek „sdělování veřejnosti“ nelze dovozovat pouze z fyzické existence přístroje, který toto sdělování potenciálně umožňuje (bod 40). Z hlediska potenciálního zásahu do autorských práv a s tím souvisejícím vymáháním bezdůvodného obohacení pak je nutno vždy dokázat: a) umístění zařízení prokazatelně umožňujícího zásah do autorských práv v inkriminovaném objektu, b) skutečný zásah prostřednictvím tohoto zařízení do autorských práv, c) těch subjektů, které je KS oprávněn zastupovat (bod 23).

Za povšimnutí též stojí, že Ústavní soud explicitně označil kolektivní správce povinnosti uložené kolektivním správcům autorským zákonem jsou do určité míry povahy veřejnoprávní (např. kontrolní povinnost) a že vztahy mezi kolektivními správci a uživateli předmětů ochrany nemají výlučně soukromoprávní charakter (bod 20).

SMLUVNÍ OCHRANA DATABÁZÍ

Soud:	Soudní dvůr Evropské unie
Věc:	C-30/14
Datum:	15. 1. 2015
Dostupnost:	curia.europa.eu

Ve sporu, o němž SDEU rozhodoval, proti sobě stála PR Aviation, nabízející vyhledávání nízkonákladových letů různých leteckých společností, srovnání cen a za poplatek pak i rezervaci letu, a letecká společnost Ryanair, která před možností procházet její katalog letů, vyžaduje od návštěvníka webových stránek dát najevo souhlas s obchodními podmínkami společnosti. Součástí podmínek byla v době pro případ rozhodné obsažena i klauzule zajišťující právo distribuce letenek výhradně společnosti Ryanair nebo dalším smluvně zmocněným subjektům. PR Aviation neuzavřela

s Ryanair dohodu o přístupu k datům a i přes to nabízela lety společnosti Ryanair, čímž se měla dopustit porušení výše zmíněných obchodních podmínek a tím pádem smluvní ochrany databáze. Ve prospěch PR Aviation rozhodl Nizozemský odvolací soud, který určil, že společnost neporušila právní ochranu databáze, protože její jednání odpovídalo běžnému užívání webových stránek Ryanair a tudíž se aplikuje výjimka z ochrany dle Směrnice. V předběžné otázce se předkládající soud ptal, zda se účinky směrnice 96/9/ES a výjimky z ochrany databázového práva vztahují i na databáze, které nejsou chráněny autorským právem ani sui generis právem pořizovatele databáze. SDEU se nejprve zabýval definicí databáze a shrnul, že nestačí, když prvek naplňuje znaky databáze ve smyslu čl. 1 odst. 2 směrnice, aby spadal do působnosti této směrnice, ale že je nezbytné naplnit i podmínky vzniku autorskoprávní ochrany nebo ochrany právem pořizovatele. V případě že toto právo nevzniká, není možné ani dovodit vznik výjimek z těchto práv. Pořizovateli databáze v tu chvíli svědčí větší míra autonomie vůle a může tak nastavit podmínky užívání své databáze, aniž by byl vázán analogií k zákonným výjimkám k vytěžování a zužitkování databází. PR Aviation tak výjimka z databázových práv nesvědčí a její jednání bylo protiprávní.

VYČERPÁNÍ PRÁVA NA ROZŠIŘOVÁNÍ PŘI ZMĚNĚ NOSIČE

Soud: Soudní dvůr Evropské unie
Věc: C-419/13
Datum: 22. 1. 2015
Dostupnost: curia.europa.eu

Předběžná otázka vyvstala v řízení u nizozemského Hoge Raad der Nederlanden ve sporu mezi společností Art & Allposters International BV (dále jen „Allposters“) a Stichting Pictoright (dále jen „Pictoright“). Prvně jmenovaná vytvářela reprodukce chráněných děl, ke kterým spravovala práva Pictoright, takovým způsobem, že z papírového plakátu přenesla tyto speciální chemickou metodou na malířské plátno. Tyto reprodukce

následně prodávala. Allposters odmítala uhradit příslušnou licenční odměnu za užití děl s tím, že se k danému předmětu ochrany vyčerpalo právo na rozšiřování dle čl. 4 odst. 2 InfoSoc směrnice. SDEU pak, s ohledem na hlavní cíl InfoSoc směrnice,[3] konstatoval, že se vyčerpání práva na rozšiřování týká pouze konkrétního původního hmotného nosiče, nikoliv dalších natolik změněných, „nových" rozmnoženin (bod 46). Při posuzování vyčerpání tohoto práva pak je rozhodnou otázka, zda *„změněný předmět – posuzovaný jako celek – je jako takový fyzicky předmětem, který byl uveden na trh se svolením nositele práv."* (bod 45). Pokud ne, právo na rozšiřování se nevyčerpá. SDEU se ovšem nevyjádřil ke klíčovému aspektu takového posuzování, totiž jaká je rozhodná úroveň nutné změny média. Stejně tak zůstává nadále problematické, zda lze o vyčerpání práva na rozšiřování uvažovat v případě digitálních rozmnoženin. Rozsudek SDEU, který klade důraz na hmotnou povahu rozmnoženiny (např. v bodech 37, 40), naznačuje, že spíše ne.

JURISDIKCE PŘI ZÁSAHU DO AUTORSKÝCH PRÁV

Soud: Soudní dvůr Evropské unie
Věc: C-441/13
Datum: 22. 1. 2015
Dostupnost: curia.europa.eu

Pez Hejduk je fotografkou specializující se na fotografování architektonických děl. Zaměřuje se zejména na fotografování děl rakouského architekta Georga W. Reinberga. Tento architekt použil fotografie Pez Hejduk na kolokviu pro účely ilustrace svých staveb se souhlasem fotografky. Pořadatelem kolokvia byla německá společnost EnergieAgentur, která posléze bez souhlasu autorky a bez uvedení toho, komu náleží autorská práva, zpřístupnila uvedené fotografie k prohlížení a ke stažení na svých domovských internetových stránkách. Spor byl žalován fotografkou u rakouského soudu. Žalovaná EnergieAgentur ale

[3] Tj. zavedení vysoké úrovně ochrany autorů (body 9 a 10 recitálu InfoSoc Směrnice).

vznesla námitku mezinárodní a územní nepříslušnosti rakouského soudu, když tvrdila, že její internetové stránky (provozované v ccTLD doméně .de) nejsou určeny pro Rakousko a že pouhá možnost zobrazení v členském státě nepostačuje ke vzniku příslušnosti uvedeného rakouského soudu. Bylo tedy nutno interpretovat čl. 5 odst. 3 nařízení nařízení Rady (ES) č. 44/2001 („Brusel I“) a zjistit, jestli jsou ve výše popsaném případě příslušné pouze soudy členského státu, ve kterém má údajný porušitel sídlo nebo rovněž ty soudy členského státu, na které jsou internetové stránky vzhledem ke svému obsahu zaměřeny. Soudní dvůr již v obdobném rozhodoval a konstatoval, že čl. 5 odst. 3 nařízení nevyžaduje, aby byly dotčené internetové stránky zaměřeny na členský stát sídla soudu, jemuž byl předložen spor. Není tedy důležitá skutečnost, že internetové stránky nejsou primárně směřovány na členský stát, kde má soud sídlo (tedy Rakousko). Soudní dvůr tedy řekl, že žalovat lze *de facto* kdekoli, kde se škoda projevila, což prakticky znamená, že lze nejdříve spor zažalovat v příslušném státě a posléze u jakéhokoli soudu příslušného k rozhodnutí o škodě způsobené na území členského státu, kde má soud sídlo.

SPECIFICKÝ MECHANISMUS PRO IMPORT LÉKŮ

Soud: Soudní dvůr Evropské unie
Věc: C-539/13
Datum: 12. 2. 2015
Dostupnost: curia.europa.eu

Kapitola 2 přílohy IV aktu o přistoupení z roku 2003, nazvaná „Právo obchodních společností“ stanovila pro některé nově přistupující státy specifický mechanismus pro dovoz a uvádění léčiv na trh. Tento mechanismus stanovuje výjimku ze zásady volného pohybu zboží v EU, kdy držitelé patentu nebo dodatkového ochranného osvědčení (“DOO”) mohou pokračovat v uplatňování svých práv, aby zabránili paralelnímu dovozu jejich produktu z některého z nových členských států, který neumožňoval patentování farmaceutických výrobků před vstupem do EU. Každý, kdo

zamýšlí dovézt nebo uvést na trh výrobek v členském státě, kde výrobek požívá patentové nebo dodatkové ochrany, musí v žádosti týkající se takového dovozu prokázat příslušným orgánům, že majiteli nebo oprávněnému z takové ochrany bylo zasláno oznámení s předstihem jednoho měsíce. Odvolací soud v souvislosti s výkladem specifického mechanismu položil Soudnímu dvoru tři okruhy otázek: (i) jaké podmínky musí držitel patentu naplnit před tím, než podá žalobu pro nesplnění povinnosti; (ii) kdo je osobou, která předkládá záměr pro paralelní dovoz; (iii) jak identifikovat osobu, které musí být takový záměr předložen. Specifický mechanismus (i) neukládá majiteli (nebo oprávněnému z patentu či DOO) povinnost oznámit, že nehodlá souhlasit s plánovaným dovozem, před tím, než uplatní svá práva podle prvního pododstavce tohoto mechanismu. Pokud však majitel nevyjádří takový úmysl v jednoměsíční čekací lhůtě, osoba, která plánuje dovážet léčivý přípravek, může legitimně požadovat, aby příslušné orgány schválily dovoz tohoto přípravku, a může jej případně začít dovážet a uvést na daný trh. (ii) Oznámení musí být adresováno majiteli, přičemž tento pojem označuje jakoukoli osobu, která je oprávněným držitelem práv majitele patentu či dodatkového ochranného osvědčení. (iii) Specifický mechanismus neukládá povinnost učinit oznámení přímo osobě, která hodlá dovážet či uvést dotčený léčivý přípravek na trh, pokud lze v tomto oznámení tuto osobu jednoznačně identifikovat.

SKRYTÁ KAMERA PŘI NATÁČENÍ REPORTÁŽE

Soud: Evropský soud pro lidská práva
Věc: stížnost č. 21830/09
Datum: 24. 2. 2015
Dostupnost: hudoc.echr.coe.int

V rámci přípravy dílu pořadu Kassensturz, který měl informovat o pochybných obchodních praktikách pojišťovacích zprostředkovatelů, byl v roce 2003 pořízen dvěma skrytými kamerami záznam domluvené

schůzky. V rámci schůzky jeden z novinářů vystupoval jako spotřebitel. Na konci tohoto setkání byl přítomný zprostředkovatel informován o tom, že byl nahrán skrytou kamerou, a novináři ho požádali o komentář záznamu ze schůzky. Zprostředkovatel toto odmítl a záznam byl později odvysílán. Tvář zprostředkovatele i jeho hlas byly změněny tak, aby nebylo možné jeho osobu identifikovat. Švýcarský soud pak v roce 2007 udělil čtveřici novinářů pokutu s tím, že právo veřejnosti na informace v podobě ochrany svobody projevu je sice chráněným zájmem, ale stejně je chráněným zájmem i soukromí jednotlivce. Novináři tak měli podle konstatování soudu postupovat tak, aby zásah do soukromí na záznamu zachyceného zprostředkovatele minimalizovali.

ESLP v rámci rozhodování ve věci konstatoval, že touto sankcí porušilo článek 10 Úmluvy o ochraně lidských práv a svobod. ESLP zohlednil, že fakta prezentovaná v reportáži nebyla nikdy rozporována žádnou ze stran sporu. Také konstatoval, že rozmazání obličeje a pozměnění hlasu za účelem znemožnění identifikace na záznamu zachyceného zprostředkovatele bylo dostatečným opatřením vedoucím k minimalizaci zásahu do soukromí. Na záznamu zachycený zprostředkovatel totiž nebyl zachycený jako jednotlivec, ale vystupoval jako neidentifikovaný příslušník určité profesní skupiny.

PRÁVNÍ JISTOTA PŘI APLIKACI EVROPSKÝCH PŘEDPISŮ

Soud: Nejvyšší správní soud
Věc: 1 As 113/2012
Datum: 25. 2. 2015
Dostupnost: www.nssoud.cz

NSS rozhodoval případ Františka Ryneše, jehož skutkový stav je shrnutý výše v části věnované rozhodnutí SDEU C-212/13, o předběžné otázce týkající se zpracování osobních údajů pro osobní účely. Žalobce v kasační stížnosti nabídl celou řadu námitek, proč dle jeho názoru bylo rozhodnutí ÚOOÚ o udělení pokuty a následné potvrzení tohoto rozhodnutí Městským

soudem v Praze protiprávní. Žalobce napadal nesprávné právní posouzení situace, kdy se dle něj vůbec nejednalo o zpracování osobních údajů a pokud ano, měla by se aplikovat výjimka pro osobní potřebu. Většinu z námitek NSS zamítl jako nedůvodné, včetně námitek týkajících se informační a registrační povinnosti Františka Ryneše jako správce. Soud potvrdil názor ÚOOÚ, že žalobce pochybil, když se nezaregistroval a neupozornil lidi procházející kolem jeho zahrady, že jsou monitorováni. Jedinou námitkou, kterou soud shledal jako důvodnou, byla nekonzistentní rozhodovací praxe ÚOOÚ. Soud provedl detailní analýzu rozhodnutí, stanovisek a pasáží výročních zpráv ÚOOÚ týkajících se režimu zpracování osobních údajů při užití kamer pro účely ochrany zdraví a majetku a přesvědčivě prokázal naprostou rozporuplnost v prezentovaných právních názorech. Zatímco některé z materiálů tvrdily, že se jedná o osobní potřebu, další tvrdily naprostý opak a osobní potřebu při ochraně zdraví a majetku vylučovaly. To mělo, v kombinaci s nejednoznačností evropské směrnice a zákona o ochraně osobních údajů, dle soudu za následek faktickou nemožnost adresátů právních norem seznámit se s účinným právem a plnit zákonné požadavky. Při hledání zákonného důvodu pro zpracování osobních údajů Františkem Rynešem NSS přesvědčivě užil testu proporcionality a dovodil, že v tomto případě je důvodné užít pro zpracování osobních údajů legitimizačního důvodu ochrany práv a právem chráněných zájmů správce. Rozsudek NSS tak zrušil rozhodnutí Městského soudu i obě správní rozhodnutí ÚOOÚ a vrátil věc k jednání v prvním stupni správního řízení.

DAROVACÍ DAŇ A POVOLENKY NA EMISE SKLENÍKOVÝCH PLYNŮ

Soud: Soudní dvůr Evropské unie
Věc: C-43/14
Datum: 26. 2. 2015
Dostupnost: curia.europa.eu

ŠKO-ENERGO bezplatně nabyla v letech 2011 a 2012 povolenky na emise skleníkových plynů pro výrobu elektřiny. Stalo se tak v období, pro které předepisoval článek 10 směrnice 2003/87/ES členským státům povinnost přidělit alespoň 90 % emisních povolenek zdarma. Česká republika nicméně učinila bezúplatné nabytí povolenek subjekty vyrábějícími elektřiny spalováním paliv předmětem darovací daně (§ 6 odst. 8 zákona č. 357/1992 Sb., o dani dědické, darovací a z převodu nemovitostí), kdy základ stanovila jako průměrnou tržní hodnotu povolenky, kterou vyhlásí Ministerstvo životního prostředí, násobenou počtem nabytých povolenek (§7a odst. 1 a 2 zákona č. 357/1992 Sb.). Sazba daně pak byla stanovena na 32 % (§ 14a zákona č. 357/1992 Sb.).

Předběžná otázka položená Nejvyšším správním soudem tak směřovala k vyjasnění povahy danění přidělených emisních povolenek ve vztahu k požadavku na bezplatné poskytnutí nejméně 90 % z nich v období 2008-2012. SDEU konstatoval v souladu se svojí předchozí rozhodovací praxí, že článek 10 brání výběru poplatků za přidělení emisních povolenek. Členské státy sice mohou přijmout opatření, která mohou ovlivnit hospodářské důsledky použití emisních povolenek, ale tato opatření nesmí neutralizovat zásadu bezplatného přidělení povolenek.[4] SDEU tak konstatoval, že zdanění přidělených emisních povolenek, které je omezené na určité odvětví, představuje poplatek toto přidělování zatěžující. Nejvyšší správní soud tak musí prověřit, zdali tato daň respektuje 10% horní hranici pro přidělení emisních povolenek za úplatu.

[4] SDEU zde citoval rozhodnutí ve věci Iberdrola a další, spojené věci C-566/11, C-567/11, C-580/11, C-591/11, C-620/11 a C-640/11. Body 27-31.

K POPLATKU ZA SOUKROMÉ ROZMNOŽOVÁNÍ

Soud: Soudní dvůr Evropské unie
Věc: C-463/12
Datum: 5. 3. 2015
Dostupnost: curia.europa.eu

Předběžná otázka směřovala k výkladu čl. 5 odst. 2 písm. b) a článku 6 InfoSoc směrnice 2001/29/ES. Copydan, jako organizace pro správu autorských práv zastupující nositele práv ke zvukovým a audiovizuálním dílům, v původním řízení tvrdila, že na paměťové karty mobilních telefonů je nutné aplikovat systém spravedlivé odměny z titulu výjimky z práva na rozmnožování. Společnost Nokia, která do svých mobilních telefonů umisťovala dodatečné paměťové karty, tak měla tuto spravedlivou odměnu doplatit za období 2004 až 2009. Hlavním argumentem Nokia bylo tvrzení, že se takový poplatek neplatí, pokud rozmnožena není legální a pokud k rozmnožení udělili nositelé autorského práva souhlas (např. po stažení díla z internetového obchodu). Poplatek by se měl vztahovat pouze na legální rozmnoženiny pro soukromé užití, ke kterým nositel práv neudělil svolení – tyto se přitom vyskytují na paměťových kartách mobilních zařízení pouze zřídkakdy. Také namítala, že není možné, dle zásady rovného zacházení, zatěžovat poplatek paměťová média, ale nikoli součástí zařízení (např. vnitřní paměti MP3 přehrávačů).

SDEU konstatoval, že není nutné zkoumat faktické použití paměťového média, ale stačí jeho způsobilost k tomuto užití – poplatek se tedy stanovuje na základě domněnky. Samotná schopnost vybavení sloužit k ukládání pro soukromé užití, ke kterému nositel práv neudělil svolení, legitimizuje uplatnění poplatku za soukromé rozmnožování. K otázce rovného zacházení pak SDEU konstatoval, že členské státy mají možnost odlišit dodání nosičů od dodání součásti, ovšem pouze za předpokladu, že tyto kategorie nejsou srovnatelné nebo je rozdílné zacházení mezi nimi odůvodněné. Toto uložil ověřit soudu, který předběžnou otázku předložil.

DAŇOVÁ SLEVA NA ELEKTRONICKÉ KNIHY

Soud: Soudní dvůr Evropské unie
Věci: C-479/13, C-502/13
Datum: 5. 3. 2015
Dostupnost: curia.europa.eu

V obou případech (které byly rozhodovány samostatně se stejným výsledkem i argumentací) se Evropská komise domáhala toho, aby soudní dvůr určil, že Francie (resp. Lucemburské vévodství) uplatňováním snížené sazby DPH ve výši 5,5 % (resp. 3 %) v případě poskytování digitálních (elektronických) knih, porušuje ustanovení směrnice o společném systému daně z přidané hodnoty. Sazba daně byla na elektronické knihy aplikována ve stejné výši, jako v případě knih tištěných. Snížené sazby daně z přidané hodnoty je však možno využít jen v případě dodání knih na jakémkoli fyzickém nosiči. I když je ke čtení elektronických knih nutný fyzický nosič (počítač, elektronická čtečka, tablet), soud argumentoval tím, že takový nosič není součástí dodání elektronických knih. Rovněž bylo zdůrazněno, že je vyloučena možnost uplatňovat sníženou sazbu DPH u jakýchkoli elektronicky poskytovaných služeb. Za takovou službu je přitom nutné považovat i dodání elektronických knih. Bylo tedy jednoznačně stanoveno, že sníženou sazbu DPH na elektronické knihy (na rozdíl od těch tištěných) uplatňovat nelze. Je ale nutno poukázat na reakci jednotlivých států a zdůraznit nutnost zajistit technologickou neutralitu knihy bez ohledu na to, zda mají tištěnou či elektronickou podobu. S ohledem na to tak evropská Komise naznačila, že v budoucnu plánuje daňové zákony v této oblasti upravit tak, aby dosáhla harmonizace.

PŘENOSY SPORTOVNÍCH UTKÁNÍ A SDĚLOVÁNÍ VEŘEJNOSTI

Soud: Soudní dvůr Evropské unie
Věc: C-279/13
Datum: 26. 3. 2015
Dostupnost: curia.europa.eu

Linus Sandberg, který byl v původním sporu v pozici žalovaného, vkládal na internetovou stránku odkazy, které umožňovaly zájemcům přístup k přímým přenosům zápasů ledního hokeje na jiné internetové stránce. Ti tak nemuseli zaplatit částku požadovanou provozovatelem a k obsahu se dostávali zdarma.

Rozhodnutí v této věci představuje ve své podstatě doplnění k rozhodnutí SDEU ve věci C-466/12. Předkládající soud totiž po jmenovaném rozhodnutí vzal zpět čtyři ze svých otázek a nadále žádal vyjasnění pouze páté položené otázky s tím, jestli mohou členské státy přiznat nositelům práv širší výlučné právo a stanovit, že sdělování veřejnosti zahrnuje více úkonů, než uvádí čl. 3 odst. 2 směrnice 2001/29/ES. Ve vztahu k čl. 3 odst. 1 téže směrnice již totiž SDEU v rámci C-466/12 judikoval, že členským státům je bráněno v tom, aby stanovily, že pojem „sdělování veřejnosti" zahrnuje více úkonů, než stanovuje směrnice.

SDEU v řízení o této předběžné otázce nakonec dospěl k závěru, že živé vysílání sportovních přenosů nelze považovat za zpřístupňování veřejnosti, protože není, striktně vzato, „on-demand". Národní úpravě tak nic nebrání v rozšiřování práva vysílajících organizací na úkony sdělování veřejnosti, které by mohly představovat přímé přenosy sportovních utkání na internetu. To vše pod podmínkou, že takovým rozšířením není dotčena ochrana autorského práva.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

KYBERNETICKÁ BEZPEČNOST JAKO AKTUÁLNÍ FENOMÉN ČESKÉHO PRÁVA[*]

RADIM POLČÁK[**]

ABSTRAKT

Česká republika je jedním z prvních civilizovaných států, který zavedl komplexní právní úpravu národní kybernetické bezpečnosti. Z hlediska právní vědy jde o relativně nový regulatorní fenomén, kterému je třeba se věnovat za užití specifické metody a při zohlednění pro právo netradičních faktorů. Článek se vedle metodického přístupu k právním problémům národní kybernetické bezpečnosti věnuje též jednotlivým institutům tohoto nového právního odvětví. V závěru pak je provedena diskuse možného dalšího vývoje legislativy i organizačních resp. technických forem řešení bezpečnostních rizik majících původ ve službách informační společnosti.

KLÍČOVÁ SLOVA

kybernetická bezpečnost; kritická informační infrastruktura; zákon o kybernetické bezpečnosti; bezpečnostní opatření; kybernetický bezpečnostní incident

ABSTRACT

Czech Republic was among first civilised countries that implemented complex national legislation on cybersecurity. This relatively new legal regulatory phenomenon requires specific methodological approach that, quite unusually for continental Europe, acknowledges a number of extra-legal factors. The paper tackles the basic methodological issues and it also analyses particular institutes

[*] Tento článek vznikl jako součást plnění projektu OPPI 5.1 SPTP02/029 Energetická a kybernetická bezpečnost.

[**] Doc. JUDr. Radim Polčák, Ph.D. je vedoucím Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: radim.polcak@law.muni.cz.

of cybersecurity law. In conclusions, it tries to discuss further development on the Czech legislation as well as of organisational and technical solutions for cybersecurity risks.

KEYWORDS

cybersecurity; critical information infrastructure; Cybersecurity Act; security measures; cybersecurity indicent

1. METODOLOGIE PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Obecně lze v právním instrumentariu nalézt tři typy právních metod, a to metody pozitivistické, naturalistické a realistické (či pragmatické). Pozitivistické metody vyznačují se pojmovým oddělením pravidel od faktických informací[1]. Znamená to mimo jiné, že pravidlo nemůže svým obsahem vycházet z informace o skutečnosti (z výroku), ale je vždy vytvořeno jako originální informace o povinnostech. Fakticita se zde v obsahu pravidel nijak neprojevuje a s fakty pracujeme pouze jako s faktory naplnění subsumpčních podmínek[2]. Jinak řečeno je tedy v tomto metodologickém pojetí právo systémem originálně tvořených povinnostních informací a fakta jsou pro právo důležitá pouze co do rozhodování v otázce, zda právo pro konkrétní situace formuluje nějaké konkrétní imperativy (tj. v otázce, zda jsou ad hoc naplněny znaky hypotéz příslušných právních norem).

Obecně se oddělení faktických a povinnostních informací u právního pozitivismu projevuje absencí vztahu mezi právem a morálkou[3]. Morálka jako faktická kategorie totiž nemůže v pozitivistickém pojetí práva ovlivňovat obsah právních pravidel[4]. To samozřejmě neznamená, že právní

[1] Toto oddělení je založeno na Humově základní filozofické distinkci mezi bytím (is) a mětím (ought) – viz Hume, D. A Treatise on Human Nature. *Project Gutenberg*, 2003, dostupný online na adrese www.gutenberg.org/etext/4705.

[2] Kelsen označuje toto pojetí práva za „ryzí," tj. oproštěné od všeho, co do něj nepatří – viz Kelsen, H. *Pure Theory of Law*, přel. Knight, M. Berkeley: University of California Press, 1978, str. 1.

[3] K tomu srov. např. Alexy, R. *The Argument from Injustice*, přel. Paulson, S., Litschewski Paulson, B. Oxford: Oxford University Press, 2002, str. 85 a násl.

[4] Kritika nedostatku tohoto přístupu spočívajícího obecně v pojmové nemožnosti hodnotové reflexe obsahu platného práva je možno najít např. v díle Vladimíra Čemáka – viz Baroš, J. (ed.) *Vladimír Čermák – člověk, filozof, soudce*. Brno: Masarykova univerzita, 2009, str. 248.

pravidla musí být nutně amorální – jejich konstrukci ani aplikaci však morálka v tomto pojetí přímo neovlivňuje.

V oboru práva informačních a komunikačních technologií se základní motiv pozitivistické metodologie projevuje neexistencí přímého vztahu mezi faktickou situací určité technologie (tj. jejími parametry, fungováním apod.) a obsahem právních pravidel regulujících její užití. Důsledná aplikace pozitivistické metodologie v tomto směru může vést k takovým důsledkům, kdy je právně formulován právně perfektní (bezvadný) takový právní předpis nebo takové soudní rozhodnutí, jejichž praktická aplikace je z nějakého praktického důvodu vyloučena – k tomu může dojít tehdy, jsou-li např. stanoveny nereálné požadavky na nějakou technologii, právo požaduje řešení, které téměř nelze organizačně zvládnout nebo je vyžadováno splnění takové povinnosti, která je z ekonomického hlediska absurdní. Z právě uvedeného plyne, že užití této metody k řešení problému kybernetické bezpečnosti není vhodné[5].

Druhou možností je naturalistická právní metodologie[6] postavená ve vztahu k pozitivismu na zcela opačné tezi spojení faktických a povinnostních informací. Obecnou implikací této teze je možnost přímého dovození právních pravidel z morálky a jí odpovídající předpoklad, že objektivní právo je jen konstatováním existence přirozených pravidel (de facto přírodních zákonů) a že právotvorba není ve skutečnosti o originárním vytváření právních pravidel ale pouze o jejich nalézání.

Aplikace naturalistické metodologie v právu informačních a komunikačních technologií vede k závěru formulovaného předním americkým konstitucionalistou Lawrencem Lessigem, že totiž „kód je zákonem kyberprostoru.[7]“ Znamená to, že právo pro informační síť je resp. má být pouze dovozováno z technických pravidel definujících možnosti chování uživatele. Lessigem popsaný stav již v řadě ohledů reálně funguje. Především v případech, kdy brání uplatnění práva některý z právních nebo

[5] Nepomáhá v tomto směru ani výjimečná zásada impossibilium nulla obligatio – její aplikace je totiž podmíněna aletickou nemožností. V technologicky exponovaných situacích však je nutno z pohledu práva nezřídka šlápnout i na kluzký svah organizační resp. obchodní nemožnosti. To je pro právní pozitivismus neakceptovatelné, neboť může následná normativní eroze vést až k důsledkům shrnutelným slovy klasika do postulátu „když nemůžu, tak nemusím.“

[6] Obecně k pojmu viz Finnis, J. *Natural Law.* New York: New York University Press, 1991.

[7] Viz Lessig, L. *Code V. 2*. New York: Basic Books, 2006.

přirozených limitů (tj. např. otázka jurisdikce, absence věcné působnosti, vysoké náklady na výkon práva apod.), je kód skutečně dominantním normativním faktorem ovlivňujícím, často výlučně, chování uživatelů.

Z právě popsaného důvodu nelze s iusnaturalistickou metodologií pracovat pro potřeby řešení problému kybernetické bezpečnosti. Přijetí tohoto přístupu by totiž v prostředí informačních sítí znamenalo popření základní premisy, na níž zde v současnosti stojí legitimita práva, tj. že právo je legitimováno veřejným zájmem vyjádřeným prostřednictvím instituce státu. Iusnaturalistické pojetí totiž přisuzuje možnost definovat obsah právních pravidel subjektům majícím pod kontrolou technické parametry příslušných součástí informační sítě, z nichž většinou jde o soukromoprávní korporace.

Nikoli jen vylučovací metodou jeví se jako nejvhodnější k řešení problému kybernetické bezpečnosti metoda realistická[8]. Je postavena na podobném předpokladu jako právní pozitivismus, tj. že obsah právních pravidel je originárně vytvářen a je zajišťován autoritou státu, avšak netrvá na důsledném pojmovém oddělení právních pravidel od faktických informací. Zohlednění fakticity, ať technické, ekonomické nebo organizační, má formu omezení legislativních a aplikačních výstupů o ty, které jsou, stručně řečeno prakticky (pragmaticky) neproveditelné[9]. Pragmatický zákon tedy počítá jen s takovými povinnostmi, které je reálně možno splnit bez větší zátěže pro povinné subjekty a soudní rozhodnutí je založeno na předpokladu reálné (nikoli ideální) společenské, technické a ekonomické situace[10].

Zřejmá nevýhoda realistické metodologie spočívá především v riziku relativizace právních hodnot, neboť tam, kde se jejich důsledná aplikace odchyluje od toho, co považujeme za součást technické, společenské nebo ekonomické reality, prostě od nich ustoupíme. To může vést k Dworkinem kritizovanému postupnému úbytku ideálů[11] a nebezpečí tvorby situací, kdy

[8] Používá se též výrazu pragmatismus – k tomu viz např. James, W. *Pragmatism*. Rockville: ARC Manor, 2008 nebo Tamanaha, B. *Beyond the Formalist – Realist Divide*. Princeton: Princeton University Press, 2010, str. 67 a násl.

[9] K tomu viz např. Rorty, R. The Banality of Pragmatism and the Poetry of Justice. *Southern California Law Review*. 1990, roč. 63, str. 1811 a násl.

[10] Srov. Sharp, W.G. Sr. The Past, Present and Future of Cybersecurity, *Journal of National Security Law and Policy*, roč. 4, číslo 13, str. 19 a násl.

[11] Viz Dworkin, R. *Justice in Robes*. London: Belknap Press, 2006, str. 38.

právo jen kopíruje požadavky ekonomické, technické nebo obecně společenské reality resp. toho, co je za realitu aktuálně považováno politickou mocí. Na druhou stranu však realistická metodologie poskytuje jako jediná z uvedených alternativ prakticky použitelná řešení pro situace vyznačující se značnou mírou technické, ekonomické či společenské složitosti a právě takovou situací je současný stav informační společnosti[12]. Udržení úrovně hodnot a principů, jakož i idealistického charakteru právních pravidel je v tomto případě řešeno nikoli metodologicky ale institucionálně prostřednictvím legitimity orgánů veřejné moci zajišťujících tvorbu příslušných právních pravidel a jejich následnou implementaci[13].

2. LEGISLATIVNÍ ŘEŠENÍ KYBERNETICKÉ BEZPEČNOSTI

Legislativní řešení kybernetické bezpečnosti nemá v platném právu žádnou prakticky srovnatelnou paralelu. Lze sice pro partikulární otázky používat nejrůznější analogie s bezpečnostními řešeními v oborech s dominantní technologickou komponentou (typicky např. v oborech stavebnictví, protipožární ochrany, dopravy, apod.), právní fenomén kybernetické bezpečnosti se však jako takový ničemu ve své podstatě nepodobá[14].

Prvním důvodem originality kybernetické bezpečnosti je skutečnost, že hodnocení bezpečnostních aktiv má až na výjimky obvykle akcesorickou povahu. Systémy a sítě, jejichž zabezpečení je předmětem právní úpravy, totiž zpravidla nemají hodnotu per se, ale závisí na tom, čemu v konečném důsledku slouží[15]. S trochou nadsázky tedy lze prohlásit, že tentýž router může sloužit jako součást informační infrastruktury internetové kavárny

[12] Viz Polčák, R. *Internet a proměny práva*, Praha: AUDITORIUM, 2012, str. 85.

[13] K tomu srov. např. Polčák, R. Internet Legal Culture, Lex Informatica and (un)Desired Sovereignty of Lawyers. In Lindskoug, P., Manusbach, U. Millqvist, G., Samuelsson, P., Vogel, H. H. *Essays in Honour of Michael Bogdan*. 1. vyd. Lund: Författarna och Juristförlaget i Lund, 2013, str. 477 a násl.

[14] Srov. např. Fredland, J. S. Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies, *Military Law Review*, číslo 206, str. 26 a násl., nebo Brenner, S. Cyber-threats and the Limits of Bureaucratic Control, *Minnesota Journal of Law, Science and Technology*, roč. 14, číslo 1, str. 151 nebo též Grant, J. Will There Be Cybersecurity Legislation? *Journal of National Security Law and Policy*, roč. 4, str. 104. Další důvody zvláštního charakteru kybernetické bezpečnosti přidává Paul Rosenzweig v textu Rosenzweig, P. Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?, *Journal of Law and Policy for the Information Society*, roč. 8, číslo 2, str. 390.

[15] Srov. např. systematiku hrozeb dle Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace, *Harvard Journal of Law and Technology*, roč. 25, číslo 2, str. 445.

i atomové elektrárny, přičemž jeho bezpečnostní hodnota není dána jeho cenou, ale způsobem jeho užití[16].

Výjimkou ze shora uvedeného jsou systémy a sítě, jejichž smyslem a účelem je působit jako součást národní informační a komunikační infrastruktury. Typicky např. tzv. páteřní sítě neodvozují svoji důležitost od hodnoty funkcionalit, k nimž byly pořízeny, neboť jejich funkcí je udržovat v chodu informační síť jako takovou – v jejich případě tedy není nutno hodnotit, jakému primárnímu účelu slouží, neboť jejich důležitost je zpravidla dána faktory, jako jsou kapacita, zastupitelnost apod[17].

Druhým významným faktorem odlišujícím legislativní řešení kybernetické bezpečnosti od ostatních oborů platného práva je její procesní orientace. Zatímco právní úprava krizového řízení resp. úprava bezpečnosti kritických funkcionalit státu je tradičně postavena na objektovém principu, je kybernetickou bezpečnost nutno primárně vnímat jako ochranu informačních procesů[18]. Tomu pak musí odpovídat celá regulatorní logika i fungování příslušných orgánů veřejné moci, neboť primárním smyslem a účelem není ochrana existence nebo funkčnosti konkrétně definovaného objektu, ale zajištění bezproblémové existence informačních transakcí. Výsledné řešení přitom samozřejmě nemůže být vzhledem k objektům dohromady tvořícím naši informační a komunikační infrastrukturu absolutně indiferentní – objekt však má být předmětem regulatorního zájmu až v důsledku jeho konkrétní důležitosti pro kritický informační proces[19].

---

[16] Srov. např. Shane, P. M. Cybersecurity Policy as if "OrdinaryCitizens" Mattered: The Case for Public Participation in Cyber Policy Making, *Journal of Law and Policy for the Information Society*, roč. 8, číslo 2, str. 435.

[17] V českém právu je tato skutečnost zohledněna subsidiárním kritériem pro určení prvku kritické informační a komunikační infrastruktury ve smyslu ust. části VI.G.d. přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

[18] Srov. Hathaway, M. E., Klimburg, K. Preliminary Considerations: On National Cybersecurity, in Klimburg, A. *National Cybersecurity – Framework Manual*, Talinn: CCDCOE, 2012, str. 8.

[19] Viz např. Srov. např. Lin, H. Thoughts on Threat Assessment in Cyberspace, *Journal of Law and Policy for the Information Society*, roč. 8, číslo 2, str. 338. Současná česká právní úprava je naproti tomu vzhledem ke kritické informační a komunikační infrastruktuře orientována objektově. Je to dáno skutečností, že definiční kritéria pro kvalifikaci informačního systému nebo sítě obsažená v části VI.G.a., VI.G.b. a VI.G.d. přílohy k nařízení vlády č. 432/2010 Sb. jsou svázána s objektovými definicemi ostatních prvků národní kritické infrastruktury.

Třetím specifickým rysem právní úpravy kybernetické bezpečnosti je právní jev, který je doktrínou popisován jako fenomén definičních autorit. Veškeré lidské jednání totiž v prostředí informačních sítí neprobíhá bezprostředně, ale je zprostředkováváno službami informační společnosti. Člověk ani právnická osoba tedy nemůže v prostředí informačních sítí činit nic bez toho, aby se na jeho jednání fakticky nepodílela hned celá řada poskytovatelů služeb informační společnosti[20].

Označení definiční autority si tyto subjekty vysloužily z toho důvodu, že mají faktickou možnost definovat formou kódu (tzv. definiční normy) technické parametry jednání svých uživatelů. Nejedná se přitom o normu právní, neboť poskytovatelé služeb informační společnosti nedisponují právotvornou kompetencí (jde povětšinou o soukromé subjekty)[21] – přesto jde nepochybně o pravidlo, které má na jednání uživatelů zásadní vliv.

Definiční charakter těchto technických resp. faktických pravidel je od právních norem odlišuje i co do jejich fungování. Byť jde o pravidla vytvořená člověkem a zaměřená k regulaci lidského chování, nemají charakter povinnostní, ale jde o kauzální normy přímo determinující na technické úrovni výsledek lidského jednání[22]. Jsou to v podstatě člověkem vytvořené normy zaměřené k regulaci lidského chování, ale jejich technický charakter jim dává povahu kauzálního přírodního zákona.

Z právního hlediska jde o extrémně zajímavý jev mající zásadní dopady především do problematiky odpovědnosti za protiprávní jednání[23]. Především z toho důvodu, že poskytovatelé služeb informační společnosti jsou v problematických případech jedinými subjekty, které lze reálně

[20] Základem teorie definičních autorit je práce amerického konstitucionalisty Lawrence Lessiga op. cit. v pozn. 7. Z českých pramenů viz např. Polčák, R. *Internet a proměny práva*, Praha: Auditorium, 2012, str. 137 a násl.

[21] K institucionálním požadavkům na právotvůrce viz např. Kelsen H. *Pure Theory of Law*, přel. Paulson, B. L., Paulson S., Oxford: Oxford University Press, str. 91 a násl.

[22] Namísto povinnosti v tomto případě hovoříme o nutnosti člověka jednat určitým způsobem. Definiční norma nepůsobí nutnost jednat pouze v situaci, pokud ji její adresát dokáže technicky eliminovat. Definiční normou tedy není vázán pouze hacker (v pravém smyslu toho slova) – viz Polčák, R. *Internet a proměny práva*, Praha: Auditorium, 2012, str. 193.

[23] Ve státech Evropské unie vznikla za tímto účelem specifická legislativa omezující odpovědnost poskytovatelů služeb informační společnosti za protiprávnost jednání jejich uživatelů. Harmonizačním předpisem je směrnice 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu), přičemž do českého práva byla omezení implementována zákonem č. Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

nalézt, proti nimž lze uplatnit právní postih a které jsou technicky schopny problematickou situaci efektivně řešit, vznikla celá relativně samostatná teorie spoluodpovědnosti těchto poskytovatelů za protiprávní jednání jejich uživatelů[24]. Dokonce lze konstatovat i dříve nevídaný obecný trend přesouvat vymáhání subjektivních práv od jejich skutečných rušitelů (tj. od individuálních uživatelů) právě k poskytovatelům služeb, jejichž prostřednictvím k porušování těchto práv dochází, respektive která protiprávní jednání technicky zprostředkovávají[25].

V oblasti kybernetické bezpečnosti se fenomén definičních autorit rovněž projevuje zásadním způsobem, a to osobní působností příslušných právních předpisů. Povinnosti plynoucí z potřeby chránit kritické informační funkcionality státu resp. národní informační a komunikační infrastrukturu nejsou v tomto případě vůbec ukládány koncovým uživatelům, ale směřují ve velké míře na poskytovatele služeb resp. na správce zájmových systémů a sítí[26].

V tomto směru je možno vidět i další podstatný rozdíl mezi právní úpravou krizového řízení a kybernetickou bezpečností, neboť v případě krizového řízení může právní úprava bezprostředně dopadat na libovolné fyzické či právnické osoby. Rozsah osobní působnosti právní úpravy kybernetické bezpečnosti naproti tomu nepočítá s dopadem na nikoho jiného, než jsou právě poskytovatelé služeb - v případě české právní úpravy jde konkrétně o poskytovatele služeb elektronických komunikací[27].

Posledním základním rysem právní úpravy kybernetické bezpečnosti, který z ní činí specifický regulatorní fenomén, je značná míra konvergence soukromého a veřejného zájmu. Obecně bývá obvyklé, že v případě zájmu

[24] Obsáhlé zmapování aktuální české, slovenské i zahraniční rozhodovací praxe přináší publikace Husovec, M. *Zodpovednosť na internete podľa českého a slovenského práva*, Praha: CZ.NIC, 2014, ke stažení on-line na adrese http://knihy.nic.cz/files/nic/edice/Zodpovednost_web_FINAL.pdf.

[25] Důsledkem tohoto trendu jsou naneštěstí i některé extrémní právní konstrukce, jako např „třikrát a dost“ v zákoně HADOPI – srov. např. working paper Dejean, S., Pénard, T., Suire, R. *Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français*, Rennes: CREM, ke stažení on-line na adrese http://www.01net.com/genere/article/fichiersAttaches/300415066.pdf.

[26] Správcem je pro potřeby zákona č. 181/2014 Sb. analogicky s definicí obsaženou v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, subjekt, který určuje účel provozu příslušného informačního systému nebo sítě – povinnosti pak zákon stanoví právě jemu. K tomuto přístupu viz např. Berejka, M. A Case for Government Promoted Multi-Stakeholderism, *Journal on Telecommunications and High-Tech Law*, roč. 10, str. 9.

na ochraně tzv. nedistributivních[28] práv je výsledná právní úprava konfliktní se soukromým zájmem resp. s distributivními právy osob[29]. Vzájemné vyvážení soukromého a veřejného zájmu je v takových případech nezřídka otázkou právní a politické alchymie[30]. Pokud však má právní úprava nedistributivního práva jako v případě českého zákona o kybernetické bezpečnosti pouze základní rozsah, je hodnotově konzistentní s tím, co lze označit za tvrdé jádro ústavy[31], a navíc má na distributivní práva jen minimální dopad, dochází k výjimečně nekonfliktní situaci[32].

Jestliže tedy můžeme konstatovat, že naše právní úprava kybernetické bezpečnosti není zásadně konfliktní ve vztahu k distributivním právům, je to dáno především skutečností, že omezení, která reálně přináší, jsou v porovnání s důležitostí chráněných zájmů jen nepatrná. Nejzávažnějším bezprostředním zásahem do distributivních práv je v tomto případě zásah do práva vlastnického, neboť povinným subjektům může vzniknout

---

[27] Takto široký rozsah působnosti zákona uplatní se navíc pouze ve výjimečném případě vyhlášení stavu kybernetického nebezpečí. Za standardní situace běžného fungování systému národní kybernetické bezpečnosti mají konkrétní zákonné povinnosti pouze správci zvlášť určených systémů a sítí (poskytovatelé služeb elektronických komunikací mají pouze povinnost hlásit své kontaktní údaje). K tomu viz § 3 zákona č. 181/2014 Sb., přičemž zákonné povinnosti nad rámec hlášení kontaktních údajů jsou dalšími ust. ukládány pouze subjektům vypočteným v § 3 písm. c) až e) zákona č. 181/2014 Sb. – srov. zejm. § 4 odst. 1 a 2 zákona č. 181/2014 Sb.

[28] Pojem distributivnosti práv je výtečně vyložen v odlišném stanovisku Pavla Holländera k nálezu pléna Ústavního soudu ze dne 3.4.1996, č.j. Pl.ÚS 32/95, 112/1996 Sb., N 26/5 SbNU 215, dostupné z: www.nalus.usoud.cz, následovně: „Ústavní úprava postavení jedince ve společnosti obsahuje ochranu individuálních práv a svobod, jakož i ochranu veřejných statků (public goods, kolektive Gütter). Rozdíl mezi nimi spočívá v jejich distributivnosti. Pro veřejné statky je typické, že prospěch z nich je nedělitelný a lidé nemohou být vyloučeni z jeho požívání. Příklady veřejných statků jsou národní bezpečnost, veřejný pořádek, zdravé životní prostředí. Veřejným statkem se tudíž určitý aspekt lidské existence stává za podmínky, kdy není možno jej pojmově, věcně i právně rozložit na části a tyto přiřadit jednotlivcům jako podíly. (-) Pro základní práva a svobody je, na rozdíl veřejných statků, typická jejich distributivnost. Aspekty lidské existence, jakými jsou např. osobní svoboda, svoboda projevu, účast v politickém dění a s tím spjaté volební právo, právo zastávat veřejné funkce, právo sdružovat se v politických stranách atd., lze pojmově, věcně i právně členit na části a tyto přiřadit jednotlivcům."

[29] V obecné rovině se tomuto fundamentálnímu konfliktu věnuje např. Ronald Dworkin v práci Dworkin, R. *Justice for Hedgehogs*, London: Belknap Press, 2011.

[30] Z institucionálního hlediska se tomuto problému věnuje např. text Kelly, T. K., Hunker, J. Cyber Policy: Institutional Struggle in a Transformed World, *I/S: Journal of Law and Policy*, roč. 8, číslo 2, str. 210 a násl.

[31] K pojmu viz např. Höllander, P. Materiální ohnisko ústavy a diskrece ústavodárce, *Právník*, roč. 2005, č. 4, str. 318.

[32] Viz Powell, B. Is Cybersecurity a Public Good? Evidence From the Financial Services Industry, *Journal of Law, Economics and Policy*, roč. 1, číslo 2, str. 497.

povinnost investovat své prostředky do zabezpečení vlastní informační a komunikační infrastruktury.

Jak vyplynulo z jednání vedoucích k přijetí zákona o kybernetické bezpečnosti, jsou tyto investice již standardně povinnými subjekty realizovány – nikoli sice z důvodu jejich zájmu na zajištění národní kybernetické bezpečnosti, ale z čistě zištného zájmu na ochraně vlastních systémů před kybernetickými bezpečnostními incidenty. Ve většině případů tedy bude nutno ze strany povinných subjektů investovat pouze do komponent zajišťujících komunikaci s národním nebo vládním CERT resp. dokumentaci odpovídající zákonnému standardu[33].

3. PRINCIPY ČESKÉ A EVROPSKÉ PRÁVNÍ ÚPRAVY KYBERNETICKÉ BEZPEČNOSTI

V právu EU je specifická právní úprava kybernetické bezpečnosti v současné době ve stadiu návrhů základních normativních právních aktů[34], zatímco v České republice již je komplex zákona a podzákonných normativních právních aktů již účinný. Přestože vznikala nezávisle na sobě, sdílejí obě legislativní řešení stejnou regulatorní strategii a z jejich struktury lze rovněž vyčíst prakticky obdobný systémový základ. Důvodová zpráva k zákonu o kybernetické bezpečnosti shrnuje tyto principy následovně[35]:

1. Princip technologické neutrality[36] – na základě toho principu, jehož jedním z rozměrů je i tzv. síťová neutralita, dochází ke striktnímu

[33] Není v tomto směru žádným tajemstvím, že naše podzákonná úprava konkrétních náležitostí bezpečnostních opatření a jejich dokumentace vychází ze široce akceptovaného standardu organizačních norem v oblasti informační bezpečnosti z rodiny ISO 27k. Kritickou analýzu těchto standardů viz např. v příspěvku Vorobiev, V. I., Fedorchenko, L. N., Zabolotsky, V. P., Lyubimov, A. V. Ontology-based analysis of information security standards and capabilities for their harmonization, in *Proceedings of the 3rd international conference on Security of information and networks*, New York: ACM, 2010, str. 137 a násl.

[34] Viz zejm. dokumentaci k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii - COM(2013)0048 – C7-0035/2013 – 2013/0027(COD).

[35] Ze srovnání např. se strategií legislativy ke kybernetické bezpečnosti USA plynou základní rozdíly právě ve volbě jejích určujících principů – relativně větší úspěch českého resp. evropského legislativního přístupu ukazuje, že tento zřejmé více odpovídá aktuálnímu stavu politického a společenského diskursu. K tomu srov. např. Grant, J. Will there Be Cybersecurity Legislation? *Journal of National Security Law & Policy*, roč. 4, str. 103 a násl.

[36] K původnímu významu tohoto pojmu viz např. Balabanian, N. Presumed Neutrality of Technology, *Society*, roč. 17, číslo 3, str. 7.

oddělení obsahu komunikace od technologií používaných pro jeho ukládání nebo přenos. Informační a komunikační technologie jsou tedy neutrální vzhledem ke způsobu, kterým jsou používány. Důležitým aspektem technologické neutrality je rovněž nezávislost právního regulačního rámce na konkrétní technologii – právní regulace je tedy důsledně neutrální vůči produktům různých dodavatelů (žádný z nich nepreferuje ani nevylučuje).

2. Princip ochrany informačního sebeurčení člověka[37] – informační sebeurčení člověka zahrnuje nejrůznější základní informační práva, z nichž pro kybernetickou bezpečnost jsou důležité především právo na ochranu soukromí, právo na ochranu osobních údajů, právo na svobodný přístup k informacím a právo na přístup ke službám informační společnosti (to vychází ze skutečnosti, že v dnešní době nelze žít plnohodnotný soukromý život bez toho, aby měl člověk možnost tyto služby využívat)[38].
3. Princip ochrany nedistributivních práv[39] – v tomto případě jde především o ochranu národní bezpečnosti a specificky pak o ochranu bezpečnosti prostředí, v němž dochází k realizaci informačních transakcí (k tomu podrobněji viz dole).
4. Princip minimalizace státního donucení – v případě návrhu právní úpravy jde především o implementaci výstupního kritéria třetího prvku testu proporcionality[40], v němž je nutno hodnotit, zda je zásah do lidské svobody proveden jen v nezbytně nutné míře. Konkrétně jde o svobodu povinných subjektů volně užívat předmět

[37] Dokonce i v odborné literatuře převažuje přesvědčení, že kybernetická bezpečnost je v kontrapozici k základním informačním právům – srov. např. Nojeim, G. T. Cybersecurity and Freedom on the Internet, *Journal of National Security Law & Policy*, roč. 4, str. 118 a násl. Ve skutečnosti je však ochrana základních práv jediným skutečným a legitimním smyslem a účelem kybernetické bezpečnosti. To mimo jiné reflektuje i aktuální praxe a agendě ochrany základních práv Valného Shromáždění OSN – srov. např. zprávu Zvláštního zpravodaje Valného shromáždění OSN č. A/HRC/17/27 – stejný názor ve vztahu k právu na soukromí viz např. v článku Bambauer, D. Privacy versus Security, *The Journal of Criminal Law & Criminology*, roč. 103, číslo 3, str. 667.

[38] Podrobněji viz Polčák, R. *Internet a proměny práva*, Praha: AUDITORIUM, 2012, str. 326.

[39] Srov. Powell, B. J. Is Cybersecurity a Public Good? Evidence from the Financial Services Industry, *Journal of Law, Economics and Policy*, roč. 1, číslo 2, str. 497 a násl.

[40] Do našeho právního řádu byl tento test zaveden kontinuální řadou rozhodnutí Ústavního soudu, z nichž můžeme vybrat rozhodnutí ze dne 12. 10. 1994, sp.zn. Pl. ÚS 4/94 nebo ze dne 21. 3. 2002, sp.zn. III. ÚS 256/01. K pojmu a metodě viz též např. viz Alexy, R. On the Structure of Legal Principles. *Ratio Iuris.* 2000, roč. 13, č. 3, str. 1 a násl. nebo Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, str. 158 a násl.

jejich vlastnického práva (tj. jejich informační a komunikační infrastrukturu). Ve vztahu k člověku se návrh v tomto směru omezuje prakticky dokonale, neboť uživatelům služeb informační společnosti vůbec nezasahuje do jejich práv (zákon se netýká informačních práv uživatelů, nezasahuje do jejich soukromí ani jim neukládá žádná jiná omezení či povinnosti).

5. Princip autonomie vůle regulovaných subjektů – tento princip se týká metody právní regulace a projevuje se stanovením cílových parametrů bez toho, aby právotvůrce nutil regulované subjekty k nějakému specifickému konkrétnímu řešení (subjekty si tedy volí způsob, jak cílového stavu dosáhnout v podmínkách, v nichž samy působí).
6. Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství – tento princip označovaný v mezinárodním právu veřejném jako due dilligence[41] týká se odpovědnosti státu za mezinárodně škodlivé následky jednání, k němuž dojde pod jeho suverénní jurisdikcí (viz dále).

Za zvláštní pozornost stojí především princip ochrany nedistributivních práv směřující především k ochraně infrastruktury tvořené službami informační společnosti. Nedistributivní charakter bezpečnosti je v tomto případě dán skutečností, že tuto hodnotu nelze distribuovat, tj. nelze konstatovat, že z její existenci přímo plynou konkrétní práva jednotlivým subjektům. Namísto toho má bezpečnost celostní charakter (jde o ochranu prostředí jako celku) a práva k jeho ochraně vykonává výlučně stát podobně, jako je tomu např. v případě národní bezpečnosti nebo ochrany životního prostředí.

Je v tomto směru nutno zdůraznit, že bezpečnost obecně (tj. vč. kybernetické bezpečnosti) nepředstavuje hodnotu či relevantní zdroj legitimity právních norem sama o sobě. Jedná se jako u ostatních nedistributivních principů o akcesorický institut, jehož legitimita není dána přímo ale prostřednictvím primárních principů, k jejichž ochraně směřuje. Nelze tedy hovořit pouze o bezpečnosti bez dalšího resp. nelze jí per se odůvodňovat vznik nových právních povinností nebo obecně jakékoli

[41] Srov. Hessbruegge, J. A. *The Historical Development of the Doctrines of Attribution and Due Dilligence in International Law*.

zásahy do svobody subjektů. Bezpečnost jako taková pak nemůže být ani ve struktuře proporcionality přímo poměřována s ostatními (distributivními) právními principy jako např. s právem na vlastnictví, právem na svobodu projevu nebo právem na práci. Namísto toho je třeba vždy řešit otázku, co je bezpečností chráněno, tj. jaká primární hodnota resp. jaký primární princip je příslušnými konkrétními bezpečnostními instituty zajištěn[42].

Dominantním motivem české právní úpravy je tedy v tomto směru právo na informační sebeurčení[43]. To vychází genericky z práva na soukromý život, tj. práva člověka na hodnotnou osobní existenci, a to jak vzhledem k vlastní integritě (důstojnosti), tak i vzhledem k možnostem zapojení do společnosti. Komponentou informačního sebeurčení, která s rostoucí penetrací běžného života službami informační společnosti nabyla na zásadní důležitosti, je ochrana soukromí, z níž se ještě v poslední době specificky vydělila ochrana osobních údajů[44]. Bezpečnost této pasivní komponenty informačního sebeurčení má především charakter jistoty člověka ohledně rozumné míry zabezpečení soukromé informační sféry před násilnými vnějším vlivy.

Aktivní komponentou informačního sebeurčení, která má vzhledem ke kybernetické bezpečnosti přinejmenším srovnatelný význam jako ochrana soukromí a osobních údajů, je právo na komunikaci. Jeho podstatou je předpoklad, že člověk nemůže vést plnohodnotný soukromý život bez toho, aby měl možnost běžným způsobem interagovat s okolním světem, tj. především komunikovat formou, která je v příslušných sociokulturních reáliích obvyklá[45]. V aktuálních podmínkách je tak tuto komponentu

---

[42] Ke smyslu kybernetické bezpečnosti jako ochrany informačních práv člověka viz např. Polčák, R. Vygum v kyberprostoru: Právní problémy české a evropské kybernetické bezpečnosti. In Haňka, R., Kaplan, Z., Matyáš, V. Mikulecký, J. Říha, Z. *Information Security Summit 2011*. 1. vyd. Praha: Data Security Management, 2011, str. 159-165.

[43] Pojem informačního sebeurčení byl do právní praxe zaveden rozhodnutím Ústavního soudu Spolkové republiky, které se týkalo připravovaného sčítání lidu a jehož předmětem bylo primárně proporcionální vymezení informačního soukromí člověka. Viz nález Spolkového ústavního soudu ze dne 15. 12. 1983, č.j. BVerfGE 65, 1 [on-line]. Dostupné z: <www.thm.de/datenschutz/images/stories/volkszaehlungsurteil_bverfger_1983.pdf>.

[44] Srov. např. Mates, P. *Ochrana soukromí ve správním právu*. Praha : Linde Praha, 2006, str. 14. Pojmu soukromí se v českém právu věnuje jen minimum kvalitní doktrinální literatury – světlými výjimkami jsou např. sborník Šimíček, V. (ed.) *Právo na soukromí*. Brno : Mezinárodní politologický ústav, 2011 nebo monografie Matejka, J. *Internet jako objekt práva – hledání rovnováhy autonomie a soukromí*, Praha: CZ.NIC, 2013, k dispozici též on-line ke stažení na adrese https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf.

informačního sebeurčení možno přeložit jako právo na přístup k (fungujícím) službám informační společnosti[46].

Právě uvedené samozřejmě neznamená, že by stát měl povinnost zajistit všem subjektům dodávky služeb informační společnosti nebo že by uvedené služby měly být s garancí státu poskytovány bezplatně. Stát má však v situaci, kdy jsou tyto služby běžnou součástí soukromého lidského života, povinnost garantovat jejich dostupnost a na nejvyšší úrovni též jejich funkčnost. To v tomto případě mimo jiné znamená též povinnost státu zabezpečit tyto služby tak, aby mohly být poskytovány a konzumovány bez obav o jejich bezpečnost. Z právě uvedeného tedy plyne, že jen bezpečné služby informační společnosti mohou dát člověku prostor k nerušené realizaci jeho práva na informační sebeurčení.

S právě uvedeným též souvisí jiný princip, který český návrh nijak zvlášť nezdůrazňuje, ale který má ve vztahu ke kybernetické bezpečnosti rovněž zásadní význam, tj. princip svobody projevu. Na rozdíl od informačního sebeurčení se v tomto případě jedná namísto aktivní soukromé komunikace o zabezpečení možnosti veřejně vyjádřit svůj názor a případně se účastnit obecného společenského nebo politického diskursu. Stejně jako v případě informačního sebeurčení je přitom možno konstatovat, že pouze bezpečně

[45] Skutečnost, že soukromí člověka tvoří i možnost komunikovat s okolím, zdůraznil náš Ústavní soud, přičemž původně poukázal především na nutnost ochrany informačních vztahů v rámci rodiny. Doslova k tomu uvedl: „Právo na ochranu osobního soukromí je právem fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob. Přílišná akcentace pozitivní složky práva na ochranu soukromého života vede k neadekvátnímu zúžení ochrany pouze na to, aby skutečnosti soukromého života fyzické osoby nebyly bez jejího souhlasu či bez důvodu uznávaného zákonem a tak nebyla narušována integrita vnitřní sféry, která je pro příznivý rozvoj osobnosti nezbytná. Ústavní soud nesdílí toto zúžené pojetí, neboť respektování soukromého života musí zahrnovat do určité míry právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.“ – viz nález Ústavního soudu ze dne 1. 3. 2000, č.j. II. ÚS 517/99, N 32/17 SbNU 229.

[46] Ústavní soud se k této otázce vyjádřil v nálezu ze dne 07.04.2010, č.j. I.ÚS 22/10 následovně: „Lze dovodit, že člověk tak bývá netoliko objektem společenských ‚poměrů‘, ale stává se i objektem práva, je-li nucen podrobovat se mu zcela při jeho interpretaci a aplikaci, tj. bez zohlednění jeho individuálních zájmů, resp. základních práv. Vedle subjektivních faktorů na straně jednotlivce je při posuzování ‚obvyklosti, resp. oprávněnosti‘ výdaje třeba vzít v úvahu i faktory objektivní, mezi ty mimo jiné patří technologický vývoj (např. mobilní telefony, internet) a s ním související změny ve způsobech komunikace, získávaní informací, styku s úřady, sdružování apod., resp. vývoj technologií, skrze niž je realizováno právo jednotlivce na osobní rozvoj, vztahy s ostatními lidmi a vnějším světem, tedy právo na soukromý život.“

fungující služby informační společnosti mohou k takové účasti poskytnout adekvátní prostor[47].

Ostatní shora uvedené principy mají ve struktuře navrhované právní úpravy spíše implementační charakter. Princip technologické neutrality zdůrazněný hned na prvním místě týká se především skutečnosti, že česká právní úprava směřuje k zajištění funkčnosti informační a komunikační infrastruktury bez toho, aby se týkala komunikovaného obsahu[48]. Právní povinnosti subjektů ani pravomoci založené zákonem Národnímu bezpečnostnímu úřadu se tedy z podstaty nemohou týkat informací tvořících obsah komunikace prostřednictvím služeb informační společnosti. Dalším aspektem technologické neutrality je v tomto případě skutečnost, že povinné technické standardy ani technická řešení přímo implementovaná na národní úrovni nebudou zvýhodňovat nebo upřednostňovat žádnou konkrétní proprietální technologii[49].

Princip autonomie vůle regulovaných subjektů a princip minimalizace státního donucení vztahují se především k osobní působnosti, rozsahu a míře obecnosti konkrétních právních povinností definovaných právní úpravou. Ta je minimalistická v tom směru, že se vztahuje pouze na omezený okruh subjektů, přičemž míra zátěže těchto subjektů specifickými povinnostmi odpovídá důležitosti jimi spravovaných systémů a míře jejich bezpečnostní expozice.

Zohlednění maximální autonomie vůle při formulaci povinností pro subjekty spadající do osobní působnosti zákona má aspekt liberální i pragmatický. Inkorporace tohoto principu je pro regulované subjekty přirozeně příznivá, neboť jim poskytuje maximální volnost při implementaci příslušných povinností.

---

[47] Kybernetická bezpečnost se stala i jedním z ústředních motivů zprávy Zvláštního zpravodaje Valného shromáždění OSN k zásadním problémům práva na svobodu projevu – viz kap. IV., část E, Report of the Special Rapporteur on thepromotion and protection of the right to freedom of opinion and expression, Frank La Rue, č. A/HRC/17/27, ke stažení on-line na adrese www.ohchr.org.

[48] K tomu srov. např. Yoo, C. S. Network Neutrality and the Economics of Congestion. *Georgetown Law Journal*, roč. 94, str. 1847 a násl.

[49] K důležitosti tohoto principu vzhledem k fungování síťových efektů, na nichž je prakticky založen další rozvoj naší kultury v nejširším smyslu slova, viz např. Zittrain, J. The Generative Internet. *Harvard Law Review*, roč. 119, str. 1974.

Vedle toho tento princip zohledňuje i značnou rozmanitost informačních sítí a systémů, jichž se dotýká. Pokud by byla úprava rigorózní co do specifikace konkrétních povinností, znamenalo by to buďto definovat nespočet variant dle rozsahu a funkcí příslušných sítí a systémů nebo pracovat s předpokladem, že standardní zákonné varianty budou vyhovovat co do efektivity vynaložených investic pouze některým subjektům – to by v konečném důsledku vedlo na jedné straně k tomu, že by byly některé subjekty nuceny investovat prostředky do bezpečnostních opatření, která by byla vzhledem k charakteru příslušných systémů přehnaně rozsáhlá a jiné subjekty by naopak ani při splnění zákonných požadavků neochránily svoji infrastrukturu v dostatečném rozsahu. Namísto toho volí zákon stanovení cílového stavu, tj. požadované úrovně funkčnosti bezpečnostních opatření, přičemž ponechává regulovaným subjektům relativní volnost ve volbě konkrétních nástrojů pro jeho dosažení. To ostatně odpovídá i jedné ze shora zmíněných komponent principu technologické neutrality, neboť zákonné podmínky lze splnit nespočtem typů různých bezpečnostních řešení založených na technologiích od různých vzájemně si konkurujících dodavatelů.

Druhým aspektem autonomie vůle je možnost dobrovolné spolupráce soukromoprávních subjektů stojících mimo osobní působnost zákona s národním dohledovým pracovištěm. Přestože se tato zákonná konstrukce jeví být na první pohled absurdní, lze o tuto formu spolupráce očekávat velký zájem především mezi subjekty, které jsou předmětem zvýšené bezpečnostní expozice, ať už jde o aktivistické útoky na jejich infrastrukturu, konkurenční boj, průmyslovou špionáž apod. Spoluprací s národním dohledovým pracovištěm mohou tyto subjekty získat nejen přehled o tom, jaká je v reálném čase bezpečnostní situace v české informační a komunikační infrastruktuře (a tím i schopnost reagovat na aktuální kybernetické hrozby v předstihu), ale mohou získávat i průběžnou metodickou a koordinační pomoc při řešení kybernetických bezpečnostních incidentů. Nadto bude pro subjekty nabízející služby informační společnosti představovat dobrovolná spolupráce s národním dohledovým pracovištěm přidanou hodnotu, kterou budou moci prezentovat svým klientům.

Z hlediska povinných soukromoprávních subjektů však má inkorporace principu autonomie vůle též jeden problematický aspekt. Právní úprava

totiž nepočítá s tím, že by měly povinnost nechat si ex ante schvalovat nebo nějak potvrzovat vlastní řešení kybernetické bezpečnosti vzhledem ke splnění standardních zákonných požadavků. Především u středních a velkých podniků a veřejnoprávních korporací investujících podstatné prostředky do rozvoje své informační a komunikační infrastruktury je přitom stěžejní otázkou tzv. compliance, tj. ex ante kontrolovaného plnění zákonných požadavků příslušné jurisdikce. Je totiž z ekonomického hlediska neúčelné pro tyto subjekty investovat do rozvoje vlastní infrastruktury určité prostředky a přitom nemít jistotu, že tyto investice negenerují nějaké právní riziko[50]. Skutečnost, že zákon ve své struktuře neobsahuje explicitní povinnost certifikace nebo jiného schválení příslušných technických a organizačních řešení tedy je na první pohled pro regulované subjekty příznivá, neboť jim nevznikají další náklady spojené se schvalovacími procesy. Středním a velkým povinným subjektům však může způsobit zvýšení míry rizikovosti jejich investic do informační a komunikační infrastruktury, neboť neposkytuje ex ante jistotu, že jimi implementovaná bezpečnostní řešení skutečně bezezbytku plní zákonné požadavky. Nabízí se samozřejmě řešení formou regresní odpovědnosti dodavatelů – takové řešení však již není otázkou compliance a pro střední a velké subjekty představuje jen těžko postižitelné právní a ekonomické riziko[51].

Princip bdělosti ve vztahu k mezinárodnímu společenství a ostatním suverénním státům se v navrhované právní úpravě projevuje už samotnou skutečností, že se Česká republika snaží při vynaložení podstatného úsilí dostat pod kontrolu bezpečnostní problémy vyskytující se pod její jurisdikcí. Obecně totiž tento princip zakládá odpovědnost státu za škodlivé následky způsobené ostatním státům v důsledku porušení mezinárodního práva veřejného v situacích, kdy stát mohl takovému porušení zabránit.

V situaci, kdy je infrastruktury na území státu zneužito k provedení kybernetického útoku s dopady v zahraničí, mají postižené státy a mezinárodní společenství důvod ptát se, zda škodlivým následkům nebylo možno zabránit. Existují-li popsané způsoby, jak předejít kybernetickým

[50] Srov. Weill, P., Woodham, R. Don't Just Lead, Govern: Implementing Effective IT Governance. *MIT Sloan Working Paper No. 4237-02*, 2002, dostupné on-line na adrese http://ssrn.com/abstract=317319.

[51] Podrobněji k tomuto problému viz dále.

útokům resp. zneužití informační a komunikační infrastruktury, a kdy je implementace nejrůznějších bezpečnostních opatření nejen technicky možná ale též ekonomicky a sociálně akceptovatelná, pak má stát typu České republiky nikoli pouze právo ale přímo povinnost řešit svou vlastní kybernetickou bezpečnost[52].

4. INSTITUTY ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Před výkladem k jednotlivým institutům je nutno vyjádřit se ke třem populárním mýtům vztahujícím se k právu kybernetické bezpečnosti. První z nich týká se smyslu a účelu specifické legislativy a je založen na předpokladu, že právní předpis upravující práva a povinnosti k zajištění národní kybernetické bezpečnosti má ve svém textu obsahovat pro jednotlivé zainteresované subjekty komplexní návod na to, jak se správně chovat respektive důkladný popis toho, co je zakázáno. Zvláštní zákon upravující oblast národní kybernetické bezpečnosti však nemá a ani nemůže sloužit jako kuchařka – namísto toho má pouze v minimální formě upravit specifické povinnosti povinným subjektům a dále pak založit kompetence institucím, do jejichž působnosti tato oblast spadá. Je přitom třeba vycházet nikoli z předpokladu, že všem zainteresovaným je třeba zákonem detailně a nekompromisně sdělit, co mají nebo nemají dělat, ale že:

1. právo není jen zákon – konkrétní obsah zákonných povinností nebývá nutně specifikován pouze zákonem, ale může být též např. otázkou judikatury či aplikace obecných či zvláštních právních principů. Z toho mj. plyne i skutečnost, že zákon může zůstat relativně rigidní, ale obsah platného práva se může v čase výrazně měnit[53],
2. soukromým subjektům mají být zákonem stanoveny pouze konkrétní příkazy nebo zákazy – dovolené jednání není třeba

[52] Tato doktrína je ještě na počátku svého vývoje, ale lze při mírném optimismu předpokládat její brzké uplatnění v praxi – viz Glennon, M. The Dark Future of International Cybersecurity Regulation, *Journal of National Security Law and Policy*, roč. 6, str. 563.

[53] Výmluvně to ilustruje Gustav Radbruch v článku Zákonné neprávo a nadzákonné právo původně publikovaným jako Radbruch, G. Gesetzliches Unrecht und übergesetzliches Recht, *Süddeutsche Juristenzeitung*, roč. 1946, str. 105–108.

vymezovat, neboť tyto subjekty mohou činit vše, co jim zákon nezakazuje[54],

3. orgánům veřejné moci má zákon vymezit působnost, stanovit povinnosti a možnosti autoritativního jednání (orgány veřejné moci mohou totiž oproti subjektům soukromého práva dělat jen to, co jim zákon výslovně ukládá nebo umožňuje)[55],
4. není vhodné ani potřebné upravovat to, co upravují jiné právní předpisy nebo mezinárodní smlouvy resp. zakládat povinnosti, které jsou již založené jinými částmi našeho právního řádu. Z toho plyne též obecná nutnost strukturovat a formulovat zákon tak, aby do systému platného práva nevnášel redundantní nebo nekoherentní prvky[56],
5. předmětem zákona je právní povinnost a normativními modalitami jsou příkaz, zákaz a dovolení. Co z nějakého důvodu není možné nebo účelné definovat jako právní povinnost prostřednictvím některé z těchto modalit, nemá v psaném právu co pohledávat. Typickým příkladem jsou technické standardy nemající charakter právních povinností a
6. zákon nesmí odporovat Ústavnímu pořádku České republiky – žádná zákonem založená právní povinnost nesmí vybočovat z rámce proporcionality základních práv člověka a nedistributivních práv státu[57].

Z právě uvedeného mimo jiné vyplývá, že právní úprava kybernetické bezpečnosti České republiky není ani zdaleka tvořena jen zákonem o kybernetické bezpečnosti. Povinnosti při ochraně informační a komunikační infrastruktury totiž kromě něj zakládá i řada dalších součástí českého právního řádu. Následující výklad je zaměřen na instituty, které se z hlediska zajištění kybernetické bezpečnosti jeví jako

[54] Viz čl. 2 odst. 3 Listiny základních práv a svobod.

[55] Viz čl. 2 odst. 2 Listiny základních práv a svobod.

[56] V tomto případě jde o komponenty označované právní teorií jako tzv. materiální náležitosti právotvorby normativního typu. K náležitostem i technice české právotvorby viz např. Šín Z.: *Tvorba práva*. Praha: C. H. Beck, 2003.

[57] Proporcionalita je metoda poměřování právních principů, přičemž charakter právních principů mají i všechna ústavně zaručená základní práva. K používání této metody v českém právním prostředí viz učebnici Holländer, P. *Filosofie práva*, 2. Vydání, Plzeň: Aleš Čeněk, 2012.

nejdůležitější z pohledu povinných subjektů. Konkrétně se budeme věnovat otázkám

1. bezpečnostních opatření
2. protiopatření
3. odpovědnosti za nedbalost a prevenčních povinností
4. disciplinární odpovědnosti a disciplinárních povinností

4.1 BEZPEČNOSTNÍ OPATŘENÍ

Bezpečnostní opatření jsou základním kamenem zákona o kybernetické bezpečnosti a z operačního hlediska i jeho zdaleka nejdůležitější součástí[58]. Primárním účelem zákona totiž není řešení jednotlivých kybernetických bezpečnostních incidentů ale vytvoření prostředí, v němž jsou kritická informační a komunikační infrastruktura státu a další zájmové informační systémy a sítě preventivně chráněny tak, že pro ně žádná kybernetická bezpečnostní událost nepředstavuje bezpečnostní riziko.

Zákon sám zavádí povinným subjektům pouze základní povinnost mít bezpečnostní opatření v taxativně vymezených kategoriích, přičemž technické podrobnosti upravuje prováděcí předpis[59]. Zákon je postaven na dokumentačním modelu, tj. ukládá povinným subjektům povinnost především dokumentovat jednotlivé typy bezpečnostních opatření a následně pak dává právo Národnímu bezpečnostnímu úřadu kontrolovat, zda je dokumentace souladná nejen s konkrétními požadavky zákona a prováděcího předpisu, ale samozřejmě též s aktuální skutečností.

Smyslem bezpečnostních opatření je primárně vytvoření takových preventivních mechanismů, které povinným subjektům umožní vyrovnávat se autonomně k kybernetickými bezpečnostními událostmi (ať už jde o prevenci jejich samotného vzniku nebo o nástroje a mechanismy k jejich následnému pokrytí)[60]. Subsidiárně jsou pak bezpečnostní opatření formulována tak, aby jejich zavedení umožnilo efektivní fungování

[58] Zákon je v § 4 odst. 1 vymezuje jako „souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru“.

[59] Viz vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

[60] Za tímto účelem dělí zákon bezpečnostní opatření na organizační a technická a ty pak dále specifikuje v ust. § 5 odst. 2 a 3.

kybernetických bezpečnostních struktur na úrovni státu, tj. především národního a vládního dohledového pracoviště.

Systematickým problémem bezpečnostních opatření, kterému jsme se už stručně věnovali výše, je skutečnost, že jsou formulována jako technický a organizační standard, aniž by však zákon předpokládal existenci oficiálních certifikačních nebo jiných a priori procedur použitelných k verifikaci jejich kvality. Povinné subjekty tedy budou investovat do akvizic nebo úprav příslušných bezpečnostních řešení, aniž by měly možnost a priori ověřit, zda to, čím se snaží plnit zákonné požadavky skutečně je nebo není v souladu se zákonem resp. s prováděcím předpisem.

4.2 PROTIOPATŘENÍ

Protiopatřeními pro potřeby tohoto textu souhrnně nazýváme to, co zákon označuje jako „opatření“ a dělí dle typu na varování, reaktivní opatření a ochranná opatření. Všechny typy protiopatření mají povahu vrchnostenské činnosti Národního bezpečnostního úřadu, přičemž varování má charakter informativní a zbývající dvě opatření mají formu závazných individuálních právních aktů resp. opatření obecné povahy.

Institut varování může se zdát na první pohled zbytečným, neboť jeho užití nepřináší bezprostřední imperativ ani riziko přímé sankce[61]. Jeho charakter však vystihuje typický efekt zákona o kybernetické bezpečnosti v otázkách odpovědnosti za kybernetické bezpečnostní incidenty. Zákon totiž ani u imperativních institutů nepřináší žádné přímé drakonické sankce, ale zavádí přímo nebo nepřímo nové typy právních povinností, jejichž neplnění může mít za následek vznik povinnosti nahradit škodu. Povinný subjekt tedy nemůže kalkulovat právní riziko plynoucí z nově založených zákonných povinností pouze ve vztahu k možné pokutě (ta je co do své výše spíše symbolická) ale též vzhledem k velmi neurčitému potenciálu škod, k nimž může dojít v důsledku zaviněného[62] i nezaviněného[63] kybernetického bezpečnostního incidentu.

[61] Viz § 12 ve spojení s § 25 zákona č. 181/2014 Sb.

[62] Odpovědnost je v tomto případě založena na základě obecných ust. § 2910 a násl. zákona č. 89/2012 Sb., občanský zákoník.

[63] V úvahu zde u podnikatelských subjektů připadá povinnost nahradit škodu způsobenou provozní činností na základě § 2924 zákona č. 89/2012 Sb.

V případě varování tedy Národní bezpečnostní úřad sice provádí pouze adresnou osvětu ohledně konkrétních bezpečnostních rizik, ta ale ve svém důsledku vede k prokazatelné informovanosti povinných subjektů. Zprostředkovaně tím přináší povinným subjektům možnost založení povinnosti nahradit škodu způsobenou tím, že na základě varování nepřijmou přiměřená opatření k zabránění vzniku kybernetických bezpečnostních incidentů nebo zmírnění jejich následků[64].

V typickém případě tedy bude Národní bezpečnostní úřad formou varování informovat o konkrétním bezpečnostním riziku (např. o tzv. bezpečnostní díře) – jestliže povinné subjekty nebudou na základě této informace za vynaložení přiměřeného úsilí na takto identifikované riziko reagovat (např. instalací záplat) a v důsledku toho dojde ke škodě u třetích osob, mohou třetím osobám povinné subjekty přímo odpovídat z titulu nesplnění prevenční povinnosti. Je-li pak v této situaci způsobena škoda i samotnému povinnému subjektu, může být shora popsaný nedostatek reakce na varování též důvodem pro pojišťovnu, aby odmítla nebo výrazně snížila hodnotu pojistného plnění.

Z hlediska povinných subjektů tedy přináší i na první pohled bezzubý institut varování nový typ právního rizika, které je a priori jen velmi těžko ohodnotitelné – čím větší je přitom povinný subjekt a čím více spravuje systémů spadajících pod rozsah zákona o kybernetické bezpečnosti, tím je toto riziko závažnější, a to co do své potenciální hodnoty i do míry nepředvídatelnosti svého výskytu. Dokonce lze s trochou nadsázky konstatovat, že s rostoucí velikostí můžeme sledovat u povinných subjektů klesající míru zájmu o přímé sankce zákona o kybernetické bezpečnosti (tj. o pokuty) a naopak rostoucí zájmovost nepřímých sankcí ve formě právě popsaného potenciálu povinností k náhradě škody resp. limitace pojistného plnění[65].

Další dva typy protiopatření již disponují v porovnání s varováním též přímou možností autoritativního vynucení. Zákon definuje jejich věcný rozsah velmi široce - prakticky jde o jakákoli opatření „k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení

[64] K tomu srov. § 2901 zákona č. 89/2012 Sb.

[65] K nim ještě přistupují jen těžko vyčíslitelné náklady spojené s případnou kontrolou a realizací adresně uložených opatření k nápravě ve smyslu § 24 zákona č. 181/2014 Sb.

informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem“[66]. V tomto směru ale nelze na rozdíl od některých bulvárních názorů uvažovat o tom, že by takto široce definovaná věcná působnost příslušných správních rozhodnutí nebo opatření obecné povahy dávala Národnímu bezpečnostnímu úřadu do rukou nějaký totalitní nástroj ke kontrole národní informační a komunikační infrastruktury. Vedle konkrétního omezení smyslem a účelem protiopatření (resp. reaktivních nebo ochranných opatření) je v tomto případě Národní bezpečnostní úřad standardně omezen působností zákona a dále pak obecnými principy správního práva, z nichž nejdůležitějšími jsou zřejmě principy dobré správy[67] a zákaz svévole.

V rovině ústavního práva pak je Národní bezpečnostní úřad omezen především judikatorní doktrínou tzv. omezeného testu proporcionality[68]. Národní bezpečnostní úřad má tedy implicitní povinnost vybrat pro příslušné reaktivní nebo ochranné opatření takovou alternativu, která bude povinné subjekty nejméně zatěžovat.

Imperativní protiopatření zákon dělí z hlediska jejich účelu na reaktivní a ochranná. První jmenovaný typ se uplatní v případech hrozícího nebo probíhajícího konkrétního kybernetického bezpečnostního incidentu. Tomu odpovídá i procesní charakteristika reaktivních protiopatření zahrnující ve správním právu spíše výjimečné instituty okamžité vykonatelnosti a absence odkladného účinku řádného opravného prostředku (v tomto případě rozkladu)[69].

Okamžitost a bezprostřednost imperativního účinku reaktivních protiopatření odpovídá jejich charakteru jakožto bezpečnostních nástrojů výkonné moci. Přestože bylo nutno z hlediska procesní formy dostát požadavkům správního práva na dokonalý proces autoritativní aplikace, je zřejmé, že v tomto případě nejde o klasickou exekutivní aplikaci práva, ale spíše o konkrétní vrchnostenský zásah vedoucí k pokrytí okamžité

[66] Viz § 13 odst. 1 zákona č. 181/2014 Sb.

[67] K pojmu viz např. Košičiarová, S. *Princípy dobrej verejnej správy a Rada Európy,* Bratislava: Iura Edition, 2012, 556 s.

[68] Jako omezený test proporcionality označuje se výstupní část standardního testu proporcionality, která spočívá v hodnocení míry zásahu do zájmu chráněného právním principem. Platí přitom, že zásah do práv osoby nesmí být větší, než je vzhledem k okolnostem pragmaticky nutné – srov. Holländer, P. *Filosofie práva*, 2. Vydání, Plzeň: Aleš Čeněk, 2012.

[69] Srov. § 15 zákona č. 181/2014 Sb.

bezpečnostní hrozby. Připodobnit jej lze namísto jiných procesů, na jejichž konci stojí vykonatelné správní rozhodnutí (resp. opatření obecné povahy), spíše k okamžité akci bezpečnostní složky výkonné moci, tj. např. k fyzickému zásahu policie[70].

V tomto případě však z podstaty věci plyne, že Národní bezpečnostní úřad nemá možnost provést takový zásah autonomně[71]. Exekutivní reakce k zajištění národní kybernetické bezpečnosti tedy v tomto případě nemůže mít povahu přímé akce bezpečnostní složky státu, ale pouze vrchnostenského imperativu vedoucího k akci subjektu, o jehož informační systém nebo síť se jedná. Nemaje ve správním právu jiného použitelného institutu, sáhl tedy v tomto případě právotvůrce logicky po institutu správního rozhodnutí resp. opatření obecné povahy.

Ochranná opatření mají naproti tomu svou náturou blíže ke klasickému správnímu rozhodování resp. k vrchnostenské podzákonné normotvorbě, neboť jde o imperativy, jejichž implementace, lidově řečeno, až tak nehoří. Jejich podkladem jsou rovněž konkrétní kybernetické bezpečnostní incidenty, ale jejich smyslem a účelem není bezprostřední reakce, nýbrž zvýšení úrovně bezpečnosti příslušných informačních systémů a sítí[72]. Především v případech, kdy jsou ochranná opatření vydávána formou opatření obecné povahy neurčitému okruhu adresátů je lze vlastně z funkčního hlediska považovat za doplněk podzákonného předpisu konkretizujícího obsah bezpečnostních opatření.

4.3 ODPOVĚDNOST ZA NEDBALOST A PREVENČNÍ POVINNOSTI

Přestože sám zákon o kybernetické bezpečnosti se tomuto typu odpovědnosti z pochopitelných důvodů vůbec nevěnuje, představuje pro povinné subjekty možnost odpovědnosti za vědomou či nevědomou nedbalost resp. za nesplnění prevenční povinnosti zřejmě nejsilnější právní motivační faktor k faktické realizaci bezpečnostních opatření.

---

[70] Nabízí se zde například srovnání s pravomocemi policie při zajišťování bezpečnosti chráněných prostorů, objektů a osob ve smyslu ust. § 48 odst. 4 zákona č. 273/2008 Sb., o Policii české republiky, ve znění pozdějších předpisů.

[71] K tomu viz shora konstatovaný specificky rys kybernetické bezpečnosti spočívající ve zprostředkovanosti veškerých aktivit službami informační společnosti.

[72] Srov. § 14 zákona č. 181/2014 Sb.

Odpovědnost v tomto případě znamená, jak bylo uvedeno shora, nejen potencialitu povinnosti nahradit škodu způsobenou třetím osobám v důsledku nedbalosti nebo opomenutí preventivního zásahu, ale též srovnatelně důležité riziko krácení nebo ztráty nároku na pojistné plnění u škod na vlastním majetku[73] resp. na vlastní činnosti nebo i riziko subsidiární sankce za nesplnění povinnosti specificky regulovaného odvětví (např. v oblasti energetiky[74]).

K právě uvedeným typům odpovědnostních důsledků lze ještě připočíst riziko prodlení v případech, kdy kybernetický bezpečnostní incident způsobí neschopnost povinného subjektu plnit jiné právní povinnosti. Typicky může například dojít k situaci, kdy má povinný subjekt povinnost dodávat svým odběratelům zboží nebo služby a v důsledku kybernetického bezpečnostního incidentu toho není po nějakou dobu schopen. Za předpokladu, že kybernetický bezpečnostní incident vedl k takovým důsledkům kvůli neschopnosti povinného subjektu splnit si zákonnou povinnost vyplývající ze zákona o kybernetické bezpečnosti, nebude se povinný subjekt moci bránit poukazem na tento incident proti nárokům třetím osob z vadného resp. pozdního plnění.

To samozřejmě neznamená, že by povinné subjekty měly důvod obávat se toho, že budou odpovídat za veškeré škody způsobené třetím osobám kybernetickými bezpečnostními incidenty, na nichž se bude nějakým způsobem podílet jejich nedostatečně zabezpečená informační a komunikační infrastruktura. Ani v případě, byla-li by škoda třetím osobám skutečně způsobena v důsledku zanedbání specifických povinností plynoucích ze zákona o kybernetické bezpečnosti (resp. z jeho imperativních institutů), nejednalo by se ze strany povinného subjektu zřejmě o povinnost výlučnou – tam, kde byla např. v důsledku nedbalosti povinného subjektu zneužita jeho infrastruktura k provedení kybernetického útoku, zkoumal by soud u povinného subjektu míru jeho zavinění resp. míru toho, jak se nedbalá realizace opatření k zajištění

[73] K tomu viz zejm. ust. § 2800 odst. 2 zákona č. 89/2012 Sb.

[74] Vedle pokut či opatření k nápravě může jít též o nebezpečí odnětí licence nebo jiného povolení k výkonu specifické činnosti – tuto možnost dává národním regulátorům úprava např. v oblasti energetiky nebo elektronických komunikací – srov. zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), ve znění pozdějších předpisů) nebo zákon č. 127/2005 Sb, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

kybernetické bezpečnosti podílela na celkovém škodním dopadu příslušného kybernetického bezpečnostního incidentu[75].

Za připomenutí stojí v této souvislosti především typologie nedbalostního zavinění sestávající vedle vědomé (tj. hrubé – culpa lata) nedbalosti též z nedbalosti nevědomé (tj. lehké – culpa levis)[76]. Za zaviněné porušení právní povinnosti se tak považují nejen situace, kdy má povinný subjekt prokazatelně k dispozici informace o hrozícím nebezpečí a vlastní liknavostí nezabrání škodlivému následku, ale také případy, kdy povinný subjekt sice těmito informacemi objektivně nedisponuje, ale opatřit si je měl a mohl. Ve vztahu ke shora zmíněnému institutu varování to mimo jiné znamená, že ze strany povinného subjektu nebude možno namítat například nefunkčnost povinně sdělované kontaktní adresy nebo interní komunikační problémy v rámci organizace, kvůli kterým se informace o varování vydaném Národním bezpečnostním úřadem nedostane na správné místo.

Nedbalost nebo nesplnění prevenční povinnosti každopádně nemusí mít, jak bylo naznačeno výše, důsledky pouze soukromoprávní. Řada povinných subjektů působí v odvětví, která mají specifickou a často i poměrně rigorózní správní regulaci – příkladem může být energetika, elektronické komunikace, tzv. jiné utility (odpadové hospodářství, distribuce vody apod.), zdravotnictví nebo potravinářství. Ve většině z těchto odvětví mají povinné subjekty nejen povinnosti vztahující se bezprostředně k příslušnému typu činnosti, ale též související povinnosti, z nichž podstatná část se může přímo nebo nepřímo týkat provozu vnitřních informačních systémů nebo komunikačních sítí. Pokud v takovém případě dojde k narušení regulované činnosti povinného subjektu v důsledku kybernetického bezpečnostního incidentu, který povinný subjekt nedokázal zvládnout v důsledku nedbalosti nebo porušení prevenční povinnosti, může to pro něj znamenal vedle shora uvedených odpovědnostních rizik též možnost postihu dle specifických pravidel příslušného regulovaného

[75] V tomto případě je specifický charakter kybernetických bezpečnostních incidentů společně s charakterem účasti způsobené nedůslednou ochranou vlastního systému možno obecně považovat za okolnosti hodné zvláštního zřetele a je tedy důvod předpokládat, že povinnost nahradit škodu bude v tomto případě specifikována dle míry zavinění resp. dle míry účasti – k tomu viz § 2915 odst. 2, první věta zákona č. 89/2012 Sb.

[76] Viz např. Knapp, V. Některé úvahy o odpovědnosti v občanském právu. *Stát a právo* I. roč. 1956, str. 66.

odvětví. Není pak v tomto směru žádným tajemstvím, že např. pro subjekty v oboru energetiky může být takový subsidiární sankční postih dle energetického zákona nepoměrně citelnější, než primární sankce plynoucí ze zákona o kybernetické bezpečnosti.

Všechna shora uvedená právní rizika jsou v porovnání s imperativními a sankčními mechanismy zákona o kybernetické bezpečnosti pro povinné subjekty nejen mnohem závažnější, ale také co do svého důsledku mnohem méně předvídatelná. Zatímco lze vcelku snadno odhadnout, jaká výše pokuty hrozí při neprovedení reaktivního protiopatření, jen těžko se dá z pohledu povinného subjektu odhadovat, jaký dopad může mít tatáž situace z pohledu soukromoprávní odpovědnosti vůči poškozeným třetím osobám, jak velká vymahatelná škoda může vzniknout zákazníkům nebo jak bude reagovat regulátor příslušného specifického odvětví (např. Energetický regulační úřad, český telekomunikační úřad apod.)

Velká míra této subsidiární právní rizikovosti ve spojení s absencí oficiálních compliance procedur vytváří na povinné subjekty tlak projevující se v důsledku jednak chvályhodnou vůlí investovat do bezpečnostních opatření, to dokonce často i vysoko nad rámec zákonných požadavků. Kromě toho však může tato nejistota vést k tomu, že se povinné subjekty budou za každou cenu snažit o únik z osobního rozsahu zákona nebo se budou pokoušet o různé ohýbání jeho pravidel. Zabránit tomuto efektu by kromě nezávislých certifikačních procedur mohla též osvětová činnost Národního bezpečnostního úřadu realizovaná ve spolupráci s odvětvovými regulátory nebo rozšíření nabídky pojistných či zajišťovacích finančních produktů. Svou nezastupitelnou roli pak budou jistě hrát i odvětvové organizace, které mohou vedle zprostředkování komunikace mezi povinnými subjekty a Národním bezpečnostním úřadem působit i v rovině vzdělávací, koordinační nebo poradenské.

4.4 DISCIPLINÁRNÍ ODPOVĚDNOST A DISCIPLINÁRNÍ POVINNOSTI

Shora diskutovaná bezpečnostní opatření mají vést k tomu, že povinné subjekty budou mít systematicky řešenu kybernetickou bezpečnost tak, aby kybernetické bezpečnostní incidenty buďto nevznikaly nebo aby jejich výskyt neznamenal bezpečnostní riziko. Nástroje, s nimiž bezpečnostní

opatření počítají, lze z pohledu platného práva rozdělit do následujících základních skupin:

1. Technické prvky (specifický software a hardware vč. detekčních systémů, reportovacích nástrojů, autentizačních či kryptografických nástrojů, technika k zajištění fyzické bezpečnosti apod.)
2. Analytické prvky a dokumentace (typicky analýza informačních aktiv, topografie sítí, analýza rizik apod.)
3. Interní předpisy (organizační opatření, školící plány, krizové plány, interní instrukce pro vybrané skupiny zaměstnanců, interní pravidla pro nákup a outsourcing ICT apod.)
4. Lidské zdroje (specificky vyčleněný personál k zajištění realizace bezpečnostních opatření nebo personál zajišťující výjimečně ad hoc určité činnosti v oblasti kybernetické bezpečnosti)

Poslední dvě uvedené kategorie týkají se vztahu povinného subjektu a jeho pracovníků, ať už jde o zaměstnance nebo obdobně působící externisty. Běžné fungování specificky vyčleněného personálu nebo pracovníků, jimž mohou být úkoly v oblasti kybernetické bezpečnosti ukládány ad hoc, jsou pro existenci a efektivitu bezpečnostních opatření kriticky důležité. Sebelépe postavený a vybavený bezpečnostní systém totiž není k ničemu, pokud není adekvátně obsluhován resp. pokud jeho fungování brání faktická bezpečnostní rizika představovaná vlastními pracovníky povinných subjektů.

Z právního hlediska jde především o otázku povinností, které pracovníkům povinných subjektů ukládá zákon resp. povinností, které na základě zákona svým pracovníkům ukládají povinné subjekty formou interních instrukcí nebo běžné řídící činnosti v rámci korporátní hierarchie[77]. V tomto směru je předně nutno rozlišovat mezi pracovníky, jejichž pracovní náplň souvisí s tvorbou nebo realizací bezpečnostních opatření a pracovníky, jimž jsou pouze na základě bezpečnostních opatření ukládány konkrétní povinnosti s tím, že jejich běžná pracovní náplň s kybernetickou bezpečností jinak nesouvisí (tj. uživatele).

[77] Rozdíl mezi interní instrukcí a aktem řízení spočívá v tom, že zatímco interní instrukce je určena neurčitému okruhu pracovníků splňujících určitou podmínku (např. pracovníkům v určité funkci), je akt řízení adresován, tj. určen konkrétnímu člověku. K povaze interní instrukce viz např. Galvas, M. a kol. *Pracovní právo*. Brno: Masarykova univerzita, 2012, str. 50 nebo Vysokajová, M. *Zákoník práce - komentář*. Praha : Wolters Kluwer, 2012, str. 623.

Bezpečnostní personál nebo pracovníky, u nichž alespoň část běžné pracovní agendy představuje kybernetická bezpečnost lze logicky zatížit nejen větším množstvím pracovních povinností oblasti kybernetické bezpečnosti, ale lze od nich požadovat i vyšší míru odborné erudice a schopnosti plnit specifické požadavky interních bezpečnostních předpisů. Bezpečnostnímu technikovi, správci sítě nebo systémovému administrátorovi tak lze nejen uložit řadu specifických pracovních povinností, jejichž předmětem může být zabezpečení příslušné informační a komunikační infrastruktury, ale tyto povinnosti lze na úrovni interních předpisů nebo individuálních řídících aktů (tj. v rámci běžného podnikového řízení) formulovat i s vysokou mírou odbornosti a spoléhat přitom na adekvátní předvědění.

U profesí, jejichž pracovní náplň netvoří kybernetická bezpečnost, je naproti tomu v případě definice povinností týkajících se bezpečnosti informačních systémů a sítí nutno postupovat tak, aby interní instrukce nebo jiné akty řízení byly obecně srozumitelné a aby byly z pohledu běžného pracovníka technicky proveditelné. Z toho plyne, že například instrukce typu „uživatel je povinen měnit své přístupové heslo minimálně jednou týdně, heslo musí mít min. 15 znaků, z nichž min. 7 znaků musí být speciální znaky ASCII“ je vadná hned ze dvou důvodů. Jednak není možno rozumně požadovat po běžném uživateli, aby si každý týden zapamatoval nové patnáctiznakové heslo a navíc nelze předpokládat, že bude poučen v tom smyslu, co to jsou speciální znaky ASCII. Takto formulovaná interní instrukce tedy, byť její přečtení příslušný zaměstnanec potvrdí třeba podpisem vlastní krví, nikdy nepovede k právně vynutitelnému závazku.

Z právě uvedeného plyne, že problém disciplinární odpovědnosti zaměstnanců vzhledem k bezpečnostním opatřením zaváděným u povinných subjektů mandatorně na základě zákona o kybernetické bezpečnosti spočívá primárně ve způsobu, kterým budou různým kategoriím pracovníků ukládány příslušné bezpečnostní povinnosti. Neexistuje přitom žádná konkrétní judikatura, o kterou by bylo možno se opřít, to i přes skutečnost, že typově podobná situace jako v případě kybernetické bezpečnosti objevuje se dlouhodobě například v oblasti protipožární ochrany nebo bezpečnosti práce. Případy, jejichž autoritativní řešení máme k dispozici jako vodítko, týkají se spíše frapantních porušení

interních předpisů nebo jiných řídících aktů a neposkytují tím pádem adekvátní návod pro diskutabilní či hraniční případy. Ještě žádného zaměstnavatele tak doposud nenapadlo například žalovat o náhradu škody zaměstnance, který, byť byl proškolen v použití hasicího přístroje, vzal raději před požárem v odpadkovém koši nohy na ramena.

Problematika závaznosti respektive míry závaznosti interních instrukcí na úseku kybernetické bezpečnosti každopádně představuje zajímavé a vysoce žádoucí zadání, jehož řešením se česká právní věda již intenzivně zabývá[78] – přestože by ale měly být základní doktrinální poznatky k těmto otázkám k dispozici v řádů měsíců či jednotek let, budou povinné subjekty vystaveny právní nejistotě až do doby, kdy bude k dispozici adekvátní judikatura vyšších soudů.

Na tomto místě je nutno připomenout, že právě uvedené týká se pouze specifických bezpečnostních povinností, jejichž existence je podmíněna zvláštní autoritativní informací prokazatelně sdělenou zaměstnanci. Zaměstnavatel však samozřejmě nemusí zaměstnanci formou interních instrukcí nebo jiných řídících aktů sdělovat všechny možné požadavky na bezpečné fungování informačních systémů a sítí. Každé pracovní pozici totiž odpovídá implicitně předpokládaná odborná výbava zaměstnance, s níž zaměstnavatel může počítat a kterou nemusí ani zvlášť ověřovat.

Pracovní pozice, u níž se předpokládá znalost práce s osobním počítačem, tedy implicitně předpokládá, že bude zaměstnanec bez dalšího chápat například zákaz psaní přístupových hesel na žluté lístečky a jejich lepení na okraj monitoru (podobně není nutno kancelářské síly školit například v tom, že nemají strkat kancelářské sponky do elektrických zásuvek nebo v pracovní době skákat z oken). Analogicky pak bude zřejmě možno ze strany zaměstnavatele i bez nutnosti přijímat interní instrukce předpokládat, že systémový administrátor je obeznámen se skutečností, že nesmí používat triviální heslo nebo že se má při každém odchodu od počítače odhlásit ze své virtuální identity. Ani v těchto otázkách však nemáme k dispozici žádnou použitelnou judikaturu a vyjma evidentních případů lze spíše předpokládat, že soudy nebudou příliš respektovat presumpci nedbalostního zavinění a budou spíše v případě sporu požadovat

[78] Viz např. aktuálně řešený projekt GAMU MUNI/M/1052/2013, Experimentální výzkum chování uživatelů ICT v oblasti bezpečnosti perspektivou sociálních věd, práva a informatiky.

po zaměstnavateli důkaz skutečnosti, že zaměstnanec příslušné bezpečnostní pravidlo znát mohl a hlavně, že jej vzhledem ke svému pracovnímu zařazení znát měl[79].

5. PERSPEKTIVY DALŠÍHO VÝVOJE ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Shora provedená analýza má, jak bylo na několika místech zvlášť zdůrazněno, pouze doktrinální charakter a bez specifické judikatury nelze konstatovat konkrétní tvar jednotlivých institutů aktuálně tvořících českého právo kybernetické bezpečnosti. I v případě právních nástrojů, které již máme v našem právu k dispozici, totiž není jasno v tom, jaké formy může mít jejich aktuální aplikace. Diskutovat za této situace možnosti dalšího vývoje našeho práva kybernetické bezpečnosti je tedy podobno věštění z kávové sedliny.

Následující výklad je zaměřen především na možnosti dalšího vývoje české legislativy, přičemž vychází kromě shora diskutovaného současného stavu též z tendencí patrných v zahraničních právních řádech. České právo má v této souvislosti určitou výhodu spočívající v tom, že máme přístup k dobrým i špatným zkušenostem s různými typy legislativních nástrojů ze států, pro které kybernetická bezpečnost představovala a představuje v porovnání s naší situací daleko naléhavější problém. Můžeme se tedy díky spojeneckým svazkům a tradičním přátelským vazbám poučit ze zkušeností realizovaných v podobném právním prostředí, tj. v situaci standardního demokratického právního státu, ve státech, které kvůli své velikosti nebo zahraničněpolitické aktivitě staly se terčem závažných kybernetických útoků dříve a ve větší míře, než je tomu u nás.

Skutečnost, že v případě USA, Spojeného království nebo například Izraele jde o země fungující na jiných právně-kulturních základech, v tomto případě nebrání vzájemnému srovnání a využití příslušných zkušeností a dalších právních poznatků. Technika fungování právních mechanismů příslušné právní kultury totiž vzhledem k nastavení právních nástrojů pro

[79] K tomu ještě přistupuje podstatný rozdíl mezi interní instrukcí a právním předpisem nebo vrchnostenským aktem spočívající v tom, že interní instrukce se nemůže spoléhat na presumpci správnosti resp. presumpci platnosti – srov. Bělina, M. a kol. *Pracovní právo.* 5. dopl. a podstat. přeprac. vyd., Praha : C.H.Beck, 2012, str. 66.

zajištění národní kybernetické bezpečnosti není nikterak podstatná - hlavní roli při posuzování použitelnosti určitého přístupu, nástroje nebo institutu hraje zde spíše příbuznost hodnotových základů příslušných právních kultur, jimiž jsou v případě českém i v případě právě jmenovaných zemí shodně priorita práv člověka a základní principy demokratického právního státu.

Příkladem takové zkušenosti, která nám ušetřila čas a nemalé zdroje finanční, personální i politické, je původní záměr severoamerické vlády koncipovat národní úpravu kybernetické bezpečnosti na bázi identifikace útočníka[80]. Jedná se o jeden ze dvou způsobů, jak strategicky nastavit právní instituty chránící veřejný zájem na fungování kritické informační a komunikační infrastruktury, který však je vysoce problematický vzhledem k proporcionalitě práv uživatelů služeb informační společnosti (v USA není sice zakotveno právo na ochranu osobních údajů a ochrana soukromí má poněkud jiný charakter než v Evropě, ale právo na anonymní vystupování v prostředí informačních sítí je i tak extrémně silné díky prvnímu dodatku americké ústavy). Politická neprůchodnost tohoto přístupu posloužila nám za vodítko při stanovení základní strategie české resp. evropské právní úpravy kybernetické bezpečnosti, která je namísto zmíněného modelu postavena na strategické prioritě ochrany prostředí[81] s tím, že identifikace a postih útočníka je ponechán na režimu běžného fungování trestního práva resp. na standardní působnosti orgánů činných v trestním řízení.

5.1 ZÁKONNÁ TYPOLOGIE UŽIVATELŮ VYBRANÝCH SYSTÉMŮ A SÍTÍ

Z právě uvedeného plyne, že individuální odpovědnost koncového uživatele, ať je jím útočník nebo i jen subjekt, jehož systém se z nějakého důvodu podílí na kybernetickém bezpečnostním incidentu, představuje politicky velmi citlivou otázku. Předpokladem uplatnění individuální odpovědnosti uživatele, ať už má jít o odpovědnost soukromoprávní nebo trestní, je totiž jeho ztotožnění. To přitom vyžaduje použití takových mechanismů, které mohou obecně ohrozit shora zmíněnou anonymitu (jako

[80] Srov. Sales, S. A. Regulating Cyber-Security, *Northwestern University Law Review*, roč. 107, číslo 4, str. 1503.

[81] K tomu viz např. věcný záměr zákona o kybernetické bezpečnosti nebo průvodní dokumentaci k návrhu směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, COM/2013/048 final - 2013/0027 (COD).

nutnou komponentu práva na svobodu projevu) a mohou být především kontradiktorní s kategorickými požadavky výjimečně rigorózně nastavené evropské ochrany soukromí a osobních údajů.

Právě ochrana soukromí, osobních údajů, svobody projevu či obecně vzato práva na informační sebeurčení jsou důvodem toho, že se zřejmě v dohledné době nesetkáme s ničím takovým, jako internetový občanský či řidičský průkaz. Na druhé straně však je možno uvažovat o proporcionální ochraně vitálních zájmů na fungování kritických součástí informační a komunikační infrastruktury prostřednictvím specifické individuální odpovědnosti lidí, kteří na profesionální bázi s kriticky důležitými informačními systémy nebo sítěmi pracují.

Jednou z možností legislativního řešení je maďarský model definice stupňů bezpečnostní důležitosti informačních systémů a sítí a založení práva pracovat s těmito systémy pouze uživatelům s určitým stupněm znalostní certifikace[82]. Nemusí přitom jít pouze o povinnost pro správce příslušného systému nebo sítě spočívající v nutnosti proškolit své zaměstnance respektive najmout si pro jejich obsluhu odborně náležitě vybavený personál. Zprostředkovaně může jít též o vytvoření specifických povinností na straně samotného uživatele založených předpisy na úseku kybernetické bezpečnosti, zakládajících správní odpovědnost za přestupky nebo jiné správní delikty spočívající v neodborném přístupu ke kriticky důležitým systémům nebo sítím a odstupňované adekvátně k jejich bezpečnostní klasifikaci.

Je docela pravděpodobné, že potřebu takové úpravy pocítí v první řadě především správci kritické informační a komunikační infrastruktury poté, co konstatují nutnost až příliš sofistikované tvorby interních instrukcí tak, aby bylo v případě problému na straně uživatele nebo operátora kriticky důležitého systému nebo sítě možno regresně vyvodit alespoň disciplinární odpovědnost. Problémem interních instrukcí totiž je, že jejich závaznost či praktická vynutitelnost není jen otázkou jejich bezrospornosti se zákonem, ale též jejich srozumitelnosti a formy komunikace (viz dále). Byť to může

[82] Srov. maďarský zákon o elektronické informační bezpečnosti ústředních a místních správních orgánů ze dne 15. dubna 2013 – ke stažení v anglické verzi on-line na adrese http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx.

znít na první pohled poněkud problematicky, je proto pro zaměstnavatele nepoměrně jednodušší, pokud se může spolehnout na zákonnou nebo podzákonnou definici konkrétních bezpečnostních povinností svých zaměstnanců, než pokud by takovou definici měl sám vytvářet a implementovat. Individuální správní odpovědnost je navíc sama o sobě silným motivačním faktorem, který může pro příslušné zaměstnance představovat ještě pádnější důvod k obeznámení se s bezpečnostními pravidly a k jejich dodržování, než je tomu v případě disciplinární odpovědnosti nebo omezené odpovědnosti za škodu způsobenou zaměstnavateli.

Ve vazbě k výše uvedenému je možno uvažovat též o zákonem založené povinnosti pro správce vybraných typů vysoce bezpečnostně exponovaných informačních systémů a sítí vyčlenit resp. zaměstnat pracovníka přímo odpovědného za plnění požadavků zákona o kybernetické bezpečnosti. Podobně, jako je tomu v agendě ochrany utajovaných informací[83] nebo v některých členských státech v agendě ochrany osobních údajů[84], mohl by tento zaměstnanec mít v organizační struktuře příslušného správce ze zákona dané specifické postavení a jeho disciplinární odpovědnost by mohla být rozdělena mezi zaměstnavatele a národního regulátora (tj. v našem případě zřejmě Národní bezpečnostní úřad).

5.2 OMEZENÁ ODPOVĚDNOST BĚŽNÝCH UŽIVATELŮ

Nejen z politických důvodů je zřejmě nereálné předpokládat, že by právní úprava kybernetické bezpečnosti v dohledné době specificky založila objektivní odpovědnost koncových uživatelů nebo zavedla nějaký zvláštní mechanismus jejich identifikace. Přes všechny více či méně argumentované požadavky na to, aby uživatelé odpovídali za bezpečné fungování svých systémů bez ohledu na své zavinění, je totiž třeba v první řadě zohlednit skutečnost, že i relativně jednoduché technologie určené k běžnému použití v domácnostech (typicky např. mobilní telefony, domácí wifi routery apod.) jsou z podstaty extrémně technicky složité. Běžný uživatel tedy

[83] Srov. § 71 zákona č. 412/2005 Sb.

[84] Povinnost zřídit u větších subjektů tuto funkci se plánuje k celoevropskému zavedení v připravované nové úpravě evropské ochrany osobních údajů – k tomu viz dokumentaci k návrhu nařízení 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, 2012/0011 (COD).

nejenže nechápe (resp. nemusí chápat) ani základní principy jejich fungování, ale nelze po něm požadovat ani to, aby se zvlášť věnoval jejich zabezpečení proti možnému zneužití. Jestliže tedy prostý spotřebitel např. neprovede instalaci bezpečnostní záplaty a v důsledku toho je jeho systém zneužit k útoku typu DDoS, není v dohledné době možno uvažovat o tom, že by za takový útok měl nést spoluodpovědnost.

Z hlediska proporcionality dotčených práv nesrovnatelně schůdnějším řešením by byla regulace spotřebitelské dostupnosti informačních a komunikačních technologií v závislosti na míře jejich bezpečnosti. Lze tedy uvažovat o tom, že budou pro určité typy informačních a komunikačních technologií zavedeny mandatorní požadavky na jejich kvalitu, které zahrnou i nutnou jejich bezpečnostní výbavu. Podobně, jako je tomu pravidlem v síťových odvětvích, tj. např. v energetice, telekomunikacích nebo v dopravě, může i v oblasti kybernetické bezpečnosti vzniknout katalog požadavků na shodu, který zahrne nejnutnější bezpečnostní prvky a bez jejichž dodržení nebude možno příslušnou technologii spotřebitelsky šířit na tuzemském trhu. I v tomto případě by šlo zprostředkovaně o zatížení koncového uživatele – nikoli sice přímými povinnostmi či odpovědností, ale nutností zaplatit příslušné zabezpečení včetně jeho administrativních externalit v konečné ceně produktu nebo služby. Takové řešení je však stále z hlediska ochrany práv nesrovnatelně schůdnější, než shora diskutovaná objektivní odpovědnost.

Velmi zajímavou možnost řešení individuální odpovědnosti uživatele přinesl doposud výjimečný případ, který řešily americké soudy. Šlo v něm, stručně řečeno, o infekci využívající bezpečnostní díru v systémech společnosti Microsoft, která umožňovala skryté využití napadených systémů jako součástí botnetu pro útoky typu DDoS. Spol. Microsoft se v tomto případě odhodlala k právně originálnímu řešení, když zažalovala organizátory botnetu a v návrhu rozhodnutí též de facto navrhla postihnout i uživatele, kteří své systémy nezabezpečili bezpečnostní záplatou[85].

Pro právní řády z právní kultury common law je totiž typické, že umožňují uplatnit civilní postih i proti osobám, které sice nejsou určeny jménem a adresou, ale jejichž specifikace je dostatečně přesná na to, aby

[85] Viz rozhodnutí ve věci 3:13-CV-00319-GCM okresního soudu pro Western District of Notrh Carolina, Charlotte Division, ke stažení on-line na adrese http://botnetlegalnotice.com/citadel/files/Order_Granting_Def_Jdgmt_PI.pdf.

bylo možno podle příslušného znaku konkrétní subjekt v důsledku identifikovat. Žalovaný tedy v tomto případě může být určen konkrétním znakem bez toho, aby žalobce znal jeho přesnou identitu. V důsledku to pak znamená, že žalovaný ani nemusí vědět o tom, že je žalován (přestože je mu doručováno za známý e-mail).

Plán založit nepřímou odpovědnost koncových uživatelů jeví se být sice ve světle shora uvedených argumentů jako prostá marnost. V tomto případě se však spol. Microsoft podařilo velmi inovativním způsobem vyřešit rovnováhu mezi deliktem a jeho odpovědnostním důsledkem. Žalobní petit totiž nezněl na náhradu škody nebo jiné plnění, ale „pouze" na povinnost uživatele strpět dálkový zásah do svého systému, kterým Microsoft přesměruje za účelem vyšetření celého incidentu případný útok na své vlastní servery. Tento nárok byl díky tomu shledán proporcionálním k deliktu a následně přiznán. Microsoft tedy mohl nepozorovaně zasáhnout do infikovaných systémů a díky přesměrování jejich komunikace nejen zabránit škodám, které by botnet mohl způsobit, ale též získat cenná data k vyšetření celého incidentu.

Tento případ není pro českou právní praxi inspirativní do té míry, že by bylo snad možno uvažovat o podobném řešení v našich podmínkách. Naše procesní právo totiž nedovoluje žalovat na základě identifikačního znaku, nelze-li podle něj přímo v řízení ztotožnit konkrétní subjekt. I pro naše právní prostředí je však zajímavá úvaha soudu ohledně toho, že i běžný uživatel má určitou míru povinnosti vědět o potřebě zabezpečení svého vlastního systému a že tuto povinnost lze uvést do souvislosti s adekvátním typem odpovědnostního následku, tj. nikoli např. hradit škodu ale „pouze" strpět dálkový zásah do svého systému.

Prostředkem, který by bylo možno využít namísto shora popsaného řešení, mohlo by se stát opatření obecné povahy. To totiž umožnuje identifikovat své adresáty na základě obecných znaků a uložit jim určitou povinnost. Je pak možno svěřit konkrétnímu úřadu (v našem případě by zřejmě šlo o Národní bezpečnostní úřad nebo Český telekomunikační úřad) kompetenci vydávat za přesně stanovených okolností tato opatření a ukládat jimi i běžným (nic netušícím) uživatelům podobné povinnosti strpět zásah do jejich systémů, jako se stalo ve shora zmíněném případě.

5.3 SPECIFICKÁ ÚPRAVA OUTSOURCINGU

Jádrem aktuální zákonné úpravy i podzákonných prováděcích předpisů v oblasti kybernetické bezpečnosti jsou bezpečnostní opatření. Požadavky na standard zabezpečení informační a komunikační infrastruktury spravované povinnými subjekty jsou zákonem stanoveny velmi obecně a prováděcí předpisy pak obsahují jen takovou míru jejich konkretizace, která nezasahuje do principu technologické neutrality a umožňuje povinným subjektům autonomii při volbě konkrétních řešení. Tento model jeví se jako vhodný hned ze dvou důvodů – předně je povinný subjekt tím nejvíce povolaným, pokud jde o detailní technické znalosti příslušného informačního systému nebo sítě a má tedy nejlepší možnost posoudit, jaká konkrétní bezpečnostní řešení nejlépe splní zákonné požadavky. Vedle toho je velmi pravděpodobné, že relativní otevřenost standardních požadavků povede společně s jistotou investic k motivaci dodavatelů různých bezpečnostních řešení k investicím do vývoje. To může přinést vítaný impuls k dalším inovacím v oboru ICT bezpečnosti.

Relativně velká míra autonomie u povinných subjektů ohledně způsobu plnění zákonných požadavků však na druhé straně vyvolává i nejistotu ohledně řešení typických případů, kdy správce nerealizuje jednotlivá bezpečnostní opatření sám nebo alespoň ve vlastní režii, ale provádí jejich komplexní outsourcing. Především u středně velkých a menších povinných subjektů lze kromě vzájemné koordinace jejich aktivit při akvizicích bezpečnostních řešení očekávat i společné postupy při komplexním řešení bezpečnostních opatření včetně jejich fungování v reálném čase. Lze si tedy například představit, že místní utility typu vodáren nebo tepláren vytvoří společný podnik, který bude jim bude zajišťovat realizaci a fungování bezpečnostních opatření např. i včetně provozu lokálního CERT, reportování incidentů, spolupráce s národním nebo vládním dohledovým pracovištěm apod.

Zákon a podzákonné předpisy sice možnost outsourcingu bezpečnostních opatření nevylučují a v konkrétních částech s ní přímo počítají. Pravidla pro externí dodavatele bezpečnostních řešení však se omezují pouze na obecné povinnosti mít dokumentovány a kontrolovány vztahy s externími dodavateli.

Vzhledem k tomu, že zákon o kybernetické bezpečnosti stojí na výlučné odpovědnosti správce příslušného informačního systému nebo sítě, není v jeho současné struktuře obsažena speciální úprava postavení dodavatele nebo provozovatele bezpečnostních opatření. Je tedy plně na správci, jak si vztahy s externími subjekty vyřeší a jak bude ve vztahu k nim zajišťovat například plnění povinností vyplývajících z kontrolních pravomocí Národního bezpečnostního úřadu nebo regresní nároky v případě deliktní odpovědnosti.

Zatímco volnost ve smyslu konkrétní formy bezpečnostních opatření jeví se jako vhodná a není důvod předpokládat v brzké budoucnosti nějaké zásadní změny, je otázku totální volnosti povinných subjektů ohledně outsourcingu bezpečnostních opatření možno považovat za místo, kde bude zákonná úprava průběžně doplňována na základě praktických zkušeností. Nejde pouze o možnost založení přímých pravomocí Národního bezpečnostního úřadu vůči subjektům poskytujícím bezpečnostní řešení jako službu, ale například i o možnost správní regulace činnosti takových subjektů (nabízí se například varianta speciální vázané živnosti). Především ve vztahu k informačním systémům veřejného sektoru spadajících pod rozsah zákona o kybernetické bezpečnosti (tj. k informačním systémům veřejné správy a dalším informační systémům provozovaným veřejnoprávními korporacemi, které budou spadat pod rozsah kritické informační infrastruktury nebo významných systémů) lze očekávat i podrobnější úpravu požadavků na outsourcing, která by měla odstranit standardní bezpečnostní nešvary vyskytující se v procesech zadávání veřejných zakázek na ICT.

Vedle konkrétnější úpravy zákonných a podzákonných parametrů outsourcingu bezpečnostních opatření lze předpovědět i nepoměrně rychlejší vývoj smluvních nástrojů a alternativních forem řešení obchodních sporů, a to především u soukromoprávních povinných subjektů. Dokonce ještě před platností (nikoli až účinností) zákona o kybernetické bezpečnosti byly některé velké korporace včetně energetických společností nuceny zahrnovat do outsourcingových smluv klauzule zakládající pro dodavatele resp. poskytovatele služby specifické povinnosti v návaznosti na budoucí zákonné bezpečnostní požadavky.

Konstrukce těchto klauzulí, kontrola příslušných plnění v reálném čase (může totiž jít o mnohaleté smlouvy) nebo mechanismy řešení vzájemných sporů představují oblast smluvního ICT práva, která sice u nás není úplně zanedbána, bude však zřejmě ještě procházet velkým rozvojem. Namísto legislativní asistence však je v tomto směru spíše nutno očekávat, že si budou muset soukromoprávní povinné subjekty, zjednodušeně řečeno, pomoci samy – přispět ke zdárnému vývoji smluvních nástrojů, procedur výběru dodavatelů nebo procedur řešení dodavatelských sporů mohou kromě organizací typu Hospodářské komory především oborové asociace. Kvalitně fungující vztahy s dodavateli bezpečnostních opatření totiž nepředstavují otázku vzájemné konkurence mezi subjekty působícími na týchž trzích a přímo se tak nabízí vzájemná bezkonfliktní spolupráce a koncentrace zdrojů k zajištění efektivně fungujících právních řešení.

5.4 DALŠÍ VÝVOJOVÉ PERSPEKTIVY PRÁVA KYBERNETICKÉ BEZPEČNOSTI

K právě uvedenému lze spekulativně připojit i další oblasti, z nichž na prvním místě se bude zřejmě jednat o postupnou národní i mezinárodní konkretizaci pojmu informační suverenity státu. Primárním těžištěm tohoto problému bude zřejmě mezinárodní právo veřejné a výstupy můžeme očekávat především z jeho doktríny. Přestože ideálním řešením by v tomto směru byla mezinárodní úmluva, nedá se vzhledem ke zcela rozdílným pohledům na věc a zcela odlišným zájmům jednotlivých národních vlád očekávat, že by k přípravě takové úmluvy mohlo v dohledné době dojít. Příliš pravděpodobný není ani vznik judikatury Mezinárodního soudního dvora, neboť státy, které by toho byly schopny, nemají, stručně řečeno, k přednesení aktuálně se vyskytujících konfliktních situací tomuto fóru prakticky žádnou motivaci. Namísto toho je spíše důvod očekávat další rozvoj vzájemné spolupráce na základě existujících obecných spojeneckých svazků, z nich nejvýznamnější a doposud nejproduktivnější je spolupráce v rámci NATO[86].

[86] Z doktrinálního hlediska nejvýznamnější výstupem této spolupráce je činnost centra excelence CCD CoE v estonském Talinu, jejíž manuál se stal všeobecně uznávaným standardem doktríny mezinárodního práva veřejného pro kybernetickou bezpečnost. Manuál je on-line ke stažení ze http://issuu.com/nato_ccd_coe/docs/tallinnmanual.

Nesrovnatelně jednodušší je co do synergie základních hodnot a zájmů situace v rámci Evropské unie. Díky tomu lze v brzké době očekávat finalizaci směrnice o kybernetické bezpečnosti (resp. směrnice o síťové a informační bezpečnosti) a další rozvoj stávajících evropských bezpečnostních struktur, zejm. ENISA a CERT-EU. Poslední vývoj návrhu cit směrnice směruje sice spíše k obecnějšímu rozsahu a nižšímu standardu povinností členských států – podobně jako v případě českého zákona o kybernetické bezpečnosti je však i v tomto případě zřejmě vhodné přistoupit k fixaci určitého právně bezproblémového a politicky akceptovatelného řešení a to pak dále rozvíjet institucionální a legislativní aktivitou na základě praktických zkušeností.

V českém právním prostředí můžeme nad rámec toho, co bylo diskutováno v předchozích kapitolách, očekávat především konkretizaci spolupráce vládního a národního CERT, jakož i konkretizaci spolupráce Národního bezpečnostního úřadu s ostatními orgány veřejné moci, do jejichž zájmu spadá oblast národní kybernetické bezpečnosti (vedle bezpečnostních služeb jde především o Policii ČR, Armádu ČR a ústřední orgány státní správy mající jurisdikci nad kritickými či významnými informačními systémy a sítěmi)[87]. Podobně lze očekávat též rozvoj spolupráce mezi Národním bezpečnostním úřadem a soukromoprávními korporacemi, profesními sdruženími a akademickou sférou – ta může mít charakter neformálních aktivit, memorand, činnosti expertních skupin apod. a může řešit problémy, které z nějakého důvodu není možno nebo vhodno pokrýt veřejnoprávními aktivitami (typicky např. otázky certifikace, vzdělávání, podpory inovací apod.)

Jako nanejvýš vhodná jeví se v tomto směru být tendence zahrnovat kybernetickou bezpečnost mezi aktuální politické priority – to umožní podporovat shora uvedené činnosti v rámci standardních forem spolupráce mezi soukromým, akademickým a veřejným sektorem typu podpory vědeckých nebo rozvojových projektů, exportu, investic, rozvoje občanské společnosti aj.

[87] Národní bezpečnostní úřad již v tomto směru publikoval několik podpůrných dokumentů jako např. blokové schéma zákona o kybernetické bezpečnosti nebo pomůcky k určení prvku kritické informační infrastruktury a významných systémů – dokumenty jsou ke stažení on-line na adresách: www.govcert.cz.

6. PERSPEKTIVY DALŠÍHO POLITICKÉHO A ORGANIZAČNÍHO VÝVOJE AGENDY KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

6.1 CERTIFIKACE A COMPLIANCE CHECK

Jak uvedeno shora, pracuje návrh české právní úpravy s principem autonomie vůle regulovaných subjektů. Jedním z projevů tohoto principu ve spojení s principem technologické neutrality je mandatorní stanovení cílových charakteristik bezpečnostních opatření (organizačních i technických) a ponechání konkrétní formy realizace na úvaze příslušného povinného subjektu. Vhodnost takového řešení je vedle obecně menší regulatorní zátěže pro povinné subjekty dána též skutečností, že příslušné bezpečnostní řešení může být vždy realizováno na míru konkrétního systému. Regulovaný subjekt má tedy praktickou volnost ve výběru architektury, technologie i dodavatelů.

Určitou nevýhodou tohoto jinak vhodně zvoleného řešení však je skutečnost, že povinné subjekty budou mít jen omezenou míru právní jistoty ohledně otázky, zda právě jejich konkrétní řešení odpovídá zákonným požadavkům, tj. zda v případě kontroly ze strany Národního bezpečnostního úřadu nebudou shledány vzhledem k zákonným požadavkům nějaké nedostatky. Byť jsou totiž požadované parametry bezpečnostních opatření definovány s maximální mírou určitosti, nelze se, a to ani při konkretizaci jednotlivých parametrů formou podzákonných právních předpisů, ubránit relativně velké míře abstrakce a výsledné nejistoty plynoucí vedle relativně abstraktních zákonných a podzákonných pojmů též z velkého množství různých organizačních a technických kritérií.

K relativní neurčitosti zákonných resp. podzákonných požadavků pak ještě přistupuje určitá míra nejistoty ohledně implementace a následného provozu bezpečnostních opatření. Zákonné požadavky totiž nesměřují jen ke statické formě bezpečnostních opatření (tj. k jejich statickým formálním parametrům) ale též k jejich implementaci a fungování v reálném čase. I bezpečnostní řešení dostatečně dimenzované vzhledem k zákonným požadavkům totiž může ve svém výsledku porušovat zákonné podmínky

kvůli neadekvátní implementaci nebo nedostatečné pozornosti vzhledem k jeho trvalému provozu.

Nejistota ohledně toho, zda projektované, pořízené, implementované a provozované bezpečnostní řešení splňuje zákonné parametry, představuje závažný problém především pro střední a velké podniky, jakož i pro veřejnoprávní korporace. U středních a velkých podniků jedná se především o otázku compliance, přičemž především nadnárodní korporace často řeší otázky a priori plnění zákonných požadavků v příslušných jurisdikcích jako naprostou prioritu. Aktuálně se to týká např. otázek ochrany osobních údajů, bezpečnosti práce, požární bezpečnosti, utajovaných informací apod. Pro podnik velkého rozsahu je totiž zásadně důležité vyčíslení nákladů na plnění právních povinností v příslušné jurisdikci a priori – jen tak s nimi totiž lze kalkulovat do finančních plánů. Situace, kdy je velká nebo střední korporace nucena kalkulovat potenciální náklady na plnění právních povinností a posteriori, vždy generuje značnou míru nejistoty, neboť právní odpovědnost (postih) se v komplexních případech jen velmi těžko odhaduje a těžké je i provést takovou kalkulaci do všech možných důsledků (k tomu viz výše).

V případě naší právní úpravy kybernetické bezpečnosti tak jde příkladně o to, jaké mohou být právní následky implementace a používání takového systému bezpečnostních opatření, o kterém se následně prokáže, že nesplňuje zákonné požadavky. U velkého nebo středního podniku je v tomto směru případná pokuta jen jedním z mnoha možných následků, neboť nezákonnou implementací mohou být způsobeny např. škody třetím osobám nebo může v důsledku nařízených opatření k nápravě dojít k omezení provozu či k potřebám zásadních organizačních změn.

Dokonce i tam, kde lze počítat s konkrétní výší např. pokut, náhrad škody nebo škod způsobených zastavením nebo omezením provozu, představuje u všech typů podnikatelských subjektů a posteriori řešení právní rizikovosti velmi nevítanou alternativu. Není totiž žádným tajemstvím, že podnikatelské aktivity mohou být významně poškozeny už tím, že se orgány státní moci nějakou formou o příslušný podnik zajímají. Typicky pak může i pouhá kontrola nebo vyšetřování ze strany oprávněných orgánů státní moci způsobit jen těžko předvídatelné komplikace a vést ke ztrátám, jejichž hodnotu lze jen stěží předem vyčíslit.

To platí samozřejmě i pro případy, kdy vyšetřování nebo kontrola nevedou ve vztahu k příslušnému orgánu veřejné moci k žádném sankčnímu důsledku, neboť i pouhá vrchnostenská přítomnost na kontrolovaných pracovištích může se negativně projevit na výkonu celého podniku.

U veřejnoprávních korporací je otázka a priori souladu s požadavky právního řádu ještě důležitější než u podnikatelských subjektů. V porovnání se soukromoprávními subjekty jde dokonce o prioritní otázku bez ohledu na jejich velikost. Je-li totiž k pořízení nebo provozu bezpečnostních opatření užito veřejných prostředků, nelze riskovat dodatečnou kvalifikaci těchto opatření jako nesouladných se zákonnými požadavky.

Lze navíc předpokládat, že investice veřejného sektoru do kybernetické bezpečnosti budou minimálně z podstatné části kryty prostředky z různých rozvojových projektů – příjemce takových prostředků si pak dvojnásob nemůže dovolit rizikovost investice vzhledem ke splnění zákonných požadavků resp. nemůže si dovolit riskovat situaci, kdy projektové prostředky použije způsobem, který je dodatečně (např. na základě kontroly) označen za nikoli souladný s platnou právní úpravou. Poskytovatel dotace má totiž v takovém případě právo či dokonce povinnost dovolávat se podmínek jejího poskytnutí a požadovat vrácení poskytnutých prostředků.

Z právě popsaných důvodů lze mezi středními a velkými soukromoprávními subjekty a veřejnými korporacemi očekávat velkou poptávku po a priori aprobačních procedurách poskytujících nezávislé ujištění ohledně toho, že implementované resp. provozované řešení bezpečnostních opatření je v souladu s požadavky účinné právní úpravy. Objektivně ideální variantou řešení tohoto problému by byla zákonná certifikační procedura realizovaná přímo příslušným orgánem státní exekutivy (v českém právním prostředí zřejmě Národním bezpečnostním úřadem) nebo jím pověřeným a dozorovaným nezávislým expertním pracovištěm.

Skutečnost, že taková procedura není součástí struktury navrhované právní úpravy, však lze jen sotva vnímat jako chybu právotvůrce nebo jako pravou mezeru v právu. Taková procedura musela by totiž být podrobně a rigorózně upravena, aby nevzniklo riziko privatizace výkonu nedistributivních práv resp. aby nebyl indukován korupční potenciál. Je

přitom jen velmi obtížné takovou rigorózní úpravu provést v situaci, kdy jsou k dispozici v tomto ohledu jen velmi omezené zkušenosti (zde je nutno připomenout, že stávající komerční certifikační procedury zaměřují se především na problematiku organizačních opatření, nikoli už na technologie k zajištění kybernetické bezpečnosti nebo na spolupráci s centrálními dohledovými pracovišti).

Zavedení státní certifikace by rovněž vyžadovalo důkladnou přípravu institucionální a personální a je třeba v tomto směru konstatovat, že na našem pracovním trhu zdaleka není přebytek pracovní síly disponující dostatečnou mírou kvalifikace v oboru kybernetické bezpečnosti a k tomu náležitě motivované za aktuálních platových podmínek ke vstupu do státní služby. Příprava adekvátní procedury by tedy z hlediska organizačního i personálního vyžadovala takovou časovou a finanční dotaci, kterou si vzhledem k vývoji bezpečnostní situace nemůže v současné době Česká republika dovolit (kromě toho je třeba po bohatých našich legislativních zkušenostech připomenout, že nemá smysl uvádět v účinnost právní úpravu, na jejíž implementaci není státní exekutiva náležitě připravena).

Ve prospěch státního řešení certifikace může naopak hovořit pozitivní zkušenost s obdobnou procedurou v agendě ochrany utajovaných informací. Ani v tomto případě přitom nebylo možno ji realizovat okamžitě, ale příslušné kapacity se postupně vytvářely. Skutečnost, že v tomto případě nejde o korupčně exponovanou situaci, navíc ukazuje, že je v případě Národního bezpečnostního úřadu možno předpokládat takovou kvalitu institucionálních opatření, která vzniku a rozvoji korupčního rizika účinně brání. V případě kybernetické bezpečnosti by navíc bylo možno v porovnání s technologiemi a postupy pro ochranu utajovaných informací učinit celý certifikační proces ještě transparentnějším (tj. vystavit jej ve větší míře veřejné kontrole v tomto případě vykonávané především dodavateli vzájemně konkurenčních bezpečnostních řešení) a lze tedy konstatovat, že korupční rizikovost by bylo možno v takovém případě prakticky vyloučit.

Problémem však každopádně zůstává shora konstatovaná a jen těžko okamžitě řešitelná dlouhodobost náběhu veřejnoprávní certifikační procedury daná nutností vytvořit na straně NBÚ odborně zdatný

a dostatečně robustní personální substrát[88]. Jedinou variantou přímého zapojení orgánu veřejné moci do a priori certifikace bezpečnostních řešení tedy zůstává institucionální nebo produktová aprobace certifikační procedury realizované nezávislým subjektem s dostatečnou personální kapacitou, tj. akademickou institucí, profesním či oborovým sdružením nebo komerčním poskytovatelem.

Role zájmových sdružení a organizací zajišťujících expertní spolupráci soukromého a veřejného sektoru je v tomto směru zřejmě klíčová. Ve vzájemné spolupráci s orgány odpovědnými za výkon vrchnostenské správy na úseku kybernetické bezpečnosti a nezávislými akademickými institucemi mohou tyto organizace pomoci s vytvořením nezávislých certifikačních procedur praeter legem, které nebudou mít vrchnostenský charakter, ale přesto poskytnou zájemcům z řad soukromého a veřejného sektoru nezávislé komplexní posouzení jejich bezpečnostních opatření vzhledem k zákonným a podzákonným požadavkům. Charakter zájmového sdružení v tomto případě kombinuje aspekt transparentnosti (tj. je jasné, že jde o aktivitu obchodní komunity) a profesní specializaci (tj. zaměření na konkrétní ekonomické odvětví) s legitimitou společného postupu, tj. nejde pouze o zájem jednoho podnikatele, ale aktivita sdružení odráží vůli jinak si vzájemně konkurujících subjektů.

Takové certifikační procedury samozřejmě nebudou disponovat vrchnostenským charakterem a jejich výstupy nebudou zavazovat orgány veřejné moci při hodnocení souladu příslušných bezpečnostních řešení se zákonem a podzákonnými předpisy. Při nalezení adekvátního modelu spolupráce s vrchnostenskými orgány však lze tímto prostřednictvím docílit faktické akceptace těchto certifikačních procedur alespoň v procesním smyslu. Jinými slovy tedy takový certifikát nemůže sice absolutně ochránit příslušný subjekt před kontrolou nebo následnou sankcí, jeho udělení však může být při případné kontrole fakticky zohledněno. Zatímco tedy může být za běžných podmínek prováděna kontrola bezpečnostních opatření bez jakékoli presumpce, může Národní bezpečnostní úřad kontrolovat certifikovaná bezpečnostní řešení s presumpcí souladu. Takové procesní řešení může pak pragmaticky posloužit nejen povinným osobám, ale

[88] S tímto problémem se každopádně nepotýká jen Česká republika – srov. Devost, M. G., Moss, J. Pollard, N. A. Stratton, R. J. III. All Done Except the Coding, *Georgetown Journal of International Affairs*, roč. 11, str. 197 a násl.

samotnému Národnímu bezpečnostnímu úřadu – logicky ale jeho implementace vyžaduje především vzájemnou důvěru, kterou může zajistit pouze skutečná nezávislost certifikační procedury, jakož i její vysoká odborná úroveň. Obojí je v našem prostředí řešitelné v první řadě spoluprací s renomovanými akademickými institucemi.

Především z hlediska povinných subjektů užívajících k investicím do pořízení nebo provozu bezpečnostních opatření veřejné prostředky (v tomto případě je lhostejno, zda jde o soukromoprávní nebo veřejnoprávní organizace) je shora popsané řešení vhodné i z důvodu možné inkorporace do zadávací dokumentace resp. do mandatorních požadavků na dodavatelská řešení. Namísto relativně neurčitých formulací ohledně souladu bezpečnostních opatření s platnou právní úpravou budou tyto subjekty moci v implementačních nebo realizačních smlouvách využít ujednání odkazující na získání konkrétních typů certifikací a sjednat si tím vyšší míru právní jistoty. Obdobná může být též situace u dlouhodobých outsourcingových kontraktů, kde požadavek na certifikaci příslušného bezpečnostního řešení na aktuálně účinný standard může být na straně odběratele adekvátně řešit jistotu ohledně průběžného plnění zákonných resp. podzákonných povinností, u nich lze oprávněně očekávat, že se budou v čase výrazně vyvíjet a měnit (k tomu viz výše).

K právě uvedenému je nutno doplnit, že příslušná certifikační řešení zdaleka nemusí být unikátní nebo monopolní resp. že pro různé typy bezpečnostních řešení mohou fungovat různé procedury. Certifikace tak může být prováděna např. formou prověrky ve fázi projektu informačního systému nebo sítě, kontroly jeho implementace nebo provozních zkoušek jako součásti různých fází akceptace příslušných dodávek. Formu certifikace mohou mít též například i penetrační testy nebo jiné typy operačních prověrek běžících systémů nebo sítí. Tento model může být využíván především u dlouhodobých outsourcingových kontraktů, přičemž odběratel může mít díky němu stálou kontrolu nad kvalitou dodávané služby a nad skutečností, že služba např. i po několika letech stále plní aktuální požadavky právní úpravy (v tomto směru je třeba připomenout relativně vysokou pravděpodobnost postupných změn požadavků na bezpečnostní opatření v návaznosti na obecný technický vývoj). Certifikací mohou konečně procházet vedle celých bezpečnostních řešení i jen dílčí

systémy nebo dokonce jejich jednotlivé komponenty – typicky tak může být systém nebo síť podrobena experimentální bezpečnostní expozici v testovacím polygonu a na základě kvality její odezvy může být certifikační autoritou doporučena/nedoporučena pro nasazení v určitém typu informačního systému nebo sítě.

Vzhledem k tomu, že bezpečnostní opatření mohou být dle platné právní úpravy šita přímo na míru konkrétním systémům nebo sítím, je vhodné podporovat i takové certifikační iniciativy, které budou směřovány do konkrétních hospodářských resp. veřejnoprávních sektorů[89]. Lze očekávat, že profesně resp. sektorově orientované iniciativy mohou být v tomto směru mnohem efektivnější – je přitom logické, že typická bezpečnostní řešení v justici se budou zřejmě na úrovni technické i organizační zásadně odlišovat od bezpečnostních opatření aplikovaných v oblasti energetických systémů a sítí. Profesně resp. sektorově orientované iniciativy mohou v tomto směru přinést ve smyslu efektivity nejen odpovídající úroveň znalostí v oboru kybernetické bezpečnosti ale také poznatky ohledně specifických požadavků v příslušném odvětví nebo oboru.

Jako problematická jeví se konečně v současné situaci též rizika plynoucí z čistě podnikatelsky orientovaných iniciativ, které může indukovat shora popsaná poptávka. Nebude-li totiž problematika a priori aprobace bezpečnostních opatření řešena formou spolupráce orgánů veřejné moci, akademických institucí a odborně orientovaných a ideálně i agregovaných soukromých iniciativ, vytvoří se tím prostředí pro živelný vznik samozvaných razítkovacích produktů. Bude pak extrémně složité dostat takový čistě ekonomicky motivovaný chaos do situace, kdy bude možno se na příslušné certifikáty či jiné formy potvrzení z odborného hlediska skutečně spolehnout. Jen těžko si pak lze představit, jaké praktické důsledky by mohla mít situace, kdy by aprobaci bezpečnostních opatření nezávisle prováděli např. jednotliví znalci (bude-li zachována současná situace ohledně podmínek pro výkon a odbornou úroveň znalecké činnosti).

[89] Ke specifickým požadavkům v oboru energetiky viz např. Oliveira, D. Cyber-Terrorism & Critical energy Infrastructure Vulnerability to Cyber-Attacks, *Environmental & Energy Law & Policy Journal*, roč. 5, číslo 2, str. 519 a násl.

6.2 AKTIVNÍ OBRANA – BEST PRACTICES

K tématu aktivní obrany je nutno předeslat, že v současné době neexistuje žádná obecně uznávaná taxonomie jejích typických forem. Pokud už je téma aktivní obrany[90] předmětem odborných publikací, zaměřuje se debata buďto na technické aspekty konkrétních typů obranných opatření nebo na základní systematiku v rámci relativně úzce vymezených typů. Nelze však hovořit o žádné komplexní systematice a dokonce ani o definici, která by mohla pojem aktivních obranných opatření (aktivních protiopatření) alespoň rámcově popsat.

Za této situace je problematika aktivní obrany logicky spíše vědeckým zadáním a měla by být řešena spíše formou výzkumných aktivit a iniciativ. Jediným použitelným zárodkem obecné taxonomie aktivních protiopatření je tzv. Dagstuhlská taxonomie[91], která byla sestavena v rámci specializovaného semináře Leibnizovy nadace na podzim 2013 a reflektovala požadavky na systematiku z hlediska informatiky i právní vědy. Ani tato taxonomie však není prakticky použitená, neboť obsahuje pouze náznak základních kategorií a bude tedy nutno ji dále vyvíjet a doplňovat.

Aktuální praxe kybernetické bezpečnosti však nemůže čekat na výstupy vědeckých projektů, neboť aplikace aktivních protiopatření představuje v běžném fungování služeb informační společnosti každodenní nutnost. Vzhledem k tomu, že reálně užívaná aktivní protiopatření často zasahují do vlastnických či závazkových práv nebo dokonce naplňují formální znaky skutkových podstat trestných činů, představuje jejich uplatňování doposud šedou zónu a podnikatelé, kteří tato opatření používají, tak zpravidla činí skrytě. Dokonce ani technici vyvíjející a aplikující tato opatření na objednávku soukromoprávních subjektů často ani nejsou s těmito subjekty v žádném oficiálním právním vztahu.

Poněkud lepší je v tomto směru situace ve veřejném sektoru, přičemž typicky výkonné orgány mohou při užití aktivních protiopatření aplikovat

[90] K pojmu viz Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, *Harvard Journal of Law And Technology*, roč. 25, číslo 2, str. 431.

[91] Viz Freiling, F. C., Hornung. G. Polcak, R. (eds.) Forensic Computing – report from Dagstuhl Seminar 13482, Dagstuhl: Dagstuhl Publishing, 2014, str. 204-205, publ. on-line na adrese http://drops.dagstuhl.de/opus/volltexte/2014/4442/pdf/dagrep_v003_i011_p193_s13482.pdf

obecná oprávnění založená jim v návaznosti na charakter chráněného zájmu. Ani v tomto případě však není situace úplně ideální, neboť při aplikaci obecných oprávnění často vyvstávají otázky ohledně rozsahu příslušných institutů. Orgány veřejné moci jsou rovněž v užití aktivních ochranných prostředků obecně omezeny mlhavými hranicemi vlastní institucionální legitimity – typicky tak armádní složky mohou užít svých extrémně širokých oprávnění pouze za situace, kdy jde o věc národní suverenity, bezpečnostní složky mohou aktivně jednat pouze v zájmu vnitřní nebo vnější národní bezpečnosti a orgány činné v trestním řízení mají manévrovací prostor vymezen agendou vyšetřování a stíhání trestných činů resp. ochranou veřejného pořádku.

Na jednoduchou otázku, jaké aktivní prostředky může užít policista zařazený do obvodního oddělení (je-li toho samozřejmě technicky schopen), když zjistí útok na web místního podnikatele, tedy neexistuje dokonce ani obecná odpověď. Podobně nejsme schopni odpovědět dokonce ani na mnohem prozaičtější otázky nemající charakter bezpečnostních problémů, typicky na otázku, jaké konkrétní aktivní prostředky lze použít při získávání elektronických důkazů z informační a komunikační infrastruktury.

Jak je však uvedeno shora, nemůžeme si dovolit reagovat na faktickou situaci jen pokrčením ramen a vývojem či tolerováním šedé zóny prakticky používaných, účinných a potřebných aktivních opatření, která však existují zcela mimo účinnou právní úpravu. Roli soukromoprávních iniciativ lze v tomto směru vidět především v komunikaci praktických potřeb a sběru a vyhodnocování informací ohledně prakticky používaných technik v různých odvětvích hospodářství a společenského života a v následném zpracovávání těchto poznatků do podoby technických resp. právovědných zadání pro další výzkum a legislativní praxi.

V porovnání se shora popsanou potřebou řešení certifikačních procedur však každopádně platí, že v otázce aktivní obrany nemáme prozatím k dispozici ani představu ohledně konkrétních potřeb a z nich vycházejících zadání pro organizační, technickou nebo legislativní realizaci. O to víc je samozřejmě nutno tuto otázku aktivně zpracovávat a řešit. V tomto směru je však nutno připomenout, že nemá smysl začít pracovat na řešení jakýchkoli partikularit bez současné představy o smyslu a účelu aktivních

protiopatření jako takových a o jejich reflexi základními principy, na nichž stojí náš právní řád.

6.3 KYBERNETICKÁ BEZPEČNOST JAKO AGENDA PODPORY INVESTIC

Jedním ze základních principů, na nichž stojí legitimita české právní úpravy, je princip bdělosti vzhledem k ostatním státům a mezinárodnímu společenství. Vedle shora popsané, byť stále nikoli prakticky uplatňované, částečné přičitatelnosti kybernetického útoku státu neschopnému při vynaložení rozumného úsilí zabránit zneužití informační a komunikační infrastruktury pod vlastní jurisdikcí, projevuje se tento princip i mnohem bezprostředněji, a to ve vztahu k ochraně investic. Česká republika je vázána obecnými procedurálními pravidly řešení sporů mezi státy a soukromoprávními investory doplněnými řadou bilaterálních dohod o ochraně investic zakládající pravomoc příslušných rozhodčích institucí – tato právní úprava vede ve výsledku k možnému založení odpovědnosti České republiky za investice zmařené v důsledku nelegitimního výkonu státní moci resp. v důsledku toho, že stát příslušné investice adekvátně neochrání.

Ve vztahu ke kybernetické bezpečnosti je možno konstatovat, že investor má v našich geopolitických reáliích oprávněná očekávání nejen co do fyzické bezpečnosti ale též co do obecné funkčnosti služeb informační společnosti. V případě, že stát není schopen zajistit fungující informační a komunikační infrastrukturu, jedná se z hlediska investora nejen o faktor při rozhodování o samotné lokalizaci investice ale může se jednat i o důvod založení odpovědnosti státu v případě, že investice byla uskutečněna a informační a komunikační infrastruktura není v důsledku bezpečnostní expozice adekvátně funkční.

Jedná se o podobnou situaci, jako kdyby stát nejprve nalákal investory na fungující dopravní infrastrukturu – ta by ale po nějakém čase přestala být použitelnou v důsledku častého výskytu dopravních přestupků, které policie nezvládá řešit. Podobnost s dopravní infrastrukturou však z hlediska investic samozřejmě není úplná - z tohoto srovnání však každopádně vychází jako dokonale absurdní zjištění, že kybernetická bezpečnost stále není předmětem agendy investiční konkurenceschopnosti České republiky.

V porovnání s dopravní infrastrukturou je potřeba investic do kybernetické bezpečnosti z hlediska nákladovosti o několik řádů méně náročnou. Současně lze poukázat na skutečnost, že bezpečně fungující informační a komunikační infrastruktura je relevantním faktorem lokalizace přesně těch typů investic, které jsou pro Českou republiku prioritní, tj. investic do oborů s vysokou mírou přidané hodnoty- Naproti tomu investice do dopravní infrastruktury, nepoměrně ve všech směrech náročnější, zdaleka neindukují jen ten typ investičního potenciálu, o který má mít Česká republika zájem (namísto toho jde o investice do nekvalifikované mechanické práce nebo jen manipulace se zbožím typu montoven nebo logistických center). Z toho plyne, že je absurdní, pokud Česká republika investuje v režimu podpory investic do rozvoje silniční nebo železniční sítě, aniž by ve stejném režimu investovala do zajištění služeb informační společnosti nebo kybernetické bezpečnosti.

Úloha soukromoprávních iniciativ typu oborových či profesních sdružení je v tomto směru evidentní především v otázkách přenosu informací mezi podnikatelským sektorem a veřejnou mocí. K náležitému nastavení resp. zaměření příslušných investic je totiž třeba především znát reálné potřeby adresátů investiční podpory. Platí přitom, že středně velcí a velcí mezinárodní investoři zpravidla nemají zájem o podporu nebo dokonce o zajištění interních systémů bezpečnosti informací. Naopak lze podle zahraničních zkušeností předpokládat, že adekvátní zaměření investiční podpory má vést k zajištění bezpečného fungování služeb informační společnosti a poskytovat v reálném čase metodiku a asistenci pro zvládání závažných kybernetických bezpečnostních incidentů s původem mimo příslušné podnikatelské subjekty.

Jinými slovy má z hlediska investora význam, pokud hostitelský stát investuje do nástrojů k obecnému zajištění bezpečného fungování informační a komunikační infrastruktury. V tomto směru je nutno připomenout, že investory vedle provozu jejich vlastních informační struktur zajímá též dostupnost informačních a komunikačních technologií ze strany jejich obchodních partnerů a široké veřejnosti, jakož i využití veřejně dostupných služeb informační společnosti k interním organizačním procesům (práce z domova, komunikace mezi pobočkami, provoz distančních spotřebitelských terminálů apod.) Profesní či oborové

organizace přitom mohou pomoci identifikovat konkrétní otázky v příslušných průmyslových odvětvích a koordinovat komunikaci mezi obchodní komunitou a orgány veřejné moci.

Pozitivní příklady důvěryhodné, efektivní a oboustranně výhodné vzájemné spolupráce na odborné úrovni není každopádně nutno brát jen ze zahraničí, byť je tato forma účasti průmyslových podniků na řešení odborných otázek veřejnou mocí běžná například v Německu, Spojeném Království nebo USA. Příkladem dobré praxe může být i shora zmíněný proces přípravy věcného záměru a posléze i textu paragrafového znění zákona o kybernetické bezpečnosti, kde se podařilo vést věcný dialog mezi podnikatelskou sférou a dotčenými veřejnoprávními korporacemi.

6.4 KYBERNETICKÁ BEZPEČNOST JAKO AGENDA ROZVOJOVÉ POMOCI

V současné době existují mezi jednotlivými státy velké rozdíly co do formy a intenzity řešení problematiky národní kybernetické bezpečnosti. Nedávná studie UNODC ukázala v tomto směru nikoli překvapivé obrovské rozdíly mezi rozvojovými a rozvinutými státy zjednodušeně označované jako rozdíly mezi severem a jihem[92]. Při následném projednávání výstupů této studie v rámci expertní skupiny UNODC pro kyberkriminalitu a kybernetickou bezpečnost byly tyto rozdíly nejen evidentní ale z nebývale ostré výměny názorů vyplynula potřeba zabývat se otázkou kybernetické bezpečnosti jako integrální součástí agendy rozvojové pomoci. Důležitost dostupnosti bezpečně fungující informační a komunikační infrastruktury je totiž možno srovnat s důležitostí ostatních základních společenských funkcionalit. Vlády rozvojových států však nedisponují dostatečnými finančními ani technickými kapacitami k jejímu zajištění[93].

Z výše uvedeného plyne, že účast rozvinutých států na investicích do bezpečnosti informační a komunikační infrastruktury v rozvojových státech má být motivována a legitimována stejnými morálními důvody jako např. potravinová pomoc nebo pomoc s rozvojem základní technické nebo

[92] Viz dokument Srovnávací studie počítačové trestné činnosti, publ. on-line na adrese http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[93] Srov. Bande, L. C. A Case for Cybercrime Legislation in Malawi, *Malawi Law Journal*, roč. 5, str. 93.

dopravní infrastruktury. V tomto případě však nemusí být motivace rozvinutých států pouze morální resp. sociální, ale může jít o prostý důsledek utilitaristické úvahy ekonomické resp. politické.

Obecně platí, že je z hlediska nákladovosti výhodnější pokrývat kybernetické bezpečnostní incidenty pokud možno co nejblíže místu jejich vzniku, a to z hlediska časového i geografického. Poskytují-li pak rozvojové země z důvodu neschopnosti investovat do bezpečnostních opatření něco jako bezpečné přístavy pro vznik a vývoj kybernetických bezpečnostních incidentů, je logicky zájmem cílových států (a většinou jde naopak právě o státy rozvinuté) pokrýt příslušná bezpečnostní rizika shora popsaným způsobem.

Strategické zaměření rozvojové pomoci do sektoru kybernetické bezpečnosti může nikoli jen zprostředkovaně ale přímo pomoci řešení bezpečnostní situace nejen ve státech, kam pomoc přímo směřuje ale možná i významnějším způsobem v zemích, kde se kybernetické bezpečnostní incidenty projevují. Dárce tedy v tomto případě chrání prostřednictvím své intervence sám sebe (podobně jako např. rozvojová pomoc směřující ke zvyšování kvality života vede ke snižování nelegální migrace a omezování následných problémů ekonomických, sociálních apod.)

Rozvojová pomoc v sektoru kybernetické bezpečnosti má speciálně v případě České republiky ještě další rozměr, a to podporu tuzemského výzkumu, vývoje a průmyslu v oboru pokročilých informačních a komunikačních technologií. Česká republika se, dlužno říci i přes dosavadní absenci prakticky jakékoli veřejné resp. politické podpory, dostala na špici v oboru kybernetické bezpečnosti, ať už jde o oblast primárního výzkumu (nikoli jen v oboru ICT, ale i v oboru práva, psychologie nebo sociálních věd), experimentálního a aplikovaného vývoje či komerčních aplikací. Existuje tedy v současné době u nás řada akademických pracovišť a podnikatelských subjektů, jejichž výsledky jsou plně srovnatelné v mezinárodním (nikoli jen evropském) měřítku a mohou řešit nejen aktuální problémy naší národní kybernetické bezpečnosti, ale jsou použitelné prakticky v libovolném národním nebo nadnárodní prostřední. Zaměří-li se pak do toho sektoru prostředky určené na rozvojovou pomoc (tj. pokud budou české instituce díky českým

rozvojovým programům řešit problémy kybernetické bezpečnosti rozvojových zemí), bude tímto způsobem možno obecně podporovat další rozvoj tohoto sektoru v České republice, to přitom bez toho, aby se jednalo o zakázanou veřejnou podporu nebo jinou formu zakázaného narušování tržního prostředí.

7. SHRNUTÍ

V tomto textu jsme se zabývali vybranými problémy českého pojetí právní úpravy fenoménu kybernetické bezpečnosti. První část je věnována pojmové klasifikaci kybernetické bezpečnosti, jejím specifickým rysům a především pragmatické metodě, jejíž implementace jeví se být vhodná k řešení partikulárních regulatorních otázek. Ohledně metodologie práva kybernetické bezpečnosti dospěli jsme k závěru, že určující význam technologických aspektů tohoto regulatorního fenoménu prakticky vylučuje důsledné využití metod pozitivistických i přirozenoprávních. Za riziko pragmatické (realistické) metody jsme pak označili náchylnost k postupné hodnotové degradaci, přičemž jsme jako preventivní faktory identifikovali solidnost institucionálního a personálního zajištění implementace příslušných právních pravidel.

Další část textu byla věnována principům českého zákona o kybernetické bezpečnosti a dále pak stručnému rozboru základních institutů, na nichž zákon obsahově spočívá. Z pochopitelných důvodů nebylo možno zde provést kritickou analýzu účinné právní úpravy vzhledem k aktuální judikatuře a vzhledem k relativní unikátnosti českého legislativního řešení nebylo možno učinit ani odpovídající srovnání s příbuznými právními řády. Pokusili jsme se však alespoň kriticky diskutovat smysl a účel jednotlivých našich zákonných institutů, popsat jejich vzájemné systematické vazby a též zhodnotit formální konzistenci s deklarovanými principy resp. s hodnotovými fundamenty českého práva.

Poslední část textu byla věnována perspektivám dalšího vývoje fenoménu kybernetické bezpečnosti v České republice. Výklad byl rozdělen na legislativní zadání a na úkoly k politickým či organizačním úvahám. Společným motivem legislativních i politicko-organizačních perspektiv byla na prvním místě úzká spolupráce mezi veřejným a soukromým sektorem,

která jako jediná může vzhledem k zásadní důležitosti konkrétních forem technické implementace zákonných povinností zajistit skutečné fungování celého regulatorního systému. Druhým podstatným momentem diskutovaným v této části pak byly výjimečně dobré výsledky české vědy a průmyslu v oboru informační bezpečnosti i pozoruhodné úspěchy té části veřejné moci, do jejíž kompetence spadal vývoj a implementace specifických právních pravidel – k nim však stojí v naprosté kontrapozici pouze občasný verbální zájem o tuto problematiku ze strany českých politických elit. Přestože tedy na poli kybernetické bezpečnosti hrají některé české akademické, soukromé i veřejné instituce příslovečnou Ligu mistrů, je povědomí a podpora ze strany politických špiček v této oblasti spíše na úrovni župního přeboru.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

OFFICE 365 V. GOOGLE APPS: SROVNÁNÍ Z HLEDISKA OCHRANY OSOBNÍCH ÚDAJŮ[*]

JAN TOMÍŠEK[**]

ABSTRAKT

Tento článek analyzuje poskytování softwaru jako služby z hlediska ochrany osobních údajů. Autor rozebírá možné role zákazníka a poskytovatele softwaru jako služby z pohledu ochrany osobních údajů, shrnuje požadavky na obsah smlouvy mezi zákazníkem jako správcem a poskytovatelem jako zpracovatelem osobních údajů a srovnává smlouvy na Google Apps for Work a Microsoft Office 365 ve světle těchto požadavků. Závěrem jsou čtenáři předloženy úvahy de lege ferenda a kritické zhodnocení připravované novely evropské regulace ochrany osobních údajů v kontextu cloud computingu.

KLÍČOVÁ SLOVA

software-as-a-service, SaaS, cloud, osobní údaje, smlouva, Google Apps, Office 365

ABSTRACT

This article analyses the provision of software as a service in terms of data protection. The author discusses possible roles of a client and a provider of software as a service in terms of protection of personal data, summarizes the requirements on contents of the contract between the client as a controller and the provider as a processor of personal data and compares the contracts for Google Apps for Work and Microsoft Office 365 in the light of these

[*] Tento článek byl ve zkrácené podobě a anglickém znění publikován v Masaryk University Journal of Law and Technology, 2015, roč. 9, č. 1.

[**] Mgr. Bc. Jan Tomíšek je absolvent Právnické fakulty a Fakulty informatiky Masarykovy univerzity a junior associate advokátní kanceláře ROWAN LEGAL. Věnuje se problematice software, ochraně osobních údajů, cloud computingu a kybernetické bezpečnosti. Kontaktní e-mail: jantomisek@gmail.com

requirements. As a conclusion are provided considerations de lege ferenda and critical evaluation of the prepared amendment to the European data protection regulation in the context of cloud computing.

KEYWORDS

software-as-a-service, SaaS, cloud, data protection, contract, Google Apps, Office 365

1. ÚVOD

Cloudové služby nejsou v technologickém světě žádnou novinkou, není je tedy třeba čtenáři dlouze představovat.[1] V případě, že zákazník využívající cloudové služby působí v Evropské unii (dále jen „EU“) a data zpracovávaná pomocí cloudové služby mohu sloužit k identifikaci jakékoli fyzické osoby, může poskytování cloudové služby spadat pod režim směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Směrnice 95/46/ES stanoví řadu požadavků na vztah mezi zákazníkem využívajícím cloudové služby a jejich poskytovatelem.

Od cloudových řešení se očekává podstatné zvýšení efektivity, zejména pro malé a střední podniky (dále jen „SME“), které si obvykle nemohou dovolit, ani plně využít rozsáhlá IT řešení vyhrazená pouze pro jejich potřebu.[2] SME v EU z cloudových služeb nejčastěji využívají e-mail a úložiště dat v cloudu.[3] Tyto služby jsou často integrované v on-line kancelářských balíčcích, jako jsou Microsoft Office 365 nebo Google Apps for Work. Pro SME však může být obtížné posoudit nabídky poskytovatelů těchto cloudových služeb z hlediska ochrany osobních údajů, neboť právní úprava stejně jako smluvní rámce poskytovatelů jsou velmi složité.

---

[1] Pro podrobnější úvod do problematiky cloudových služeb a software jako služby viz TOMÍŠEK, Jan. Licence při poskytování software jako služby. *Revue pro právo a technologie*, Masarykova univerzita, 2014, roč. 2014, č. 10, s. 47-69. ISSN 1804-5383.

[2] Viz Unleashing the Potential of Cloud Computing in Europe. *Evropská komise* [online]. 27 9. 2012 [cit. 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF, s. 4.

[3] Viz Use of cloud computing services. *Eurostat* [online]. Publikováno 16. 1. 2015 [cit. 15. 2. 2015]. Dostupné z: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cicce_use&lang=en

Cílem tohoto článku je proto v prvé řadě sumarizovat požadavky na obsah smlouvy mezi poskytovatelem a zákazníkem cloudových služeb plynoucí ze směrnice 95/46/ES s přihlédnutím k ustanovením některých národních implementací. Následně budou na základě těchto požadavků z hlediska ochrany údajů vyhodnoceny a porovnány smlouvy na poskytování služby Google Apps for Work a Microsoft Office 365 nabízené SME. Na závěr budou diskutovány nedostatky stávajícího právního rámce pro ochranu údajů ve vztahu ke cloud computingu a analyzována potenciální zlepšení, která může přinést připravované obecné nařízení o ochraně údajů.

2. OCHRANA OSOBNÍCH ÚDAJŮ V CLOUDU

Povinnosti zákazníků a poskytovatelů cloudových služeb ve vztahu k ochraně osobních údajů silně závisí na rolích, které jsou jim v konkrétním vztahu přiřazeny směrnicí 95/46/ES. Tyto role jsou dány mnoha faktory, z nichž prvním je charakter dat zpracovávaných v cloudu. V případě, že data nejsou osobními údaji, se směrnice 95/46/ES nemusí vůbec aplikovat. Směrnice 95/46/ES definuje osobní údaje jako „veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů)[,]“ kde „identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity[.]“[4] Široký záběr této definice je dále podporován preambulí směrnice 95/46/ES, která uvádí, že „pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby[.]“[5]

Rozumná šance, že konkrétní prostředek bude použit a umožní identifikaci, je dána především kontextem každého jednotlivého zpracování.[6] Existují určitá technická opatření, která mohou být v rámci

[4] Viz článek 2 písm. a) směrnice 95/46/ES.

[5] Viz recitál 26 směrnice 95/46/ES.

[6] Lord Hope v odst. 26 rozhodnutí Sněmovny lordů Spojeného království ze dne 9. 7. 2008, Common Services Agency v Scottish Information Commissioner (Scotland), věc [2008] UKHL 47 uvádí: „Kdyby pro příjemce […] dat bylo nemožné identifikovat tyto jednotlivce, informace by v jeho rukách nebyly ‘osobními údaji.‘“

cloudových služeb uplatněna, aby se zabránilo příjemci dat identifikovat dotčené jednotlivce, jako je například anonymizace nebo šifrování dat. Tato opatření mohou zbavit data jejich charakteru osobních údajů ve smyslu směrnice 95/46/ES ve vztahu ke konkrétnímu příjemci,[7] možnost jejich praktického uplatnění je však limitovaná. Například, pokud by adresář v rámci služby cloudového e-mailu byl zašifrovaný tak, že by poskytovatel služby neměl přístup k uloženým adresám, uživatel by nemohl mít k dispozici funkce prohledávání těchto adres, třídění přijatých e-mailů ve své schránce, prevence označení e-mailů z těchto adres za SPAM apod. Pokud by všechny dokumenty, které by měly být uloženy v cloudovém úložišti dokumentů, musely být nejprve prohledány a zbaveny všech odkazů na identifikovatelné jednotlivce, nahrané dokumenty by se v mnoha případech staly zcela nepoužitelnými. Proto musíme předpokládat, že v případě nejčastěji využívaných cloudových služeb, jako je e-mail nebo úložiště dokumentů, uložená a zpracovaná data představují osobní údaje ve smyslu směrnice 95/46/ES.

Je rovněž otázkou, zda jsou osobní údaje v cloudu skutečně zpracovány ve smyslu směrnice 95/46/ES. Vzhledem k tomu, že definice zpracování ve směrnici 95/46/ES[8] je velmi široká obdobně jako definice osobního údaje a že všechny běžné cloudové služby zahrnují ukládání dat, což je operace, která je považována za zpracování, odpověď bude v naprosté většině případů kladná.

Pokud mohou být data nebo jejich části považovány za osobní údaje ve smyslu směrnice 95/46/ES a jsou v cloudu zpracovávána ve smyslu směrnice 95/46/ES, pak alespoň jedna z osob podílejících se na této činnosti musí být správcem těchto osobních údajů. Správcem osobních údajů je podle směrnice 95/46/ES subjekt, který „určuje účel a prostředky zpracování[.]“[9] V případě těch cloudových služeb, které jsou nabízeny

---

[7] Viz HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. The problem of ‘personal data’ in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law* [online]. 2011, vol. 1, no. 4, p. 211-228 [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/1/4/211.full.pdf+html, s. 214.

[8] Zpracováním se dle článku 2 písm. b) směrnice 95/46/ES rozumí „jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace[.]“

[9] Viz článek 2 písm. d) směrnice 95/46/ES.

široké veřejnosti (tj. nejsou vytvořeny na míru individuálním požadavkům zákazníka), je to vždy poskytovatel, kdo určuje vlastnosti služby, jako je formát a rozsah dat, způsob, jakým jsou uložena a prostředky jejich ochrany, přičemž prostor pro jednání o jednotlivých parametrech, může být velmi omezený.[10] Může se proto zdát, že tato rozhodnutí posouvají poskytovatele do role správce osobních údajů.[11] Ve skutečnosti je to však rozhodnutí zákazníka přijmout nabídku konkrétního poskytovatele, které určuje způsob zpracování.[12] Bez tohoto rozhodnutí poskytovatel nebude data vůbec zpracovávat. V případě, že rozhodnutí využít určitou cloudovou službu je na zákazníkovi, pak by on měl být považován za správce osobních údajů, které jsou pomocí této služby zpracovávány.

To však nevylučuje možnost, aby byl poskytovatel správcem také. V případě, že se poskytovatel rozhodne použít data pro jiné účely než ty zvolené zákazníkem, může se také stát správcem údajů,[13] stejně jako když poskytovatel otevřeně využívá data pro marketingové a reklamní účely (jako je poskytování cílené reklamy pro uživatele služeb).

Ve většině situací však bude poskytovatel zpracovatelem osobních údajů - subjektem, který zpracovává osobní údaje pro správce.[14] Toto rozdělení rolí předpokládá i Article 29 Data Protection Working Party (Pracovní skupina pro ochranu dat podle článku 29 směrnice 95/46/ES, dále jen jako „WP29“) stejně jako mnoho národních úřadů pro ochranu údajů ve svých

---

[10] Individuální úpravy služby by většinou výrazně zvýšily náklady pro poskytovatele, a tím narušily jeho obchodní model. Podle zkušeností autora je prostor pro jednání s významnými poskytovateli cloudových služeb velmi omezený i v případě velkých zákazníků, proto jsou jakékoli změny služby nebo jejích podmínek pro SME nedosažitelné.

[11] Tuto možnost diskutují Hon a kol. Viz HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2 *International Data Privacy Law* [online]. 2012, vol. 2, no. 1, pp. 3-18 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/1/3.full.pdf+html, s. 6.

[12] Viz Opinion 05/2012 on Cloud Computing. *Evropská komise* [online]. Article 29 Data Protection Working Party, 2012 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (dále jen „WP196“), s. 8.

[13] Tento scénář nastal např. v případě Společnosti pro celosvětové mezibankovní finanční telekomunikace (SWIFT), která provedla některé operace jako předání dat dalším příjemcům (konkrétně Ministerstvu financí USA) bez vědomí orgánů, které ji pověřily jako zpracovatele. Následně WP29 vydala stanovisko, že SWIFT by měla být považován za správce zpracovávaných osobních údajů. Viz Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). *Evropská komise* [online]. Article 29 Data Protection Working Party, 2006 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf, p. 26.

[14] Viz článek 2 psím. e) směrnice 95/46/ES.

stanoviscích a doporučeních ve vztahu ke zpracování osobních údajů v cloudu.[15] Přesto se mohou vyskytovat případy, kdy situace nebude tak jasná.

Když poskytovatel cloudu poskytuje zákazníkovi pouze úložnou kapacitou pro nestrukturovaná data (tedy ne například chytré úložiště dokumentů s možností vyhledávání atd.) nebo výpočetní výkon, nemusí mu být (a obvykle není) známa povaha dat, která se zákazník rozhodne zpracovávat prostřednictvím poskytovaných zdrojů. Přesto definice zpracování ve směrnice 95/46/ES nerozlišuje, zda si je zpracovatel vědom osobní povahy údajů, nebo ne. V takovém případě by se pozice poskytovatele měnila v závislosti na typu dat, která se zákazník rozhodne zpracovávat, a to aniž by o tom poskytovatel věděl. Takové rozdělení rolí může mít za následek nevyvážené rozložení povinností a zatěžování jak zákazníka, tak poskytovatele v míře, která není přiměřená v poměru k možnému riziku, které přináší zapojení poskytovatele do činnosti zákazníka.[16]

V tomto směru nám může poskytnout vodítko směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. Tato směrnice vytváří systém bezpečných přístavů omezujících určité aspekty odpovědnosti některých poskytovatelů služeb informační společnosti. Mezi poskytovateli, jejichž odpovědnost je omezena, jsou také poskytovatelé hostingových služeb,[17] kteří neodpovídají za informace uložené uživatelem služby, pokud „nebyl[i] účinně seznámen[i] s protiprávní činností nebo informací[.]“[18]

---

[15] Viz *Stanovisko č. 65/2013/4* [online]. Úřad pro ochranu osobních údajů, publikováno 1. července 2013 [cit. 11. 2. 2015]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002, s. 3.

Guidance on the use of cloud computing [online]. Srov. též Information Commissioner's Office, 2012, [cit. 11. 2. 2015]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf, p. 8. *Guía para clientes que contraten servicios de Cloud Computing* [online]. Srov. také Agencia Española de Protección de Datos, 2013 [cit. 11. 2. 2015]. Dostupné z: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf, p. 13.

[16] Viz HON, MILLARD, WALDEN, 2012, op. cit., s 11.

[17] Za hosting se dle článku 14 odst. 1 směrnice o elektronickém obchodu považují „služby informační společnosti spočívající v ukládání informací poskytovaných příjemcem služby[.]“

[18] Viz článek 14 odst. 1 písm. a) směrnice o elektronickém obchodu.

Směrnici o elektronickém obchodu můžeme vnímat jako zdroj obecných pravidel týkajících se odpovědnosti poskytovatelů služeb informační společnosti a směrnici 95/46/ES jako zdroj zvláštních pravidel týkajících se odpovědnosti v případech, kdy poskytovatelé služeb informační společnosti zpracovávají osobní údaje. Pak by nebylo možné povinnosti takových poskytovatelů na základě směrnice o elektronickém obchodu ve vztahu k ochraně osobních údajů omezit. Nicméně směrnici 95/46/ES můžeme též vnímat jako obecné pravidlo pro všechny zpracovatele osobních údajů a směrnici o elektronickém obchodu jako zvláštní předpis upravující otázky odpovědnosti, který je aplikovatelný také na nakládání s osobními údaji ze strany poskytovatelů hostingu podle směrnice o elektronickém obchodu. Takovým výkladem v podstatě říkáme, že osobní působnost směrnice o elektronickém obchodu je užší než směrnice 95/46/ES). Na základě této interpretace pak mohou být poskytovatelé hostingu vyňati z postavení zpracovatele osobních údajů.[19]

Může být diskutabilní, zda všechny povinnosti zpracovatele osobních údajů a všechny odpovídající povinnosti správce osobních údajů ve vztahu ke zpracovateli mohou spadat pod pojem „odpovědnost". Navíc, zatímco vynětí poskytovatelů hostingu z pozice zpracovatele osobních údajů může být vyváženým řešením ve vztahu ke cloud computingu, nemusí fungovat v jiných případech a je třeba vzít v úvahu potenciální vedlejší dopady takového závěru.

Nicméně i když uzavřeme, že na poskytovatele hostingu se vztahuje výjimka z povinností zpracovatele osobních údajů dle směrnice 95/46/ES, tato výjimka se bude vztahovat pouze na poskytovatele obsahově neutrálních zdrojů, jakými jsou úložný prostor a výpočetní výkon.[20] V případě Google Apps for Work a Microsoft Office 365 je situace zcela jiná. Obě služby poskytují svým uživatelům e-mailovou schránku, adresář, úložiště dokumentů apod. Je tedy zřejmé, že údaje zpracovávané za použití těchto služeb budou způsobilé k identifikaci jednotlivých uživatelů a dokonce i dalších osob, je tedy třeba považovat je za osobní údaje ve

[19] Tato stanovisko zastává též Sartor. Viz SARTOR, Giovanni. Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? *International Data Privacy Law* [online]. 2013, vol. 3, no. 1, pp. 3-12 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/3/1/3.full.pdf+html

[20] Většina takových služeb spadá do kategorie Infrastructure-as-a-service (IaaS).

smyslu směrnice 95/46/ES. Navíc lze veškerý obsah těchto služeb prohledávat pomocí fulltextových indexů sestavených poskytovateli. Pro vytvoření těchto indexů je nezbytné aktivní zpracování ukládaných dat. Proto budeme dále vycházet ze skutečnosti, že využívání těchto služeb představuje zpracování osobních údajů ve smyslu směrnice 95/46/ES, kdy zákazník je správcem osobních údajů a poskytovatel služeb je jejich zpracovatelem.

3. POŽADAVKY NA SMLOUVU O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Z výše popsaného rozdělení rolí vyplývá řada požadavků na právní vztah mezi poskytovatelem a zákazníkem. Prvním a nejdůležitějším požadavkem je existence právního aktu upravujícího vztahy mezi zákazníkem jako správcem a poskytovatelem jako zpracovatelem osobních údajů.[21] Zatímco samotná směrnice 95/46/ES neurčuje formu tohoto právního aktu, vnitrostátní právní úpravy jednotlivých členských států často vyžadují, aby měl formu smlouvy.[22] Poskytovatel cloudových služeb, který cílí na zákazníky z celého trhu EU, by měl proto předpokládat, že je z hlediska ochrany osobních údajů nutné se zákazníkem uzavřít smlouvu (obvykle nazývanou smlouva o zpracování osobních údajů, data processing agreement, DPA), která musí být v písemné nebo v jiné ekvivalentní formě.[23]

Směrnice 95/46/ES vyžaduje, aby smlouva stanovila, že „zpracovatel jedná pouze podle pokynů správce[.]“[24] Tento požadavek odráží zásadu omezenosti účelem zpracování, která je zakotvena v článku 6 odst. 1 písm. b) směrnice 95/46/ES, neboť je to zákazník cloudové služby jako správce osobních údajů, kdo určuje účel zpracování. V případě, že by poskytovatel překročil pokyny zákazníka, stal by se sám správcem údajů, jak je popsáno výše.

---

[21] Viz článek 17 odst. 3 směrnice 95/46/ES.

[22] Viz oddíl 1, část II, odst. 12 Data Protection Act 1998 (britský zákon o ochraně osobních údajů). Viz též § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých předpisů, ve znění pozdějších předpisů. Srov. též článek 12 odst. 2 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (španělský zákon o ochraně osobních údajů).

[23] Viz článek 17 odst. 4 směrnice 95/46/ES.

[24] Viz článek 17 odst. 3 směrnice 95/46/ES.

Vzhledem k tomu, že dodržování zásady omezenosti účelem je klíčovou povinností poskytovatele, účel zpracování by měl být uveden ve smlouvě.[25] Jeho vymezení nemusí být totožné s vymezením účelu, pro který byly údaje shromážděny, ale tyto dva účely musí být ve vzájemném souladu (článek 6 odst. 1 písm. b) směrnice 95/46/ES zakazuje zpracování pro účely, které jsou neslučitelné s účelem původním). Aby bylo zajištěno, že jsou pomocí dané cloudové služby zpracovávána pouze data pro daný účel legálně získaná, měla by smlouva uvádět výčet typů osobních údajů, které budou zpracovávány (tj. jméno, emailová adresa, polohové údaje, atd.), stejně jako celkový rozsah a způsob zpracování.[26]

Stanovisko WP29 ke cloud computingu dále doporučuje, aby ve smlouvě byly obsaženy „podrobnosti o rozsahu a způsobu dávání instrukcí zákazníka, které může dávat poskytovateli zejména s ohledem na aplikované SLA (které by mělo být objektivní a měřitelné) a příslušné sankce (finanční nebo jiné včetně možnosti žalovat poskytovatele v případě neplnění).“[27] Ačkoli požadavek na obsažení těchto podrobností ve smlouvě nemá přímou oporu ve směrnici 95/46/ES, jejich absence může způsobit nevymahatelnost smlouvy o zpracování osobních údajů a tím porušení článku 6 odst. 3 směrnice 95/46/ES. Z tohoto důvodu lze jejich zapracování důrazně doporučit nejen z obchodního hlediska, ale také z hlediska ochrany osobních údajů.

Druhou klíčovou povinností poskytovatele cloudových služeb jako zpracovatele osobních údajů, která musí být zahrnuta ve smlouvě, je povinnost dodržovat dohodnutá technická a organizačních opatření zavedená na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu a všem dalším formám nedovoleného zpracování.[28]

Směrnice 95/46/ES nespecifikuje konkrétní bezpečnostní opatření, která k ochraně osobních údajů musí být zavedena. Jediným požadavkem

[25] Nedostatečné vymezení účelu zpracování bylo švédským úřadem pro ochranu osobních údajů Datainspektionen v případě Salem shledáno jako porušení práva na ochranu osobních údajů. Viz SVANTESSON, Dan Jerker B. Data protection in cloud computing – The Swedish perspective. *Computer Law & Security Review* [online]. 2012, vol. 28, issue 4, s. 476-480 [cit. 15. 2. 2015]. Dostupné ze ScienceDirect: http://linkinghub.elsevier.com/retrieve/pii/S0267364912001021, s. 479.

[26] Viz WP196, s. 13.

[27] Viz WP196, s. 12. Viz také SVANTESSON, 2012, op. cit., s. 479.

[28] Viz článek 6 odst. 1 a 3 směrnice 95/46/ES.

směrnice je, aby zajišťovala „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.“[29] Některé národní úpravy se drží úrovně podrobnosti směrnice 95/46/ES (například zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých předpisů, ve znění pozdějších předpisů), ale jiné stanoví specifické požadavky nebo opatření zaměřená na různé rizikové profily (například ve Španělsku nebo v Polsku[30]). Poskytovatel cloudových služeb by proto měl zvážit výsledky své analýzy rizik jako základ pro rozhodnutí, zda dále studovat vnitrostátní právní předpisy členských států. Toto bližší nastudování může být u rizikovějších služeb nezbytné, aby bylo zajištěno, že služba bude v souladu s právní úpravou, a tudíž zákaznicky atraktivní na trzích všech jednotlivých členských států EU.

Bezpečnostním opatřením by měl zákazník věnovat pozornost již v okamžiku, kdy vybírá poskytovatele cloudových služeb. Zajištění dodržování těchto opatření zpracovatelem je povinností zákazníka, která musí být plněna průběžně po celou dobu zpracování.[31] Smlouva o zpracování osobních údajů by proto měla dávat zákazníkovi patřičné nástroje, jež mu umožní dohlížet nad dodržováním těchto opatření ze strany poskytovatele, stejně jako prostředky nápravy pro situaci, kdy povinnost dodržovat opatření byla porušena.[32]

Není nezbytné, aby zákazník měl právo provádět audit poskytování služeb osobně přímo u poskytovatele – takový požadavek by byl nepřijatelný pro většinu velkých poskytovatelů.[33] Nicméně poskytovatel

[29] Viz článek 17 odst. 1 směrnice 95/46/ES.

[30] Prováděcí předpis k španělskému zákonu o ochraně osobních údajů stanovuje opatření pro nízkou, střední a vysokou úroveň ochrany a zároveň stanoví, kde se tyto úrovně aplikují. Viz článek 80 Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Obdobný přístup je aplikován v prováděcím předpise k polskému zákonu o ochraně osobních údajů. Viz článek 6 odst. 2 Rozporządzenie Ministra spraw wewnętrznych i administracji Dz. U. z 2004 r. Nr 100, poz. 1024, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[31] Viz článek 17 odst. 2 směrnice 95/46/ES.

[32] Viz WP196, s. 13.

[33] Jejich pozice je v tomto směru pochopitelná. Pokud by každý z velkého počtu jejich zákazníků měl právo provést audit u poskytovatele osobně, strávil by poskytovatel více času řešením auditů než poskytování služeb, což by se neudržitelným způsobem promítlo do jeho nákladů a tedy i ceny služeb, navíc by zvýšený pohyb osob v prostorách poskytovatele mohl ve výsledku spíše ohrozit bezpečnost jeho služeb.

cloudových služeb by měl být povinen poskytnout zákazníkovi dostatečný důkaz plnění bezpečnostních opatření z jeho strany, jakým je bezpečnostní certifikace nebo auditní zpráva, například certifikace dle ISO 27001 nebo nedávno schváleného standardu týkajícího se zpracování osobně identifikovatelných informací v cloudu ISO 27018. Tato povinnost by měla být dále doprovázena právem zákazníka požadovat doplňující informace, pokud shledá předložené důkazy o plnění bezpečnostních opatření jako nedostatečné.

Pokud jde o prostředky nápravy, zákazník zůstává primárně odpovědný za veškeré bezpečnostní incidenty vzniklé v průběhu zpracování,[34] měl by proto mít možnost smluvně převést příslušnou část odpovědnosti na poskytovatele cloudových služeb. Odpovědnost poskytovatele by tedy neměla být limitovaná v takovém rozsahu, aby byla téměř veškerá odpovědnost ponechána na zákazníkovi.[35] Kromě toho by měl zákazník mít možnost vypovědět smlouvu o zpracování osobních údajů, pokud zjistí podstatné porušení dohodnutých opatření, které nebude poskytovatelem v přiměřeném čase napraveno.

Jelikož některé národní právní řády vyžadují, aby vztah mezi poskytovatelem a zákazníkem byl upraven smlouvou, všechny jeho podmínky by měly být výsledkem konsensu obou smluvních stran a neměly by být měněny jednostranně (jinak by takové právní jednání nebylo možné považovat za smlouvu). Přinejmenším ne ty, které se týkají základních podmínek upravujících pokyny zákazníka a bezpečnostní opatření.[36]

Všechny tyto podmínky stanovené ve smlouvě o zpracování osobních údajů musí být zároveň zachovány i v případě, kdy cloudová služba není zajišťována pouze poskytovatelem samotným, ale jeho subdodavateli.

---

[34] To zdůrazňuje Svantesson. Viz SVANTESSON, 2012, op. cit., s. 479.

[35] Na tento problém upozorňuje též MCGILLIVRAY, Kevin. Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology & Intellectual Property*. 2014, roč. 17, č. Fall 2014, pp. 217–253. s. 248.

[36] Švédský úřad pro ochranu osobních údajů dospěl k závěru, že smlouva umožňující jednostranné změny ze strany poskytovatele je v rozporu se švédským zákonem o ochraně osobních údajů. SVANTESSON, 2012, op. cit., s. 477. Podobně Dánský úřad pro ochranu údajů Datatilsynet zakázal magistrátu města Odense používat Google Apps, protože (mezi jinými důvody) smlouva na jejich poskytování mohla být ze strany Google jednostranně měněna. Viz DEBUSSCHE, Julien; VAN ASBROECK, Benoit; CHLOUPEK, Vojtěch a kol. Cloud computing and privacy series: the data protection legal framework (part 2 of 6). *Bird&Bird* [online]. 24 11. 2014 [cit. 15. 2. 2015]. Dostupné z http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-and-privacy-series-the-data-protection-legal-framework

Vzhledem k tomu, že zákazník jako správce osobních údajů musí zajistit, aby byla dodržována vhodná technická a organizační opatření, musí být plnění této povinnosti zajištěno i pokud jde o subdodavatele poskytovatele. Podmínky subdodavatelské smlouvy by proto ve vztahu k ochraně osobních údajů měly kopírovat podmínky smlouvy uzavřené mezi zákazníkem a poskytovatelem. Zákazník by měl být informován o všech subdodavatelích podílejících se na zpracovávání osobních údajů a jeho souhlas by měl být vyžadován k zapojení jakéhokoli nového subdodavatele, který by se na této činnost měl podílet. Předchozí souhlas zákazníka však nemusí být v mnoha případech udržitelným řešením.[37] Smlouva by proto měla poskytovatele zavazovat alespoň k tomu, aby zákazníka o zapojení nového poskytovatele upozornil s dostatečným předstihem, a dávat zákazníkovi právo smlouvu ukončit v případě, že s volbou nového subdodavatele nebude souhlasit.[38]

Pokud je účel zpracování naplněn nebo odpadne titul pro zpracování, typicky tehdy, když subjekt údajů odvolá svůj souhlas se zpracováním nebo je ukončena smlouva o zpracování mezi zákazníkem a poskytovatelem, pak osobní údaje nesmí být dále zpracovávány.[39] Tato možnost by měla být ve smlouvě ošetřena zejména stanovením postupu a časového rámce pro vymazání dat po ukončení smlouvy.[40]

Zákazník musí plnit své povinnosti jako správce osobních údajů, které má vůči subjektům údajů, i v případě, že jsou osobní údaje zpracovávány v cloudu.[41] V některých případech toho však nemusí být schopen bez asistence poskytovatele. Proto by smlouva měla stanovovat povinnost poskytovatele cloudových služeb poskytnout zákazníkovi součinnost v plnění požadavků subjektů osobních údajů zpracovávaných pomocí

---

[37] Např. tam kde má poskytovatel velký počet zákazníků.

[38] „Transparentnost v cloudu znamená, že je nutné, aby zákazník cloudové služby byl informován o všech subdodavatelů podílejících se na poskytování příslušné cloudové služby[.]“ WP196, s. 11. Podobné požadavky byly vzneseny švédským úřadem pro ochranu osobních údajů v případě Salem. Viz SVANTESSON, 2012, op. cit., s. 477. Tento požadavek byl také potvrzen španělským Nejvyšším soudem. DEBUSSCHE, VAN ASBROECK, CHLOUPEK, 2014, op. cit.

[39] Viz článek 6 odst. 1 písm. a) směrnice 95/46/ES.

[40] Viz WP196, s. 13. Tento požadavek je opodstatněný, avšak z technického hlediska velmi problematický např. ve vztahu k dlouhodobým zálohám dat. Jednotlivé zálohy mohou být uloženy v jednom souboru na médiu se sekvenčním přístupem, jako je magnetická páska. V takovém případě je výmaz dat jednotlivého zákazníka prakticky nerealizovatelný.

[41] Práva subjektů údajů jsou stanovena v článcích 12, 14 a 15 směrnice 95/46/ES.

příslušné cloudové služby.[42] Kromě toho by zákazník měl být informován o všech bezpečnostních incidentech týkajících se osobních údajů, jinak by nebyl schopen plnit svoji informační povinnost vůči subjektům zpracovávaných údajů.[43]

Poslední klíčový požadavek na smlouvu o zpracování osobních údajů se vztahuje k umístění zpracovávaných dat. Poskytovatel cloudových služeb nemusí být schopen informovat zákazníka o umístění konkrétní části dat, ale může mu poskytnout seznamem lokalit, kde data mohou být zpracovávána. Zejména jde o datová centra používaná pro poskytování služby zákazníkovi, ale též pracoviště technické podpory a další místa, odkud pracovníci nebo subdodavatelé poskytovatele mohou k datům přistupovat. Tento seznam nemusí nutně specifikovat jednotlivá místa, ale měl by uvádět aspoň země nebo regiony, ve kterých mohou být osobní údaje uloženy nebo odkud k nim může být přistupováno. Bez této informace si nemůže zákazník být jist, že smlouva splňuje veškeré požadavky na předávání osobních údajů do jiných států.

Osobní údaje mohou být předány mimo EU pouze do zemí s odpovídající úrovní ochrany, které jsou určeny rozhodnutími Evropské komise.[44] Do USA mohou být osobní údaje volně předávány, pokud je poskytovatel cloudových služeb jako příjemce těchto údajů certifikován v programu Safe Harbor organizovaném Ministerstvem obchodu USA a zůstává takto certifikovaný po celou dobu zpracování. Do tzv. třetích zemí, které nezajišťují odpovídající úroveň ochrany, mohou být osobní údaje volně předávány ke zpracování za podmínky, že se zákazník a poskytovatel cloudových služeb zaváží dodržovat závazná podniková pravidla (binding corporate rules, BCR) proces schvalování takových pravidel je však složitý a nákladný, zvláště pro SME.[45]

Druhou možnou cestou k předávání osobních údajů do zahraniční bez potřeby zvláštního souhlasu dozorového orgánu je začlenění standardních

[42] Viz WP196, s. 13. Viz také SVANTESSON, 2012, op. cit., s. 478.

[43] Viz WP196, s. 13.

[44] Viz článek 25 směrnice 95/46/ES. Za takové země jsou považovány např. Švýcarsko, Kanada nebo Izrel. Blíže viz. Evropská komise. *Commission decisions on the adequacy of the protection of personal data in third countries* [online]. 18. 12. 2014 [cit. 14. 3. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[45] MCGILLIVRAY, 2014, op. cit., s. 246.

smluvních doložek podle rozhodnutí Komise 2010/87/EU do smlouvy o zpracování údajů.[46] Cílem těchto doložek je smluvní cestou překonat nedostatek náležité ochrany osobních údajů v cílové zemi.

Tyto standardní smluvní doložky nemusí být jedinými podmínkami smlouvy o zpracování osobních údajů. Rozhodnutí Komise 2010/87/EU výslovně uvádí, že „[v]ývozce údajů a dovozce údajů […] mohou do smluv libovolně začlenit jakékoli další doložky, které se vztahují k předmětu obchodu a které jsou podle jejich názoru vhodné pro účely dané smlouvy, nejsou-li v rozporu se standardními smluvními doložkami.“[47]

Existuje samozřejmě mnoho dalších otázek, které by měly být ošetřeny ve smlouvách na poskytování cloudových služeb a které přispívají k nejvyšším standardům v oblasti ochrany osobních údajů, jako je například notifikace o přístupu orgánů činných v trestním řízení k zpracovávaným datům nebo otázka interoperability,[48] ale žádná z nich není z hlediska směrnice 95/46/ES vyžadována.

4. ANALÝZA SMLOUVY O POSKYTOVÁNÍ GOOGLE APPS FOR WORK

Poskytování služby Google Apps pro práci jejím uživatelům se řídí smlouvou Google Apps Enterprise (Online) Agreement[49] (Smlouva GA), která je uzavírána při registraci k službám. Tato smlouva může být dále změněna, pokud zákazník vyjádří souhlas s dodatkem Data Processing Amendment to a Google Apps Agreement[50] (Dodatek DP) nebo Model contract clauses for Google Apps[51] (MCC). Nicméně přijetí těchto dalších smluvních dokumentů je dobrovolné a vyžaduje zvláštní kroky, které musí

[46] Viz články 27 a 26 odst. 4 směrnice 95/46/ES.

[47] Viz recitál 4 rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES.

[48] Viz WP196, s. 13.

[49] Viz *Google Apps Enterprise (Online) Agreement* [online]. Google, únor 2014 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html

[50] Viz *Data Processing Amendment to Google Apps Agreement* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/dpa_terms.html

[51] Viz *Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/mcc_terms.html.

zákazník provést v administrátorské konzoli.[52] U zákazníků se sídlem v EU je smlouva uzavírána s Google Commerce Limited, společností založenou podle irského práva se sídlem v Dublinu (dále jen „Google“).

Smlouva GA sama o sobě nesplňuje základní požadavky na smlouvu o zpracování osobních údajů. Ačkoli stanoví, že zákazník je správcem osobních údajů a Google jejich zpracovatelem, stejně jako že Google bude vázán pokyny zákazníka,[53] bezpečnostní opatření k ochraně osobních údajů nejsou ošetřena dostatečně.

Odst. 2.2 Smlouvy GA uvádí, že Google může zpracovávat data zákazníka „k následujícím účelům: (a) naplnění Instrukcí; (b) poskytování služeb (jak byly zvoleny zákazníkem prostřednictvím administrátorské konzole); (c) poskytování funkcí produktů s cílem usnadnit Zákazníkovi používání služby, jakož i nástrojů pro Zákazníka k vytváření obsahu; (d) provozu, údržbě a podpoře infrastruktury sloužící k poskytování služeb a (e) reagování na žádosti o zákaznickou podporu“ (překlad JT). Kromě toho Google tamtéž zaručuje, že „bude Data zákazníka zpracovávat pouze v souladu s touto dohodou a nebude zpracovávat Data zákazníka k žádnému jinému účelu“ (překlad JT). Instrukce zákazníka Googlu jsou řešeny v definici pojmu „Instrukce“, kterým se rozumí: „pokyny dané Zákazníkem prostřednictvím administrátorské konzole, pokyny iniciované Zákazníkem a Koncovými uživateli v rámci jejich užívání Služeb, písemné pokyny Zákazníka jak jsou uvedené v této Smlouvě (ve znění pozdějších dodatků a změn) a všechny následné písemné pokyny Zákazníka Googlu a uznané Googlem“ (překlad JT)[54] Nicméně smlouva neuvádí, jaké typy údajů budou na jejím základě zpracovávány. Ostatní podrobnosti ve vztahu k pokynům klienta, jako je například dohoda o úrovni služeb (Service Level Agreement, SLA), jsou ve smlouvě ošetřeny s přijatelnou mírou detailu.

Nedostatečně jsou ve Smlouvě GA upravena bezpečnostní opatření. Smlouva pouze uvádí, že „Google přijme a uplatní vhodná technická a organizační opatření na ochranu Dat zákazníka proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému

[52] Viz Model contract clauses for Google Apps. *Google Apps Help Center* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://support.google.com/a/answer/2888485?hl=en

[53] Viz odst. 2.3 Smlouvy GA.

[54] Viz článek 15 Smlouvy GA.

sdělování nebo přístupu“ (překlad JT),[55] a to bez dalších podrobností. Takovýto obecný popis nesplňuje požadavky směrnice 95/46/ES, protože podle této směrnice opatření musí být přezkoumána a schválena zákazníkem ve vztahu k jeho vlastnímu posouzení rizik.

Google řeší tento nedostatek Smlouvy GA tím, že nabízí svým zákazníkům sídlícím v EU možnost uzavřít Dodatek DP, ale využití této možnosti není zákazníkům automaticky doporučováno.[56] Přitom ti zákazníci, kteří si aktivně nevyhledají tuto možnost a nevyužijí ji, porušují používáním služeb Google Apps své povinnosti plynoucí z legislativy na ochranu osobních údajů.

Dodatek DP překonává některé z nedostatků Smlouvy GA. Dále omezuje účely zpracování tak, že společnost Google může zpracovávat data zákazníka k „(i) poskytování Služeb (což zahrnuje detekci, prevenci a řešení bezpečnostních a technických problémů) a (ii) reagování na žádosti zákazníků o podporu“ (překlad JT).[57] Ve své příloze č. 1 uvádí typy zpracovávaných osobních údajů. Nejdůležitějším zlepšením, které Dodatek DP přináší, je však popis implementovaných bezpečnostních opatření v jeho příloze č. 2. Tento popis je podrobný a umožňuje zákazníkovi, aby zhodnotil, zda jsou tato opatření dostatečná pro jeho rizikový profil.

Pokud jde o důkaz skutečné implementace deklarovaných opatření, Google se zavazuje, že bude pro služby udržovat certifikaci ISO/IEC 27001:2005 nebo srovnatelnou certifikaci, a to po celou dobu trvání Smlouvy GA,[58] a dále auditní zprávu SSAE č. 16 typ II / SAE č. 3402 nebo srovnatelnou zprávu o logických bezpečnostních opatřeních, fyzických bezpečnostních opatřeních a dostupnosti systémů používaných pro poskytování těchto služeb.[59] Tyto smluvní povinnosti by měly být dostatečné k ověření souladu společnosti Google s bezpečnostními opatřeními. Kromě toho Google v současné době uveřejňuje svoji pečeť

[55] Viz odst. 2.5 Smlouvy GA.

[56] Například by mohla být zdůrazněna v rámci průvodce "Začínáme," který se zobrazí při prvním přihlášení k službám.

[57] Viz odst. 5.2 Dodatku DP.

[58] Viz odst. 2.8 Smlouvy GA a odst. 6.4 Dodatku DP.

[59] Viz odst. 2.9 Smlouvy GA a odst. 6.5 Dodatku DP.

věrohodnosti SOC 3 a odpovídající auditní zprávu, které pokrývají další otázky.[60]

Pokud jde o prostředky nápravy pro případ nedodržení bezpečnostních opatření, smlouva umožňuje zákazníkovi, aby ji vypověděl pro porušení, pokud jde o porušení podstatné a nenapravitelné, opakované nebo není napraveno do třiceti dnů po obdržení upozornění na porušení.[61] Kromě toho může zákazník po Googlu požadovat náhradu škody, ale odpovědnost Googlu je v rámci Smlouvy GA značně omezena. Google není odpovědný za ztrátu skutečných nebo předpokládaných zisků, ztráty očekávaných úspor, ztráty obchodních příležitostí, ztrátu reputace nebo poškození dobrého jména, zvláštní, ani nepřímé nebo následné škody a jeho celková odpovědnost nesmí překročit 125% z celkové částky, kterou zákazník zaplatil a měl zaplatit dle Smlouvy GA v daném smluvním roce nebo 50.000 liber.[62] Toto omezení se nevztahuje na odpovědnost za „zneužití důvěrných informací" („misuse of confidential information", překlad JT).[63] Není jasné, jak interpretovat tuto výjimku. Skutečnost, že nebyly použity žádné jednoznačné výrazy jako „porušení povinnosti mlčenlivosti" spíše naznačuje, že by se tato výjimka měla vztahovat pouze na úmyslné, nikoliv nedbalostní jednání. Pokud by tato interpretace měla mít přednost, což je varianta, kterou je nutno na straně zákazníka předpokládat, pak jakákoli odpovědnost společnosti Google za porušení povinností týkajících se ochrany osobních údajů v rámci GA Ageement je značně omezena. Zákazník tedy může nést nepřiměřenou část odpovědnosti za porušení právních povinností, kterému není schopen zabránit.

Stabilita smlouvy může být ovlivněna jednostrannými změnami. Google je oprávněn jednostranně měnit služby[64] a zákazník nemá žádné nástroje nápravy pro případ, že taková změna negativně ovlivní jeho soulad s právními předpisy o ochraně osobních údajů. Tento scénář je přitom možný, neboť způsob fungování služeb určuje způsob zpracování osobních

[60] Viz *SOC 3 Seal of Assurance* [online]. WebTrust, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/soc3_google.html *Service Orgnaization Control (SOC) 3 Report* [online]. Ernst & Young, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/pdfs/soc3_google_2014.pdf

[61] Viz odst. 11.1 Smlouvy GA.

[62] Viz odst. 13.1 a 13.2 Smlouvy GA.

[63] Viz odst. 13.1 Smlouvy GA.

[64] Viz odst. 1.2 Smlouvy GA.

údajů. Kromě toho, Google může jednostranně změnit svou politiku přijatelného použití služeb (Acceptable Use Policy), dohodu o úrovni služeb (Service Level Agreement) a pravidla technické podpory, nicméně u takových změn musí být zákazník informován s 30denním předstihem a může změnu odmítnout. V případě takového odmítnutí se změna na zákazníka nebude vztahovat až do konce aktuálního platebního období.[65] Kromě toho může Google měnit bezpečnostní opatření k ochraně osobních údajů zaručená přílohou č. 2 k Dodatku DP. Ačkoli „žádná taková změna nesmí způsobit podstatnou degradaci bezpečnosti Služeb[,]“[66] nemá zákazník žádnou záruku, že opatření budou po změně odpovídat jeho rizikovému profilu.

Pokud jde o subdodávky, Smlouva GA opravňuje Google používat subdodavatele za podmínky, že smlouvy na subdodávky budou respektovat podmínky Smlouvy GA, pokud jde o přístup a využívání dat zákazníka. Zákazník je oprávněn požadovat informace týkající se subdodavatelů a jejich působiště.[67] Podle Dodatku DP má Google navíc povinnost zajistit soulad subdodávek s MCC a musí provést audit postupů subdodavatele v oblasti bezpečnosti a ochrany osobních údajů.[68] Zákazník však nemá právo být předem informován o zapojení nového subdodavatele, ani právo takové zapojení předem schválit, ani smlouvu z důvodu zapojení nového subdodavatele ukončit.

Je-li poskytování služeb ukončeno, má Google povinnost vymazat data zákazníka v maximální lhůtě 180 dnů.[69] Tato povinnost by měla být dostatečná k naplnění požadavků legislativy na ochranu osobních údajů. Stejně tak přístup k údajům, jejich oprava a výmaz jsou řešeny v Dodatku DP dostatečně na to, aby byl zákazník schopen naplnit požadavky subjektů údajů.[70]

Geografická lokalizace zpracování se může různit, protože Google může předávat data zákazníka „do Spojených států nebo jiné země, ve kterých

[65] Viz odst. 1.3 a 15 Smlouvy GA.
[66] Viz Přílohu č. 2 k Dodatku DP.
[67] Viz odst. 2.15 Smlouvy GA.
[68] Viz článek 11 Dodatku DP a článek 5 přílohy č. 2 k Dodatku DP.
[69] Viz odst. 7.2 Dodatku DP.
[70] Viz odst. 7.1 a 8 Dodatku DP.

mají Google a jeho subdodavatelé svá zařízení“ (překlad JT),[71] což potenciálně mohou být jakékoliv země. Proto je třeba počítat s tím, že data budou předávána i do zemí, které nezaručují odpovídající úroveň ochrany osobních údajů. Pro tento případ Google nabízí zákazníkovi možnost přijmout MCC obsahující standardní smluvní doložky vydané Evropskou komisí, ale nevyužití této možnosti zřejmě nemá vliv na fungování služeb. Zákazníci, kteří se nerozhodnou přijmout MCC, proto nejspíše umožňují nelegální předávání osobních údajů do jiného státu.

Znění MCC, které Google používá, se liší od znění vydaného Evropskou komisí o odstavec doplněný ke klauzuli 6. Tento čtvrtý odstavec stanoví, že celková odpovědnost každé strany v rámci nebo v souvislosti s MCC je omezena na částku zaplacenou společnosti Google za služby v předchozích 12 měsících. Z formulace „aniž jsou dotčeny odstavce 1, 2 a 3 klauzule 6,“ (překlad JT) není jasné, zda odstavec 4 nemá mít žádný dopad na odpovědnost podle odstavců 1, 2 a 3, nebo prostě jen nevylučuje jejich existenci, ale omezuje výši odpovědnosti, která z nich vyplývá. Druhý zmíněný význam se zdá být zamýšlený Googlem, jelikož kopíruje omezení odpovědnosti stanovené ve Smlouvě GA.[72] Je zřejmé, že omezení odpovědnosti je ujednání obchodní povahy, tedy přípustného typu, avšak je možné, že orgány pro ochranu údajů shledají, že takové omezení je v rozporu s předchozími odstavci doložky o odpovědnosti za škodu. Smyslem doložky 6 je zajistit plnou náhradu škody, kterou subjekt údajů utrpěl v průběhu zpracování dat, které se řídí MCC. V případě, že subjekt údajů není schopen čerpat plné odškodnění v důsledku zavedení odstavce 4, je takové ujednání v rozporu se standardními smluvními doložkami, jak byly vydány Evropskou komisí.

Další problém, který může představovat rozpor s MCC, spočívá v auditních právech. Dodatek DP uvádí, že povinnosti v oblasti certifikace bezpečnosti a auditu v rámci Dodatku DP naplňují právo zákazníka na audit a právo na audit jeho orgánu pro ochranu údajů, poskytnuté na základě ustanovení doložky 5 písm. f) a doložky 12 odst. 2 MCC.[73] Skutečnost, že audit není prováděn klientem, není v rozporu s MCC, pokud

[71] Viz odst. 10.1 Dodatku DP.
[72] Viz odst. 13 Smlouvy GA.
[73] Viz odst. 6.7 Dodatku DP.

Google vybere pro audit „kontrolní orgán složený z nezávislých členů s požadovanou odbornou kvalifikací“ (překlad JT).[74] Problémem je výběr auditora, který je zcela ponechán na Googlu, zatímco MCC požadují, aby auditor byl vybrán „vývozcem údajů, popřípadě po dohodě s příslušným orgánem dohledu“ (překlad JT).[75]

5. ANALÝZA SMLOUVY O POSKYTOVÁNÍ MICROSOFT OFFICE 365

Základní podmínky upravující poskytování Office 365 jsou dány Microsoft Online Subscription Agreement[76] (dále jen “Smlouva MOS”) a Privacy Notice,[77] se kterými zákazník vyjadřuje souhlas při objednávání placené verze služeb. Nejdůležitějším dokumentem, na který odkazuje Smlouva MOS, jsou Online Services Terms[78] (dále jen „Podmínky OS“), které konkretizují podmínky pro poskytování on-line služeb, včetně služeb Office 365. Smlouva MOS je uzavírána s Microsoft Ireland Operations Limited, společností založenou podle irského práva se sídlem v Dublinu (dále jen „Microsoft“).

Základní prvky smlouvy o zpracování osobních údajů jsou obsaženy v oddílu Additional European Terms Podmínek OS, která se vztahuje pouze na klienty z Evropského hospodářského prostoru a Švýcarska, a stanoví, že Microsoft je zpracovatel osobních údajů jednající jménem svých zákazníků a že bude jednat pouze na základě pokynů zákazníka. Jako účel zpracování Podmínky OS uvádějí, že „Data zákazníka budou použita pouze k poskytnutí Online služeb zákazníkovi, včetně účelů slučitelných s poskytováním těchto služeb“ a „Microsoft nebude používat data zákazníka nebo z nich odvozovat informace pro jakoukoli reklamu nebo podobné komerční účely.“ (překlad JT) [79] Kategorie zpracovávaných údajů jsou specifikovány jako „e-maily, dokumenty a další data v elektronické

[74] Viz doložku 5 písm. f) MCC.

[75] Viz doložku 5 písm. f) MCC.

[76] Viz *Microsoft Online Subscription Agreement* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Po registraci dostupné z: portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK (aktuální veřejně dostupné znění nebylo nalezeno).

[77] Viz *Privacy Notice* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoft.com/online/legal/v2/?docid=18&langid=en-UK

[78] Viz *Online Services Terms January 1, 2015* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248.

[79] Viz Část General Privacy and Security Terms, odst. Use of Customer Data Podmínek OS.

podobě v rámci Online služeb.“ (překlad JT) [80] Rozsah pokynů zákazníka je omezen pouze na pokyny uvedené ve Smlouvě MOS a Podmínkách OS.[81]

Podmínky OS popisují bezpečnostní opatření, která Microsoft uplatňuje. Popis je spíše obecný, ale pokrývá velké množství oblastí.[82] Pokud jde o důkaz skutečného uplatňování opatření, Microsoft dává zákazníkovi k dispozici svou bezpečnostní politiku, která je v souladu s normami ISO 27001 a 27002 a zároveň zajistí prověření této bezpečnostní politiky nezávislým odborníkem. Shrnutí auditní zprávy Microsoft zákazníkovi na jeho žádost zpřístupní.[83] Microsoft je také nově certifikovaný podle standardu ISO 27018, který cílí právě na ochranu osobních údajů v cloudu.[84]

V případě porušení smlouvy má zákazník zvláštní právo pouze na náhrady, které jsou uvedeny v dohodě o úrovni služeb (Service Level Agreement).[85] Smlouva MOS neopravňuje klienta ukončit smlouvu speciálně pro porušení povinnosti společnosti Microsoft, nicméně i při dlouhodobém předplatném služby může zákazník smlouvu ukončit bez udání důvodu s výpovědní dobou jeden měsíc a právem na vrácení za zbývající části předplatného.[86] Kromě toho má zákazník právo ukončit smlouvu při porušení jeho instrukcí nebo standardních smluvních doložek vydaných Evropskou komisí podle klauzule 5(b) těchto doložek v příloze č. 3 k Podmínkám OS.

Odpovědnost Microsoftu za škody způsobené porušením povinnosti vyplývající z dohody o MOS je omezena na částky zaplacené za služby v průběhu současného smluvního období, které může trvat pouhých 30 dnů[87] a odpovědnost za ušlý zisk, nepřímé škody, narušení podnikání

[80] Příloha č. 1 k Standardním smluvním doložkám v příloze č. 3 k Podmínkám OS.

[81] Viz Část Data Processing Terms, oddíl Additional European Terms, odst. Intent of the Parties Podmínek OS.

[82] Viz Část Data Processing Terms, oddíl Security Podmínek OS.

[83] Viz Část Data Processing Terms, oddíl Certifications and Audits Podmínek OS.

[84] Viz Microsoft adopts first international cloud privacy standard. *Microsoft on the Issues* [online]. Microsoft, publikováno 16. 12. 2015 [cit. 16. 3. 2015]. Dostupné z: http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/

[85] Viz článek 4 odst. a(i) Smlouvy MOS. Srov. též *Service Level Agreement for Microsoft Online Services* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8222

[86] Viz článek 3 odst. b(ii) Smlouvy MOS.

[87] Viz článek 6 odst. a Smlouvy MOS.

a ztrátu obchodních informací je vyloučena, a to i v případě, že byly tyto škody pro příslušnou smluvní stranu rozumně předvídatelné.[88] Toto omezení ponechává významnou část břemene odpovědnosti vůči subjektu údajů na zákazníkovi.

Ani Smlouva MOS ani Podmínky OS neumožňují jednostranné změny. Smlouvu lze měnit pouze po uplynutí smluvního období prostřednictvím postupu pro její prodloužení.[89]

Vyjádřením souhlasu se Smlouvou MOS zákazník rovněž souhlasí s tím, aby Microsoft využíval při poskytování služeb subdodavatele.[90] Každá subdodavatelská smlouva musí obsahovat ujednání, která budou zákazníka chránit alespoň tak, jak jej chrání část Data Processing Terms Podmínek OS. Microsoft je zároveň povinen zákazníka informovat o každém novém subdodavateli, který se má účastnit na poskytování služeb, a to s předstihem nejméně 14 dnů. Pokud zákazník subdodavatele neschválí, může v této lhůtě ukončit smlouvu ve vztahu k dotčené službě.[91]

Microsoft se zavazuje, že vymaže data zákazníka nejpozději do 90 dnů od ukončení poskytování služeb.[92] Microsoft je rovněž povinen poskytnout zákazníkovi možnost opravit, mazat, nebo blokovat zpracovávaná data, nebo učinit takové opravy, odstranění nebo blokování jeho jménem,[93] aby zákazník mohl plnit požadavky subjektů zpracovávaných údajů.

Z hlediska geografické lokalizace zpracování dat Microsoft zaručuje, že bude ukládat nejcitlivější část dat zákazníků z EU v této oblasti.[94] Co se týče ostatních dat, Microsoft je a zavazuje se zůstat certifikovaný v programu Safe Harbor a Podmínky OS ve své příloze č. 3 obsahují standardní smluvní doložky vydané Evropskou komisí. Text těchto doložek není nijak pozměněn. Pokud jde o možné rozpory doložek se Smlouvou MOS a Podmínkami OS, problematickým aspektem je audit poskytování služeb. Podmínky OS uvádějí, že zákazník souhlasí s tím, aby vykonával své právo

[88] Viz článek 6 odst. b Smlouvy MOS.
[89] Viz článek 2 odst. d Smlouvy MOS.
[90] Viz část General Privacy and Security Terms, oddíl Use of Subcontractors Podmínek OS.
[91] Viz část Data Processing Terms, oddíl Privacy, odst. Subcontractor Transfer Podmínek OS.
[92] Viz část Data Retention Podmínek OS.
[93] Viz část Data Processing Terms, oddíl Additional European Terms, odst. Customer Data Access Podmínek OS.
[94] Viz část Data Processing Terms, oddíl Location of Customer Data at Rest, odst. Office 365 Services Podmínek OS.

auditu dle standardních smluvních doložek tím, že dává Microsoftu pokyn nechat audit provést nezávislým profesionálem v oblasti bezpečnosti, jak bylo popsáno výše. Nicméně zákazník má právo tento pokyn změnit. I když to není výslovně uvedeno, toto právo zákazníka může být vykonáváno například tak, že zákazník změní svůj pokyn, pokud neschválí auditora vybraného Microsoftem, a tudíž může ovlivnit výběr auditora, jak požadují standardních smluvní doložky. Podmínky OS navíc výslovně uvádějí, že nic v příslušné části jejich textu nemá měnit nebo upravovat Standardní smluvní doložky ani omezovat práva jakéhokoli dozorčího orgánu či subjektu údajů na základě standardních smluvních doložek.[95] Zbývající část textu Podmínek OS by proto měla být vykládána v duchu tohoto záměru.

6. SROVNÁNÍ SMLUV A DISKUZE

Smluvní rámec Googlu pro poskytování služby Google Apps for Work celkově trpí několika nedostatky, které mohou způsobit jeho rozpor se směrnicí 95/46/ES a jejími vnitrostátními implementacemi. Nejviditelnějším nedostatkem je skutečnost, že smlouva s náležitostmi smlouvy o zpracování osobních údajů není se zákazníky z EU uzavírána automaticky. Místo toho je k jejímu uzavření zapotřebí specifický úkon ze strany zákazníka, přičemž provedení tohoto úkonu není ze strany Google aktivně doporučováno. Za těchto okolností se může snadno stát, že zákazník z EU bude využívat Google Apps for Work, aniž by vyjádřil souhlas s Dodatkem DP a MCC, a tím bude porušovat povinnosti plynoucí z legislativy na ochranu osobních údajů. Google se v takovém případě stane správcem osobních údajů, které mu budou zákazníkem předány, přičemž bude také jednat v rozporu s právními předpisy o ochraně osobních údajů, neboť nelze očekávat, že by Google plnil odpovídající povinnosti, jakými je získání titulu pro zpracování nebo informování subjektů údajů. Není přitom známo, kolik procent uživatelů Google Apps for Work z EU nevyjádřilo souhlas s Dodatkem DP a MCC, ale lze přepokládat, že toto procento nebude zanedbatelné.

Formulace ustanovení Smlouvy GA, která ošetřují omezení odpovědnosti, jsou nejednoznačná a zákazník musí vzít v úvahu možnost, že odpovědnost společnosti Google na základě této smlouvy bude striktně

[95] Viz část Data Processing Terms, oddíl Certifications and Audits Podmínek OS.

omezena. Podobně nejasné formulace jsou vloženy do MCC a mohou být potenciálně v rozporu s rozhodnutím Komise 2010/87/EU. Google je oprávněn jednostranně měnit bezpečnostní opatření stanovená na ochranu osobních údajů, která jsou esenciální náležitostí smlouvy o zpracování osobních údajů. Zákazník nemá právo vznést námitky proti výběru subdodavatelů Googlu podílejících se na zpracování osobních údajů. Právo zákazníka na audit zakotvené v MCC je omezeno v Dodatku DP do té míry, že to může být shledáno v rozporu rozhodnutím Komise 2010/87/EU.

Smluvní rámec pro poskytování Microsoft Office 365 také trpí určitými nedostatky. Nejdůležitější z nich je striktní omezení odpovědnosti, které se vztahuje i na škody způsobené porušením práva na ochranu údajů. Lhůta, ve které musí Microsoft oznámit nového subdodavatele, dává zákazníkovi pouze velmi krátký předstih pro migraci na jinou službu, než se nový subdodavatel začne podílet na poskytování služby a tedy získá potenciální přístup k jeho datům. Také úprava práva auditu v Podmínkách OS může být potenciálně v rozporu se standardními smluvními doložkami.

Porovnáme-li smlouvy na obě služby z hlediska ochrany osobních údajů, vychází z tohoto srovnání podstatně lépe Microsoft Office 365. Nejvýznamnější nedostatek smlouvy na tuto službu, omezení odpovědnosti, není v přímém rozporu s právními předpisy o ochraně osobních údajů, pouze vytváří nerovnováhu smluvního rámce. Další nedostatky jsou diskutabilní a Smlouva MOS spolu s Podmínkami OS jsou obecně v souladu s požadavky směrnice 95/46/ES. Naopak v případě Google Apps for Work jsou nedostatky smlouvy podstatné. Částečně je možné je napravit uzavřením Dodatku DP a MCC, ale některé z nich zůstávají nevyřešeny. Klienti se sídlem v EU používající Google Apps for Work proto čelí riziku porušení zákona o ochraně osobních údajů a následné sankci od svých vnitrostátních orgánů pro ochranu údajů, a to zejména v případě, že neodsouhlasili Dodatek DP a MCC.

Obecně, Smlouva MOS a zejména Podmínky OS ukazují, že Microsoft věnuje otázkám soukromí a ochrany osobních údajů značnou pozornost a požadovaná opatření a obecně doporučované postupy jsou realizovány v rámci výchozího nastavení. To potvrzuje i pokračující a úspěšná spolupráce Microsoftu s WP29. Výsledkem této spolupráce jsou změny provedené v smluvní dokumentaci Microsoftu, které by měly zajistit shodu

s evropskými právními předpisy o ochraně osobních údajů.[96] Smlouva GA nevykazuje takovou úroveň pozornosti věnované otázkám ochrany osobních údajů. Google by mohl pro zákazníky se sídlem v EU zahrnout podmínky Dodatku DP a MCC do smluvního rámce již ve výchozím nastavení.[97] Spolupráce Google s WP29 se také nezdá být tak plodná jako spolupráce Microsoftu.[98]

Důvody těchto rozdílů mohou být různé, přičemž jedním z nich může být nedostatek zkušeností Googlu s evropským trhem. Microsoft vstoupil na evropský trh dlouho před založením Googlu. Zároveň Microsoft jako výrobce softwaru musel čelit vládám jako odběratelům i regulátorům téměř od počátku své existence. Tyto zkušenosti mohou Microsoftu pomáhat, aby se přizpůsobil požadavkům evropských regulačních orgánů rychleji a efektivněji než Google, což vyúsťuje v současné rozdíly v jejich přístupu k ochraně osobních údajů v souvislosti s jejich cloudovými službami.

Společným znakem obou smluv je pak výrazný přenos obchodního rizika na stranu zákazníka (zejména skrze ujednání o omezení odpovědnosti), a to do té míry, která nemusí být vždy akceptovatelná.[99] Vzhledem k nerovnováze sil mezi smluvními stranami se postavení SME vůči poskytovatelům blíží postavení spotřebitele. Tomu odpovídá i podobnost některých ujednání ve smlouvách pro podnikatele a smlouvách nabízených

---

[96] Viz *Letter from the Article 29 Working Party to Microsoft on a new version of the Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 2. 4. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf nebo *Letter for the Article 29 Working Party to Microsoft on the Microsoft Service Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 22. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf

[97] Těmto zákazníkům je předkládána smlouva, která se uzavírá s Google Commerce Limited se sídlem v Irsku, jistý stupeň geografické diferenciace uživatelů tedy straně Google nutně musí probíhat.

[98] Viz *Letter from the Article 29 Working Party to Google on Google Privacy Policy* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 23. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf

[99] Dosud nejsou známy žádné medializované případy, kdy by zákazníkovi cloudové služby vznikla jejím užíváním zásadní škoda, kterou by poskytovatel odmítl zaplatit na základě takových ujednání. I malý počet takovýchto medializovaných případů by však mohl náhled zákaznické veřejnosti na toto obchodní riziko změnit.

spotřebitelům.[100] Ve vztahu ke spotřebitelům přitom může nastoupit přísnější režim ochrany, v jeho světle se taková ujednání mohou ukázat jako zakázaná.[101] Pokud by poskytovatelé byli stíháni např. ze strany správních orgánů[102] za použití takovýchto zakázaných ujednání ve vztahu ke spotřebitelům a následně své podmínky z tohoto důvodu modifikovali, je otázkou, zda by se změny nepromítly i od smluv pro SME.

Samotné služby jsou z technického hlediska v jádru jednotné jak pro podnikatele, tak pro spotřebitele, proto je nepravděpodobné, že by se změny vyvolané prosazováním spotřebitelských práv dotkly právě tohoto jádra. Podstata problémů ve vztahu ke spotřebiteli (stejně jako k podnikateli), totiž netkví v technických otázkách, ale v nastavení smluvních podmínek, které jsou pro spotřebitele a podnikatele samostatné a nezávislé. Jelikož oba diskutovaní poskytovatelé, Google i Microsoft, i přes určité podobnosti, nabízí odlišné podmínky pro podnikatele a spotřebitele, ačkoli nabízené služby jsou ve své podstatě identické,[103] nelze předpokládat, že by od této praxe v budoucnu upustily. Za těchto okolností poskytovatelé nemají důvod promítat případné změny ve prospěch spotřebitelů také do podmínek pro podnikatele. Jedinou nadějí pro podnikatele (vedle budoucího působní tržních sil) je proto použití obecných ustanovení o ochraně slabší smluvní strany,[104] avšak posouzení, zda rozhodné právo, tj. právo anglické,[105] resp. irské,[106] obsahuje relevantní ustanovení, která by byla v tomto směru aplikovatelná, překračuje rozsah tohoto článku. Podrobná komparace mezi podnikatelskými

[100] Viz body Naše záruky a odmítnutí odpovědnosti a Odpovědnost za naše služby Smluvní podmínky společnosti Google. *Ochrana soukromí a smluvní podmínky* [online]. Google, aktualizováno 14. 4. 2014 [cit. 22. 3. 2014]. Dostupné z: http://www.google.com/intl/cs/policies/terms/ Též srov. čl. 11 Smlouva o poskytování služeb společnosti Microsoft. *Windows* [online]. Microsoft, aktualizováno 11. 6. 2014 [cit. 22. 3. 2014]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/microsoft-services-agreement

[101] Srov. např. § 1811 odst. 1 a § 1813 an. občanského zákoníku.

[102] Ať už pro porušení s norem spotřebitelského práva či práva na ochranu osobních údajů.

[103] Nelze vyloučit, že z hlediska technického zabezpečení jsou služby pro podnikatele provozovány na odlišné infrastruktuře, která může být např. lépe zajištěná proti výpadkům, atd.

[104] Srov. § 433 občanského zákoníku. Ve vztahu k podnikatelským smlouvám se však občanský zákoník zpravidla neuplatní díky volbě jiného než českého práva, kdežto spotřebitelé se o kogentní normy českého práva mohou opřít díky čl. 6 nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I)

[105] Odst. 14.11 Smlouvy GA.

[106] Článek 8 odst. h. Smlouvy MOS.

a spotřebitelskými smlouvami a možností prosazení ochrany slabší smluvní strany tak zůstávají možným tématem dalšího výzkumu.

7. DISKUZE SOUČASNÉ A BUDOUCÍ PRÁVNÍ ÚPRAVY

Zákazníci a poskytovatelé musí při působení na trhu cloudových služeb čelit řadě právních překážek. Pro dodržení požadavků směrnice 95/46/ES a její národní implementace na používání služby musí zákazník zajistit, aby byly splněny mnohé požadavky. Tento článek popisuje pouze základní požadavky, které vycházejí ze směrnice 95/46/ES, ale zákazník může být vystaven dalším požadavkům vycházejícím z vnitrostátních právních předpisů na ochranu osobních údajů. Rozdíly mezi národními implementacemi směrnice 95/46/ES komplikují situaci i pro poskytovatele. Ti mohou čelit obtížím při snaze nabízet jednotné služby s podmínkami, které by byly v souladu s právními předpisy o ochraně údajů ve všech členských státech EU.

Ne všechny požadavky jsou přitom výslovně stanoveny právními předpisy a zákazník tedy musí studovat pokyny vydané různými orgány, aby zajistil jejich plné splnění. Např. povinnosti ve vztahu k subdodavatelům vůbec nelze vyčíst ze směrnice 95/46/ES. Úprava předávání osobních údajů do jiných států mimo EU je natolik složitá, že jen malé množství zákazníků bude schopno odvodit odpovídající povinnosti přímo ze směrnice 95/46/ES. Zákazník tak může tápat při určování svých vlastních povinností a následně tím pádem i při posuzování nabídky poskytovatele.

V mnoha případech budou data zpracovávaná pomocí cloudové služby obsahovat pouze omezené množství osobních údajů a tyto údaje nebudou vnímány jako citlivé ze strany příslušných subjektů údajů. V těchto případech mohou být povinnosti stanovené poskytovateli jako zpracovateli osobních údajů nepřiměřené. Na druhé straně v případech, kdy je pomocí cloudové služby zpracováváno velké množství subjektivně citlivých dat, může rámec ochrany údajů postrádat dostatečnou podrobnost, aby vztah mezi poskytovatelem a zákazníkem účinně reguloval.[107]

[107] Například nemusí dostatečně specifikovat bezpečnostní opatření, která by měla být v takovém případě uplatňována.

Nejpodstatnějším nedostatkem současné úpravy je však nevhodné rozložení odpovědnosti mezi správcem a zpracovatelem. Zákazník jako správce osobních údajů je ze zákonného hlediska téměř výlučně odpovědný za prováděné zpracování, což poskytovatelům dovoluje aby svou odpovědnost smluvně omezili na minimum.[108]

Stávající právní rámec tedy trpí nedostatky v oblasti unifikace, srozumitelnosti, škálovatelnosti a vyváženého rozložení odpovědnosti. Budoucí regulace by měla sjednotit právní režim alespoň v rámci celé EU, aby se zjednodušila situace jak pro zákazníky, tak pro poskytovatele. Dále by měla jasně a výslovně stanovit povinnosti na straně zákazníka a poskytovatele cloudových služeb a podobných řešení a přizpůsobovat rozsah povinností podle rizika, které zpracováním vzniká (včetně úrovně rizika, se kterým nebudou spojeny žádné povinnosti dle této regulace, tj. de minimis pravidla).

Obecné nařízení o ochraně údajů, navrhované Evropskou komisí,[109] ve znění pozměňovacích návrhů Evropského parlamentu.[110] si klade za cíl reagovat na výše popsané výzvy. Jednou z hlavních ambicí nařízení je sjednotit právní rámec pro ochranu údajů v EU.[111] Místo další harmonizace vnitrostátních právních předpisů prostřednictvím novely současné směrnice bylo jako právní nástroj zvoleno nařízení, které zajistí maximální unifikaci díky své přímé použitelnosti. Kromě toho obecné nařízení obsahuje ustanovení, která upravují spolupráci a koordinaci mezi nezávislými vnitrostátními orgány pro ochranu údajů.[112] Na druhou stranu přetrvávají pochybnosti, do jaké míry nařízení ponechává členským státům možnost

[108] Ke stejnému závěru dospívá MCGILLIVRAY, 2014, op. cit., s. 250.

[109] Viz *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final* [online]. Evropská komise, 2012 [cit. 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN

[110] Viz *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [online]. Evropský parlament, publikováno 12. 3. 2014 [cit. 15. 2. 2015]. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

[111] Tento pozitivní efekt ve vztahu ke cloudovým službám je předpokládán Evropskou komisí. Viz Unleashing the Potential of Cloud Computing in Europe, 2012, op. cit.

[112] Kapitola VII obecného nařízení.

přijmout zvláštní právní úpravu zpracování osobních údajů v některých odvětvích, jako je např. zdravotnictví, nebo bankovnictví.[113]

Ačkoli je text obecného nařízení podstatně delší a podrobnější než text směrnice 95/46/ES, ne všechny povinnosti správce osobních údajů v souvislosti se zpracováním osobních údajů v cloudu jsou uvedeny jasněji.[114] Například znění obecného nařízení navržené Evropskou komisí stanovovalo výslovně povinnost správce zajistit ověření účinnosti bezpečnostních opatření,[115] tj. jejich audit, ale tato povinnost byla odstraněna a nahrazena obecnou povinností být schopen prokázat přiměřenost a účinnost těchto opatření.[116] Takovou úpravou však vzniká nejistota, jaký standard prokazování bude od správců ve vztahu ke cloud computingu požadován, a může dokonce vznikat nejednotnost v aplikační praxi nezávislých vnitrostátních orgánů napříč EU. Kromě toho obecné nařízení dává Evropské komisi pravomoc vydat četné prováděcí předpisy a orgány pro ochranu údajů mohou schvalovat různé kodexy chování a další prováděcí dokumenty, což může vytvářet potenciálně nejasné hranice mezi závaznými a nezávaznými pravidly. Zda tedy obecné nařízení pomůže objasnit a zvýšit srozumitelnost povinností zákazníků a poskytovatelů cloudových služeb je přinejmenším diskutabilní.

Jako pozitivní aspekt lze vnímat, že obecné nařízení výslovně řeší svůj vztah ke směrnici o elektronickém obchodu, a to ve prospěch této směrnice.[117] Z toho lze dovodit, že v režimu obecného nařízení by na poskytovatele cloudových služeb měly vztahovat výluky z povinností zpracovatele osobních údajů na základě jejich kvalifikace jako poskytovatele hostingu dle směrnice o elektronickém obchodu. Dále návrh nařízení výslovně rozšiřuje povinnosti zpracovatele v oblasti dokumentace, spolupráce s orgány dohledu, bezpečnostních opatření, hodnocení dopadů

[113] K pochybnostem srov. BLUME, Peter. The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp: 269-273 [cit. 24. 4 2015]. Dostupné z Oxford Journals: idpl.oxfordjournals.org/content/4/4/269.full.pdf+html. s. 271. KOTCHY, Waltraut. The proposal for a new General Data Protection Regulation—problems solved? *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp. 274-281 [cit. 24. 4 2015] Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/4/4/274.full.pdf+html. s. 275.

[114] Rozsáhlost textu kritizuje BLUME, 2014, op. cit., s. 270.

[115] Viz článek 22 odst. 3 obecného nařízení ve znění návrhu Evropské komise.

[116] Viz článek 22 odst. 3 obecného nařízení ve znění návrhu Evropského parlamentu.

[117] Viz článek 3 odst. 3 obecného nařízení. Srov. SARTOR, 2013, op. cit., s. 4.

a hodnocení shody s legislativou i na zpracovatele.[118] Dále koncept sektorů zpracování (processing sectors, v českém překladu návrhu Komise nešťastně označených jako odvětví zpracování), které mohou být prohlášeny za oblasti s náležitou úrovní ochrany, může usnadnit předávání osobních údajů do zahraničí.[119] Nařízení také řeší problematiku subdodavatelů, ale v současnosti navrhované znění je velmi obecné.[120]

I přes tato zlepšení flexibility a rozložení odpovědnosti, prostor pro zlepšení zůstává výrazný. Místo sloučení role správce a zpracovatele v jeden odpovědný subjekt s odstupňovanými povinnostmi a odpovědností, návrh nařízení kopíruje původní dichotomii zavedenou směrnicí 95/46/ES. Kromě toho návrh nařízení neobsahuje skutečné pravidlo de minimis, které by osvobodilo zpracování malého rozsahu s nízkým rizikem z jeho působnosti. Velikost zpracování tak ovlivňuje pouze povinnosti s okrajovým vlivem na správce, jako je jmenování inspektora ochrany údajů.[121] Místo toho nařízení přidává správcům další povinnosti[122] a nebere v úvahu rozsah a rizikový profil zpracování. Pokud jde o rozložení odpovědnosti, zpracovatel stále nesdílí se správcem v plném rozsahu primární odpovědnost za bezpečnost a legálnost zpracování.[123]

Specifickou změnou, kterou obecné nařízení přináší, je právo subjektu údajů domáhat se svých práv přímo vůči správci a zpracovateli u soudu.[124] Toto právo je navíc podpořeno tím, že nárok může v zastoupení spotřebitele vymáhat i organizace jednající ve veřejném zájmu.[125] Je otázkou, jaké nároky by mohli dotčení jednotlivci a jejich zástupci

[118] Srov. čl. 28, 29, 30, 33 and 33a obecného nařízení ve znění návrhu Evropského parlamentu. Srov. též. BLUME, Peter. It Is Time for Tomorrow: EU Data Protection Reform and the Internet. *Journal Of Internet Law*. 2015, vol. 18, no. 8, pp. 3-13 [cit. 24. 4 2015]. s. 7.

[119] Srov. čl. 41 obecného nařízení ve znění návrhu Evropského parlamentu. Srov. též. BLUME, 2015, op. cit., s. 9.

[120] Srov. čl. 26 odst. 2 obecného nařízení ve znění návrhu Evropského parlamentu. Původní znění navržené Komisí bylo striktnější a jednoznačnější. Srov. též MCGILLIVRAY, 2014, op. cit., s. 248.

[121] Viz článek 35 odst. 1 písm. b) obecného nařízení.

[122] Viz READING, Viviane. The European data protection framework for the twenty-first century. *International Data Privacy Law* [online]. 2012, vol. 2, no. 3, pp. 119-129. [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/3/119.full.pdf, s. 126.

[123] Zpracovatel není zahrnut v článku 22 odst. 1 navrhovaného nařízení. Srov. též. BLUME, 2015, op. cit., s. 7. MCGILLIVRAY však namítá, že veškerá odpovědnost by neměla být přenášena na zpracovatele, srov. MCGILLIVRAY, 2014, op. cit., s. 248.

[124] Viz. článek 75 obecného nařízení ve znění návrhu Evropské komise. Též srov. READING, 2012, op. cit., s. 126.

uplatňovat v případě cloud computingu obecně a diskutovaných služeb konkrétně. Cloud computing jako takový svou podstatou neodporuje principům ochrany osobních údajů a žádné z výše diskutovaných porušení není natolik flagrantní, aby přímo ohrožovalo subjekty zpracovávaných údajů. Těžko lze tedy z jejich strany očekávat preventivní kroky. Nároky proto mohou být vznášeny spíše v případě bezpečnostních incidentů, které by měly dopad na jednotlivce. Rovněž je možné, že při zásadní změně bezpečnostních opatření by mohli jednotlivci a jejich zástupci napadat možnost těchto změn a případný nedostatek auditních práv. Ve vztahu k současnému stavu tak mohou přímé nároky přinést zlepšení pouze jako hrozba pro poskytovatele, která je může přivést k přísnějšímu uplatňování bezpečnostních opatření. Nelze však předpokládat, že by vedly k úpravě smluvních podmínek.

Celkově se upravený návrh obecného nařízení ve vztahu ke cloud computingu zdá být dosti problematický. S výjimkou alespoň částečné unifikace by v současnosti navrhované znění nejspíše nepřineslo v oblasti cloud computingu výrazná zlepšení. Budoucí revize by se proto měly zaměřit na jeho zjednodušení, zlepšení srozumitelnosti a vyšší škálovatelnost povinností.

Bez ohledu na to, zda by obecné nařízení bylo prospěšné pro zákazníky a poskytovatele cloudových služeb nebo ne, jeho účinnost nelze vzhledem k složitosti unijního legislativního procesu a množství angažovaných organizovaných zájmů očekávat v blízké budoucnosti, stejně jako jakoukoli jinou změnu směrnice 95/46/ES. Proto je třeba pro zákazníky hledat řešení, jak efektivně hodnotit nabídky poskytovatelů cloudových služeb a zajistit soulad zpracování osobních údajů pomocí těchto služeb se směrnicí 95/46/ES.

V reakci na tuto výzvu zřídila Evropská komise oborovou pracovní skupinu pro cloud computing (Cloud Select Industry Group) a v rámci ní podskupinu zaměřenou na standardizaci smluv na poskytování cloudových služeb (Service Level Agreement v širším smyslu). Tato podskupina vydala doporučení pro standardizaci těchto smluv (Cloud Service Level Agreement

[125] Viz. články 73 odst. 2 a 76 obecného nařízení ve znění návrhu Evropského parlamentu. Též srov. REDING, 2012, op. cit., s. 126.

Standardisation Guidelines), které pokrývá i otázky ochrany osobních údajů.[126]

Doporučení je vystavěné na konceptu cílových úrovní služeb (Service Level Objectives), které pokrývají také otázku ochrany osobních údajů. Doporučení je v tomto ohledu relativně podrobné a reflektuje doporučení WP29. Odpovídající cílové úrovně služeb se týkají certifikace, vymezení účelu, minimalizace zpracovávaných údajů, omezení uchovávání a vydání údajů, prokazatelnost záznamů, lokalizaci dat a řešení požadavků subjektů údajů. Kromě toho doporučení zmiňuje také cílové úrovně služeb pro bezpečnost, jako jsou autentizace a řízení přístupu, šifrování, řešení bezpečnostních incidentů, logování a monitorování, audity a ověření bezpečnosti. Doporučení se také věnuje výkonnosti a řízení dat. Pro každou cílovou úroveň služeb doporučení uvádí, jak by měla být ve smlouvě ošetřena.

Podle zkušeností autora jsou tato doporučení v praxi velmi dobře použitelná jak při posuzování, tak při sepisování smluv o zpracování osobních údajů pro cloudové služby. Bylo by proto z praktického hlediska vítaným přínosem, kdyby byla tato doporučení v budoucnu rozpracována např. do standardního smluvního nástroje. Není přitom nezbytné, aby tento nástroj musel být používán povinně jako např. standardní smluvní podmínky pro předávání osobních údajů do třetích zemí bez odpovídající úrovně ochrany. Postačí, pokud tyto standardní podmínky budou kvalitně formulované a vytvořené na základě konsenzu zástupců poskytovatelů, zákazníků i regulátorů. Z pohledu SME by toto řešení bylo podstatným zjednodušením situace, protože v případě nabídky, která by stavěla na standardním smluvním nástroji, by pro ně bylo její posouzení podstatně snadnější. Zároveň by jim tento postup dával dostatečnou míru jistoty o souladu jejich postupu s ochranou osobních údajů.

8. ZÁVĚR

Poskytování cloudových služeb zákazníkům se sídlem v Evropské unii může často spadat do působnosti evropského práva na ochranu údajů, které je

[126] Viz Cloud Service Level Agreement Standardisation Guidelines. *Evropská komise* [online]. Cloud Select Industry Group, Subgroup on Service Level Agreement, publikováno 24. 06. 2014 [cit. 30. 10. 2014]. Dostupné z: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138.

reprezentováno směrnicí 95/46/ES. Zákazníkům a poskytovatelům cloudových služeb mohou být v rámci směrnice 95/46/ES v závislosti na povaze zpracování přiřazeny různé role a z toho vyplývající práva a povinnosti. Zákazník je ve většině případů správcem osobních údajů. Poskytovatel může být správcem osobních údajů, pokud zpracovává osobní údaje pro své vlastní účely, jako je například reklama. Zpracovatelem osobních údajů může být, pokud údaje zpracovává pro zákazníka podle jeho pokynů. Může být také zcela vyňat z působnosti směrnice 95/46/ES, pokud se kvalifikuje jako poskytovatel hostingu podle směrnice o elektronickém obchodu tím, že mu není známa povaha dat zpracovávaných pomocí jeho služby.

V případech, kdy je poskytovatel cloudových služeb zpracovatelem osobních údajů (jako například když je zřejmé z povahy příslušné služby, že jejím prostřednictvím budou zpracovávány osobní údaje) vztah mezi poskytovatelem a zákazníkem cloudových služeb musí být upraven smlouvou o zpracování osobních údajů. Tato smlouva musí stanovit, že poskytovatel je vázán pokyny zákazníka, musí určovat rozsah pokynů zákazníka, účel zpracování a typy zpracovávaných údajů. Dále smlouva musí popisovat bezpečnostní opatření, způsob prokazování uplatňování těchto opatření ze strany poskytovatele a nápravné prostředky pro případ jejich nedodržení. Smlouva nesmí umožňovat jednostranné změny podstatných ujednání a musí upravovat využívání subdodavatelů ze strany poskytovatele. Poskytovatel musí garantovat, jak dlouho po ukončení využívání služeb ze strany zákazníka budou vymazány příslušné osobní údaje, a musí být povinen poskytnout zákazníkovi součinnost při plnění žádosti subjektů údajů. Mají-li být osobní údaje pomocí dané služby zpracovávány mimo EU a země s odpovídající úrovní ochrany, musí být poskytovatel certifikován v programu Safe Harbor pro zpracování v USA a smlouva musí obsahovat standardní smluvní doložky vydané Evropskou komisí pro zpracování v ostatních zemích.

Smluvní rámec pro poskytování Microsoft Office 365 se zdá být v souladu s výše uvedenými požadavky s výjimkou drobných nedostatků a nerovnováhy v otázce odpovědnosti. Smluvní struktura pro poskytování služby Google Apps for Work trpí více závažnými nedostatky, které mohou vést k porušování legislativy na ochranu osobních údajů. Aby byla zajištěna

alespoň minimální úroveň plnění požadavků směrnice 95/46/ES, je třeba ze strany zákazníka provést dodatečné úkony. Google také silně omezuje právo zákazníka na audit a svou odpovědnost vůči zákazníkovi. Smlouva Googlu rovněž umožňuje jednostranně měnit její podstatná ujednání. Přístup společnosti Microsoft vykazuje vyšší stupeň pozornosti věnovaný ochraně osobních údajů. Tento rozdíl může být dán větší zkušeností Microsoftu s evropským trhem a regulací obecně.

Stávající právní rámec pro ochranu údajů při poskytování cloudových služeb trpí nedostatkem unifikace, srozumitelnosti, škálovatelnosti a vyváženého rozložení odpovědnosti. S výjimkou unifikace nelze předpokládat, že připravované obecné nařízení o ochraně osobních údajů přinese podstatné zlepšení, bude-li přijato v aktuálním znění. V dalších revizích by mělo být nařízení zjednodušeno, zapracována klauzule de minimis a rozsah povinností přizpůsoben velikosti a rizikovému profilu zpracování.

Pro potřeby práce se současnou evropskou úpravou ochrany osobních údajů reprezentovanou směrnicí 95/46/ES mohou zákazníci a poskytovatelé cloudových služeb používat Cloud Service Level Agreement Standardisation Guidelines vydané pracovní skupinou Evropské komise. Do budoucna by bylo pro praxi významným přínosem, kdyby tato doporučení byla rozpracována do standardního smluvního nástroje.

Ve vztahu ke cloud computingu by byla z hlediska ochrany osobních údajů vhodná bližší analýza připravovaného obecného nařízení, rozbor podmínek poskytovatelů cloudových služeb cílených na spotřebitele a jejich srovnání s podmínkami pro podnikatele, popřípadě možnost vymáhání změn podmínek pro podnikatele na základě ochrany slabší smluvní strany či zneužití dominantního postavení. Zajímavá by rovněž byla analýza případného právního nástupnictví v kontextu kombinovaných smluvních závazků na poskytování cloudových služeb.

9. POUŽITÉ PRAMENY

9.1 PRÁVNÍ PŘEDPISY A JUDIKATURA

[1] Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I).

[2] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.

[3] 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.

[4] Ústavní zákon č. 23/1991 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.

[5] Zákon č. 89/2012 Sb., občanský zákoník.

[6] Zákon Španělska Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[7] Zákon Spojeného království Data Protection Act 1998.

[8] Zákon Německé spolkové republiky č. RGBl. 1896 S. 195, Bürgerliche Gesetzbuch, ve znění pozdějších předpisů.

[9] Title 17 of the United States Code, Copyright Act, ve znění pozdějších předpisů.

[10] Rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES

[11] Nařízení Španělska Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[12] Nařízení Polské republiky Rozporządzenie Ministra spraw wewnętrznych i administracji Dz. U. z 2004 r. Nr 100, poz. 1024, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[13] Rozhodnutí Sněmovny lordů Spojeného království ze dne 9. 7. 2008. Common Services Agency v Scottish Information Commissioner (Scotland). Věc [2008] UKHL 47.

9.2 MONOGRAFIE A ČASOPISECKÉ ČLÁNKY

[14] BLUME, Peter. It Is Time for Tomorrow: EU Data Protection Reform and the Internet. *Journal Of Internet Law*. 2015, vol. 18, no. 8, pp. 3-13 [cit. 24. 4 2015].

[15] BLUME, Peter. The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp: 269-273 [cit. 24. 4 2015]. s. 270. Dostupné z Oxford Journals: idpl.oxfordjournals.org/content/4/4/269.full.pdf + html

[16] HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2 *International Data Privacy Law* [online]. 2012, vol. 2, no. 1, pp. 3-18. ISSN 2044-4001 [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/1/3.full.pdf + html

[17] HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law* [online]. 2011, vol. 1, no. 4, pp. 211-228 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/1/4/211.full.pdf + html

[18] KOTCHY, Waltraut. The proposal for a new General Data Protection Regulation—problems solved? *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp. 274-281 [cit. 24. 4 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/4/4/274.full.pdf+html

[19] MCGILLIVRAY, Kevin. Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology & Intellectual Property*. 2014, roč. 17, č. Fall 2014, pp. 217–253.

[20] REDING, Viviane. The European data protection framework for the twenty-first century. *International Data Privacy Law* [online]. 2012, vol. 2, no. 3, pp. 119-129. [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/3/119.full.pdf

[21] SARTOR, Giovanni. Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? *International Data Privacy Law* [online]. 2013, vol. 3, no. 1, pp. 3-12 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/3/1/3.full.pdf+html

[22] SVANTESSON, Dan Jerker B. Data protection in cloud computing – The Swedish perspective. *Computer Law & Security Review* [online]. 2012, vol. 28, issue 4, pp. 476-480 [cit. 15. 2. 2015]. Dostupné ze ScienceDirect: http://linkinghub.elsevier.com/retrieve/pii/S0267364912001021.

[23] TOMÍŠEK, Jan. Licence při poskytování software jako služby. *Revue pro právo a technologie*, Masarykova univerzita, 2014, roč. 2014, č. 10, s. 47-69. ISSN 1804-5383.

9.3 OSTATNÍ LITERATURA

[24] DEBUSSCHE, Julien; VAN ASBROECK, Benoit; CHLOUPEK, Vojtěch a kol. Cloud computing and privacy series: the data protection legal framework (part 2 of 6). *Bird&Bird* [online]. 24 listopadu 2014 [cit. 15. 2. 2015]. Dostupné z http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-and-privacy-series-the-data-protection-legal-framework

[25] Cloud Service Level Agreement Standardisation Guidelines. *Evropská komise* [online]. Cloud Select Industry Group, Subgroup on Service Level Agreement, publikováno 24. 06. 2014 [cit. 30. 10. 2014]. Dostupné z: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138.

[26] *Data Processing Amendment to Google Apps Agreement* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/dpa_terms.html

[27] *Google Apps Enterprise (Online) Agreement* [online]. Google, únor 2014 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html

[28] *Guía para clientes que contraten servicios de Cloud Computing* [online]. Agencia Española de Protección de Datos, 2013 [cit. 11. 2. 2015]. Dostupné z: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

[29] *Guidance on the use of cloud computing* [online]. Information Commissioner's Office, 2012, [cit. 11. 2. 2015]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[30] *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [online]. Evropský parlament, publikováno 12. 3. 2014 [cit. 15. 2. 2015]. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

[31] *Letter from the Article 29 Working Party to Google on Google Privacy Policy* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 23. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf

[32] *Letter from the Article 29 Working Party to Microsoft on a new version of the Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 2. 4. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf

[33] *Letter for the Article 29 Working Party to Microsoft on the Microsoft Service Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 22. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf

[34] Microsoft adopts first international cloud privacy standard. *Microsoft on the Issues* [online]. Microsoft, publikováno 16. 2. 2015 [cit. 16. 3. 2015]. Dostupné z: http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/

[35] *Microsoft Online Subscription Agreement* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Po registraci dostupné z: portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK

[36] Model contract clauses for Google Apps. *Google Apps Help Center* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://support.google.com/a/answer/2888485?hl=en

[37] *Online Services Terms January 1, 2015* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248

[38] Opinion 05/2012 on Cloud Computing. *Evropská komise* [online]. Article 29 Data Protection Working Party, 2012 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[39] Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). *Evropská komise* [online]. Article 29 Data Protection Working Party, 2006 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf, p. 26.

[40] *Privacy Notice* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoft.com/online/legal/v2/?docid=18&langid=en-UK

[41] *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final* [online]. Evropská komise, 2012 [cit. 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN

[42] *Service Level Agreement for Microsoft Online Services* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8222

[43] *Service Orgnaization Control (SOC) 3 Report* [online]. Ernst & Young, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/pdfs/soc3_google_2014.pdf

[44] Smlouva o poskytování služeb společnosti Microsoft. *Windows* [online]. Microsoft, aktualizováno 11. 7. 2014 [cit. 22. 3. 2014]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/microsoft-services-agreement

[45] Smluvní podmínky společnosti Google. *Ochrana soukromí a smluvní podmínky* [online]. Google, aktualizováno 14. 4. 2014 [cit. 22. 3. 2014]. Dostupné z: http://www.google.com/intl/cs/policies/terms/

[46] *SOC 3 Seal of Assurance* [online]. WebTrust, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/soc3_google.html

[47] *Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/mcc_terms.html

[48] *Stanovisko č. 65/2013/4* [online]. Úřad pro ochranu osobních údajů, publikováno 1. 7. 2013 [cit. 11. 2. 2015]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002.

[49] Unleashing the Potential of Cloud Computing in Europe. *Evropská komise* [online]. 27 9. 2012 [cit 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[50] Use of cloud computing services. *Eurostat* [online]. Publikováno 16. 1. 2015 [cit. 15. 2. 2015]. Dostupné z: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cicce_use&lang=en

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

ELEKTRONICKÝ PODPIS PODLE NAŘÍZENÍ eIDAS[*]

VLADIMÍR SMEJKAL[**], JINDŘICH KODL[***], MIROSLAV UŘIČAŘ[****]

ABSTRAKT

Právní vymezení elektronického podpisu v ČR bylo doposud dáno Směrnicí Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, na jeho základě vytvořeným zákonem č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů (dále také jen „EPZ“) a novým občanským zákoníkem, zákonem č. 89/2012 Sb. (dále také jen „NOZ“).

Dne 23. července 2014 bylo vydáno Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále také jen „Nařízení“), které je – s určitými výjimkami – účinné od 1. července 2016. Protože jde o přímo působící předpis, bude jeho důsledkem s největší pravděpodobností zrušení, nebo značná redukce zákona o elektronickém podpisu, jakož i další změny v české legislativě.

Článek se zabývá jak právními, tak věcnými důsledky tohoto nového Nařízení v oblasti elektronického podpisu a hodnotí nové definice v Nařízení použité v kontextu s dosavadní právní úpravou.

[*] Příspěvek je výstupem projektu specifického výzkumu „Efektivní využití ICT a kvantitativních metod pro optimalizaci podnikových procesů“ Interní grantové agentury Vysokého učení technického v Brně s registračním číslem FP-S-15-2787.

[**] Prof. Ing. Vladimír Smejkal, CSc. LL.M. působí na Fakultě podnikatelské Vysokého učení technického v Brně a na Unicorn College v Praze. Zabývá se mj. problematikou informatické kriminality a právních aspektů informačních systémů a jejich bezpečností. V letech 2004 - 2014 byl členem Legislativní rady vlády ČR. Je soudním znalcem v oborech kybernetika, kriminalistika, ekonomika a autorská díla.

Kontaktní e-mail: smejkal@znalci.cz.

[***] Ing. Jindřich Kodl, CSc. je konzultantem a soudním znalcem v oblasti bezpečnosti informačních systémů a kryptologie. Je členem ISACA.

[****] Mgr. Miroslav Uřičař je ředitelem úseku práva, regulace, vnějších vztahů a bezpečnosti společnosti T-Mobile Czech Republic a.s. a předsedou legislativní komise České asociace pro soutěžní právo. Je dále členem představenstva Asociace provozovatelů mobilních sítí, členem výkonné rady UNICEF ČR a působí jako rozhodce Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky.

KLÍČOVÁ SLOVA

elektronická identifikace; elektronický podpis; elektronická značka; elektronická pečeť; elektronické časové razítko; dynamický biometrický podpis; elektronické právní jednání; služby vytvářející důvěru

ABSTRACT

The legal definition of electronic signature in the Czech Republic, has so far been given by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, was established on its basis by Act no. 227/2000 Coll., on electronic signatures, as amended and the new Law no. 89/2012 Coll., Civil Code.

The Regulation No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC that was issued on July 23, 2014 is – with certain exceptions – effective from 1 July 2016. Since this is a direct-acting prescription, it will be most likely the cause of the abolition or substantial reduction of the Act on Electronic Signatures as well as other changes in the Czech legislation.

The article deals with both legal and factual consequences of this new regulation in the field of electronic signature and evaluates new definitions of the Regulation used in the context of existing legislation.

KEYWORDS

electronic identification; electronic signature; electronic mark; electronic seal; electronic time stamp; dynamic biometric signature; electronic legal transactions; trust services

SEZNAM POUŽITÝCH ZKRATEK

ArchZ	zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů
ČR	časové razítko
DBP	dynamický biometrický podpis
DS	datová schránka podle zákona č. 300/2008 Sb., o elektronic-

	kých úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
ElÚkZ	zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
EP	elektronický podpis
EPZ	zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů
EZ	elektronická značka
ISDS	informační systém datových schránek podle § 14 zákona č. 300/2008 Sb. ve znění pozdějších předpisů
KvCt	kvalifikovaný certifikát
KvEP	kvalifikovaný elektronický podpis
NOZ	nový občanský zákoník, zákon č. 89/2012 Sb.
ObčZ	zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.
ZEP	zaručený elektronický podpis

1. ÚVOD – CÍLE A OBLAST PŮSOBNOSTI NAŘÍZENÍ

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu ve znění opravy ze dne 28. srpna 2014[1], známějšímu pod zkratkou „Nařízení eIDAS“ (což znamená *electronic identification and services*), se zaměřuje na více aspektů budování důvěryhodnosti v on-line prostředí. Hlavním mottem nařízení je zajištění interoperability na bázi kvalifikovaných služeb vytvářejících důvěru vykazujících srovnatelnou úroveň bezpečnosti a odpovědnosti v rámci EU.[2]

Podle čl. 1 je cílem nařízení zajistit řádné fungování vnitřního trhu a současně usilovat o odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru. Toto nařízení:

[1] Official Journal of the European Union, L 257, 28. 8. 2014, s. 73 – 114 a L 327, 12. 11. 2014, s. 9

[2] Viz body 4., 6., 7., 19., 20., 54., 77. Preambule Nařízení eIDAS

a) stanoví podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu;
b) stanoví pravidla pro služby vytvářející důvěru, zejména u elektronických transakcí; a
c) stanoví právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.

Cílem v oblasti elektronické identifikace je interoperabilita. V oblasti služeb vytvářejících důvěru je cílem harmonizace. V preambuli se uvádí obvyklé EU proklamace o hospodářském a sociálním rozvoji, k čemuž údajně přispěje jednotný digitální trh usnadněním přeshraničního využívání on-line služeb. To je poněkud vzdálenější cíl, nicméně bezprostředním smyslem Nařízení je sjednocení elektronické identifikace a její vzájemné uznávání v ostatních členských státech. Jeho cílem je zajistit, aby u přístupu k přeshraničním on-line službám poskytovaným členskými státy byla možná bezpečná elektronická identifikace a autentizace. Zásada vzájemného uznávání pro účely on-line služeb by se měla použít, jestliže systém elektronické identifikace oznamujícího členského státu splňuje podmínky pro oznámení a toto oznámení bylo zveřejněno v Úředním věstníku Evropské unie. Přitom úrovně záruky by měly vyjadřovat míru spolehlivosti prostředků pro elektronickou identifikaci při určování totožnosti osob, a tím poskytovat záruku, že osoba deklarující konkrétní totožnost je skutečně osobou, s níž je tato totožnost spojena. Podstatné je, že „*Stanovené požadavky by měly být z technologického hlediska neutrální. Měla by tedy existovat možnost splnit nezbytné bezpečnostní požadavky různými technologiemi.*[3]“

Jde o dokument, který odstraňuje řadu nepřesností vyplývajících v oblasti elektronického podpisu ze Směrnice 1999/93/ES a jejích národních implementací, které nebyly vždy konzistentní, a to ani vůči Směrnici, ani mezi sebou.[4] Nařízení se snaží integrovat vše, co nějakým způsobem souvisí s elektronickou identifikací a autentizací. Za tímto

[3] Bod 16 Preambule Nařízení eIDAS

účelem vystavělo poměrně složitou strukturu nástrojů o různých úrovních co do požadavků na ně kladených. Ne vždy zcela nutných, ne vždy zcela šťastných a – přinejmenším v jednom případě – vysloveně nevhodných, nebo přinejmenším zavádějících (viz čl. 25 odst. 2, k tomu pak dále).

Najdeme zde poněkud nešťastné rozlišování na „kvalifikované a nekvalifikované poskytovatele služeb vytvářejících důvěru"; nelze se přitom domnívat, že by uživatelé byli ochotni přehnaně využívat poskytovatele, jež budou označováni jako „nekvalifikovaní" a je otázkou, zda jde pouze o nešťastně zvolené označení, nebo o úmysl odradit jejich potenciální zákazníky. Přesto se jejich existence připouští s vymezením, že „*Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru by měli podléhat nezatěžujícím a pružným činnostem následného dohledu, odůvodněným povahou jejich služeb a činností. Orgán dohledu by proto neměl mít obecnou povinnost vykonávat nad nekvalifikovanými poskytovateli služeb dohled.*[5]"

Nařízení ponechává námi trvale kritizované možnosti používání pseudonymů v certifikátech,[6] když poněkud licoměrně říká, že „*ustanovení o používání pseudonymů v certifikátech by neměla členským státům bránit v tom, aby vyžadovaly identifikaci osob podle práva Unie nebo podle vnitrostátního práva.* [7]" Autorům není příliš jasné, jak používání pseudonymů může pomoci žádoucímu vylepšení nástrojů pro elektronickou identifikaci a autentizaci. A contrario: proč si pořizovat pseudonymní, tedy v podstatě anonymní certifikát pro komunikaci, kde se chci nějakým způsobem podepsat. Autoři jsou si samozřejmě vědomi dikce ust. § 79 NOZ o pseudonymu a zde tedy také hledají odůvodnění smyslu tohoto institutu v EPZ a nyní i v Nařízení.

Nařízení zavádí režim odpovědnosti, podle kterého by všichni poskytovatelé služeb vytvářejících důvěru měli odpovídat za škodu, kterou fyzické nebo právnické osobě způsobí v důsledku nesplnění povinností podle tohoto nařízení.

---

[4] DUMORTIER, Jos a kol. *Study on legal and market aspects of the application of Directive 1999/93/EC laying down a Community framework for electronic signatures and on the practical applications of the electronic signature.* Catholic Univestity of Leuven, Belgie, zpracováno pro European Commission, Directorate General Information Society, Brusel 2003.

[5] Bod 36 Preambule Nařízení eIDAS

[6] Např. MATES, Pavel; SMEJKAL, Vladimír. *E-government v České republice. Právní a technologické aspekty.* 2. vydání. Praha: Leges, 2012.

[7] Bod 33 Preambule Nařízení eIDAS

Jak budou realizovány některé návrhy, těžko říci. To se týká např. bodu 42., podle kterého v případě, že poskytovatel poskytuje své služby na území jiného členského státu a nepodléhá v něm dohledu, nebo pokud se počítače poskytovatele nacházejí na území jiného členského státu, než ve kterém je usazen, by měl být zřízen systém vzájemné pomoci mezi orgány dohledu v členských státech.

Abychom uklidnili společnosti, které dnes zahájily poměrně razantní přechod na dynamický biometrický podpis (dále také jen „DBP“)[8], je třeba hned v úvodu zdůraznit, že podle čl. 2 se Nařízení nevztahuje na poskytování služeb vytvářejících důvěru, které jsou používány výhradně v rámci uzavřených systémů vyplývajících z vnitrostátního práva nebo z dohod mezi určeným okruhem účastníků. Nařízení se vztahuje na systémy elektronické identifikace oznámené členskými státy a na poskytovatele služeb vytvářejících důvěru – viz níže – usazené v Unii. Nařízení nemá vliv na vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy.

Nařízení (regulation) je součástí tzv. sekundárního práva EU a svou povahou je obdobné zákonu, protože je bezprostředně závazné ve všech členských státech, nevyžaduje žádné implementace v národní legislativě a členské státy jsou povinny podle něj postupovat, jako by se jednalo o jejich vlastní právní předpis. Je závazné v celém rozsahu a přímo použitelné ve všech členských státech. Vyplývají z něj práva a povinnosti pro stát i jednotlivé osoby. Není tedy třeba provést transpozici do národního práva, jako tomu bylo v případě směrnice 1999/93/ES, která se stala zdrojem práva pro zákon o elektronickém podpisu č. 227/2000 Sb. Pokud nařízení stanoví něco jiného než národní právní předpis, musí mu dát členský stát přednost.

Obecné právní instituty týkající se právního jednání, uzavírání smluv na dálku apod. (u nás nyní soustředěné do nového občanského zákoníku) nebo postupy popsané v procesních předpisech (občanský soudní řád, trestní řád, daňový řád, zákon o elektronických právních úkonech a konverzi dokumentů) by tímto neměly být dotčeny; pokud se to nedá vyloučit, uvádíme to níže.

[8] Viz např. BERNÁŠEK, Aleš. Vlastnoruční digitální podpis a jeho implementace v O2 – část I. a II. *Data Security Management*, 2014, č. 3, s. 39 -39 a č. 4, s. 22 – 27.

Z výše uvedeného mj. vyplývá, že pokud budeme chtít realizovat něco jinak, nežli je popsáno v Nařízení, musíme si tedy vybudovat uzavřený systém, který u nadnárodních subjektů může být rovněž přeshraniční. A opačně – pro systémy otevřené, které předem neomezují nikoho v přístupu ke službám prostřednictvím sítí elektronických komunikací, platí Nařízení přímo a v plném rozsahu.

2. CÍLE NAŘÍZENÍ

Cíle Nařízení v sobě koncentrují zásady obsažené v citované Směrnici, ale i v dalších právních aktech EU[9]. Jsou to především:

- zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu [rozuměj EU] (bod 2. Preambule),
- odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci (bod 12. Preambule),
- zavedení a oznámení prostředků pro účely elektronické identifikace pro přístup k on-line službám včetně povinnosti je uznávat v členských státech (body 13. a 15. Preambule),
- stanovení obecného právního rámce pro využívání služeb vytvářejících důvěru včetně možnosti je použít jako důkaz v soudním a správním řízení (body 21. a 22. Preambule),
- stanovení odpovědnosti pro všechny poskytovatele služeb vytvářejících důvěru (bod 37. Preambule),
- zajištění soudržného rámce, který by v souvislosti se službami vytvářejícími důvěru zabezpečil vysokou úroveň bezpečnosti a právní jistotu (bod 44. Preambule),
- stanovení požadavků na kvalifikované prostředky pro vytváření elektronických podpisů, které mají zajistit funkčnost zaručených elektronických podpisů (bod 56. Preambule),
- zajištění dlouhodobého uchovávání informací, aby zajistilo dlouhodobou platnost elektronických podpisů a elektronických pečetí a zaručilo, že mohou být ověřeny bez ohledu na budoucí technologické změny (bod 61. Preambule),

[9] Např. Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle Směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu. OJ L 274, 20. 10. 2009, s. 36 – 37.

- stanovení právního rámce, který usnadní přeshraniční uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy (bod 66. Preambule),
- stanovení povinnosti v oblasti bezpečnosti a odpovědnosti pro služby autentizace internetových stránek (bod 67. Preambule),
- zrušení směrnice 1999/93/ES, a to z důvodu právní jistoty a jasnosti (bod 73. Preambule).

Co se týká elektronických podpisů, uvádí se zde, že „*nařízení by mělo zavést zásadu, že elektronickému podpisu by neměly být upírány právní účinky na základě skutečnosti, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis. Ačkoliv k zajištění vzájemného uznávání elektronických podpisů je zapotřebí vysoká úroveň bezpečnosti, měly by být ve zvláštních případech, například v kontextu rozhodnutí Komise 2009/767/ES 10, přijímány rovněž elektronické podpisy s nižší zárukou bezpečnosti. Právní účinky elektronických podpisů v členských státech by však měly být vymezeny vnitrostátním právem, s výjimkou požadavků stanovených v tomto nařízení, podle něhož by měl mít kvalifikovaný elektronický podpis rovnocenný právní účinek jako podpis vlastnoruční*“.[10]

Nařízení se zabývá i formáty elektronických podpisů a razítek – nově označovaných jako „pečetě“. Podle bodu 50. Preambule „*Jelikož v současnosti používají příslušné orgány v členských státech při podepisování svých dokumentů elektronickými prostředky různé formáty zaručených elektronických podpisů, je cílem Nařízení zajistit, aby členské státy mohly při přijímání dokumentů, které byly podepsány elektronickými prostředky, technicky podporovat alespoň určitý počet formátů zaručených elektronických podpisů. Pokud příslušné orgány v členských státech používají zaručené elektronické pečetě, bude obdobně nutné zajistit, aby podporovaly přinejmenším určitý počet formátů zaručených elektronických pečetí*“. K tomu se vztahuje také svěření pravomoci Komisi upravit formáty zaručených elektronických podpisů a pečetí podle bodu 64. Preambule – viz dále.

Objevuje se zde nový institut „dočasného pozastavení platnosti kvalifikovaných certifikátů“. Podle názoru autorů toto spíše vnese větší zmatek do ověřování platnosti právních jednání či jiných transakcí, protože na rozdíl od současného binárního stavu „platný – neplatný, resp.

[10] Body 48 a 49 Preambule Nařízení eIDAS

zneplatněný“ certifikát, bude nutno zkoumat, zda byl úkon učiněn v době, kdy byl či nebyl certifikát pozastaven. Smysl této novinky je poněkud nejasný a přínos sporný, přičemž bude mít velký dopad na procesy spojené s revokací certifikátů.

Předpokládá se certifikace bezpečnosti IT systémů založená na mezinárodních normách, přičemž výslovně je uvedena ISO 15408. Jedná se o poměrně známá „Common Criteria“, která vznikla na základě již dříve používaných norem, především amerických TCSEC, evropských ITSEC a kanadských CTCPEC. Mezinárodní norma ISO/IEC 15408:1999 má status české technické normy. Česká verze nese označení ČSN ISO/IEC 15408. Jednotlivé díly jsou ve shodě s originálem normy označeny jako 15408-1, 15408-2 a 15408-3.[11] Pravděpodobně by to mohly být i normy řady ISO/IEC 27000, resp. ČSN ISO/IEC 27000.

Nařízení – na rozdíl od Směrnice z roku 1999 – kodifikuje také to, co známe z českého zákona o elektronickém podpisu: elektronické značky a časová razítka. Zavádí elektronickou pečeť a elektronické časové razítko.

Kromě toho článek 46 Nařízení proklamuje něco, co je např. u nás tvrzeno různým způsobem již přes 15 let, tj. že „*Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu.*“ Autoři si nemyslí, že je toto dnes třeba uvádět, protože za posledních dvacet let diskuse, zpočátku značně bouřlivá, o uznávání tzv. elektronických důkazů v podstatě utichla a všeobecně se nepochybuje o možnosti použít k dokazování i elektronické stopy.[12] V našich podmínkách pak lze poukázat na dikci § 3026 odst. 1 NOZ „*Nevylučuje-li to povaha písemnosti, platí ustanovení tohoto zákona o listině obdobně i pro jinou písemnost bez zřetele na její podobu.*“, přičemž jak podle autorů, tak podle důvodové zprávy k NOZ se touto jinou písemností myslí písemnost elektronická. Na druhou stranu proklamace článku 46 Nařízení ničemu nezaškodí; její smysl může spočívat ve snaze unifikovat právní úpravy napříč členskými státy, protože ty nedosahují stejného standardu.

[11] SMEJKAL, Vladimír; RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, str. 303 an.

[12] Ke stopám viz např. SMEJKAL, Vladimír. Metodika vyšetřování kybernetické kriminality. In: PORADA, Viktor; STRAUS, Jiří et al. *Kriminalistika (výzkum, pokroky, perspektivy)*. Plzeň: Ales Čeněk, 2013 nebo PORADA, Viktor; STRAUS, Jiří. *Kriminalistické stopy - Teorie, metodologie, praxe.* Aleš Čeněk, s.r.o., Plzeň, 2012.

Autoři Nařízení si patrně uvědomili neustálý vývoj technologií, ale i kybernetické kriminality[13]. Reakcí na tento vývoj jsou ustanovení, podle kterých by měla být Komisi svěřena pravomoc *„přijímat akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o kritéria, která musí splňovat subjekty odpovědné za certifikaci kvalifikovaných prostředků pro vytváření elektronických podpisů*[14]“. Účelem svěření této pravomoci totiž má být pružné a rychlé doplnění určitých podrobných technických aspektů tohoto nařízení. Komisi by měly být svěřeny prováděcí pravomoci, zejména k určení referenčních čísel norem, jejichž použití zakládá předpoklad shody s určitými požadavky stanovenými v tomto nařízení, přičemž se předpokládá spolupráce zejména s Evropským výborem pro normalizaci (CEN), Evropským ústavem pro telekomunikační normy (ETSI), Mezinárodní organizací pro normalizaci (ISO) a Mezinárodní telekomunikační unií (ITU).

Poslední téma Nařízení, které je nicméně již mimo záběr tohoto článku, jsou služby autentizace internetových stránek, proto se jím detailně nezabýváme.

A konečně, jak již vyplývá z názvu Nařízení, ruší se jím směrnice 1999/93/ES. Tento krok je nezbytný, neboť cíle Nařízení jsou podstatně širší a řada definic, které do právního řádu EU citovaná směrnice zavedla, je zde přeformulována. Jedná se tedy o standardní legislativní postup.

3. DEFINICE V OBLASTI ELEKTRONICKÉHO PODPISU DŘÍVE A NYNÍ

V rámci nově formulovaných definic v Nařízení dochází k celé řadě změn, mnohé z nich mají pouze formální či upřesňující charakter, je však i nemálo těch, které jsou zásadní. Pro snadnější orientaci čtenáře jsme vytvořili tabulku zásadních pojmů, v níž jsme zahrnuli porovnání těchto pojmů dle právního řádu ČR, zejména podle zákona o elektronickém podpisu, a dle Nařízení, přičemž ty změny, které jsou dle našeho názoru zásadní, jsme označili **tučně.** Podtržením jsou pak označena místa, která nejsou podle názoru autorů ani v novém Nařízení dostatečně definována či snadno vyložitelná a která diskutujeme dále.

[13] Podrobně viz SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015.
[14] Bod 70 Preambule Nařízení eIDAS

TABULKA 1. POROVNÁNÍ ZÁKLADNÍCH POJMŮ

Pojem	**Podle zákona o elektronickém podpisu nebo jiného právního předpisu v české legislativě**	**Podle Nařízení**
podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby	fyzická osoba, která vytváří elektronický podpis
elektronický podpis	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a **které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě**	data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a **která podepisující osoba používá k podepsání**
zaručený elektronický podpis	elektronický podpis, který splňuje následující požadavky 1. je jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby **ve vztahu k datové zprávě,** 3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, 4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat	elektronický podpis, který splňuje požadavky stanovené v článku 26: a) je jednoznačně spojen s podepisující osobou; b) umožňuje identifikaci podepisující osoby; c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s **vysokou úrovní důvěry** použít pod svou výhradní kontrolou; a d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změ-

		nu dat
kvalifikovaný elektronický podpis	**není výslovně definován**, nicméně je opisován frází „*použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu*“ – viz § 3 EPZ	zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy
data pro vytváření elektronických podpisů	jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu	jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů
certifikát pro elektronický podpis	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a **umožňuje ověřit její identitu**, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,	elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a **potvrzuje alespoň jméno nebo pseudonym této osoby**
kvalifikovaný certifikát pro elektronický podpis	certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb Podle § 12: (1) Kvalifikovaný certifikát musí obsahovat a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona, b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je	certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze I: Kvalifikované certifikáty pro elektronické podpisy obsahují a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako

	kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen, c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym, d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu, e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby, f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává, g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb, h) počátek a konec platnosti kvalifikovaného certifikátu, i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,	kvalifikovaný certifikát pro elektronický podpis; b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a - v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech, - v případě fyzické osoby: jméno osoby; c) alespoň jméno podepisující osoby nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena; d) data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů; e) označení začátku a konce doby platnosti certifikátu; f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru; g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifi-

	j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít. (2) Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám. (3) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.	kovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává; **h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);** i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu; j**) pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.**
služba vytvářející důvěru	- - -	elektronická služba, která je zpravidla poskytována za úplatu a spočívá: a) ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo

		b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami
kvalifikovaná služba vytvářející důvěru	- - -	služba vytvářející důvěru, která splňuje použitelné požadavky stanovené v tomto nařízení
poskytovatel služeb vytvářejících důvěru	poskytovatelem certifikačních služeb se rozumí fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy	fyzická nebo právnická osoba, která poskytuje jednu či více služeb vytvářejících důvěru buď jako kvalifikovaný, nebo jako nekvalifikovaný poskytovatel služeb vytvářejících důvěru
kvalifikovaný poskytovatel služeb vytvářejících důvěru	kvalifikovaným poskytovatelem certifikačních služeb se rozumí poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů a **splnil ohlašovací povinnost podle § 6**	poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému **orgán dohledu udělil status kvalifikovaného poskytovatele**
produkt	nástrojem elektronického podpisu se rozumí technické zařízení nebo programové vybavení, nebo jejich součásti, používané poskytovatelem certifikačních slu-	technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb vytvářejících důvěru

	žeb pro vytváření nebo ověřování elektronických podpisů nebo pro zajištění certifikačních služeb,	
prostředek pro vytváření elektronických podpisů	technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů	konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů
kvalifikovaný prostředek pro vytváření elektronických podpisů	- - -	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II: 1. Kvalifikované prostředky pro vytváření elektronických podpisů vhodnými technickými prostředky a postupy přinejmenším zajistí, aby: a) byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů, která byla použita při vytváření elektronického podpisu; b) data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu se mohla prakticky vyskytnout pouze jednou; c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu nelze odvodit a že elektronický podpis je v současnosti dostupnými

		technickými prostředky spolehlivě chráněn proti padělání; d) oprávněná podepisující osoba měla možnost data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu spolehlivě chránit před jejich zneužitím třetí osobou. 2. Kvalifikované prostředky pro vytváření elektronických podpisů nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním. 3. Data pro vytváření elektronických podpisů může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru. 4. Aniž je dotčen bod 1 písm. d), smějí kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří spravují data pro vytváření elektronických podpisů jménem podepisující osoby, kopírovat data pro vytváření elektronických podpisů pouze pro účely zálohování a jsou-li splněny tyto požadavky:

		a) bezpečnost zkopírovaných souborů dat je na stejné úrovni jako u původních souborů dat; b) počet zkopírovaných souborů dat nepřesáhne minimum potřebné pro zajištění kontinuity služby.
pečetící osoba	označující osobou se rozumí **fyzická osoba, právnická osoba nebo organizační složka státu,** která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou	**právnická osoba**, která vytváří elektronickou pečeť
elektronická pečeť	elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky 1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, 2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, 3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat	data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu

zaručená elektronická pečeť	- - -	elektronická pečeť, která splňuje požadavky stanovené v článku 36: a) je jednoznačně spojena s pečetící osobou; b) umožňuje identifikaci pečetící osoby; c) je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou; a d) je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat
kvalifikovaná elektronická pečeť	- - -	zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť
data pro vytváření elektronických pečetí	daty pro vytváření elektronických značek se rozumí jedinečná data, která označující osoba používá k vytváření elektronických značek	jedinečná data, která pečetící osoba používá k vytváření elektronických pečetí
certifikát pro elektronickou pečeť	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování	elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí

	elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,	s určitou právnickou osobou a potvrzuje název této osoby
kvalifikovaný certifikát pro elektronickou pečeť	kvalifikovaným systémovým certifikátem se rozumí certifikát, který má náležitosti podle § 12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb Podle § 12a: Kvalifikovaný systémový certifikát musí obsahovat a) označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona, b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen, c) jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek, d) data pro ověřování elektronických značek, která	certifikát pro elektronickou pečeť, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze III: Kvalifikované certifikáty pro elektronické pečetě obsahují: a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronickou pečeť; b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a - v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech, - v případě fyzické osoby: jméno osoby;

	odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby, e) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává, f) číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb, g) počátek a konec platnosti kvalifikovaného systémového certifikátu, h) omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.	c) alespoň jméno pečetící osoby a případné registrační číslo uvedené v úředních záznamech; d) data pro ověřování platnosti elektronických pečetí, která odpovídají datům pro vytváření elektronických pečetí; e) označení začátku a konce doby platnosti certifikátu; f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru; g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává; h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g); i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu; j) pokud jsou data pro vytváření elektronických pečetí spojená s daty pro

		ověřování platnosti elektronických pečetí obsažena v kvalifikovaném prostředku pro vytváření elektronických pečetí, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.
prostředek pro vytváření elektronických pečetí	prostředkem pro vytváření elektronických značek se rozumí zařízení, které používá označující osoba pro vytváření elektronických značek a které splňuje další náležitosti stanovené tímto zákonem,	konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických pečetí
kvalifikovaný prostředek pro vytváření elektronických pečetí	- - -	prostředek pro vytváření elektronických pečetí, který přiměřeně splňuje požadavky stanovené v příloze II
elektronické časové razítko	- - -	data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a **prokazují, že tato jiná data existovala v daném okamžiku**
kvalifikované elektronické časové razítko	kvalifikovaným časovým razítkem se rozumí datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a **zaručuje, že uvedená data v elektronické**	elektronické časové razítko, které splňuje požadavky stanovené v článku 42: a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat; b) je založeno na zdroji přesného času, který je

	podobě existovala před daným časovým okamžikem	spojen s koordinovaným světovým časem; a c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou
elektronický dokument	- datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru (podle EPZ) - dokumentem každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena (ArchZ)	jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka
služba elektronického doporučeného doručování	upraveno zákonem o elektronických úkonech a autorizované konverzi dokumentů[15]	služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání

[15] Podrobný rozbor viz SMEJKAL, Vladimír. *Datové schránky v právním řádu ČR. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, s komentářem*. 1. vydání. Praha: ABF, a.s., 2009 nebo MATES, Pavel; SMEJKAL, Vladimír. *E-government v České republice. Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vydání. Praha: Leges 2012, s. 162 an.

		s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn
kvalifikovaná služba elektronického doporučeného doručování	upraveno zákonem o elektronických úkonech a autorizované konverzi dokumentů	služba elektronického doporučeného doručování, která splňuje požadavky stanovené v článku 44: a) jsou poskytovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru; b) s vysokou úrovní spolehlivosti zajišťují identifikaci odesílatele; c) zajišťují identifikaci příjemce před doručením dat; d) odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat; e) odesílatel a příjemce dat jsou jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat; f) datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného e-

		lektronického časového razítka.
data pro ověřování platnosti	daty pro ověřování elektronických podpisů se rozumí jedinečná data, která se používají pro ověření elektronického podpisu, daty pro ověřování elektronických značek se rozumí jedinečná data, která se používají pro ověření elektronických značek,	data, která se používají k ověření platnosti elektronického podpisu nebo elektronické pečeti
ověřování platnosti	- - -	postup ověřující shodu a potvrzující platnost elektronického podpisu nebo elektronické pečeti

4. ELEKTRONICKÁ ČASOVÁ RAZÍTKA

Elektronická časová razítka (dále jen „ČR“) máme v české legislativě od roku 2004, byť pouze jako kvalifikovaná, což autoři dlouhodobě nepovažují za metodicky správné a ostatně ani za logicky odůvodněné (začínat definici hned „vyšším stupněm“ bez definování základního, jak tomu je u elektronického podpisu, je přinejmenším zvláštní). Nařízení obsahuje obě definiční úrovně (bod 33. a 34. čl. 3) a podle čl. 41 Nařízení podobně jako u elektronického podpisu a pečeti zdůrazňuje, že ani „*elektronickému časovému razítku nesmějí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické časové razítko*“.

U kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny. Definiční čl. 3 Nařízení to říká výslovně (a správněji nežli stávající EPZ): „*elektronickým časovým razítkem jsou data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku*“. Došlo tedy k odstranění nevhodné definice časového razítka podle stávajícího zákona,

na kterou bylo v minulosti opakovaně upozorňováno. Pokud se totiž v definici KvČR dle ust. § 2 písm. r) EPZ praví, že „*kvalifikovaným časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem*“, pak existuje jistá past doslovného výkladu této definice, která vychází ze zahraničního dokumentu, tvořeného technology.[16] Lze totiž diskutovat o tom, jak dlouho data existovala před daným časovým okamžikem – hodinu, týden, rok, desetiletí? Podle názoru autorů cit. práce, by bylo přesnější použít definici jinou, právnicky přesnější, tj. typu „data existovala v okamžiku doručení vzorku (hash) dokumentu k poskytovateli“.[17] Definice v Nařízení tento problém odstraňuje při zachování vysoké míry obecnosti a technologické nezávislosti.

Kvalifikované elektronické časové razítko vydané v jednom členském státě se uznává jako kvalifikované elektronické časové razítko ve všech členských státech. Především, ale nejen pro tento účel jsou v čl. 42 definovány požadavky na kvalifikovaná elektronická časová razítka:

a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat;

b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem[18]; a c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru (viz Kapitola III Nařízení) nebo označeno jinou rovnocennou metodou.

5. ELEKTRONICKÉ PEČETI

Směrnice 1999/93/ES neznala elektronické značky, na rozdíl od českého EPZ, kam byly zavedeny novelou EPZ zákonem č. 440/2004 Sb. společně s časovými razítky. V Nařízení se značky objevily, neboť všeobecná

[16] Viz Např. RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), Part. 1. Introduction: A time-stamping service supports assertions of proof that a datum existed before a particular time. Similarly ETSI TS 102 023 V1.2.1 (2003-01), part 3.1.

[17] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 152.

[18] Koordinovaný světový čas (Coordinated Universal Time), pro který je používána zkratka UTC, je celosvětový časový standard vycházející z tzv. mezinárodního atomového času, jehož časová pásma jsou definována svými odchylkami od UTC.

užitečnost takového nástroje je známa, a to jako „elektronické pečeti". Anglický termín „seal" mohl být ovšem přeložen také jako „razítko", neboť o to v Nařízení právě jde. V definici v čl. 3 bod 24. najdeme, že „*pečetící osobou je právnická osoba, která vytváří elektronickou pečeť*", a dále v bodu 29., že „*certifikátem pro elektronickou pečeť je elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí s určitou právnickou osobou a potvrzuje název této osoby*" – pro laiky lze připodobnit ke klasickému razítku.

Čl. 35 až 39 říkají pro pečeti totéž, co čl. 25 až 29 pro elektronické podpisy. Je otázkou legislativní techniky, zda nešlo konstatovat – vzhledem k totální shodě textů – pouze to, že ustanovení o podpisech se pro pečetě použijí obdobně. Je zajímavé, že v čl. 39 a 40 toto bylo možno použít s odkazem na čl. 29 až 34.

Podle bodu 29. jsou tedy vyloučeny osoby fyzické. Nevíme proč, lze se domnívat, že zřejmě proto, že ty mohou používat svůj elektronický podpis, což je ovšem něco zcela odlišného. V případě podpisu podle Nařízení jde o data, která podepisující osoba používá k podepsání (viz čl. 3 bod 10), neboli jedná se nepochybně o projev vůle (podle NOZ právní jednání). U pečeti jde o data, „*která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu*" (čl. 3 bod 25). Elektronická pečeť je tedy jakýmsi průkazem kvality, příp. původu dat a autorům není jasné, proč jsou o tuto možnost fyzické osoby (typicky pak fyzické osoby podnikající) ochuzeny. To, že místo elektronické značky, kterou podle českého zákona může označovat fyzická i právnická osoba, budeme mít elektronickou pečeť a tu pouze pro právnické osoby, považujeme za nepřijatelné omezení fyzických osob, zejména fyzických osob podnikajících, či dokonce těch, kdo na základě nějakého pověření vykonávají činnost orgánů veřejné správy.[19]

Lze připomínkovat i další definice Nařízení:

1. kvalifikovaný certifikát pro elektronický podpis – velmi obtížně lze dovodit, co v příloze I se rozumí pod písmenem j), kde se praví „*pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena*

[19] Že takové osoby mohou existovat, je poměrně známým faktem a připouští to i EPZ v § 11 odst. 1 písm. e) nebo zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů v § 2 písm. c). Týká se to např. notářů a exekutorů.

v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování“; autoři tuší, že formulace je převzata z norem ETSI a má říci, že kvalifikovaný certifikát obsahuje pár klíčů, kdy privátní klíč je uložen bezpečně (např. v zařízení HSM) a je zaručena jeho nepopiratelnost (nonrepudiation), přičemž daný certifikát nemusí být vydán certifikační autoritou. V některých systémech mohou být totiž vyvářeny lokální certifikáty, k nimž jsou připojeny poznámky, resp. provozní data, která blíže specifikují prostředek, ve kterém byl certifikát vytvořen; poznámka pak dává informace, že i takto vytvořený certifikát je pro daný účel důvěryhodný;

2. prostředek pro vytváření elektronických podpisů a stejně prostředek pro vytváření elektronických pečetí – proč je třeba zdůrazňovat, že se jedná o „konfigurované“ programové vybavení nebo technické zařízení, resp. každé smysluplně použitelné zařízení by mělo být nějako konfigurováno,
3. certifikát pro elektronickou pečeť – proč certifikát potvrzuje název této osoby: proč jen název; nevíme, jak tomu je v jiných státech, ale lze se domnívat, že zaměnitelných názvů právnických osob i zde bude značné množství.

6. ELEKTRONICKÉ PODPISY

6.1 PODPISY PODLE SOUČASNÉ A NOVÉ PRÁVNÍ ÚPRAVY

Definice elektronického podpisu patří podle názoru autorů mezi ty, které si zasluhují hlubší zamyšlení. Podle rušené Směrnice[20] byl elektronický podpis definován jako „*údaj v elektronické podobě, který je připojen či logicky spojen s jinými elektronickými daty a který slouží jako metoda ověření pravosti*[21]“. Pravdou je, že tvrzení „údaj slouží jako metoda“ je poněkud neortodoxní, nicméně je zřejmé, že Směrnici šlo o *ověření pravosti podpisu*. Původní znění

[20] Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy

[21] Čl. 2 bod 1 Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy

českého EPZ v roce 2000[22] jej definovalo jako „*údaje… které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě*[23]“, podle stávajícího EPZ je elektronický podpis definován jako „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*[24]“. Vidíme, že českému zákonodárci nevadí nesmyslné ztotožnění údaje = metoda, ale zato důsledně nahradil ověření pravosti podpisu *ověřením identity podepsané osoby*. Pravděpodobně vzhledem k dikci § 40 odst. 4 předchozího občanského zákoníku (ObčZ), podle kterého „*Písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.*“. Tento požadavek ale nesouvisí s podpisem samotným, ale písemnou formou právního úkonu (podle ObčZ). Přes všechny nepřesnosti jsme nicméně stále věděli, že jde o atributy, které nám umožní ověřit pravost podpisu a to tak, že jsme schopni identifikovat osobu, která jej učinila.

Nařízení ale činí zásadní posun, když tvrdí, že elektronický podpis jsou „*data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.*[25]“

Jinými slovy, nejde nám již o následnou možnost ověření pravosti podpisu či identity osoby pomocí dat nazvaných „elektronický podpis“, ale o to, že je položeno rovnítko mezi elektronický podpis a data, „*která podepisující osoba používá k podepsání.*[26]“ Z našeho pohledu to je rozhodně pozitivní. Tím totiž dochází k chápání podpisu podle jeho primární funkce, tj. jako k doložení skutečnosti, že určitá osoba projevila svoji vůli, případně že se v určitou dobu nacházela na určitém místě, popř. že stvrzuje platnost určitého dokumentu.[27] Jak říká americké právo, „*podpis spočívá v umístění jména na konec listiny, s cílem potvrdit její platnost. Může být vlastnoruční, vytištěný, vyražený na razítku, napsaný psacím strojem, vyrytý, ofotografovaný,*

[22] Zákon č. 227/2000 Sb. o elektronickém podpisu
[23] Ustanovení § 2 odst. a) zákona č. 227/2000 Sb. o elektronickém podpisu
[24] Ustanovení § 2 odst. a) zákona č. 227/2000 Sb. o elektronickém podpisu v platném znění
[25] Čl. 3 bod 10 Nařízení eIDAS
[26] Čl. 3 bod 10 Nařízení eIDAS
[27] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 271 an.

vyříznutý z jedné listiny a připojený ke druhé. Rovněž litografovaný podpis na listině postačuje k potvrzení její platnosti, přičemž je nepodstatné, jakým nástrojem se podpis udělá.“[28] Osoba si může za svůj podpis zvolit jakýkoli znak, symbol nebo kresbu. Současná právní úprava daná směrnicí 1999/93/ES a EPZ posouvala podpis někam jinam a přiřazovala mu funkci metody k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě (viz § 2 písm. a/ EPZ).

V rámci současných technologických možností přichází v úvahu řada variant skutečného provedení elektronického podpisu. V následujícím textu se proto budeme věnovat rozboru všech možností, přičemž budeme předpokládat, že čtenářům jsou známy principy podpisů na bázi asymetrické kryptografie,[29] které donedávna představovaly hlavní variantu realizace zaručeného elektronického podpisu podle směrnice a EPZ.

Pokud podepisující osoba používá k podepsání elektronickým podpisem data dle bodu 13 čl. 3 Nařízení, podle kterého „*daty pro vytváření elektronických podpisů jsou jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů*“, pak při použití metody asymetrické kryptografie je těmito daty tajný (soukromý) klíč.

Ale pojďme v úvahách dále. Pokud tedy má mít osoba nějaká data (elektronická), jež může použít k podepsání, znamená to, že elektronickým podpisem jsou jakákoliv data v elektronické podobě, která jsou schopna být „*připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena*“[30]. Čili vlastně cokoliv, co můžeme zdigitalizovat. Elektronickým podpisem (prostým) podle Nařízení je tedy PIN, heslo, fráze, obrázek atd., tedy jakýkoliv digitální záznam, který má podobu nul a jedniček a který připojíme k podepisovanému dokumentu. To je také správně, protože v minulosti jsme složitě konstruovali výklad, jak podle Směrnice, resp. EPZ prohlásit použití PIN u platební karty za podepsání elektronické transakce. Naskýtá se také zajímavá možnost používat pro „prostý“ elektronický podpis hlas: hlas nepochybně digitalizovat lze, dokonce je sám o sobě jedinečným natolik, že jej prý lze jen velmi stěží napodobit, aniž by to při

[28] Maricopa County v. Osborn, 60 Ariz. 290, 136 P.2d 270, 274. Cit. dle BLACK, Henry Campbell; NOLAN, Joseph R.; NOLAN-HALEY, Jacqueline M. *Blackův právnický slovník.* 6. vyd., v ČR 1. Praha: Victoria Publishing, 1993, s. 1268.

[29] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 281 an.

[30] Čl. 3 bod 13 Nařízení eIDAS

následné analýze zůstalo skryto. Tím bychom vlastně vytvořili požadovanou vícefaktorovou autentizaci[31] u základního typu elektronického podpisu.

Klasický, tedy vlastnoruční podpis (který není definován právním řádem a ten s ním pracuje jako s notorietou) není vytvářen žádnými daty. *„Vlastnoruční podpis je výsledkem uplatnění návyku psaní, získaného v podobě individuálního a relativně stálého písemného projevu člověka. Vznik individuálnosti písma je důsledkem vytvoření dynamického stereotypu psaní, tedy vypracování složitého systému podmíněných reflexů, které jsou závislé na stupni procvičování. Při vytvoření konkrétního písemného projevu – tedy např. podpisu – se uplatňují ale i aktuální vnější a vnitřní podmínky, za kterých psaní probíhá a v jejichž důsledku může být získaný dynamický stereotyp narušen. Zkoumání pravosti písma (podpisu), které je zaměřeno na grafickou stránku směřující k identifikaci pisatele, je prováděno pomocí různých metod. Jak u podepisování, tak u zkoumání pravosti (ověřování) podpisu jde tedy o procesy převážně subjektivního charakteru, v nichž se promítají obecné a individuální vlastnosti zúčastněných osob. Tyto vlastnosti se dnes využijí i při ověřování pravosti tzv. dynamického biometrického podpisu, který kombinuje vlastnosti jak grafického, tak elektronického podpisu.*[32]*“*

Jde o tzv. biomechanický proces vzniku lidského podpisu, který není nikterak jednoduchý. Primární vzruch vzniká v centrálním nervovém systému – v lidském mozku s předem definovanou intenzitou a trváním. Nervový systém pak aktivuje příslušné svaly v definovaném pořadí. Pohyb pera po papíře, což je výsledek stahování a uvolňování svalů, zanechává stopu hrotu psacího nástroje.

Pokud se osoba vlastnoručně podepisuje, pak existují v zásadě dvě možnosti:

a) podepisuje se na nějakém fyzickém nosiči nástrojem (tužka, pero), který zanechává grafickou stopu – obraz podpisu (statický obraz), typicky na papíru, ale v podstatě jakémkoliv hmotném nosiči;

---

[31] Viz např. SMEJKAL, Vladimír; KODL, Jindřich. Development trends of electronic authentication. In: *Proceedings of the 42nd Annual Konference 2008 IEEE International Carnahan Conference on Security Technology*, Diplomat Hotel Prague, Czech Republic, October 13 - 16, 2008, s. 1 – 6.

[32] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s., s. 271.

b) podepisuje se na zařízení, které kromě obrázku snímá i neviditelné dynamické vlastnosti tohoto podpisu, spojené s typickým chováním podepisující se osoby – časy, rychlosti, zrychlení apod. Tím vzniká dynamický biometrický podpis (DBP).[33]

Podle autorů nová definice elektronického podpisu posiluje postavení DBP v právním řádu EU a ČR a vytváří možnosti pro přijetí i dalších, v budoucnu se objevivších metod pro elektronické podepisování, zejména, ale nikoliv pouze na bázi biometrie. Proto mu věnujeme níže více pozornosti.

Dynamický biometrický podpis je podobný případ, jako ve fyzice elektromagnetické záření, na které lze nahlížet jako na částici – kvantum energie v podobě fotonů, ale stejně dobře i jako na vlnění, a to v závislosti na uspořádání experimentu a způsobu pozorování.[34] Hovoříme o tzv. dualitě. Stejně tak DBP můžeme chápat dvěma paralelními způsoby, a to současně jako:

1. vizuální, viditelný, vlastnoruční podpis,
2. neviditelný, digitální, elektronický podpis.

Při vytvoření DBP vzniknou současně obě formy podpisu, kdy data použitá k podepsání jsou snímána 3D snímačem a mohou být jak uložena, tak zobrazena. DBP má tedy rovněž duální charakter, nicméně – na rozdíl od světla jakožto nejznámější formy elektromagnetického záření – můžeme u DBP jednotlivé složky oddělit a nakládat s nimi samostatně. Přitom stále se bude jednat o určitou formu podpisu, v 1. případě okem viditelného, ve 2. případě neviditelného, nicméně zobrazitelného prostřednictvím technického zařízení stejně, jako tomu je u podpisu kryptografického. Rozdílem mezi kryptografickým podpisem a DBP je mj. i to, že i z biometrických parametrů můžeme získat obrázek podpisu, zatímco u podpisu kryptografického je to pouze řada čísel.

---

[33] Viz SMEJKAL, Vladimír; KODL, Jindřich. Strong authentication using dynamic biometric signature. Proceedings of 45th Annual 2011 IEEE International Carnahan Conference on Security Technology (ICCST), 18-21 October 2011, Tecnocampus Mataró Maresme, Barcelona, Španělsko, s. 340 – 344 a SMEJKAL, Vladimír; KODL, Jindřich; KODL, Jindřich Jr. Implementing Trustworthy Dynamic Biometric Signature according to the Electronic Signature Regulations. In: *Proceedings of 47th Annual 2013 IEEE International Carnahan Conference on Security Technology (ICCST)*, 9-11 October 2013, Medellín, Colombia, ISBN: 978-958-8790-65-7, s. 165 – 170.

[34] Tzv. myšlenku duality částic a vlnění formuloval v roce 1905 Albert Einstein pro objasnění fotoelektrického jevu.

Data vytvořená vlastnoručním podpisem nejsou absolutně konstantní a neměnná, jako tomu je v případě soukromého klíče při asymetrické kryptografii, ale jsou dostatečně přesná a podrobná pro to, abychom je strojově, případně s pomocí písmoznalce ověřili.[35] Výhodou oproti kryptografickému elektronickému podpisu je existence oné „vlastnoručnosti", která je u soukromého klíče zajišťována pouze právním prohlášením podle § 5 odst. 1 písm. a) EPZ, podle kterého je podepisující osoba povinna zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití.[36]

V obou případech jsou tato data těmi daty, *která podepisující osoba používá k podepsání*[37], a s různou mírou věrohodnosti a námahy jsou daty, které nám umožní ověřit pravost podpisu prostřednictvím identifikace osoby, která jej učinila.

Nařízení se týká – jak název naznačuje – elektronické identifikace, ale především služeb s ní spojených, jež jsou nazývány „služby vytvářející důvěru". Co se týká oblasti, kterou bychom mohli nazvat „elektronický podpis – elektronická značka – časové razítko", pak zde nedochází k žádné dramatické změně oproti stávajícímu stavu. Na druhou stranu ale také byly promeškány některé příležitosti. V bodu (27) odůvodnění Nařízení se uvádí: „*Toto nařízení by mělo být z technologického hlediska neutrální. Právních účinků, které přiznává, by mělo být možné dosáhnout jakýmikoli technickými prostředky, jsou-li splněny požadavky tohoto nařízení.*" Podle názoru autorů to není zcela tak; EU se v roce 1999 vydalo – z tehdejšího pohledu pochopitelně a oprávněně – v oblasti elektronického právního jednání cestou jedinou: prostřednictvím elektronického podpisu na bázi asymetrické kryptografie, byť ve Směrnici 1999/93 v čl. 2 definice ad (4) zní „*daty pro vytváření podpisu se rozumí jedinečná data, jako jsou kódy nebo soukromé kryptografické klíče…*", takže již tato směrnice vytvořila prostor

[35] Viz SMEJKAL, Vladimír; KODL, Jindřich. Assessment of the authenticity of Dynamic Biometric Signature. The results of experiments. In: *Proceedings of 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST)*, 13-16 October 2014, Roma, Italia, ISBN: 978-1-4799-3530-7, s. 45 – 49.

[36] SMEJKAL, Vladimír; KODL, Jindřich. Vícefaktorová autentizace a dynamický biometrický podpis. In: *Sborník 16. ročníku mezinárodní konference Information Security Summit (IS2)*, 27. – 28. května 2015, Praha: TATE International, s.r.o., s. 107 – 119.

[37] Čl. 3 bod 10 Nařízení eIDAS

pro jiné než kryptografické EP. Nicméně v posledních 5-10 letech se stále více diskutuje o vícefaktorové autentizaci[38] a o využití biometrických nástrojů pro identifikaci a autentizaci včetně podepisování.[39] Pouhý podpis jako obrázek představuje stejně jako heslo pouze jeden autentizační faktor a současným trendem je vícefaktorová autentizace[40], tj. k obrázku potřebujeme přidat něco dalšího, například biometrický záznam.

Podpis coby součást písemných právních úkonů byl v našem právním řádu upraven dříve v ust. § 40 odst. 3 a 4 ObčZ, nyní v ust. § 561 – 562 NOZ. Tomu odpovídala i úprava v EPZ, jež vycházel ze směrnice 1999/93/ES. Nařízení v tomto nepřináší žádnou změnu, neboť jak kryptografický elektronický podpis, tak dynamický biometrický podpis je vlastnoručním podpisem ve smyslu ust. § 561 odst. 1 věta první NOZ a vyhovuje požadavkům na písemnost podle § 562 odst. 1 NOZ. Oba jsou elektronickým podpisem podle platného EPZ a rovněž elektronickým podpisem podle Nařízení. Vyplývá to jak z výše citovaných definic, tak z principů, které se nacházejí v bodech 48 až 65 Nařízení a které se týkají přijímání elektronických podpisů s nižší zárukou bezpečnosti, jež nesplňují požadavky na kvalifikovaný elektronický podpis.[41] Tento princip je v čl. 25 odst. 1 Nařízení formulován následovně: *„1. Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.“*

Ve speciálních případech by zřejmě pak jako „obyčejný“ elektronický podpis ve smyslu Nařízení obstál i jiný druh digitálního záznamu, jak je uvedeno výše. Dikce věty druhé odst. 1 § 561 NOZ *„Jiný právní předpis*

---

[38] Viz SMEJKAL, Vladimír; KODL, Jindřich. Strong authentication using dynamic biometric signature. In: *Proceedings of 45th Annual 2011 IEEE International Carnahan Conference on Security Technology (ICCST)*, 18-21 October 2011, Tecnocampus Mataró Maresme, Barcelona, Španělsko, s. 340 – 344.

[39] Viz např. SMEJKAL, Vladimír; KODL, Jindřich, op. cit; SMEJKAL, Vladimír; KODL, Jindřich. Dynamický biometrický podpis – místo mýtů fakta. *Data Security Management*, XVI., 2012, č. 2, str. 20 – 23; DOSTÁLEK, Libor. Formáty pro zaručené elektronické podpisy. *Data Security Management*, XVI., 2012, č. 3, str. 42 – 45; Bernášek, Aleš, op. cit.

[40] SMEJKAL, Vladimír, KODL, Jindřich. Development trends of electronic authentication. In: *Proceedings of the 42nd Annual Konference 2008 IEEE International Carnahan Conference on Security Technology*, Diplomat Hotel Prague, Czech Republic, October 13 - 16, 2008, s. 1–6.

[41] Viz Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím "jednotných kontaktních míst" podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu (Úř. věst. L 274, 20. 10. 2009, s. 36).

stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat“ bude zřejmě použitelná i po nabytí účinnosti Nařízení, které nepochybně může být oním „jiným právním předpisem“.

6.2 VLASTNORUČNÍ PODPIS DLE NAŘÍZENÍ

V čl. 25 odst. 2 Nařízení nalezneme konstatování, že „*Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.“* Je to vhodné, správné a přiměřené? Nutno předeslat, že příznivci elektronické komunikace již mnoho let poukazují na to, že „vyšší“ druhy elektronického podpisu podle EPZ (kvalifikovaný a zaručený elektronický podpis) by mohly být považovány za podpis vlastnoruční, neboť vykazují stejnou, spíše pak vyšší míru bezpečnosti, než klasický vlastnoruční podpis.

Ve skutečnosti tomu tak není. Jedním z rozdílů mezi kryptografickým a vlastnoručním podpisem (ať již s nebo bez biometriky) je skutečnost, že soukromý klíč není chráněn proti porušování právních a bezpečnostních opatření jeho vlastníkem. Typickou situací, s níž se autoři běžně setkávají, je použití soukromého klíče určité osoby (manažera, advokáta) jinou osobou (sekretářkou, asistentem), a to s jeho vědomím a na jeho výslovný pokyn. Statická biometrie není sice také zcela chráněna před použitím jinou osobou, ale s „propůjčením identity“ pomocí např. otisku prstu vytvořeného z vhodné umělé hmoty se v běžné praxi nesetkáváme. Ovšem zločinný útok na identitu je u statické biometrie daleko snazší, nežli u biometrie dynamické.

Je vhodné uvést, že formulaci „vlastnoruční podpis“ v českém právním řádu nenajdeme, naproti tomu je zde používán termín „podpis“, čímž se myslí právě podpis vlastnoruční (jak nasvědčuje dikce mnoha předpisů, např. § 33a odst. 4 zákona o účetnictví[42], přičemž se připouští, že tento „může být nahrazen mechanickými prostředky tam, kde je to obvyklé“[43]), případně pak podpis elektronický (obvykle s odkazem na EPZ).

V souvislosti se závěťmi používáme v právní terminologii označení „alografní závěť“ pro závěť, kterou zůstavitel nenapsal vlastní rukou, a „holografní závěť“ pro závěť sepsanou vlastní rukou (nyní viz ust. § 1533

[42] Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
[43] § 561 odst. 1 věta druhá NOZ

– 1534 NOZ).[44] Bude zajímavé pak v návaznosti na zmíněný čl. 25 odst. 2 diskutovat, zda Nařízení může změnit stávající jednoznačný výklad ust. § 1534 předpokládající, že závěť, jež může být napsána na stroji či počítači, musí zůstavitel podepsat vlastní rukou, tj. učinit vlastnoruční podpis, nebo zda to může být kvalifikovaný elektronický podpis.

Vlastnoruční podpis je výsledkem uplatnění návyku psaní, získaného v podobě individuálního a relativně stálého písemného projevu člověka. Vznik individuálnosti písma je důsledkem vytvoření dynamického stereotypu psaní, tedy vypracování složitého systému podmíněných reflexů, které jsou závislé na stupni procvičování. Při vytvoření konkrétního písemného projevu – tedy např. podpisu – se uplatňují ale i aktuální vnější a vnitřní podmínky, za kterých psaní probíhá a v jejichž důsledku může být získaný dynamický stereotyp narušen.[45]

Kvalifikovaný elektronický podpis (dále také jen „KvEP“) je definován v čl. 3 odst. 12 Nařízení jako „*zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy*“. Kvalifikovaným prostředkem pro vytváření elektronických podpisů se rozumí podle odst. 23) prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II Nařízení. Tato příloha je formulována technologicky neutrálně a „nežene“ nás rovnou do hájemství asymetrické kryptografie. Ovšem druhý požadavek, podle kterého „*zaručený elektronický podpis… je založen na kvalifikovaném certifikátu pro elektronické podpisy*“ již vede přes certifikát k asymetrické kryptografii. Znamená tedy dikce čl. 25 odst. 2, že jiný než KvEP nemůže být považován za rovnocenný vlastnoručnímu podpisu?

Podle názoru autorů nelze toto tvrdit. Nařízení pouze činí jednoduchou cestu k uznání kryptografického podpisu na úrovni KvEP jako podpisu vlastnoručního a zavádí pravidlo, že kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech. (čl. 25 odst. 3). Nařízení ale neříká, že za vlastnoruční

[44] Tato terminologie vychází z použití předpon „alo“ pro odlišný či jiný a „holo“ pro celý, úplný, nedotčený.

[45] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 271.

podpis nemůže být v souladu s národním právním řádem považován i jiný druh podpisu, neboť „obyčejný“ elektronický podpis podle čl. 3 odst. 10 nebo zaručený elektronický podpis („ZEP“) podle odst. 11 čl. 3 již může být realizován jinou technologií, pokud splní zde formulované pojmové znaky (a v případě ZEP ještě požadavky stanovené v článku 26 – viz tabulka výše. V takovém případě budeme vycházet z dikce ust. § 561 a § 562 NOZ:

„§ 561 – (1) K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé. Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat. § 562 – (1) Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby.“

Jiným právním předpisem podle § 561 odst. 1 věty třetí je současný zákon o elektronickém podpisu. Pokud by byl nějakým způsobem změněn (v důsledku Nařízení), pak s přihlédnutím k dikci Nařízení v bodu (49) odůvodnění by se za podpis měly považovat všechny formy elektronického podpisu podle Nařízení. A kromě toho čl. 27 odst. 1 Nařízení, podle kterého se výslovně připouští pro využití určité on-line služby, která je poskytována subjektem veřejného sektoru nebo jeho jménem, zaručené elektronické podpisy, zaručené elektronické podpisy založené na kvalifikovaném certifikátu pro elektronické podpisy a kvalifikované elektronické podpisy.

Autoři se obávají, že čl. 25 odst. 2 může být státními orgány, resp. jimi vytvořenou legislativou interpretován úzce a v rozporu s principy tohoto Nařízení tak, že pouze KvEP je tím jediným, který může být považován za podpis vlastnoruční. Konec konců s restriktivním přístupem jsme se setkali již v rámci zákona č. 167/2012 Sb., kterým se změnil zákon č. 499/2004 Sb., o archivnictví a spisové službě, zákon č. 227/2000 Sb., o elektronickém podpisu a další zákony, přičemž provedené změny nebyly vždy zcela vhodné. Novela mj. v EPZ vypustila bez náhrady definici elektronické veřejné listiny a ve všech dosavadních předpisech původně požadovaný „zaručený elektronický podpis založený na kvalifikovaném certifikátu“ byl nahrazen podpisem vyššího stupně, tj. „uznávaným elektronickým podpisem“, ačkoliv k tomu nejsou žádné právní, ani technické důvody.

Takovýto závěr by autoři považovali za zcela nesprávný a navíc nemající oporu v odst. 2, když toto ustanovení výslovně klade rovnítko mezi KvEP a vlastnoruční podpis, žádné jiné formy podpisu nezmiňuje a pokus o uplatnění argumentu a contrario zde autoři nepovažují za možný – ani z jiných ustanovení Nařízení, ani z Nařízení jako celku nelze dovodit, že by jeho cílem bylo jakkoli se vymezit vůči jiným formám elektronického podpisu, v Nařízení výslovně neupraveným, což je nejvýrazněji, ale nikoliv jako jediný právě příklad dynamického biometrického podpisu, a to navzdory poněkud nešťastnému ustanovení čl. 25 odst. 2 Nařízení. Pokud by se v odst. 2 místo o vlastnoručním podpisu hovořilo o úředně ověřeném podpisu, bylo by takové ustanovení plně na místě. Současný zákon o elektronickém podpisu zatím neobsáhl takovou právní úpravu, aby nahradil úředně ověřený podpis, pouze vytvořil alternativu k podpisu vlastnoručnímu, jakkoliv by to drobnou úpravou § 11 EPZ a využitím sítě Czech POINT bylo zřejmě řešitelné.[46]

Je ale především zvláštní, jak po celou dobu oněch 15 let od vydání Směrnice jsou na elektronické podpisy stále znovu a znovu kladeny nepoměrně vyšší požadavky, nežli na podpisy na papíru, ačkoliv podpis na papíru je snadněji padělatelný nežli podpis elektronický. Obecně stále platí již od dob římského práva, že zákonodárce by se měl vyhýbat kazuistickým úpravám a usilovat naopak o co nejobecnější definice. Autoři jsou si vědomi toho, že v praxi je však bohužel situace často opačná – právě kazuistické předpisy čím dál více znejasňují právní řád ČR i EU. Zejména v oblasti vyvíjející se natolik dynamicky, jako je tomu v oblasti informačních technologií (např., ale nikoliv pouze u elektronického podpisu), se k tomu navíc přidává požadavek technické neutrality – je zřejmé, že vývoj se nezastaví u dnes používaných forem elektronického podpisu a lze očekávat, že dříve, či později (dle názoru autorů spíše dříve) budeme řešit výkladové problémy způsobené tím, že reálný vývoj opět předběhl text Nařízení.

Řešením splňujícím požadavek bodu (49) a realizujícím princip technologické neutrality bude rozšíření českého EPZ, resp. pravděpodobného torza, které vzhledem k Nařízení z něj zůstane, o ustanovení, které bude deklarovat, že za vlastnoruční podpis budeme

[46] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 254.

považovat i zaručený elektronický podpis, tedy nikoliv jako doposud absolutizovaný uznávaný EP[47]. Jenže vzhledem k silné lobby poskytovatelů certifikačních služeb na příslušných orgánech, se lze obávat spíše pravého opaku, a to přes existenci rozsudku Nejvyššího správního soudu ze dne 16. 3. 2007, podle kterého „*Zaručený elektronický podpis jako jeden z druhů elektronického podpisu představuje ekvivalent "ověřeného podpisu" na papíru a využívá takových technologických postupů, které umožňují jednoznačnou identifikaci a autentizaci osoby, která podpis vytvořila. Zaručený elektronický podpis zaručuje, že datovou zprávu podepsala oprávněná osoba. Zaručené elektronické podpisy podložené osvědčením vydaným ověřovatelem informací (poskytovatelem certifikačních služeb) budou potom uznány jako vlastnoruční podpis v případech, kdy takový vlastnoruční podpis požadují právní předpisy nebo dohoda stran.*[48]“

Článek 27, který upravuje elektronické podpisy ve veřejných službách, v odst. 3 uvádí, že „*Členské státy nesmějí v případě přeshraničního využívání on-line služby poskytované subjektem veřejného sektoru vyžadovat elektronický podpis s vyšší zárukou bezpečnosti než kvalifikovaný elektronický podpis.*“ Vzhledem k tomu, že komunikace s orgány veřejné moci musí být i přeshraniční, mohlo by tímto dojít k potlačení hypertrofického nasazení uznávaného elektronického podpisu podle § 11 EPZ, ke kterému došlo v rámci velmi svérázné novely EPZ zákonem č. 167/2012 Sb. Ta nahradila ust. § 11 novým zněním a především do dalších předpisů týkajících se soukromoprávních subjektů „natvrdo“ místo zaručeného elektronického podpisu na bázi kvalifikovaného certifikátu navedlo požadavek na používání uznávaných podpisů. Potom vzhledem k rovnému přístupu k osobám v rámci EU by v souladu s odst. 3 nemělo být ani pro tuzemské osoby požadováno použití uznávaných podpisů.

Ostatně, výše zmiňovaný příklad dynamického biometrického podpisu není jistě jediným příkladem podpisu, který vybočuje z poněkud svazujících definic Nařízení. Autoři se ve své praxi setkali s otázkou, jak je tomu například u smluv uzavíraných dnes poměrně běžně u řady finančních institucí, či operátorů elektronických komunikací v rámci telefonického hovoru. Telefonický hovor v současnosti v sítích elektronických komunikací

[47] Viz např. rozhodnutí II. ÚS 218/06-1, II. ÚS 299/06-1, 7 Afs 83/2006-97.
[48] Rozsudek Nejvyššího správního soudu ze dne 16. 3. 2007, spis. zn. 5 Afs 110/2006-113.

(viz ust. § 2 písm. h) a i) zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů v platném znění) bezesporu probíhá „elektronicky“. O tom, že lze tímto způsobem platně uzavřít smlouvu, také nelze mít pochybnosti. Lze však takto uzavřenou smlouvu také elektronicky podepsat?

První otázkou je, zda lze právní jednání učiněné hlasem, bez jeho písemného zachycení, spolehlivě přiřadit konkrétní fyzické osobě. Na tuto otázku odpovídá odvětví tzv. audioexpertizy (fonoskopie, tedy odvětví zabývající se zkoumáním lidského hlasu s cílem ztotožnit neznámého mluvčího s mluvčím, u kterého je jeho identita známa, tedy takového mluvčího verifikovat) a odpovídá na ni kladně – navzdory tomu, že hlas fyzické osoby není s plynutím času a vlivem dalších okolností (vnějších i vnitřních – např. zdravotních) zcela neměnný, lze po provedení analýzy učinit jednoznačný závěr o totožnosti mluvčího.

Pakliže je možno hlasem, a tedy nepísemně, přesto však elektronicky, uzavřít smlouvu, co je u takto uzavřené smlouvy oním podpisem? Přikláníme se k závěru, že takovýmto „podpisem“ je u hlasem uzavírané smlouvy samotný hlasový projev kontrahenta/mluvčího – osvědčuje jeho souhlas s textem uzavírané smlouvy a přitom – podobně jako vlastnoruční podpis, resp. mnohdy patrně i jednoznačněji – splňuje kritérium jednoznačnosti. V režimu podle NOZ se jedná o právní jednání ve smyslu ust. § 545 an. NOZ, a to jako jednání realizované konáním ve smyslu § 546 jako jednání spíše výslovné (hlasem), nežli konkludentní (chováním).

Lze zde však hovořit o podpisu elektronickém jen proto, že je hlasový projev učiněn s využitím elektronických prostředků (a případně jeho nahrávka zaznamenána na elektronické médium)? Samotná skutečnost, že smlouva byla hlasově uzavřena za použití sítě elektronických komunikací, je pro učinění závěru ohledně jejího elektronického podpisu irelevantní. Rozhodující je, zda by „hlasový podpis“ bylo možno zahrnout do definice elektronického podpisu, ať již při použití definice v ZEP, či při použití definice dle Nařízení. Hlas je sice logicky spojen s datovou zprávou – hlasovou nahrávkou, která je oním hlasem činěna, navíc – ve světle výše uvedeného ohledně jednoznačnosti závěru analýzy hlasu - slouží jako metoda k ověření identity podepsané osoby, tím spíše svůj hlas podepisující osoba používá k podepsání (a dokonce lze říci, že hlas/hlasový podpis: 1. je

jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě a 3. nepochybně byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou), lze však učinit paralelu mezi hlasem coby „údajem v elektronické podobě"? Tuto úvahu ponechávají autoři k diskusi.

7. OVĚŘOVÁNÍ PLATNOSTI KVALIFIKOVANÝCH ELEKTRONICKÝCH PODPISŮ A DALŠÍ SLUŽBY

Podle čl. 32 Nařízení se potvrdí platnost kvalifikovaného elektronického podpisu, pokud:

a) certifikát, na němž je podpis založen, byl v okamžiku podpisu kvalifikovaným certifikátem pro elektronický podpis, jenž je v souladu s přílohou I;
b) kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a v okamžiku podpisu byl platný;
c) data pro ověřování platnosti podpisu odpovídají datům poskytnutým spoléhající se straně;
d) spoléhající se straně je řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu;
e) pokud byl v okamžiku podpisu použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;
f) elektronický podpis byl vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů;
g) nebyla ohrožena integrita podepsaných dat;
h) v okamžiku podpisu byly splněny požadavky stanovené v článku 26, který obsahuje požadavky na zaručené elektronické podpisy.

Zajímavá je dikce písm. b), podle níž je možné ověřovat KvEP i po vypršení platnosti certifikátů; podstatné je, že certifikát byl platný v okamžiku podpisu. Naproti tomu český zákon o archivnictví výslovně požaduje přidání časového razítka, aby mohl být podepsaný dokument považován za pravý – viz § 69a odst. 5 zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů (dále také jen

ArchZ) a podobně tomu je i při provádění konverze podle § 24 odst. 1 písm. b) zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále také jen ElÚkZ). I v tomto směru tedy autoři hodnotí Nařízení pozitivně; otázkou ovšem je, jak budeme moci určit bez časového razítka, kdy byl podpis učiněn. Podle názoru autorů časové období, v němž byl podpis vytvořen, by bylo možné vysledovat z metod a procesů, kterými byl podpis vytvořen, tedy podle metody RSA (konkrétně podle použité délky klíčů), podle typu hash funkce (dříve SHA-1, nyní SHA-256) apod. Jedná se však o údaje, u nichž je nutno počítat s tolerancí cca 5 let; přesný časový okamžik, kdy byl podpis ve skutečnosti vytvořen, bez vazby na důvěryhodný časový údaj nezjistíme.

Následující články Nařízení kodifikují „přídavné“ služby týkající se elektronických podpisů. Čl. 33 zavádí „kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů“, kterou může poskytovat kvalifikovaný poskytovatel služeb vytvářejících důvěru. Čl. 34 pak definuje „kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů“. V tomto případě, stejně jako u podpisů, certifikátů, pečetí, časových razítek atd. může Komise prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů. Nechme se tedy překvapit, jaké metody budou doporučeny.

8. ODPOVĚDNOST ZA ŠKODU

Jedním z cílů Nařízení je podle bodu 18. Preambule „*stanovit odpovědnost oznamujícího členského státu, strany vydávající prostředky pro elektronickou identifikaci a strany provozující postup autentizace za nedodržení příslušných povinností z tohoto nařízení vyplývajících*“. Tato odpovědnost za škodu je definována v čl. 11 Nařízení a týká se přeshraničních transakcí.

Dalším cílem je podle bodu 35 definování odpovědnosti poskytovatelů služeb vytvářejících důvěru. Nařízení v čl. 13 zavádí režim odpovědnosti, podle kterého by všichni poskytovatelé služeb vytvářejících důvěru měli odpovídat za škodu, kterou fyzické nebo právnické osobě způsobí v důsledku nesplnění povinností podle tohoto nařízení. Posoudit finanční riziko, které poskytovatelé služeb vytvářejících důvěru mohou být nuceni nést nebo které by mělo být kryto jejich pojistnou smlouvou, není snadné.

Za účelem snížení tohoto rizika (příp. jeho snadnějšího posouzení) Nařízení poskytovatelům služeb vytvářejících důvěru umožňuje stanovit za určitých podmínek omezení týkající se využívání jimi poskytovaných služeb a zprostit se tak odpovědnosti za škody vyplývající z využívání služeb nad rámec těchto omezení. Zákazníci by měli být o těchto omezeních předem řádně informováni a tato omezení by měla být rozpoznatelná pro třetí osoby, například tím, že informace o těchto omezeních budou zahrnuty v podmínkách poskytované služby, nebo jinými rozpoznatelnými prostředky. Za účelem účinného uplatňování těchto zásad by se toto nařízení mělo použít v souladu s vnitrostátními pravidly odpovědnosti. Tato vnitrostátní pravidla týkající se například vymezení škody, úmyslu nebo nedbalosti nebo související platná procesní pravidla proto tímto nařízením nejsou dotčena.

Povinnost nahradit škodu je dnes vymezena v ust. § 2909 až § 2913 NOZ, a to na základě: 1. porušení dobrých mravů (§ 2909), 2. porušení zákona (§ 2910) nebo 3. porušení smluvní povinnosti (§ 2913). Podle § 2910 *„Škůdce, který vlastním zaviněním poruší povinnost stanovenou zákonem a zasáhne tak do absolutního práva poškozeného, nahradí poškozenému, co tím způsobil. Povinnost k náhradě vznikne i škůdci, který zasáhne do jiného práva poškozeného zaviněným porušením zákonné povinnosti stanovené na ochranu takového práva.*“ První věta chrání osobnostní práva, věcná práva a práva k nehmotným statkům. V případě věty druhé se musí jednat o porušení speciální prevenční normy, kterou v daném případě je Nařízení, které je přímo použitelnou právní normou EU a kde se v čl. 13 odst. 1 konstatuje, že „*poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení*“. Pokud se zde konstatuje, že „V *případě kvalifikovaného poskytovatele služeb vytvářejících důvěru se úmysl nebo nedbalost předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že škoda podle prvního pododstavce nastala bez jeho úmyslu nebo nedbalosti.*“, pak podle názoru autorů je zřejmě v rozporu s českým právem, aby se prokazování či neprokazování zavinění vztahovalo pouze na určitou skupinu poskytovatelů služeb. Podle NOZ osoba způsobí škodu zaviněně, pokud ji spáchala úmyslně nebo z nedbalosti, přičemž podle § 2911 se předpokládá, že k porušení povinnosti ze zákona došlo

z nedbalosti. Škůdce je tedy za škodu odpovědný zpravidla pouze v případě, že ji skutečně zavinil, bez ohledu na to, jak je označen či jakému dohledu podléhá. Nicméně toto by měl řešit odst. 3 čl. 13, podle kterého platí, že „*odstavce 1 a 2 se použijí v souladu s vnitrostátními pravidly upravujícími odpovědnost za škodu*“. Je otázkou, zda bude ust. čl. 13 odst. 1 Nařízení vnímáno v ČR jako lex specialis k NOZ, či nikoliv.

Co se týká odst. 2 čl. 13, podle kterého „*Pokud poskytovatelé služeb vytvářejících důvěru své zákazníky předem řádně informují o omezeních týkajících se využívání jimi poskytovaných služeb a tato omezení jsou rozpoznatelná pro třetí osoby, neodpovídají poskytovatelé služeb vytvářejících důvěru za škody způsobené využíváním služeb nad rámec uvedených omezení.*“, pak v současnosti lze tato omezení definovat funkčně (postupy poskytovatelů nebo vlastnosti služeb či produktů); omezení ve formě limitace náhrady škody případně vzniklé využíváním služeb vytvářejících důvěru patrně čl. 13 odst. 2 neměl na mysli, když z jeho textu vyplývá, že má jít o „omezení týkající se využívání poskytovaných služeb“. Nehledě na toto ustanovení je však obecně v českém právním řádu možné i limitovat výši náhrady škody, a to dle NOZ, což by bylo možno uplatnit i na služby vytvářející důvěru – v daném případě by se ovšem s ohledem na dikci § 2898 NOZ takováto limitace vztahovala pouze na případy „běžné nedbalosti“, neboť dle téhož ustanovení NOZ „*Nepřihlíží se k ujednání, které předem vylučuje nebo omezuje povinnost k náhradě újmy způsobené člověku na jeho přirozených právech, anebo způsobené úmyslně nebo z hrubé nedbalosti; nepřihlíží se ani k ujednání, které předem vylučuje nebo omezuje právo slabší strany na náhradu jakékoli újmy. V těchto případech se práva na náhradu nelze ani platně vzdát.*“

9. SLUŽBA ELEKTRONICKÉHO DOPORUČENÉHO DORUČOVÁNÍ

Bod (66) odůvodnění Nařízení konstatuje, že „*Je nezbytné stanovit právní rámec, který usnadní přeshraniční uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy. Tento rámec by mohl rovněž přinést nové tržní příležitosti pro poskytovatele služeb vytvářejících důvěru z Unie, kteří budou moci nabízet nové panevropské služby elektronického doporučeného doručování.*“. Autorům není zcela zřejmý důvod, pro který byl použit termín „doporučené doručování“ místo např. vhodnějšího

„důvěryhodné doručování“. Podstatnější problém ale zjistíme později při čtení dalších ustanovení.

Koncepce tohoto doručování není příliš specifikována. Čl. 43 odst. 1 Nařízení vychází z již tradiční proklamace o tom, že „*Datům odeslaným a přijatým prostřednictvím služby elektronického doporučeného doručování nesmějí být upírány právní účinky a nesmějí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nesplňují požadavky na kvalifikovanou službu elektronického doporučeného doručování.*“.

Teprve odst. 2 nám prozradí, oč by se asi mělo jednat. Podle něj „U *dat odeslaných a přijatých prostřednictvím kvalifikované služby elektronického doporučeného doručování platí domněnka integrity dat, odeslání těchto dat identifikovaným odesílatelem, jejich přijetí identifikovaným příjemcem a správnosti data a času odeslání a přijetí, jež jsou u kvalifikované služby elektronického doporučeného doručování uvedeny.*“. Všechny tyto požadavky splňují datové schránky podle ElÚkZ. Až bychom se mohli domnívat, že se tvůrci Nařízení inspirovali právě jimi.

Požadavky na kvalifikované služby elektronického doporučeného doručování dle čl. 44 jsou ale zbytečně kazuistickým popisem, který vyžaduje striktní řešení tam, kde lze postupovat i prostřednictvím jiných mechanismů. Zatímco požadavky odst. 1 písm. a), b), c)e a f) lze považovat za standardní, nejproblematičtější je dikce písm. d), podle kterého „*odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat“*.

Existuje řada jiných možností, jak zajistit, „*aby byla vyloučena možnost nezjistitelné změny dat“,* zejména s využitím kryptografických nástrojů, které nicméně nebudou ani zaručeným elektronickým podpisem, ani zaručenou elektronickou pečetí. Nebo opačně: pokud autoři Nařízení chtěli, aby byly zprávy elektronicky podepsány či orazítkovány, měli to napsat rovnou a jednoznačně.

Protože nevíme, jakými postupy jsou požadavky čl. 44 realizovány v informačním systému datových schránek (viz ust. § 14 ElÚkZ), bude na správci IS DS, kterým je Ministerstvo vnitra, aby tyto aspekty prozkoumal

a zaujal k nim stanovisko. V tomto případě se jeví jako obzvlášť důležité a současně náročné, zajistit interoperabilitu mezi různými systémy elektronického doporučeného doručování. Je otázkou, zda a jak to bude dosažitelné, resp. zda se kvůli požadované interoperabilitě nevrátíme od datových schránek zpět do minulosti. Pokud bychom brali v potaz splnění všech požadavků čl. 44 odst. 1, pak totiž asi nebudeme potřebovat IS DS, ale spíše jen nějaké prostředí pro užívání EP/EZ/ČR.

10. ZÁVĚR

V Nařízení se tvrdí, že „*Budování důvěryhodnosti on-line prostředí má pro hospodářský a sociální rozvoj klíčový význam. Nedostatečná důvěra, zejména v důsledku pocitu nedostatku právní jistoty, vede k tomu, že se spotřebitelé, podniky a orgány veřejné moci zdráhají provádět transakce elektronickými prostředky a přijímat nové služby.*“ Po seznámení s jeho obsahem, přinejmenším v oblasti elektronického podpisu, můžeme sice mít pocit, že by mohlo vést ke zvýšení právní jistoty, a to i přesto, že jeho text je těžkopádný a legislativně poněkud nešťastný. Je třeba ocenit, že byl po 15 letech vydán nový dokument, nicméně další rozvoj vědy a techniky v oblasti elektronické identifikace a autentizace se do něj promítl v tak malé míře, že je třeba si položit otázku, zda rozsah a především praktický přínos změn je skutečně adekvátní dlouhotrvajícímu legislativnímu procesu příprav na text zcela nového nařízení. Je zřejmé, že terminologie je v mnohém poplatná normám ETSI bez snahy o větší obecnost a univerzálnost. Hlavní problém vidíme v jejím rigidním lpění na asymetrické kryptografii a zejména certifikátech, jako údajně jediné možné variantě pro bezpečný elektronický podpis, resp. jakoukoliv autentizaci s vyšší úrovní zaručenosti.

To se týká jak elektronického podpisu, resp. povýšení KvEP na podpis vlastnoruční (čl. 25 odst. 2 Nařízení), jakož i některých požadavků na systémy elektronického doporučeného doručování (čl. 44 odst. 1 písm. d). Naštěstí vzhledem k výše zmíněné „dualitě“ dynamického biometrického podpisu lze očekávat přinejmenším diskusi v souvislosti s ním a vlastnoručním podpisem.

Z našeho pohledu není dynamický biometrický podpis náhradou kryptografického elektronického podpisu, ale významnou alternativou,

kterou lze použít v případech, kdy implementování certifikátů, bezpečné ukládání a „hlídání" privátních klíčů apod., by významným způsobem narušilo rutinní a ustálené procesy, případně působilo jako bariéra odrazující běžné uživatele (smluvní strany).[49] Zasloužil by si proto větší podporu zejména v tomto Nařízení.

Zásadní novou kvalitu Nařízení prakticky nepřináší, byť v detailech je lze považovat za lepší variantu oproti směrnici 1999/93/ES. Určitě pak ne v České republice, která některé velice pokročilé nástroje eGovernmentu, jako jsou např. elektronická značka, časové razítko a především systém důvěryhodného doručování pomocí datových schránek zakotvila ve své legislativě a prakticky jej realizovala již před několika lety. Mohlo by mít význam spíše z hlediska interoperability, ale to uvidíme až podle toho, jak budou nastaveny technické parametry a jak se s Nařízením vypořádají členské země. Jak si autoři pamatují z projednávání implementace Směrnice o elektronických podpisech v roce 2003[50], ani po pěti letech od jejího vydání se to členským zemím nepodařilo a v některých se tak nestalo doposud. Proto neočekáváme, že by došlo k zásadnímu zlomu brzy po nabytí účinnosti Nařízení.

Tento příspěvek se pokusil vyložit jednotlivá ustanovení Nařízení eIDAS týkající se elektronického podpisu a témat souvisejících alespoň tak, aby Nařízení neškodilo stávajícím dobrým a zavedeným institutům a bylo aplikovatelné nejen v České republice. Nejsme si bohužel jisti, že to vždy bude možné (viz výše k čl. 25 odst. 2 a k čl. 44). Jsme však přesvědčeni, že by si jej přečíst všichni, kdo přicházejí do kontaktu s elektronickými podpisy, aby nepodlehli různým účelovým, ba mnohdy dokonce přímo „katastrofickým výkladům" o dopadech vyvolaných Nařízením, jež se nyní objevují a s nimiž se autoři setkávají nezřídka i v odborných příspěvcích a diskusích na Internetu.

Toto dílo podléhá licenci Creative Commons Uveďte původ-Zachovejte licenci 4.0 Mezinárodní. Pro zobrazení licenčních podmínek navštivte http://creativecommons.org/licenses/by-sa/4.0/.

[49] SMEJKAL, Vladimír, KODL, Jindřich. Vícefaktorová autentizace a dynamický biometrický podpis. In: *Sborník 16. ročníku mezinárodní konference Information Security Summit (IS2)*, 27. – 28. května 2015, Praha: TATE International, s.r.o., s. 107 – 119.

[50] DUMORTIER, Jos a kol., op. cit.

INSTRUCTIONS FOR AUTHORS

The Review of Law and Technology is a peer-reviewed scientific journal. Only the contributions submitted for the Topic and Discussion sections are peer-reviewed. Manuscripts are reviewed anonymously by two independent reviewers and the final decision on publication is the in the sole discretion of the editorial board.

More information available from the editors upon request at the e-mail address revue@law.muni.cz. Contributions to the Review of Law and Technology should be sent to revue@law.muni.cz in common text formats (.doc, .docx, .rtf, .odt). Please consult using different formats with the editors at the above mentioned e-mail address.

The contribution should use a maximum of two levels of headings.

RECOMMENDED EXTENT OF THE CONTRIBUTIONS:

Topic section:	54 000 – 144 000 characters
Discussion section:	9 000 – 36 000 characters
Case annotation:	3 600 – 18 000 characters
Book review:	1 800 – 9 000 characters

For further information about structure and formalities of the contributions please consult the „Instructions for Authors“ section at www.revue.law.muni.cz.

CITATIONS FORMAT

Citations are governed primarily by the directive of the Dean of the Faculty of Law, Masaryk University No. 4/2013 (available from http://is.muni.cz/do/law/ud/predp/smer/S-04-2013_O_citacich_dokumentu.pdf), then by the ISO 690 standard, 3rd edition published in March 2011. Individual sources are referenced in the text by index. The actual citation of the source is then contained in a footnote.

CITATION STRUCTURE

PRIMARY COPYRIGHT DATA. *Title: subtitle of the information source*. Secondary copyright data. Issue. Place of publication: Publisher, year. Physical description.

For further information about citations and examples of citations please consult the „Instructions for Authors“ section at https://journals.muni.cz/revue/about/submissions.

DEADLINES FOR CONTRIBUTIONS SUBMISSIONS

For the summer issue: 31th of March

For the winter issue: 30th of September

By submitting a contribution the author consents to the use of his or her contribution in the electronic databases of the companies Wolters Kluwer, a.s., C.H. BECK Publishing, s. r. o. and ATLAS Consulting spol. s. r. o., and consequently in the legal information systems ASPI, Beck-online and Codexis, operated by these companies.

The journal is also freely available at https://journals.muni.cz/revue and http://revue.law.muni.cz under Creative Commons BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0/legalcode).

REVIEW OF LAW AND TECHNOLOGY

VOLUME 6 | YEAR 2015 | NUMBER 11

DISCUSSION

REVIEWS

ANNOTATIONS

TOPICS

Review of Law and Technology
reviewed scientific journal for technological fields of law and jurisprudence, listed in the List of non-impact peer-reviewed journals published in the Czech Republic and ERIH PLUS database.
Only the contributions submitted for the Discussion and Topic sections are peer-reviewed.
Published bi-annually. This issue was published on 30. 6. 2015.
ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. č. MK ČR E 19707.
Published by: Masaryk university, Žerotínovo nám. 9, 601 77 Brno, Czech republic, IČ 00216224.
Editor-in-chief: doc. JUDr. Radim Polčák, Ph.D.
Deputy editor-in-chief and contact person: JUDr. Matěj Myška, Ph.D., Institute of Law and Technology, Faculty of Law MU, Veveří 70, 611 80 Brno, ČR, tel: +420 549 494 751, fax: +420 541 210 604, e-mail: revue@law.muni.cz | https://journals.muni.cz/revue , www.revue.law.muni.cz.
Editorial Staff: Mgr. Michal Koščík, Ph.D., Mgr. Václav Stupka, JUDr. Bc. Jaromír Šavelka, Mgr. Jakub Harašta.
Editorial Secretary: Martin Loučka.
Editorial Board: JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., Mgr. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., Mgr. Antonín Panák, LL.M., doc. JUDr. Radim Polčák, Ph.D., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Layout: Martin Loučka, JUDr. Matěj Myška, Ph.D.
Print: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno.
The publication of this issue of the Review of Law and Technology was funded by the project „Právo a technologie III“, MUNI/A/1320/2014.
© 2015 Masarykova univerzita.

Diskuze

Recenze

Anotace

Téma

muni PRESS

9 771804 538006 51