20

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 10 / Rok 2019 / Číslo 20

Revue.law.muni.cz

MUNI
LAW

LL.M. v právu informačních a komunikačních technologií

Moderní odborné vzdělávání, atraktivní zaměření

Mezinárodně uznávaný program LL.M. v právu informačních a komunikačních technologií je úzce zaměřené dvouleté postgraduální studium určené pro zájemce o právní aspekty informačních a komunikačních technologií. Cílovou skupinou programu jsou praktikující právníci všech právních profesí se zájmem o informační a komunikační technologie. Díky volitelnému propedeutickému modulu je program určen též zájemcům bez právnického vzdělání - IT specialistům, manažerům v oboru ICT, bezpečnostním expertům, vedoucím pracovníkům veřejné správy aj.

Elitní pracoviště a odborníci s mezinárodním renomé – předpoklad kvalitního vzdělávání

Program LL.M. je odborně zajišťován a garantován **Právnickou fakultou Masarykovy univerzity** a za jeho realizaci odpovídá **Ústav práva a technologií**. Tento ústav byl na Právnické fakultě zřízen v roce 2010 jako první odborné pracoviště v České republice zaměřené na výzkum a výuku v oblastech právní úpravy pokročilých technologií. Během své existence si ústav vybudoval v oboru práva informačních a komunikačních technologií mezinárodní renomé a stal celoevropsky uznávanou institucí. Vedle vědecké a pedagogické činnosti ústav úzce spolupracuje s českými a evropskými justičními orgány, bezpečnostními sbory, státními orgány, špičkovými advokátními kancelářemi a poradenskými společnostmi.

Povinné moduly

Akademické psaní a právní kontext
Normativní systémy v kyberprostoru
Soukromé právo ICT
Veřejné právo ICT
Ochrana soukromí a osobních údajů
Duševní vlastnictví on-line
Elektronické důkazy
Softwarové právo
Kyberkriminalita
Právo e-commerce
Informační technologie v právní praxi

Volitelné moduly

Kryptografie a bezpečnostní technika
Právo kybernetické bezpečnosti
On-line řešení sporů
eGovernment a eJustice
Evropské a mezinárodní právní informační systémy

Další informace

Podrobné informace o programu naleznete na **www.llm.law.muni.cz**, případně je poskytne

Mgr. Lenka Sochorová
(Lenka.Sochorova@law.muni.cz)

Obsah a zaměření programu – moderní informační a komunikační technologie a jejich právní aspekty, úzká specializace

Právo informačních a komunikačních technologií se dotýká řady oblastí soukromého a veřejného práva. Neopomenutelný je též jeho evropský a mezinárodní rozměr. Moduly studijního programu jsou zaměřeny tak, aby reflektovaly aktuální praktické problémy právní regulace vývoje a použití pokročilých informačních a komunikačních technologií. Cílem programu je předat maximum znalostí a praktických dovedností z tohoto vysoce specializovaného oboru.

Personální zabezpečení

Odborným garantem programu je **Radim Polčák**, vedoucí Ústavu práva a technologií. Výuku v programu zajišťují členové Ústavu práva a technologií a zástupci dalších odborných pracovišť Právnické fakulty a Fakulty informatiky Masarykovy univerzity. Na výuce se ve značné míře podílejí též špičkoví odborníci z právní praxe. Mezi lektory programu jsou: **Josef Donát** (ROWAN LEGAL), **Jaroslav Fenyk** (PrF MU), **Tomáš Gřivna** (PrF UK), **Jan Hajný** (VUT), **Jakub Harašta** (PrF MU) **František Korbel** (Havel & Holásek), **Josef Kotásek** (PrF MU), **Zdeněk Kučera** (Baker & McKenzie), **Matěj Myška** (PrF MU) a další.

Cena

Cena za semestr je stanovena následovně:

- pro absolventy právnických fakult: 37 500 Kč (bez DPH)
- pro ostatní zájemce: 40 500 Kč (bez DPH) – cena zahrnuje odborný kurs propedeutického základu pro neprávníky

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 10 | ROK 2019 | ČÍSLO 20

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 31. 12. 2019.
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 a kontaktní osoba: JUDr. Matěj Myška, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, Veveří 70, 611 80 Brno, ČR, tel: +420 549 494 751, fax: +420 541 210 604, e-mail: revue@law.muni.cz | www.revue.law.muni.cz
Zástupce šéfredaktora: Ing. Mgr. František Kasl
Redakce: JUDr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek
Tajemnice redakce: Anna Blechová
Editorka: Anna Blechová
Redakční rada: doc. JUDr. Radim Polčák, Ph.D. (čestný předseda), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, doc. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Grafická úprava: Mgr. Martin Loučka, JUDr. Matěj Myška, Ph.D.
Tisk: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
Vydání tohoto čísla časopisu Revue pro právo a technologie bylo financováno z projektu „Právo a technologie VII“, MUNI/A/1006/2018.

POKYNY PRO AUTORY

Revue pro právo a technologie je specializovaným odborným recenzovaným časopisem, který je zaměřen na technologické obory práva a právní vědy.

Časopis je zařazen od 1. 1. 2015 na Seznam recenzovaných neimpaktovaných periodik vydávaných v ČR a od 24. 6. 2015 do databáze ERIH PLUS.

Příspěvky zaslané do sekcí Téma a Diskuze jsou anonymně posuzovány minimálně dvěma nezávislými recenzenty a konečné rozhodnutí o publikaci příspěvků zaslaných do všech sekcí je v kompetenci redakční rady. Orientační doba recenze je jeden měsíc. Články neprochází jazykovou korekturou.

Příspěvky se podávají prostřednictvím redakčního systému dostupného na adrese www.revue.law.muni.cz.

DOPORUČENÝ ROZSAH PŘÍSPĚVKŮ:

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

(včetně mezer, poznámek pod čarou a seznamu použitých zdrojů)

CITAČNÍ STANDARD

Použité prameny je nutné citovat v souladu s citační směrnicí ČSN ISO 690:2011.

Způsob citování a praktické příklady jsou dostupné v interpretacích normy ISO 690:2011, které jsou dostupné např. na www.ezdroje.muni.cz/prehled/zdroj.php?lang=cs&id=441

Na jednotlivé prameny se odkazuje v textu číslem poznámky psané horním indexem (metoda průběžných poznámek).

TERMÍNY PRO DODÁNÍ PŘÍSPĚVKŮ

Do letního čísla: 31. března

Do zimního čísla: 30. září

Časopis se hlásí k politice otevřeného přístupu realizovaného zlatou cestou.

Příspěvky jsou přebírány do příslušných elektronických právních informačních systémů společností Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) a ATLAS consulting spol. s r. o. (CODEXIS).

Detailní informace ohledně publikačního procesu, struktury a formálních náležitostí příspěvků, recenzního řízení a autorských práv jsou dostupné v sekci „Pro autory“ na webu časopisu www.revue.law.muni.cz resp. Vám je na vyžádání ráda sdělí redakce (kontaktní e-mail: revue@law.muni.cz).

https://doi.org/10.5817/RPT2019-2-1

BEZPEČNOSŤ INFORMAČNÝCH SYSTÉMOV VEREJNEJ SPRÁVY VO SVETLE ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI A ZÁKONA O INFORMAČNÝCH TECHNOLÓGIÁCH VO VEREJNEJ SPRÁVE[1]

JOZEF ANDRAŠKO[2]

ABSTRAKT

Autor sa v predkladanom príspevku venuje otázke bezpečnosti informačných systémov verejnej správy v zmysle novej legislatívy, ktorá významným spôsobom pozmenila právnu úpravu bezpečnosti informačných systémov verejnej správy. Autor sa v prvom rade zameral na novoprijatý zákon o informačných technológiách verejnej správy, ktorý upravuje problematiku bezpečnosti informačných technológií verejnej správy. Autor príspevku v druhom rade upriamuje pozornosť na bezpečnosť informačných systémov verejnej správy v zmysle zákona o kybernetickej bezpečnosti, podľa ktorého sú informačné systémy verejnej správy zaradené medzi základné služby. V závere autor upriami pozornosť na prepojenie a rozdiely v otázkach bezpečnosti informačných systémov verejnej správy v zmysle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe. Autor skúma danú problematiku z pohľadu právneho poriadku Slovenskej republiky.

[1] Tento príspevok vznikol v rámci projektu APVV-17-0403 Vplyv vzájomného uznávania prostriedkov elektronickej identifikácie na elektronické služby verejnej správy.

[2] JUDr. Jozef Andraško, PhD., odborný asistent, Ústav práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave, Právnická fakulta, e-mail: jozef.andrasko@flaw.uniba.sk.

KLÍČOVÁ SLOVA

informačné systémy verejnej správy, informačné technológie, kybernetická bezpečnosť

ABSTRACT

The author deals with the issue of security of public administration information systems in accordance with the new legislation which significantly changed the legal regulation of security of public administration information systems. The author focuses primarily on the newly adopted Information Technologies of Public Administration Act which regulates the issue of security of information technologies of public administration. Secondly, the author focuses on the security of public administration information systems pursuant to the Cyber Security Act in which public administration information systems are considered as the essential services. In conclusion, the author will draw attention to the interconnection and differences in security issues of public administration information systems pursuant to the Cyber Security Act and the Information Technologies in Public Administration Act. The author deals with the issue in question from the perspective of the legal order of the Slovak Republic.

KEYWORDS

public administration information systems, information technologies, cyber security

1. ÚVOD

Bezpečnosť informačných systémov verejnej správy (ďalej len „ISVS“) zohráva významnú úlohu, a to hneď z niekoľkých dôvodov. Aby verejná správa mohla prostredníctvom svojich orgánov plniť svoje úlohy, musí sa spoliehať na svoje ISVS, resp. na informácie a údaje, ktoré sú v nich spracovávané. Bez dostatočnej úrovne bezpečnosti ISVS by nemohli orgány

verejnej správy vydávať individuálne správne akty alebo iné finálne formy činnosti verejnej správy.[3]

V kontexte bezpečnosti, resp. informačnej a kybernetickej bezpečnosti je potrebné nahliadať na informačné systémy verenej správy a na informácie, ktoré sa v nich spracúvajú ako na aktíva, ktoré je potrebné chrániť. Aby došlo k zabezpečeniu dostatočnej úrovne ochrany ISVS pred rôznymi hrozbami, je potrebné, aby konkrétne subjekty realizovali bezpečnostné opatrenia, ktoré môžu znižovať dopady bezpečnostných incidentov na tieto systémy. Roztrieštenosť právnej úpravy týkajúcej sa povinnosti realizovať bezpečnostné opatrenia môže spôsobiť, že subjekty v rôznych právnych postaveniach nebudú realizovať bezpečnostné opatrenia v dostatočnej miere resp. ich nebudú realizovať vôbec. V súvislosti s bezpečnostnými incidentmi je taktiež dôležité, aby príslušné právne predpisy jasne a zrozumiteľne upravovali, ktorý subjekt je povinný hlásiť bezpečnostné incidenty, ktorému subjektu sa takéto bezpečnostné incidenty nahlasujú a v akej lehote.

V tomto príspevku sa zameriavam na problematiku bezpečnosti ISVS, a to z pohľadu právneho poriadku Slovenskej republiky. V prvom rade považujem za potrebné ozrejmiť pojmy ako bezpečnosť, informačná bezpečnosť a kybernetická bezpečnosť, a to najmä z teoretického hľadiska. Následne sa budem venovať problematike bezpečnosti ISVS, a to z pohľadu novej právnej úpravy, ktorá sa týka informačných technológií verejnej

[3] V súčasnosti zohrávajú ISVS významnú úlohu aj v kontexte cezhraničnej autentifikácie osôb. Konkrétnym príkladom je ISVS, modul IAM (Identity Access Management), taktiež známy ako autentifikačný modul, ktorý plní dôležitú úlohu pri cezhraničnej autentifikácii osôb (občanov iných členských štátov Európskej únie). Pri prvom prihlásení osoby z iného členského štátu Európskej únie do online služby poskytovanou subjektom verejného sektora Slovenskej republiky sa zapíšu z eIDAS uzla do modulu IAM údaje o danej osobe a zároveň sa mu vytvorí elektronická schránka v zmysle zákona č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente). Bez toho aby sa orgány verejnej správy nemohli spoliehať na pravosť, dôveryhodnosť a dostupnosť informácií a údajov spracovávaných v ISVS, nemohli by vykonávať svoje úlohy, čo by znemožnilo riadny chod verejnej správy. Bližšie k problematike cezhraničnej autentifikácie pozri: ANDRAŠKO, J. a MESARČÍK, M. *Problematika GDPR v kontexte nariadenia eIDAS.* In Digitalizácia, zmeny vonkajšieho prostredia a spoločnosť budúcnosti. Bratislava, Univerzita Komenského v Bratislave, Právnická fakulta, s. 8- 22.

správy, ako aj z pohľadu právnej úpravy, ktorá sa týka kybernetickej bezpečnosti vo všeobecnosti. Prepojenosť týchto právnych úprav je najviac evidentná, najmä čo sa týka bezpečnosti ISVS. V ďalšej časti príspevku upriamim pozornosť na povinnosť konkrétnych subjektov v rôznych právnych postaveniach hlásiť bezpečnostné incidenty. V tejto súvislosti budem skúmať, aké bezpečnostné incidenty je potrebné hlásiť, ktoré subjekty, v akých právnych postaveniach sú povinné hlásiť bezpečnostné incidenty, v akých lehotách a voči ktorým subjektom si musia túto povinnosť plniť. V závere poukážem na najproblematickejšie časti skúmanej problematiky a dovolím si navrhnúť aj konkrétne riešenia.

2. BEZPEČNOSŤ

Vo všeobecnosti možno povedať, že bezpečnosť je založená na ochrane aktív pred rôznymi hrozbami pri určitej zraniteľnosti.[4] Za aktíva možno považovať všetko, čo má pre danú organizáciu[5] hodnotu. Môže ísť o hmotné aktíva (zariadenie, personál a pod.) alebo o nehmotné aktíva (napr. informácie, údaje, služby, dobré meno, know-how a pod.). Akákoľvek udalosť, skutočnosť, osoba, sila, ktorá môže spôsobiť, že sa aktíva organizácie dostanú do neželaného stavu (napr. nebudú fungovať počítače, zamestnanec ochorie a pod.), sa nazýva hrozba. Najčastejšími hrozbami, ktoré možno aplikovať na aktíva sú prírodné vplyvy (napr. zemetrasenie, búrka a pod.), technické poruchy (napr. výpadok siete, výpadok podpornej infraštruktúry a pod.), chyby v programovom vybavení, neúmyselné ľudské chyby, cieľavedomá ľudská činnosť (sabotáž, prieniky hackerov do systému) a pod.[6]

---

[4] VON SOLMS, R., VAN NIEKERK, J. *From information security to cyber security. In* Computers & Security, 2013, roč. 38, s. 100.

[5] V terminológii informačnej bezpečnosti je pojem organizácia definovaná ako skupina ľudí a zariadenie, so zodpovednosťou, právomocami a vzájomnými vzťahmi. Bližšie pozri bod 2.56 štandardu ISO/IEC 27000:2016 *Overview and vocabulary*. Pre účely tohto príspevku možno za organizáciu v zmysle informačnej bezpečnosti považovať verejnú správu ako takú, spravujúce subjekty verejnej správy, a teda aj orgány verejnej správy.

[6] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, s. 7. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

Je potrebné podotknúť, že hrozba sa môže, ale nemusí uplatniť. Aby sa hrozba vôbec naplnila, musí aktívum spĺňať nejaké predpoklady, ktoré nazývame zraniteľnosť. Každé aktívum je zraniteľné, nakoľko jeho hodnotu ohrozujú rôzne vplyvy. Pod zraniteľnosťou možno chápať chybu, nedostatok v podobe nedostatočne vyškoleného zamestnanca, ktorý sa svojou neodbornosťou a neskúsenosťou môže dopúšťať chýb. Takýto nedostatok môže byť zneužitý hrozbou v takom rozsahu, že hodnota aktíva môže byť poškodená alebo dokonca zničená.[7]

Aktívum môže byť objektom hrozby ale taktiež môže byť aj cieľom útoku. Útok predstavuje úmyselný pokus o naplnenie hrozby, ktorej nositeľom je človek (poškodenie údajov, prienik do systému) a výsledkom je škoda alebo strata aktív.[8]

V prípade, že bude hrozba voči aktívu naplnená a spôsobí narušenie požadovaného stavu aktíva, dochádza k vzniku bezpečnostného incidente. Bezpečnostný incident môže byť spôsobený aktivitou užívateľa (úmyselne, neúmyselne), alebo iným pôsobením (napr. havária, chyba systému a pod.). Dôsledkom bezpečnostného incidentu je ujma na aktívach organizácie (napr. nefunkčnosť aktíva, nemožnosť poskytovania služby, materiálne škody, finančné škody a pod.). Takáto ujma sa nazýva dopad, ktorý sa dá vyjadriť kvantitatívne (napr. finančne ako cena opravy alebo náhrady poškodeného počítača, obnova jeho programového vybavenia a údajov, a pod.) alebo kvalitatívne.[9]

---

[7] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 38.

[8] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, s. 8. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[9] Pri ťažko merateľných dopadoch (napr. pri narušení reputácie) sa využíva kvalitatívne vyjadrenie dopadu bezpečnostného incidentu, a to označením nízky (ak nemá bezpečnostný incident vplyv na chod organizácie), alebo označením vysoký (organizácia nie je spôsobilá vykonávať svoje hlavné úlohy). Označenie dopadu bezpečnostného incidentu ako stredný predstavuje situáciu, kedy organizácia už pocítila dôsledky (dokáže plniť svoje primárne úlohy, ale nie v plnom rozsahu). Bližšie pozri OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 8-9. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

Organizácia počas plnenia svojich úloh čelí mnohým bezpečnostným incidentom či už tým vážnym alebo menej vážnym. Nie všetky hrozby sú pre danú organizáciu opodstatnené, a preto je potrebné vytvoriť kritéria, na základe ktorých bude organizácia rozlišovať hrozby na relevantné a tie menej relevantné. Takýmto kritériom je, napr. dopad hrozby, resp. bezpečnostného incidentu, pri ktorom došlo k naplneniu hrozby. Jedno kritérium by nebolo dostačujúce, a preto je potrebné stanoviť druhé kritérium, ktorým je pravdepodobnosť naplnenia hrozby. Tieto oba kritéria sú spojené v riziku. Vo všeobecnosti možno povedať, že riziko predstavuje možnosť (nie nutnosť), že konkrétna hrozba využije zraniteľnosť aktíva, čo spôsobí vznik ujmy vlastníkovi aktíva.[10]

Riziká vyplývajúce z hrozieb voči aktívam organizácie nepredstavujú rovnaký bezpečnostný problém, a preto je potrebné vykonať analýzu rizík, čo predstavuje stanovenie úrovne rizík. Následne sa riziká podľa závažnosti zoradia a rozhodne sa, ktorými rizikami sa bude organizácia zaoberať a ktorými nie. Hranica akceptovateľného rizika predstavuje pomyselnú čiaru v zozname rizík. Inými slovami možno povedať, že v prípade rizík, ktoré sa nachádzajú nad čiarou, musí organizácia prijať také riešenia, aby sa hodnoty daného rizika znížili. Takýmto riešením sú opatrenia, ktoré plnia niekoľko úloh. Na jednej strane znižujú dopady bezpečnostných incidentov na aktíva, a na strane druhej môžu odstraňovať zraniteľnosť aktív, čím v konečnom dôsledku znižujú pravdepodobnosť, že vôbec dôjde k bezpečnostnému incidentu. Takýmto opatrením môže byť, napr. spoľahlivá identifikácia a autentifikácia, šifrovanie citlivej informácie, zálohovanie údajov a pod.[11]

V dobe kedy sa informácie prenášajú a spracúvajú elektronicky a digitálne prostredníctvom informačných a komunikačných technológií (ďalej len „IKT“) sa problematika bezpečnosti spája najmä s pojmami informačná bezpečnosť a kybernetická bezpečnosť. V odbornej literatúre sa pojem informačná bezpečnosť častokrát zamieňa za pojem kybernetická

[10] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 9. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[11] Tamtiež, s. 9-10.

bezpečnosť a naopak. Nejasnosť v terminológii spomínaných pojmov vychádza najmä zo skutočnosti, že predmetné pojmy sú upravené v mnohých dokumentoch, národného, ako aj medzinárodného charakteru, avšak tieto dokumenty nemajú právnu záväznosť. Nejednotnosť týchto pojmov, ktoré sú používané najmä v rôznych stratégiách, ktoré upravujú bezpečnosť v kybernetickom priestore spôsobila roztrieštenosť pohľadov na skúmané pojmy.

Pojmy informačná a kybernetická bezpečnosť budem analyzovať najmä prostredníctvom medzinárodných štandardov, ktoré túto problematiku riešia už viac než 20 rokov. Hoci štandardy nie sú právne záväzné, častokrát sa na ne legislatíva odvoláva a dávajú presnejšie formulované odpovede na otázky, ktoré súvisia informačnou a kybernetickou bezpečnosťou.

Štandard možno z formálneho hľadiska definovať ako: *„dokument, ktorý vznikol na základe konsenzu a bol schválený uznaným orgánom, ktorý poskytuje pre všeobecné a opakované použitie pravidlá, smernice alebo charakteristiky činností alebo ich výsledkov zamerané na dosiahnutie optimálneho stupňa usporiadania v danom kontexte.*“[12]

Z hľadiska orgánu, ktorý prijíma konkrétny štandard, možno štandardy rozdeliť na formálne a neformálne. Zatiaľ čo formálne štandardy boli schválené národnými[13], európskymi[14] alebo medzinárodnými štandardizačnými orgánmi[15], neformálne štandardy boli publikované organizáciami pre rozvoj štandardov, ktoré však nie sú uznané za štandardizačné orgány.[16]

---

[12] ISO/IEC *Guide 2:2004 Standardization and related activities – General vocabulary,* s. 10.

[13] Zoznam národných štandardizačných orgánov dostupný z: https://standards.cen.eu/dyn/www/f?p=CENWEB:5. [citované 28.9.2019].

[14] Medzi európske štandardizačné orgány možno zaradiť *European Committee for Standardization* (CEN), *European Committee for Electrotechnical Standardization* (CENEL) a *European Telecommunications Standards Institute* (ETSI).

[15] Medzi medzinárodné štandardizačné orgány možno zaradiť *International Organization for Standardization* (ISO), *International Electrotechnical Commission* (IEC) a *International Telegraph Union* (ITU).

[16] Napr. *American Society for Testing Materials International, Society of Automotive Engineers, Internet Engineering Task Force* a i.

Problematike informačnej bezpečnosti sa venuje viacero medzinárodných štandardov. V ďalších častiach analýzy sa zameriam na medzinárodné ISO štandardy, ako aj na diela autorov, ktorí sú považovaní za odborníkov v oblasti informačnej a kybernetickej bezpečnosti.

2.1 INFORMAČNÁ BEZPEČNOSŤ - POJEM

Medzinárodný štandard ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ďalej len „ISO/IEC 27000:2016“) definuje informačnú bezpečnosť ako zachovanie dôvernosti, integrity a dostupnosti informácií.

Dôvernosť, integrita a dostupnosť predstavujú základné bezpečnostné požiadavky na ochranu informácií. Bezpečnostná požiadavka na zaistenie dôvernosti informácie znamená, že informácia je chránená pred prezradením neoprávneným osobám. Príkladom informácií, ktoré si vyžadujú ochranu pred neoprávneným prístupom sú, napr. osobné údaje, informácie týkajúce sa bezpečnosti štátu a pod.[17]

Bezpečnostná požiadavka na zaistenie integrity údajov znamená, že údaje[18] sú chránené pred náhodnou alebo úmyselnou modifikáciou, ktorá by mohla mať vplyv na platnosť údajov. Príkladom by mohla byť ochrana údajov v rámci transakcií, kde dochádza k platbe, kde by mohlo dôjsť k modifikácii sumy.[19]

---

[17] TODOROV, D. *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, s. 2.

[18] V tomto prípade je potrebné rozlišovať medzi informáciou a údajom. Ako uvádza Olejár, informácie sú obsahom údajov a údaje sú len forma zápisu informácií. To znamená, že tú istú informáciu (napr. desať) možno zapísať v rôznej forme (napr. X, ten a pod.). Bližšie pozri OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 11. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019]. K rozdielu medzi pojmom údaj a informácia taktiež pozri: POLČÁK, R. *Informace a data v právu.* In Revue pro právo a technologie 7, 2016, s. 67–91.

OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 9-10.[on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[19] TODOROV, D. *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, s. 2.

Dostupnosť informácie ako bezpečnostná požiadavka znamená, že informácie a služby, ktoré poskytujú osobám a organizáciám, musia byť dostupné používateľovi kedykoľvek, keď o to požiada. Napr. webová stránka, prostredníctvom ktorej sa osoby identifikujú a autentifikujú pre využívanie elektronických služieb verejnej správy, musí byť dostupná kedykoľvek, ak o to daná osoba požiada. Nedostupnosť webovej stránky by narušila poskytovanie služieb.[20]

Popri vyššie uvedených bezpečnostných požiadavkách na ochranu informácií, existujú aj iné bezpečnostné požiadavky ako autentickosť, súkromnosť, anonymita, pseudonymita, nepopretie pôvodu, nepopretie doručenia, resp. v prípade ochrany systémov poznáme dosledovateľnosť.[21]

V zmysle predmetného štandardu sa za informácie považujú nielen informácie v digitálnej forme (údaje uložené na elektronických alebo optických médiách), ale aj v materiálnej forme (napr. papier). Medzi informácie môžeme taktiež zaradiť informácie ako vedomosti zamestnanca. Informácie môžu byť prenášané rôznymi spôsobmi, kuriérom, elektronickou alebo verbálnou komunikáciou. Bez ohľadu na formu informácií a spôsob jej prenosu platí, že si vyžadujú dostatočnú ochranu.[22]

Whitman a Mattord definujú informačnú bezpečnosť ako: *„ochranu informácií a ich kľúčových prvkov, vrátane systémov a hardvéru, ktoré používajú, uchovávajú a prenášajú túto informácie.“*[23] Kľúčovými prvkami sú v tomto prípade dôvernosť, integrita a dostupnosť informácie.[24]

Podľa Olejára sa pojem informačná bezpečnosť používa minimálne v troch významoch:[25]

---

[20] Tamtiež, s. 2.

[21] Pre tieto bezpečnostné požiadavky bližšie pozri OLEJÁR, D. a kol.: *Informačná bezpečnosť.* Bratislava, 2013. s. 12. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[22] ISO/IEC 27000:2016, s. 15.

[23] WHITMAN, M.E. a MATTORD, H.J. *Principles of Information security*. Boston: Course Technology, 2012, s. 9.

[24] Dôvernosť, integrita a dostupnosť informácie sú v odbornej literatúre označené ako CIA trojuholník. Skratka CIA vychádza zo začiatočných písmen anglických názvov týchto základných bezpečnostných požiadaviek (*Confidentiality, Integrity, Availability*).

- je to ideálny stav systému alebo organizácie, ktorý sa dá charakterizovať tak, že všetko (IKT) funguje v súlade s požiadavkami (stanovenými napr. v bezpečnostnej politike) a v systéme/organizácii nedochádza k bezpečnostným incidentom,
- označuje činnosť smerujúcu k dosiahnutiu ideálneho stavu,
- medziodborová oblasť, ktorá skúma hrozby voči IKT a informácii a metódy eliminácie rizík, ktoré z nich vyplývajú.

2.2 KYBERNETICKÁ BEZPEČNOSŤ – POJEM

Pojem kybernetická bezpečnosť je v zmysle medzinárodného štandardu ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity (ďalej len „ISO/IEC 27032:2012“) definovaný ako zachovanie dôvernosti, integrity a dostupnosti informácií[26] v kybernetickom priestore.[27] V porovnaní s informačnou bezpečnosťou, pôjde teda len o informácie, ktoré sú prenášané a uložené v kybernetickom priestore. Kybernetická bezpečnosť sa vzťahuje na opatrenia, ktoré by zainteresované strany[28] mali stanoviť pre vytvorenie a zachovanie bezpečnosti v kybernetickom priestore.[29]

V zmysle vyššie uvedenej definície by sme mohli povedať, že kybernetická bezpečnosť je informačná bezpečnosť kybernetického

---

[25] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015. s. 16. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[26] Podľa niektorých autorov je kybernetická bezpečnosť postavená na princípoch, ktoré sa nazývajú triády kybernetickej bezpečnosi. Konkrétne ide o:

1. CIA (*Confidentiality, Integrity, Availability*)
2. Prvky kybernetickej bezpečnosti (Ľudia, Technológie, Procesy)
3. Životný cyklus kybernetickej bezpečnosti (Prevencia, Detekcia, Reakcia).

Bližšie pozri KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. s. 45-68 alebo BAYUK, L. a kol.: *Cyber security policy guidebook*. Wiley, 2012, s. 2-3.

[27] Predmetný medzinárodný štandard odkazuje na viacerých miestach na ISO štandardy, ktoré sa aplikujú v prípade informačnej bezpečnosti.

[28] Medzi zainteresované strany v kybernetickom priestore možno zaradiť užívateľov (jednotlivci, súkromné a verejné organizácie) a poskytovateľov (poskytovatelia Internetu a poskytovatelia aplikačných služieb).

[29] ISO/IEC 27032:2012, s. 17.

priestoru. Je viac ako potrebné ozrejmiť pojem kybernetický priestor *(cyberspace)*, nakoľko tento pojem určuje obsah pojmu kybernetická bezpečnosť.

Neexistuje jednoznačná, všeobecne akceptovaná definícia pojmu kybernetický priestor. Kybernetický priestor možno chápať ako systém systémov (SoS) zložený z rôznych digitálnych zariadení spojených počítačovými sieťami, pripojenými na Internet (vrátane programového vybavenia, údajov, aplikačných programov, technickej infraštruktúry) a ľudí, ktorí v tomto priestore pôsobia, činností, ktoré v ňom prebiehajú, pravidiel, ktoré upravujú činnosti a vzťahy v priestore. Iné definície chápu kybernetický priestor ako virtuálny systém informácií, vzťahov, činností, ktoré vznikajú pri spracovaní informácií prostredníctvom digitálnych IKT, ktorý však neexistuje v materiálnej forme.[30]

V zmysle medzinárodného štandardu ISO/IEC 27032:2012 predstavuje kybernetický priestor komplexné prostredie, ktoré vzniklo interakciou ľudí, softvéru a služieb na Internete prostredníctvom zariadení a sietí, technológií k nemu pripojených, ktoré neexistuje v žiadnej fyzickej podobe.[31]

Autori odbornej literatúry chápu kybernetický priestor ako geograficky neobmedzený, nefyzický priestor, v ktorom sa nezávisle od času, diaľky a miesta vykonávajú transakcie medzi ľuďmi, medzi počítačmi a medzi počítačmi a ľuďmi. Charakteristickým znakom kybernetického priestoru je nemožnosť určiť presné miesto a čas, kedy došlo k danej aktivite alebo kde došlo k presunu informácií.[32]

Hoci ISO/IEC 27032:2012 a niektorí autori odbornej literatúry chápu kybernetický priestor ako prostredie, ktoré neexistuje vo fyzickej podobe, nemožno ho chápať izolovane od jeho technologických komponentov, z ktorých je tvorený. Avšak, okrem technologickej úrovne má kybernetický

[30] Bližšie pozri: ANDRAŠKO, J. a kol.: *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 96.

[31] ISO/IEC 27032:2012, s. 12.

[32] HAMELINK, C. J. *The ethics of cyberspace.* Sage, 2001, s. 9.

priestor aj sociálno-technickú úroveň, v rámci ktorej sa vykonávajú rôzne kybernetické aktivity.[33]

Legálnu definíciu pojmu kybernetický priestor možno nájsť v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB“). Kybernetický priestor je v zmysle § 3 písm. b) predmetného zákona definovaný ako: *„globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.“* Predmetná definícia má viacero nedostatkov, nakoľko medzi prvky, ktoré patria do kybernetického priestoru zaradzuje len aktivované prvky, čím vylučuje prvky, ktoré nie sú aktivované. Ako príklad neaktivovaných prvkov možno uviesť siete, počítače a zariadenia, ktoré sa nemusia dočasne používať, avšak stále sú súčasťou technologickej infraštruktúry, ktorú je potrebné chrániť. V prípade ak by sme pripustili, že kybernetická bezpečnosť sa vzťahuje len na aktívne prvky kybernetického priestoru, potom by pasívne komponenty prestali byť prvkami kybernetického priestoru. Takéto úvahy sú namieste najmä z dôvodu, že nová právna úprava týkajúca sa ochrany informačných technológií verejnej správy sa netýka len ISVS, ale aj infraštruktúry, ktorá zabezpečujúce implementáciu a prevádzkovanie ISVS.[34]

Pre úplnosť je potrebné dodať, že kybernetická bezpečnosť sa v zmysle štandardu ISO/IEC 27032:2012 opiera o informačnú bezpečnosť *(information security)*, bezpečnosť aplikácií *(application security),* bezpečnosť siete *(network security)* a bezpečnosť Internetu *(Internet security)* ako o základné stavebné kamene. Kybernetická bezpečnosť je jednou z činností potrebných pre ochranu kritickej informačnej infraštruktúry *(critical information infrastructure protection)*. Primeraná ochrana služieb kritickej infraštruktúry súčasne prispieva k základným potrebám bezpečnosti

[33] VAN DEN BERG, J. a kol. *On (the Emergence of) Cyber Security Science and its Challenges for CyberSecurity Education.* NATO STO/IST-122 symposium, Tallinn, 13-14 október 2014, s. 12-2.

[34] Problematickým aspektom pojmu kybernetický priestor v zmysle zákona o KB je aj zaradenie ľudí medzi prvky kybernetického priestoru. Bližšie pozri ANDRAŠKO, J. a kol.: *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 95.

(bezpečnosť, spoľahlivosť a dostupnosť kritickej infraštruktúry) za účelom dosiahnutia cieľov kybernetickej bezpečnosti.[35]

V odbornej literatúre možno nájsť rôzne definície pojmu kybernetická bezpečnosť.[36] Kolouch chápe kybernetickú bezpečnosť v dvoch rovinách. V prvej rovine definuje kybernetickú bezpečnosť ako: *„súhrn právnych, organizačných, technických a vzdelávacích prostriedkov, ktoré smerujú k zaisteniu ochrany počítačových systémov a ďalších prvkov IKT, aplikácií, údajov a užívateľov.“*[37]

V druhej rovine chápe kybernetickú bezpečnosť ako: „*schopnosť počítačových systémov a využívaných služieb reagovať na kybernetické hrozby či útoky a ich následky, ako aj plánovanie obnovy funkčnosti počítačových systémov a služieb s nimi spojených.“*

Pojem kybernetická bezpečnosť je definovaný zákone o KB. V zmysle § 3 písm. g) zákona o KB je kybernetická bezpečnosť[38] definovaná ako: „*stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.“* Predmetná definícia vychádza z pojmu bezpečnosť sietí a informačných systémov v zmysle čl. 4 ods. 2 smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“).[39]

---

[35] ISO/IEC 27032:2012, s. 17.

[36] K pojmu kybernetická bezpečnosť pozri: POLČÁK, R: *Kybernetická bezpečnost*. In Právo informačních technológií. Praha: Wolters Kluwer ČR, 2018, s. 587-593 alebo POLČÁK, R. *Kybernetická bezpečnost jako aktuální fenomén českého práva.* In Revue pro právo a technologie, 2015,č. 11, s. 95. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/2980. [citované 29.9.2019].

[37] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. s. 45-68 alebo BAYUK, L. a kol.: *Cyber security policy guidebook*. Wiley, 2012, s. 45.

[38] Bližšie k pojmu kybernetická bezpečnosť v zmysle zákona o KB pozri ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 100-103.

2.3 ROZDIEL MEDZI INFORMAČNOU A KYBERNETICKOU BEZPEČNOSŤOU

V prvom rade si je potrebné uvedomiť, že v prípade skúmaných pojmov nejde o synonymá. Informačnú a kybernetickú bezpečnosť nemožno v zmysle skúmaných štandardov vnímať ako totožné pojmy a nie je ani vhodné ich rozlišovať na základe toho, ktorý pojem je širší alebo užší.

V prípade kybernetickej bezpečnosti je okrem iného taktiež cieľom ochrana informácií, ale len tých z prostredia kybernetického priestoru. V tejto súvislosti si je potrebné uvedomiť, že z pohľadu ochrany informácie ako aktíva, sú v prípade informačnej bezpečnosti chránené nie len informácie v elektronickej podobe, ale aj vo fyzickej podobe.

V druhom rade je potrebné podotknúť, že kybernetická bezpečnosť má z pohľadu štandardov za cieľ zabezpečiť zdieľanie a koordináciu medzi jednotlivými bezpečnostnými doménami. Možno povedať, že kybernetická bezpečnosť spravuje bezpečnostné problémy, ktoré nerieši žiadna z bezpečnostných domén alebo môže byť identifikovaná viacerými doménami. V druhom prípade je potrebné zdieľať a koordinovať informácií pre efektívne a komplexné riešenie bezpečnostného problému.[40]

Avšak v súčasnosti sa v právnom poriadku Slovenskej republiky nerozlišuje medzi informačnou bezpečnosťou a kybernetickou bezpečnosťou. Z právneho hľadiska, ako aj praktického hľadiska je rozlišovanie medzi informačnou bezpečnosťou a kybernetickou bezpečnosťou nepodstatné. Dôležitejšie je, aby právna úprava zabezpečila dostatočnú ochranu informačných systémov a informácií, ktoré sa v nich

[39] V zmysle smernice NIS sa bezpečnosť sietí a informačných systémov chápe ako: *„schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.“* Smernica NIS chápe bezpečnosť sietí a informačných systémov ako vlastnosť sietí a informačných systémov, zatiaľ čo v zákone o KB je chápaná kybernetická bezpečnosť ako stav.

[40] V niektorých prípadoch je pojem kybernetickej bezpečností spájaný s ochranou kritickej informačnej infraštruktúry, čo však nie je pravdou. Súvislosť medzi kybernetickou bezpečnosťou a ochranou kritickej informačnej infraštruktúry je častokrát viac ako zrejmá, nakoľko napr. infraštruktúra telekomunikačných sietí zabezpečuje prístup do kybernetického priestoru.

spracúvajú, tak aby sa dalo spoľahnúť na ich dôvernosť, dostupnosť a integritu. Taktiež je potrebné, aby sa zabezpečila nielen ochrana informácií v materiálnej podobe, ale aj informácií, ktoré sú spracúvané v elektronickej alebo digitálnej forme.

3. BEZPEČNOSŤ ISVS V PRÁVNOM PORIADKU SLOVENSKEJ REPUBLIKY

Právna úprava ISVS a otázka ich bezpečnosti prešla v poslednom období výraznými zmenami. V prvom rade, zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ISVS“) bol zrušený zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“), ktorý nadobudol účinnosť 5. mája 2019.

Problematika bezpečnosti ISVS je v súčasnosti stále upravená vo výnose Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy. Predmetný výnos obsahuje bezpečnostné štandardy.[41]

Bezpečnosť ISVS je taktiež predmetom zákona o KB, nakoľko za určitých okolností môže byť konkrétny ISVS zaradený medzi základné služby a jeho správca do registra prevádzkovateľov základných služieb (ďalej len „PZS“). V takejto situácii je správca v pôsobnosti ktorého je konkrétny ISVS povinný plniť povinnosti v zmysle zákona o KB.

V nasledujúcej časti príspevku dôjde k ozrejmeniu pojmu informačná technológia verejnej správy, ktorý v sebe zahŕňa aj pojem informačný systém verejnej správy. Taktiež upriamim pozornosť na ustanovenia zákona o ITVS, ktoré upravujú problematiku bezpečnosti informačných technológií verejnej správy. Následne poukážem na zákon o KB a jeho vzťah k zákonu o ITVS, a to najmä z pohľadu bezpečnostných opatrení resp. iných

[41] Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov zostáva platný a účinný do nadobudnutia účinnosti vykonávacieho právneho predpisu podľa § 31 zákona o ITVS, najneskôr však do 1. mája 2020.

povinností, ktoré musia konkrétne subjekty plniť, aby zabezpečili dostatočnú úroveň bezpečnosti informačných technológií verejnej správy, resp. ISVS.

3.1 BEZPEČNOSŤ ISVS V ZÁKONE O ITVS

Zákon o ITVS v porovnaní so zrušeným zákonom o ISVS definuje pojem informačné technológie verejnej správy (ďalej len „ITVS“) a rozširuje svoju pôsobnosť aj na bezpečnosť týchto technológií. V zmysle § 2 ods. 2 zákona ITVS sú ITVS definované ako: „*informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby*.“ Informačné technológie sú v zmysle § 2 ods. 1 zákona o ITVS chápané ako: „*prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe*.“ Zákon o ITVS uvádza príklady informačných technológií, konkrétne informačný systém, infraštruktúru, informačnú činnosť a elektronické služby. Definícia pojmu informačný systém verejnej správy zostala zachovaná v znení už zrušeného zákona o ISVS ako: „*informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.“* V prípade pojmu informačný systém došlo k zmene, nakoľko informačný systém predstavuje v zmysle § 2 ods. 2 zákona o ITVS: „*funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.*“[42] V porovnaní s definíciou pojmu informačný systém v zmysle zrušeného zákona o ISVS nemusia byť technické prostriedky a programové prostriedky súčasťou informačného systému a taktiež tieto prostriedky nemôžu poskytovať iný informačný systém.

Bezpečnosť ITVS je v zákone o ITVS upravená v § 18 až § 23. Predmetný zákon upravuje bezpečnosť ITVS v oblasti:

- plánovania a organizácie (§ 19),

[42] V zmysle § 2 ods. 1 písm. a) zákona o ISVS bol informačný systém definovaný ako: „*funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov, ktoré sú súčasťou informačného systému alebo ktoré informačnému systému poskytuje iný informačný systém.*“

- obstarávania a implementácie (§ 20),
- prevádzky, servisu a podpory (§ 21),
- monitoringu a hodnotenia (§ 22),

V § 18 zákona o ITVS sú základné ustanovenia týkajúce sa situácie kedy je správca aj PZS v zmysle zákona o KB. V § 23 predmetného zákona sú upravené osobitné opatrenia na úseku bezpečnosti ITVS (napr. bezpečnostný projekt).

Správcom ITVS je v zmysle § 2 ods. 5 zákona o ITVS ten orgán riadenia[43], ktorého za správcu ITVS ustanoví zákon alebo je ustanovený na základe zákona o ITVS. Povinnosť správcu zabezpečiť riadenie bezpečnosti je zakotvená v § 14 ods. 1 písm. i) zákona o ITVS. V súvislosti s bezpečnostnými opatreniami je správca povinný:

- identifikovať potrebné bezpečnostné opatrenia (§ 19 ods. 1 písm. e) zákona o ITVS),
- určiť prostriedky na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení (§ 19 ods. 1 písm. h) zákona o ITVS),
- realizovať bezpečnostné opatrenia (§ 19 ods. 3 písm. c) zákona o ITVS).

Z pohľadu správcu ITVS bude dôležité, aké bezpečnostné opatrenia musí prijať a realizovať a taktiež, ktorý právny predpis má aplikovať pri prijímaní konkrétnych bezpečnostných opatrení. V zmysle § 18 ods. 1 zákona o ITVS je správca, ktorý je zároveň aj PZS povinný prijať a realizovať bezpečnostné opatrenia vo vzťahu k ISVS v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov v zmysle § 20 zákona o KB. Inými slovami, vo všeobecnosti platí, ak je správca aj PZS v zmysle zákona o KB, prijíma a realizuje bezpečnostné opatrenia v zmysle zákona o KB.

Povinnosti správcov ITVS v oblasti bezpečnosti ITVS budú detailne upravené vo vykonávacom právnom predpise, ktorý nahradí výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch

[43] Taxatívny zoznam orgánov riadenia je uvedený v § 5 ods. 2 zákona o ITVS.

pre informačné systémy verejnej správy. Obsah bezpečnostných opatrení v novej vyhláške by mal reflektovať už existujúce bezpečnostné opatrenia, ktoré sú správcovia povinní realizovať.

3.2 NOVÁ VYHLÁŠKA

Dôležitým aspektom, ktorý ovplyvní vytvorenie právneho rámca bezpečnosti ITVS, bude prijatie vykonávacieho právneho predpisu, konkrétne vyhlášky. Predmetná vyhláška bude v zmysle § 31 písm. a) a i) zákona o ITVS upravovať:

- jednotlivé kategórie ITVS a podrobnosti o spôsobe zaraďovania do týchto kategórií,
- podrobnosti o bezpečnosti ITVS podľa § 18 až 23, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsah bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov.

Klasifikácia informácii je prejavom hodnoty a statusu informácie danej organizácie. S tým priamo súvisí aj určenie, kto je vlastníkom informácií.[44] Jednotlivé kategórie ITVS a podrobnosti o spôsobe zaraďovania do týchto kategórií sa vykoná v zmysle § 31 písm. a) zákon o ITVS s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov v zmysle zákona o KB.[45]

V súvislosti s klasifikáciou informácií vznikajú správcovi v zmysle zákona o ITVS viacero povinností. Správca v zmysle § 19 ods. 1 písm. c) zákona o ITVS zavedie a udržiava systém riadenia informačnej bezpečnosti, ktorý zabezpečí identifikovanie aktív v ITVS. Navyše správca v zmysle § 15 ods. 8 písm. a) a c) zákona o ITVS identifikuje a udržiava zoznam svojich aktív a taktiež identifikuje časti aktív, ktorých nedostupnosť alebo znížená

[44] WONG, H. *Cyber Security: Law and Guidance.* Bloomsbury Professional, 2018, s. 456.

[45] Bližšie pozri: vyhláška č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

kvalita má zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb.[46]

V súvislosti s kategorizáciou ISVS platí, že správca má v zmysle § 19 ods. 5 písm. a) zákona o ITVS povinnosť určiť kategóriu ISVS, do ktorej bude z hľadiska klasifikácie informácií a kategorizácie sietí a informačných systémov patriť už pri plánovaní vytvorenia alebo nadobudnutí ISVS.

V súvislosti s bezpečnostným projektom platí, že správca je povinný v zmysle § 23 ods. 2 zákona o ITVS vypracovať bezpečnostný projekt vždy pre ISVS, ktorý je z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov v najvyššej kategórii z hľadiska jeho významnosti, funkcie a účelu použitia s ohľadom na potrebu zabezpečenia ochrany dôvernosti a integrity a zabezpečenia dostupnosti a úrovne činností vykonávaných s jeho použitím. Inými slovami, správca je povinný vypracovať bezpečnostný projekt pre ITVS v jeho pôsobnosti, ak je predmetná ITVS zaradená v najvyššej kategórii. Výnimkou z tohto pravidla je situácia, kedy bezpečnostný audit alebo hodnotenie zraniteľnosti vykonané orgánom vedenia zistí riziko alebo hrozbu pre ITVS. V takomto prípade je správca povinný v zmysle § 23 ods. 3 písm. d) zákona o ITVS vypracovať bezpečnostný projekt bez ohľadu na kategorizáciu ITVS.

3.3 BEZPEČNOSŤ ISVS V ZÁKONE O KB

Na bezpečnosť ISVS sa možno pozerať aj z pohľadu zákona o KB. Predmetný zákon stanovil, že medzi základné služby možno zaradiť aj ISVS. Národný bezpečnostný úrad (ďalej len „NBÚ“) zaraďuje základnú službu - ISVS, do zoznamu základných služieb a jej prevádzkovateľa do registra PZS v spolupráci s príslušným ústredným orgánom. Príslušným ústredným orgánom pre oblasť ISVS je Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej len „ÚPVII“), ktorý má v sektore verejná správa v pôsobnosti podsektor ISVS.

V praxi v súčasnosti zatiaľ nedochádza k zaraďovaniu všetkých ISVS do zoznamu základných služieb a ich správcov do registra PZS, čo odzrkadľuje

[46] Bližšie k pojmom služba verejnej správy, služba vo verejnom záujme a verejná služba pozri § 3 zákona o ITVS.

požiadavku smernice NIS na PZS, ktorý má poskytovať službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností.[47] Ak by došlo k zaradeniu všetkých ISVS do zoznamu základných služieb, nebola by spomínaná požiadavka naplnená, nakoľko mnoho ISVS neposkytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností.

Konkrétne bezpečnostné opatrenia, ktoré musí PZS splniť sú stanovené v § 20 zákona o KB a vyhláške NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

3.3.1 POSTAVENIE A POVINNOSTI PZS

V súvislosti s vyššie uvedeným je potrebné ozrejmiť, akým spôsobom môže byť správca ITVS zaradený do registra PZS a jeho ISVS do zoznamu základných služieb. V zmysle zákona o KB existuje niekoľko spôsobov ako dôjde k zaradeniu základnej služby do príslušného zoznamu a zaradeniu PZS do príslušného registra.[48]

V prípade základných služieb a ich prevádzkovateľov platí, že ak entita zistí, že došlo k prekročeniu identifikačných kritérií prevádzkovanej služby a takáto entita patrí do niektorého zo sektorov podľa prílohy č. 1 zákona o KB, je povinná urobiť oznámenie do 30 dní odo dňa, keď sa o prekročení identifikačných kritérií dozvedela. Takéto oznámenie obsahuje konkrétne informácie a je adresované NBÚ. Právny základ pre zaradenie základnej služby do zoznamu základných služieb a PZS do registra PZS závisí od jednotlivých druhov základných služieb.

Slovenský zákonodarca definuje tri druhy základných služieb. V zmysle § 3 písm. k) zákona o KB je základnou službou služba, ktorá je zaradená v zozname základných služieb a:

[47] Pozri čl. 5 ods. 2 smernice NIS.

[48] PZS je v zmysle § 19 ods. 1 zákona o KB povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra PZS prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.

A. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohyč. 1 zákona o KB,
B. je informačným systémom verejnej správy[49], alebo
C. je prvkom kritickej infraštruktúry[50].

V prípade ak ide o zaradenie základnej služby typu A platí, že NBÚ zaradí túto službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS:

a) na základe oznámenia prevádzkovateľom tejto služby,
b) na základe podnetu ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18 zákona o KB,
c) z vlastnej iniciatívy, ak sa NBÚ dozvedel o prekročení identifikačných kritérií prevádzkovanej služby podľa § 18 zákona o KB a nedošlo k postupu podľa písmena a) alebo písmena b).[51]

V prípade základných služieb typu B (služba ako ISVS) platí, že NBÚ v spolupráci s príslušným ústredným orgánom zaradí základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS.[52]

V súvislosti so základnými službami typu C platí, že NBÚ zaradí takúto základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS zo zákona.[53]

Zaradenie základnej služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS oznámi NBÚ prevádzkovateľovi tejto služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.[54]

---

[49] § 2 ods. 1 písm. b) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov.

[50] § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.

[51] § 17 ods. 2 zákona o KB.

[52] Tamtiež, § 17 ods. 3.

[53] Tamtiež, § 17 ods. 4.

[54] Tamtiež, § 17 ods. 5. Oznámenie nemá charakter individuálneho právneho aktu. Na zaradenie služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS sa nevzťahuje zákon č. 71/1967 Zb. o správnom konaní (správny poriadok), čo znamená, že zaradený subjekt nemôže použiť opravné prostriedky v zmysle správneho poriadku.

Aby došlo k zaradeniu základnej služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS, musí príslušná základná služba, ktorú poskytuje entita prekročiť identifikačné kritériá prevádzkovanej služby. V zmysle § 18 zákona o KB sa identifikačné kritéria prevádzkovanej služby delia na dopadové kritéria a špecifické sektorové kritériá.

Dopadové kritériá vychádzajú z článku 6 smernice NIS, ktorý upravuje faktory pre určenie závažnosti rušivého vplyvu. Podrobnosti o dopadových a špecifických sektorových kritériách pre základnú službu sú upravené vo vyhláške NBÚ č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).[55] Na tomto mieste je potrebné podotknúť, že európsky zákonodarca určuje identifikačné kritéria PZS a nie pre základné služby. Avšak slovenský zákonodarca upravuje v zákone KB a predmetnej vyhláške identifikačné kritéria prevádzkovanej služby a ak entita tieto kritéria prekročí následne možno hovoriť o tom, že má postavenie PZS.

Z praktického hľadiska je však problematickejšia skutočnosť, že vyššie uvedená vyhláška určuje identifikačné kritériá len pre PZS typu A. Inými slovami, pri prevádzkovateľoch základnej služby typu B a C sa neskúmajú dopadové kritériá, ktoré vychádzajú z článku 6 smernice NIS. V tejto súvislosti je evidentný jasný rozpor s článkom 5 ods. 2 smernice NIS, v zmysle ktorého musí PZS kumulatívne spĺňať tieto kritériá:

- subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;
- poskytovanie tejto služby je závislé od sietí a informačných systémov a
- incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby.

[55] V zmysle § 2 predmetnej vyhlášky platí, že: „*prevádzkovaná služba spĺňa identifikačné kritériá základnej služby, ak spĺňa aspoň jedno dopadové kritérium a aspoň jedno špecifické sektorové kritérium, ak je uvedené v prílohe č. 1.*“ Avšak, v zmysle § 18 ods. 4 zákona o KB platí, že: „*ak prevádzkovateľ služby podľa prílohy č. 1 zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu do 30 dní odo dňa, keď prekročenie zistil v rozsahu podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritériá.*“ Neskoršie citované ustanovenie nevyžaduje naplnenie dopadového kritéria, čo je v rozpore so smernicou NIS.

V prípade ak sa neskúma posledné spomenuté kritérium, a teda závažný rušivý vplyv, nemožno hovoriť o PZS v zmysle smernice NIS.

Skutočnosť či správca ISVS bude zároveň aj v postavení PZS v zmysle zákona o KB, bude mať dopad najmä na to či tento subjekt bude pri realizácii bezpečnostných opatrení postupovať v zmysle zákona o ITVS alebo zákona o KB. Nejasnosť tejto situácie možno demonštrovať na prepojení zákona o ITVS a zákona o KB.

3.4 PREPOJENIE ZÁKONA O ITVS A ZÁKONA O KB

Ako už bolo spomenuté, ak je správca ITVS aj v postavení PZS v zmysle zákona o KB, prijíma a realizuje bezpečnostné opatrenia v zmysle zákona o KB. Avšak môže dôjsť k situácii, kedy správca v pozícii PZS nebude realizovať bezpečnostné opatrenia v zmysle zákona o KB ale v zmysle zákona o ITVS.

V zmysle § 18 ods. 2 zákona o ITVS platí, že: *„obsah bezpečnostných opatrení vo vzťahu k informačným systémom verejnej správy a spôsob a rozsah ich prijímania a realizácie v súlade s osobitným predpisom.“* Týmto osobitným predpisom je zákon o KB, konkrétne jeho *§ 2* ods. 2 písm. e), v zmysle ktorého sa zákon o KB nevzťahuje na: *„požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona.“* Predmetným osobitným predpisom je už zrušený zákon o ISVS.[56] Na základe vyššie uvedeného možno konštatovať, že v prípade ak zákon o ITVS stanoví pre správcu, ktorý je zároveň aj PZS, striktnejšie bezpečnostné opatrenia, bude musieť správca prijať a realizovať bezpečnostné opatrenia v zmysle zákona o ITVS. V praxi to bude pre správcu, ktorý je aj PZS znamenať, že bude musieť porovnávať bezpečnostné opatrenia v zmysle zákona o KB a zákona o ITVS.

V tejto súvislosti by bolo viac ako vhodné, aby ÚPVII ako orgán vedenia v zmysle zákona o ITVS prijal výkladové stanoviská v zmysle § 9 ods. 1 písm. a) zákona o ITVS alebo metodické usmernenia v zmysle § 8 ods. 1

[56] V zmysle § 33 ods. 1 zákona o ITVS: *„informačné systémy verejnej správy podľa doterajších predpisov sú informačnými systémami verejnej správy podľa tohto zákona.“*

písm. a) zákona o ITVS. Výkladové stanoviská alebo metodické usmernenia by mohli prispieť k tomu, aby správcovia vedeli identifikovať, prijať a realizovať konkrétne bezpečnostné opatrenia v zmysle príslušných právnych predpisov, čo by mohlo dopomôcť k právnej istote.

Ak správca nie je PZS, prijíma a realizuje bezpečnostné opatrenia v zmysle zákona o ITVS.

Možno konštatovať, že bezpečnostné opatrenia upravené v zákone o ITVS sa aplikujú na ISVS ktoré neboli zaradené do zoznamu základných služieb v zmysle zákona o KB a taktiež na tie, ktoré boli zaradené do zoznamu základných služieb v zmysle zákona o KB, ale bezpečnostné opatrenia stanovené v zákone o ITVS majú za cieľ dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako v zákone o KB.

4. HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV

Akokoľvek striktné bezpečnostné opatrenia nemôžu zabrániť tomu, že hrozba (napr. v podobe kybernetického útoku) zneužije zraniteľnosť ISVS a spôsobí narušenie požadovaného stavu aktíva, čím dôjde k bezpečnostnému incidentu. Takáto situácia znamená, že správca ITVS je povinný takýto bezpečnostný incident hlásiť konkrétnej entite. Správca je povinný hlásiť kybernetické bezpečnostné incidenty v zmysle zákona o ITVS a v prípade ak je aj PZS, tak aj kybernetické bezpečnostné incidenty v zmysle zákona o KB. Navyše, za určitých podmienok, môže kybernetický bezpečnostný incident spôsobiť aj porušenie ochrany osobných v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“).

4.1 HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV V ZMYSLE ZÁKONA O KB

PZS je v zmysle § 19 ods. 6 písm. b) zákona o KB povinný bezodkladne hlásiť závažný kybernetický bezpečnostný incident. Rovnakú povinnosť musí PZS splniť aj v zmysle § 24 ods.1 predmetného zákona. PZS

identifikuje závažný kybernetický bezpečnostný incident na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. V zmysle § 24 ods. 2 zákona o KB sa závažné kybernetické bezpečnostné incidenty členia na kategórie prvého, druhého a tretieho stupňa. Stanovenie konkrétneho stupňa závisí od nasledujúcich faktorov:

- počtu používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetickým bezpečnostným incidentom,
- dĺžky trvania kybernetického bezpečnostného incidentu,
- geografického rozšírenia kybernetického bezpečnostného incidentu,
- stupňa narušenia fungovania základnej služby alebo digitálnej služby,
- rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.[57]

Presná špecifikácia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov je predmetom vyhlášky NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov. PZS má povinnosť hlásiť kybernetické bezpečnostné incidenty prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.[58]

Na tomto mieste je potrebné podotknúť, že v zmysle čl. 14 ods. 3 smernice NIS má PZS povinnosť bezodkladne hlásiť incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú. S cieľom určiť závažnosť vplyvu incidentu sa zohľadňujú konkrétne parametre osobitne pre základné služby a digitálne služby.

Parametre pre určenie závažnosti vplyvu incidentu na kontinuitu základných služieb, ktoré PZS poskytujú sú najmä: počet používateľov postihnutých narušením základnej služby; dĺžka trvania incidentu a geografické rozšírenie z hľadiska oblasti, ktorú incident postihol.[59]

---

[57] § 24 ods. 2 písm. a) - e) zákona o KB.

[58] § 24 ods. 4 a § 25 ods. 1 zákona o KB.

[59] Čl. 14 ods. 4 smernice NIS.

Pre určenie závažnosti vplyvu na poskytované digitálne služby sú najmä tieto parametre: počet používateľov postihnutých incidentom, najmä používateľov využívajúcich danú službu na účely poskytovania vlastných služieb; dĺžka trvania incidentu; geografické rozšírenie z hľadiska oblasti, ktorú incident postihol; stupeň narušenia fungovania služby; rozsah vplyvu na hospodárske a spoločenské činnosti.[60]

V zákone o KB boli parametre pre určenie závažnosti vplyvu incidentu na kontinuitu základných služieb a pre určenie závažnosti vplyvu na poskytované digitálne služby v zmysle smernice NIS spojené do jedného, a to pre účely stanovenia stupňa závažného kybernetického bezpečnostného incidentu.

4.1.1 JEDNOTNÝ INFORMAČNÝ SYSTÉM KYBERNETICKEJ BEZPEČNOSTI

Jednotný informačný systém kybernetickej bezpečnosti predstavuje základný komunikačný kanál medzi NBÚ a ostatnými entitami v oblasti kybernetickej bezpečnosti. NBÚ je správcom a prevádzkovateľom predmetného informačného systému. NBÚ sprístupní jednotný informačný systém kybernetickej bezpečnosti do 18 mesiacov od účinnosti predmetného zákona.[61]

Jednotný informačný systém kybernetickej bezpečnosti obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. V súvislosti s prístupom k jednotnému informačnému systému kybernetickej bezpečnosti má tento informačný systém verejnú časť a neverejnú časť. Verejná časť obsahuje príslušné registre PZS, poskytovateľov digitálnych služieb, ústredných orgánov, kybernetických bezpečnostných incidentov a zoznamy základných služieb, digitálnych služieb a akreditovaných jednotiek CSIRT.[62] Do neverejnej časti jednotného informačného systému kybernetickej bezpečnosti majú prístup v elektronickej forme, v reálnom čase a v rozsahu určenom NBÚ alebo

[60] Tamtiež, čl. 16 ods. 4.

[61] § 34 ods. 1 zákona o KB.

[62] Tamtiež § 8 ods. 2. [on-line] https://www.nbu.gov.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html [citované 30.9.2019]

osobitným predpisom na základe vecnej pôsobnosti ústredný orgán, jednotka CSIRT (zaradená v zozname akreditovaných jednotiek CSIRT), PZS, poskytovateľov digitálnych služieb, Národná banka Slovenska, Úrad na ochranu osobných údajov Slovenskej republiky a iný orgán verejnej moci rozhodnutím NBÚ.[63]

Z dikcie zákona o KB vyplýva, že jednotný informačný systém kybernetickej bezpečnosti je primárnym komunikačným kanálom. Avšak, je potrebné myslieť aj na situácie, kedy by jednotný informačný systém kybernetickej bezpečnosti nemohol plniť svoj účel, napr. z dôvodu incidentu, ktorý by ochromil alebo znefunkčnil jeho prevádzku. Predpokladám, že pre tieto prípady by sa mal aplikovať § 24 ods. 6 zákona o KB. V zmysle predmetného ustanovenia platí, že NBÚ môže uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s PZS. Podobným spôsobom môže NBÚ uzavrieť zmluvu aj s poskytovateľom digitálnych služieb.[64]

4.2 HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV V ZMYSLE ZÁKONA O ITVS

V zmysle § 23 ods. 3 zákona o ITVS sú orgán riadenia podľa § 5 ods. 2 písm. a) a b)[65] a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti povinní:

- ak sú zaradení do registra PZS podľa osobitného predpisu (ISVS ako základná služba podľa zákona o KB), nahlasovať spôsobom podľa osobitného predpisu (prostredníctvom jednotného informačného systému kybernetickej bezpečnosti) aj kybernetický bezpečnostný incident, na

[63] Tamtiež, § 8 ods. 5.

[64] Tamtiež, § 25 ods. 3.

[65] Orgán riadenia je podľa § 5 ods. 2 písm. a) a b) zákona o ITVS: ministerstvo a ostatný ústredný orgán štátnej správy, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Dopravný úrad, Úrad pre reguláciu sieťových odvetví a iný štátny orgán.

ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu (§ 24 ods. 1 zákona o KB),

- ak nie sú zaradení do registra PZS, nahlasujú takýto kybernetický bezpečnostný incident ÚPVII ním určeným spôsobom,
- určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov.

V zmysle § 33 ods. 5 zákona o ITVS platí, že orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti, ktorí sú zaradení do registra PZS podľa osobitného predpisu, nahlasujú do uplynutia 30 dní odo dňa zriadenia a uvedenia do prevádzky jednotného informačného systému kybernetickej bezpečnosti [66] kybernetický bezpečnostný incident podľa § 23 ods. 3 písm. a) orgánu vedenia, ktorým je ÚPVII, ním určeným spôsobom.

Zákon o ITVS ukladá v § 23 ods. 4 zákona o ITVS plniť povinnosti v zmysle § 23 ods. 3 písm. a) aj ostatným orgánom riadenia[67]. Inými slovami, aj ostatné orgány riadenia, ak sú zaradení do registra PZS, sú

---

[66] JISKB musí byť uvedený do prevádzky najneskôr 18.10.2019 v zmysle § 34 ods. 1 zákona o KB.

[67] Ostatné orgány riadenia možno chápať ako tie, ktoré neboli uvedené v § 23 ods. 3, a teda ide o orgány riadenia podľa § 5 ods. 2 písm. c) – h):

„c)obec a vyšší územný celok,

d)Kancelária Národnej rady Slovenskej republiky, Kancelária prezidenta Slovenskej republiky, Kancelária Ústavného súdu Slovenskej republiky, Kancelária Najvyššieho súdu Slovenskej republiky, Kancelária Súdnej rady Slovenskej republiky, Kancelária verejného ochrancu práv, Úrad komisára pre deti, Úrad komisára pre osoby so zdravotným postihnutím, Ústav pamäti národa, Sociálna poisťovňa, zdravotné poisťovne, Tlačová agentúra Slovenskej republiky, Rozhlas a televízia Slovenska, Rada pre vysielanie a retransmisiu,

e)právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v písmenách a) až d),

f)komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,

g)osoba neuvedená v písmenách a) až f) okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,

h)záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.“

povinné nahlasovať prostredníctvom jednotného informačného systému kybernetickej bezpečnosti aj kybernetický bezpečnostný incident, na ktorý sa nevzťahuje povinnosť nahlasovania podľa zákona o KB. Taktiež, ak nie sú zaradení do registra PZS, nahlasujú kybernetický bezpečnostný incident, ktorý nespĺňa kritériá podľa zákona o KB ÚPVII ním určeným spôsobom. A v neposlednom rade sú ostatné orgány riadenia povinné určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov.

V prípade ak správca nie je PZS v zmysle zákona o KB, má možnosť nahlasovať aj závažné kybernetické bezpečnostné incidenty podľa § 24 ods. 1 zákona o KB, resp. príslušnej vyhlášky, a to prostredníctvom inštitútu dobrovoľného hlásenia kybernetických bezpečnostných incidentov v zmysle § 26 ods. 1 zákona o KB. V recitáli 67 smernice NIS sa uvádza, že subjekty, ktoré neboli určené ako PZS a nie sú ani poskytovateľmi digitálnych služieb, majú možnosť dobrovoľne oznamovať incidenty, ktoré majú významný vplyv na služby, ktoré poskytujú, ak sa domnievajú, že je vo verejnom záujme oznámiť, že k takýmto incidentom došlo.

4.3 PORUŠENIE OCHRANY OSOBNÝCH ÚDAJOV V ZMYSLE GDPR

V praxi môže nastať situácia, kedy si ten istý subjekt bude plniť svoju oznamovaciu povinnosť v zmysle zákona o KB, resp. zákona o ITVS a zároveň si musí splniť oznamovaciu povinnosť v zmysle GDPR. Inými slovami, subjekt bude nahlasovať rovnakú skutočnosť rôznym inštitúciám. V podmienkach Slovenskej republiky by išlo o splnenie si oznamovacej povinnosti voči NBÚ, resp. ÚPVII a Úradu na ochranu osobných údajov.[68]

[68] Príkladom entity, ktorá môže byť správcom v zmysle zákona o ITVS a zároveň aj prevádzkovateľom základných služieb v zmysle zákona KB a prevádzkovateľom v zmysle GDPR je napr. Ministerstvo vnútra Slovenskej republiky vo vzťahu k informačnému systému s názvom Evidencia vozidiel.

GDPR ukladá prevádzkovateľovi[69] a sprostredkovateľovi[70] povinnosť oznamovať porušenie ochrany osobných údajov.[71] Za porušenie ochrany osobných údajov považuje: *„porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim“*.[72]

Je potrebné podotknúť, že k splneniu si oznamovacej povinnosti v zmysle GDPR dôjde len v prípadoch, keď došlo k porušeniu ochrany osobných údajov.

V nasledujúcej tabuľke uvádzam prehľad oznamovacích povinností jednotlivých subjektov v zmysle GDPR.

Povinnosť	Lehota	Výnimka
Prevádzkovateľ oznamuje dozornému orgánu (čl. 33 ods. 1 GDPR)	Bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o porušení ochrany osobných údajov dozvedel	Oznámenie sa nevyžaduje, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.
Sprostredkovateľ oznamuje prevádzkovateľovi (čl. 33 ods. 2 GDPR)	Bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel	Oznámenie sa nevyžaduje, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva

[69] Prevádzkovateľ je v zmysle čl. 4 bodu 7 GDPR definovaný ako: *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.“*

[70] Sprostredkovateľom je v zmysle čl. 4 bodu 8 GDPR: *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.“*

[71] Bližšie k pojmom prevádzkovateľ a sprostredkovateľ pozri: MESARČÍK, M. *Základné pojmy Nariadenia*. In Všeobecné nariadenie o ochrane osobných údajov. Praha: C.H. Beck, 2018, s. 123-186.

[72] Čl. 4 ods. 12 GDPR.

		a slobody fyzických osôb.
Prevádzkovateľ oznamuje dotknutej osobe (čl. 34 ods. 1 GDPR)	Bez zbytočného odkladu	Oznámenie sa nevyžaduje ak: a) prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie; b) prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb uvedené v odseku 1 pravdepodobne už nebude mať dôsledky; c) by to vyžadovalo neprimerané úsilie. V takom prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.

Zdroj: vlastné spracovanie

K prelínaniu sa oznamovacej povinnosti v zmysle GDPR a zákona o KB, resp. zákona o ITVS, môže dôjsť v mnohých prípadoch. Ak berieme do úvahy koncept kybernetickej bezpečnosti v zmysle zákona o KB, kedy konanie, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, by mohlo zároveň spôsobiť porušenie ochrany osobných údajov v zmysle GDPR.

V teoretickej rovine možno povedať, že narušenie ochrany osobných údajov v zmysle GDPR sa spája najmä s narušením bezpečnostnej požiadavky súkromnosti, ktorá znamená, že k osobným údajom majú prístup len tie osoby, ktoré majú na to oprávnenie. Na druhej strane, zákon o KB upriamuje pozornosť na bezpečnostné požiadavky ako dôvernosť, integrita, dostupnosť a autentickosť. Napr. narušenie integrity služby, poskytovanej prostredníctvom sietí a informačných systémov a údajov, ktoré sú v rámci jej poskytovania spracované, môže znamenať aj porušenie ochrany osobných údajov v zmysle GDPR, nakoľko v mnohých prípadoch pôjde o narušenie integrity osobných údajov.

Ako už bolo vyššie uvedené, hlásený kybernetický bezpečnostný incident môže mať charakter porušenia ochrany osobných údajov. V praxi by bolo preto vhodné, aby si subjekty mohli plniť oznamovaciu povinnosť v zmysle zákona o KB, resp. zákona o ITVS a GDPR jedným oznámením. Na tieto účely by mohol slúžiť aj jednotný informačný systém kybernetickej bezpečnosti. Takéto riešenie v zásade potvrdzuje aj ust. § 8 ods. 5 písm. e) zákona o KB, v zmysle ktorého má Úrad na ochranu osobných údajov prístup k neverejnej časti jednotného informačného systému kybernetickej bezpečnosti. V tejto súvislosti je potrebné zabezpečiť, aby oznamovanie porušenia ochrany osobných údajov, ktoré sa bude vykonávať prostredníctvom oznámenia v zmysle zákona o KB, obsahovalo náležitosti oznámenia v zmysle GDPR. Preto je potrebné zabezpečiť, aby Úrad na ochranu osobných údajov bol adresátom a spracovateľom len tých údajov, ktoré sa týkajú porušenia ochrany osobných údajov.

Povinnosť hlásiť konkrétny typ kybernetických bezpečnostných incidentov, konkrétnym subjektom v zmysle zákona o ITVS, zákona o KB a GDPR uvádzam v nasledujúcej súhrnnej tabuľke.

	Zákon o ITVS I	**Zákon o ITVS II**	**Zákon o KB**	**GDPR**
Subjekt	Orgán riadenia (zároveň aj PZS)	Orgán riadenia (nie je PZS)[73]	PZS (zároveň aj správca ISVS)	Prevádzkovateľ
Druh bezpečnostného incidentu (BI)	Kybernetický BI	Kybernetický BI	Závažný kybernetický BI	Porušenie ochrany osobných údajov
Komu a akým spôsobom sa oznamuje bezpečnostný incident (BI)	NBÚ (JISKB)	Orgánu vedenie (ÚPVII), ním určeným spôsobom	NBÚ (JISKB)	Úradu na ochranu osobných údajov[74]
Lehota			Bezodkladne	Bez zbytočného odkladu/72 hodín

Zdroj: vlastné spracovanie

5. ZÁVER

Pri vhodnom nastavení a realizácii bezpečnostných opatrení v zmysle zákona o ITVS a zákona o KB budú ISVS dostatočne chránené pred rôznymi hrozbami (či už z fyzického sveta alebo z kybernetického priestoru). Avšak, pre dosiahnutie potrebnej úrovne bezpečnosti ISVS je potrebné zabezpečiť, aby správcovia tieto opatrenia vedeli identifikovať, prijať a realizovať.

[73] Orgán riadenia, ktorý nie je PZS môže hlásiť kybernetické bezpečnostné incidenty podľa zákona o KB prostredníctvom dobrovoľného hlásenia.

[74] Povinnosť hlásiť porušenie ochrany osobných údajov vznikne len za predpokladu, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

Prijatie novej legislatívy v oblasti bezpečnosti ISVS je nepochybne krokom vpred, avšak v otázke právnej istoty prináša nová legislatíva niekoľko problémov. V prvom rade, zaraďovanie všetkých ISVS do zoznamu základných služieb a ich správcov do registra PZS v zmysle zákona o KB odporuje smernici NIS, nakoľko nie všetky ISVS, resp. ich správcovia poskytujú službu, ktorá má zásadný význam z pohľadu zachovania hospodárskych alebo spoločenských činností. Navyše, ak sa pri zaraďovaní správcov ITVS do registra PZS neskúmajú dopadové kritériá, ktoré vychádzajú z článku 6 smernice NIS, dochádza k jasnému porušeniu smernice NIS.

Prepojenosť zákona o ITVS a zákona o KB môže významným spôsobom ovplyvniť dosiahnutie dostatočnej úrovne bezpečnosti ISVS. V praxi môžu nastať situácie, kedy budú subjekty v právnom postavení správcov ITVS alebo v právnom postavení PZS v istých momentoch porovnávať striktnosť bezpečnostných opatrení v zmysle zákona o ITVS a zákona o KB. V tejto súvislosti bude potrebné, aby ÚPVII prijal výkladové stanoviská alebo metodické usmernenia, ktoré by mohli prispieť k tomu, aby správcovia vedeli identifikovať, prijať a realizovať konkrétne bezpečnostné opatrenia v zmysle príslušných právnych predpisov, čo by mohlo dopomôcť k právnej istote.

K dosiahnutiu dostatočnej úrovne bezpečnosti ISVS by mohla dopomôcť aj kontrola realizácie bezpečnostných opatrení a následné sankcionovanie v prípade neplnenia si povinností v zmysle zákona o ITVS a zákona o KB. V tejto súvislosti je potrebné podotknúť, že cieľom zákona o ITVS a zákona o KB nie je represívne pôsobiť na správcov a PZS pri nesplnení si povinností, najmä v podobe nedostatočného realizovania bezpečnostných opatrení, resp. absencie realizovania bezpečnostných opatrení. V tejto súvislosti si dovolím tvrdiť, že zákon o ITVS a jeho vykonávací právny predpis bude upravovať len minimálne bezpečnostné opatrenia, ktoré je potrebné prijať a realizovať v závislosti od konkrétnej kategórie ITVS. Správcovia, ktorých ITVS budú zaradené do vyšších kategórií, budú povinní prijať striktnejšie bezpečnostné opatrenia v porovnaní s nižšími kategóriami ITVS. Taktiež je potrebné podotknúť, že už v súčasnosti sú správcovia

povinní plniť v zmysle výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy mnohé bezpečnostné opatrenia.

Predmetom spomínaného vykonávacie právneho predpisu bude taktiež pôsob zaradenia ITVS do konkrétnych kategórií a klasifikácia informácií. Vyhláška taktiež upraví obsah a rozsah bezpečnostných opatrení v závislosti od konkrétnej kategórie ITVS a obsah a štruktúru bezpečnostného projektu.

Ani tie najprísnejšie bezpečnostné opatrenia nemôžu zabrániť tomu, aby nedošlo ku kybernetickému bezpečnostnému incidentu. V takýchto prípadoch je zasiahnutý subjekt v zmysle zákona o ITVS, zákona o KB a GDPR povinný hlásiť konkrétny typ bezpečnostného incidentu, konkrétnemu subjektu. Subjekt či už v postavení PZS podľa zákona o KB, postavení správcu v zmysle zákona o ITVS alebo postavení prevádzkovateľa v zmysle GDPR si pred samotným hlásením musí uvedomiť, aký typ bezpečnostného incidentu má hlásiť, akým spôsobom, akému subjektu a v akej lehote. Bolo by viac ako vhodné, aby konkrétny subjekt mohol urobiť jedno hlásenie bezpečnostného incidentu, ktoré by bolo adresované zainteresovaným subjektom. V podmienkach Slovenskej republiky sa ako najvhodnejšie riešenie tejto situácie javí využitie jednotného informačného systému kybernetickej bezpečnosti, prostredníctvom ktorého by sa mohli hlásiť kybernetické bezpečnostné incidenty, ktoré nespĺňajú kritériá v zmysle zákona o KB, závažné kybernetické bezpečnostné incidenty podľa zákona o KB, ako aj oznámenia, ktoré majú charakter porušenia ochrany osobných údajov. Pre dosiahnutia tohto cieľa by bolo potrebné zosúladiť obsahové náležitosti formulárov, ktoré konkrétne subjekty využívajú pri hlásení konkrétnych typov bezpečnostných incidentov. K jednotnému informačnému systému kybernetickej bezpečnosti, resp. jeho neverejnej časti, kde by boli evidované jednotlivé hlásenia by mal prístup okrem NBÚ, Úradu na ochranu osobných údajov aj ÚPVII.

6. ZOZNAM LITERATÚRY

[1] ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 544 s.

[2] ANDRAŠKO, J., MESARČÍK, M.: *Problematika GDPR v kontexte nariadenia eIDAS*. In Digitalizácia, zmeny vonkajšieho prostredia a spoločnosť budúcnosti. Bratislava, Právnická fakulta UK, 2018, s. 8-21.

[3] BAYUK, L. a kol.: *Cyber security policy guidebook*. Wiley, 2012, 270 s.

[4] BERTHOTY, Jakub a kol. : *Všeobecné nariadenie na ochranu údajov*. 1. vydanie. Praha : C.H. Beck, 2018.

[5] HAMELINK, C. J. *The ethics of cyberspace.* Sage, 2001, 224 s.

[6] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. 556 s.

[7] OLEJÁR, Daniel a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, 175 s.

[8] OLEJÁR, Daniel a kol.: *Informačná bezpečnosť.* Bratislava, 2013. 246 s.

[9] POLČÁK, R. *Informace a data v právu.* Revue pro právo a technologie 7, 2016, s. 67–91.

[10] POLČÁK, R. a kol. *Právo informačních technológií.* Praha: Wolters Kluwer ČR, 2018, s 656 s.

[11] POLČÁK, R. *Kybernetická bezpečnost jako aktuální fenomén českého práva.* Revue pro právo a technologie, 2015,č. 11, s. 95-149. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/2980.

[12] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s.

[13] TODOROV, D. *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, 756 s. ISBN 978-1-4200-5219-0

[14] VAN DER HOF, Simone a kol.: *Framing Citizen's Identities: The construction of personal identities in new modes of government in the Netherlands.* Nijmegen: Wolf Legal Publishers, 2010, 258 s.

[15] VON SOLMS, R. a VAN NIEKERK, J. *From information security to cyber security. In* Computers & Security, 2013, roč. 38, s. 97-102

[16] WHITMAN, M, E. a MATTORD, H, J.: *Principles of Information security*. Boston: Course Technology, 2012, 617 s.

[17] WONG, H. *Cyber Security: Law and Guidance.* Bloomsbury Professional, 2018, 792 s.

[18] nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

[19] smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

[20] zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov

[21] zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

[22] zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

[23] zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

[24] vyhláška NBÚ č. 164/2018 z. Z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).

[25] vyhláška NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov

[26] vyhláška NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

[27] ISO/IEC 27001:2013 INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS

[28] ISO/IEC 27002:2013 INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

[29] ISO/IEC 27032:2012 *Information technology -- Security techniques -- Guidelines for cybersecurity*

[30] ISO/IEC 27000:2016 *Overview and vocabulary*

https://doi.org/10.5817/RPT2019-2-2

LEGITIMITA AUTOMATIZOVANÉHO ZPRACOVÁNÍ JUDIKATURY[1]

RADIM POLČÁK[2]

ABSTRAKT

Moderní metody zpracování velkých datových souborů umožňují mimo jiné provádět i detailní a sofistikované analýzy judikatury. Vedle základních vzájemných vazeb a odkazů lze analyzovat v prakticky neomezeném rozsahu i nejrůznější formální a obsahové aspekty soudních rozhodnutí v libovolně širokých souvislostech. Tento příspěvek se v kontextu aktuálního vývoje příslušných technologií zabývá informační kvalitou soudního rozhodnutí a jejím vztahem k informačním efektům užití judikatury v kontinentálně evropské právní kultuře. V diskusní části tohoto příspěvku pak je argumentována legitimita restriktivního regulatorního přístupu k analytickým nástrojům, jejichž užití by mohlo vést k omezení nezávislosti soudce.

KLÍČOVÁ SLOVA

Judikatura, precedens, dělba moci, právní informatika, promulgace, prediktivní analýza, profilování

ABSTRACT

Big data technologies allow for detailed and sophisticated analyses of case-law. Besides basic mutual relations or links, it is also possible to analyse various formal and material aspects of court decisions in unprecedented range and

[1] Tento příspěvek vznikl jako součást plnění výzkumného projektu č. GA17-20645S.

[2] doc. JUDr. Radim Polčák, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, e-mail: radim.polcak@law.muni.cz

depth. This paper aims at discussing, in the context of current technological developments, information properties of court decisions and their relations to information effects of case-law in continental European legal culture. Consequently, the text argues in favour of legitimacy of restrictive regulatory approaches to analytical tools that might lead to limitations of judicial independence.

KEYWORDS

Case-law, precedent, distinction of powers, legal informatics, promulgation, predictive analysis, profiling

1. PRÁVNÍ INFORMATIKA A PRAKTICKÁ DŮLEŽITOST JUDIKATURY

Pro právní informatiku je judikatura jednou z komponent informačního systému práva. Cílem zpracování judikatury je tedy informační efekt jejího užití.

Předmětem tohoto příspěvku budou externí zdroje informační kvality soudního rozhodnutí, které je publikováno a následně automatizovaně zpracováno. Budeme si všímat především způsobů, kterými je soudnímu rozhodnutí dodávána nebo naopak odebírána jeho informační kvalita a způsobilost přispívat k ultimativní teleologii práva, tj. informovat (organizovat) společnost. V závěru se pak budeme zabývat relativně novým druhem hloubkové prediktivní analýzy soudních rozhodnutí a v kontextu dostupných znalostí o možnostech této technologie se pokusíme formulovat názor na legitimitu a informační efekt aktuálně nejrestriktivnějšího přístupu zvoleného francouzským zákonodárcem.

Perspektiva pohledu na právo jako na informační systém vychází u právní informatiky ze základních myšlenek kybernetiky. Ta vznikla

v polovině minulého století a jejím základním cílem bylo popsání a napodobení mechanismu, který život používá v boji s entropií[3].

Kybernetika vycházela z výsledků filozofie a přírodních věd dosažených na přelomu devatenáctého a dvacátého století[4], přičemž dobře popsanou unikátní vlastností života byla právě jeho způsobilost čelit entropii. Ta se stala i ústředním předmětem zkoumání kybernetiky, nikoli snad z hlediska teleologického ale funkčního.

Zkoumáním procesu zvyšování organizace, tj. snižováním entropie, u živých organismů dospěla kybernetika k poznání nástroje, k jehož originální tvorbě má život jakožto přírodní fenomén unikátní způsobilost. Tímto nástrojem je informace a jednou ze základních premis kybernetiky tak je přímá logická kontradikce entropie a informace.[5]

Původní Wienerova kybernetika byla poměrně vzdálena jejím dnešním inkarnacím majícím spíše technický charakter. Jednalo se totiž o komplexní filozofii, jejímž základním předmětem zkoumání byl život jako přírodní fenomén.[6] Dnešní vysoce rozvinuté obory informatiky, robotiky nebo mechatroniky si všímají především technologií, kterými napodobujeme nebo dokonce zdokonalujeme informování v živých organismech. Jedná se tím pádem o aplikované technické formy kybernetiky.

Předmětem kybernetiky však původně byly i základní otázky informování, tj. organizace, z pohledu filozofického nebo sociálně-vědního. Disproporce mezi bouřlivým vývojem aplikovaných forem kybernetiky a její, původně možná i dominantní, filozofickou komponentou, vedou dnes k evidentním důsledkům. Máme totiž k dispozici vysoce výkonné informační technologie, jejichž užití však ve výsledku často nevede

---

[3] Základním pramenem pro studium kybernetiky je monografie Wiener, N. Cybernetics: Or the Control and Communication in the Animal and the Machine. Cambridge : MIT Press, 1961.

[4] Srov. Schrödinger, E. What is Life. Cambridge : Cambridge University Press, 1992. Dílo je volně dostupné i on-line na adrese <www.home.att.net/~p.caimi/Life.doc>.

[5] Srov. Wiener, N. Cybernetics: Or the Control and Communication in the Animal and the Machine. Cambridge : MIT Press, 1961, str. 11.

[6] Vladimír Neff ve svém slovníku dokonce označuje kybernetiku za filozofii života – viz Neff, V. Filozofický slovník pro samouky aneb Antigorgias. Praha: Mladá fronta, 1993, str.182.

k informování společnosti. Dokonce se dá při pohledu na řadu současných technologií a služeb informační společnosti velmi zjednodušeně říci, že máme v rukou skvěle funkční a vysoce výkonné nástroje, ale nevíme, k čemu nám mají být dobré.

Právní informatika či právní kybernetika původně vznikla jako aplikovaná forma kybernetiky. Tato disciplína je tedy důsledkem aplikace kybernetické metody na systém práva. Odtud pramení její shora konstatovaný předpoklad, že právo je informační systém, tj. že smyslem práva je informovat, resp. organizovat, společnost.[7]

I v tomto případě vidíme postupný posun od původního komplexního přístupu k právu jako informačnímu systému k technickým nástrojům pro zpracování právních dat. Dnes nejvíce viditelnými formami právní informatiky jsou vývoj právních informačních systémů, funkčních pomůcek pro praktikující právníky nebo dokonce systémů způsobilých díky autonomnímu zpracování právně relevantních dat nahrazovat do určité míry některé právnické profese. I zde tedy dospíváme do situace, kdy máme k dispozici vysoce výkonné nástroje pro zpracování právních dat, jejichž použití ale nemusí nutně vždy vést ke skutečné informaci, tj. ke snížení entropie ve společnosti.[8]

Vývoj kybernetiky a právní kybernetiky, jehož důsledkem je současný stav poznání v oborech informatiky a právní informatiky, je přirozeně motivován relativní jednoduchostí technologického pokroku na poli zpracování dat na jedné straně a vysokou obtížností detekce či identifikace dat způsobilých indukovat informaci na straně druhé. Jakkoli je totiž složité postavit a naprogramovat výkonný právní automat, pořád je to nesrovnatelné jednodušší než rozlišit, která právní data ve výsledku

[7] Jedním z průkopníků evropské právní kybernetiky, resp. právní informatiky, byl Viktor Knapp – srov. Knapp, V. O možnosti použití kybernetických metod v právu. Praha : Nakladatelství Československé akademie věd, 1963. Vývoj československé právní informatiky shrnuje v dobových souvislostech kapitola Polčák, R. Informační teorie práva, in Bobek, M., Molek, P., Šimíček, V. Komunistické právo v Československu, Brno: Masarykova univerzita, 2009, str. 167.

[8] Vývoj právní informatiky za poslední půlstoletí mapuje sborník Paliwala, A. A History of Legal Informatics. Zaragoza : Prensas de Universitarias de Zaragoza, 2010.

povedou k organizaci nebo naopak k chaotizaci nějakého sociálního systému.[9]

Snaha dnešní právní informatiky tedy v obecné rovině směřuje k vytvoření, pokud možno, co nejvýkonnějšího nástroje ke zpracování a případně i ke komunikaci právních dat. Příkladně u právních dat typu zákonného práva jde právní informatice o konstrukci takových mechanismů, které co nejefektivněji zpřístupní příslušné zákonné texty jejich cílové skupině.

Celá tato snaha však stojí na velmi snadno zpochybnitelné premise, že totiž veškeré zákonné právo je informací. Pokud by tomu tak skutečně bylo, platila by přímá úměra mezi dostupností zákonného práva a mírou organizace společnosti. Čím snadněji by se adresát zákona mohl seznámit s jeho textem, tím vyšší by byla ve výsledku míra společenské organizace. Tomu by pak odpovídala i objektivní legitimita snahy o co nejefektivnější proces zpracování nebo publikace zákonného práva.

Platnost zákonného práva však nijak přímo nesouvisí s jeho informační kvalitou. Zákon tedy může být dobrý, tj. informovat společnost ve smyslu jejího organizování, ale může být i špatný a vést naopak ke zvýšení míry společenské entropie. Kvalitní nástroj k efektivnímu zpracování textů zákonného práva a jejich bezproblémové distribuci jejich adresátům tedy sice u dobrého zákona posílí jeho informační efekt, u špatného zákona však naopak vede k posílení jeho chaotického dopadu.[10]

Pokud by měl být účel právního informačního systému k publikaci zákonného práva identický s původní myšlenkou právní informatiky, tj. fungování práva jako informačního systému, znamenalo by to, že by takový systém měl být schopen rozlišit dobré zákony od špatných. Ty dobré by měl co nejefektivněji komunikovat k cílové skupině a ty špatné by naopak měl před cílovou skupinou co nejefektivněji tajit.

Požadavek na to, aby se právní informatika zabývala otázkou, jak rozlišit dobrý a špatný zákon, je samozřejmě z podstaty absurdní. Nelze po

[9] Člověk totiž není vybaven schopností staticky poznat informaci - k tomu viz dále a podrobněji viz Polčák, R. Internet a proměny práva, Praha: Auditorium, 2012, str. 23.

[10] Podrobněji viz Polčák, R. Internet a proměny práva, Praha: Auditorium, 2012, str. 202.

žádné vědní disciplíně, přírodovědné nebo společenské, požadovat nemožné, tj. v tomto případě exaktní (a tím pádem objektivně ověřitelné) hodnocení informační kvality dat, nota bene a priori, tj. před jejich reálnou aplikací.

Stejně absurdní a dokonale nelegitimní je i představa, že právní informační systém za účelem informování (organizování) společnosti rozlišuje mezi dobrým a špatným zákonem a výsledek tohoto posouzení pak předurčuje metodu zpracování příslušných zákonných textů. Je pochopitelné, že právní informatika, nemoha řešit otázku informační kvality právních dat, zabývá se objektivně řešitelným problémem, jak data (bez ohledu na jejich kvalitu a způsobilost indukovat informaci) co nejefektivněji zpracovat.

Zatímco je atribut platnosti zákona binární a z hlediska praktického fungování systémů pro zpracování právních dat jen těžko zpochybnitelný, je situace v případě judikatury poněkud odlišná. Judikatura totiž tento atribut nemá, neboť o ní v naší právní kultuře neuvažujeme jako o absolutně závazné.[11] Charakter judikatury jakožto pramene práva je namísto toho definován zprostředkovanou argumentační závazností, která nastupuje v případech intenzivního tlaku rovnosti nebo právní jistoty.[12]

Relativní mnohost a částečně exaktní povaha faktorů praktické důležitosti judikatury[13] tvoří, společně s praktickou poptávkou, originální zadání pro právní informatiku. Ta totiž sice, podobně jako v případě zákonného práva, nedisponuje metodami k hodnocení informačního potenciálu určitého soudního rozhodnutí, ale díky nástrojům pro zpracování velkého množství dat může exaktními metodami přispět k indexaci judikatury. Zjednodušeně řečeno tedy může v tomto případě nabídnout právní informatika nástroje k exaktnímu měření praktické důležitosti soudního rozhodnutí.[14]

[11] K pojmu absolutní závaznosti viz Knapp, V. Teorie práva. Praha: C.H. Beck, 1991, str. 149.

[12] Podrobně viz Bobek, M., Kühn, Z. a kol. Judikatura a právní argumentace, 2. vyd. Praha: Auditorium 2013, str. 64.

[13] Viz tamtéž, str. 111.

Situace, kdy je určitý pramen práva závazný jinak než absolutně, je pro kontinentálně-evropskou právní kulturu založenou na dělbě moci poměrně výjimečná. Judikatura se v tomto případě mechanismem své závaznosti blíží z pohledu právní informatiky právním principům, u nichž rovněž není závaznost binární kategorií.[15] Podobně jako právní principy právně platí a zavazují v určité míře, platí a zavazuje v určité míře též judikatura. Na rozdíl od právních principů, kde je míra jejich závaznosti zpravidla otázkou jejich ad hoc intenzity, však může být míra závaznosti (či důležitosti) judikatury přinejmenším zčásti otázkou objektivně definovatelných a logicky souvisejících parametrů. Exaktnost právně informatických metod pak tedy může v naší právní kultuře částečně kompenzovat netradiční organickou nejistotu ohledně závaznosti judikatury jakožto pramene práva.

2. INFORMAČNÍ HODNOTA SOUDNÍHO ROZHODNUTÍ A JUDIKATURY

Při exaktním hodnocení praktické důležitosti judikatury je třeba z hlediska právní informatiky rozlišit pojem soudního rozhodnutí jakožto ad hoc výsledku procesu autoritativní aplikace práva a soudního rozhodnutí jakožto součásti judikatury a komponenty informačního systému platného práva.

Prvním hlediskem odlišení je aspekt cílového systému, jehož organizace je ambicí soudního rozhodnutí. To je v kontinentální evropské právní kultuře výstupem procesu autoritativní aplikace práva, v jehož důsledku vznikají, mění se nebo zanikají práva a povinnosti konkrétního subjektu. Na rozdíl od absolutně závazného pramene práva, typicky zákona, je tedy soudní rozhodnutí bezprostředně závazné a adresované.[16] To znamená, že

[14] Příkladem metody hodnocení praktické důležitosti je Shepardizing. Tato metoda byla pojmenována po svém vynálezci Franku Shepardovi a používá již déle něž sto let při indexaci judikatury v USA. Podrobněji k metodě viz Cole, B. Shepardizing: A Comparison of the Printed Citators and On-Line Shepardizing Services. Legal Reference Services Quarterly. 1988, roč. 7,č. 2-4, str. 261.

[15] K metodě nebinárního užití právních principů viz Alexy, R. On the Structure of Legal Principles. Ratio Iuris. 2000, roč. 13,č. 3, str. 1 a násl. Z česky psané literatury viz Holländer, P. Filosofie práva. Plzeň : Aleš Čeněk, 2006, str. 158 a násl.

[16] Podrobněji viz Knapp, V. Teorie práva. Praha: C.H. Beck, 1991, str. 186.

ambicí soudního rozhodnutí je bezprostředně informovat (organizovat) cílový systém tvořený jeho adresáty a státem.[17]

Soudní rozhodnutí jako součást judikatury však má informovat zcela jiný cílový systém a též metoda jeho informačního působení není založena na bezprostřední závaznosti.[18] Informační hodnota soudního rozhodnutí tady nespočívá v bezprostřední organizaci konkrétně definovaného cílového systému (tj. relace státu a účastníků řízení), ale ve zprostředkované organizaci neurčitého okruhu adresátů platného práva. Tento způsob organizace cílového systému je tedy obdobný jako v případě zákonného práva, neboť konkrétní právní pravidlo v tomto případě nastupuje jako hypotetický důsledek výskytu určitých právních skutečností a najisto může (a nemusí) být jeho závaznost konstatována až následně v procesu autoritativní aplikace práva.[19] Podobně jako u zákona tedy judikatura generuje obecné právní povinnosti, jejichž konkrétní závaznost může být potvrzena individuálním právním aktem – to ale pouze v případě, že se příslušná situace stane předmětem vrchnostenského rozhodování.

Z tohoto rozdílu mezi soudním rozhodnutím jako formou relativně závazného imperativu a soudním rozhodnutím jako formou obecného právního pravidla plyne řada důsledků pro jeho zpracování za užití metod právní informatiky. Pro práci se soudním rozhodnutím v prvním zmíněném případě jsou totiž rozhodující jiné formální znaky, než je tomu v případě druhém.

K jednoduššímu popisu a procesní kvalifikaci relevantních formálních prvků soudního rozhodnutí pro první či druhý typ zpracování lze tyto rozlišit na interní a externí formu. Interní forma se týká textu soudního rozhodnutí, zatímco externí forma je otázkou formálních znaků generovaných vnějším prostředím.

Pro užití soudního rozhodnutí jako relativně závazného zdroje právního imperativu je logicky důležitější jeho interní forma. Z výroku totiž plynou

[17] Srov. Bobek, M., Kühn, Z. a kol. Judikatura a právní argumentace, 2. vyd. Praha: Auditorium 2013, str. 103.

[18] Podrobně viz tamtéž, str. 108.

[19] Srov. Kelsen, H. Pure theory of Law, New Jersey: The Lawbook Exchange, 2005, str. 114.

příslušné povinnosti a odůvodnění pak slouží jednak k vysvětlení výroku vzhledem ke konkrétním skutkovým a právním souvislostem a jednak k ověření jeho legitimity vůči platnému hmotnému a procesnímu právu.[20] Externí forma soudního rozhodnutí sice rovněž zahrnuje z hlediska své relativní závaznosti podstatné prvky, typicky v případě, kdy je potvrzeno nebo zrušeno v nějakém revizním řízení (odvolání, dovolání, kasaci). Ty mají ale obvykle jednoduchou povahu a dají se snadno automatizovaně zpracovat.

Vnější forma soudního rozhodnutí je naproti tomu v případě jeho zpracování jakožto komponenty judikatury nesrovnatelně složitější. Vedle jednoduchých formálních kategorií, jakými jsou typicky právní moc nebo vykonatelnost, je třeba pracovat s řadou dalších typů dat, které mohou ve výsledku výrazně ovlivnit praktickou jeho důležitost nebo technickou dostupnost (dohledatelnost).

Typickým příkladem vnější formy mající minimální význam pro relativní závaznost soudního rozhodnutí, ale velmi důležité pro jeho roli jako součásti judikatury, je postavení příslušného soudu v hierarchii soudní soustavy. Pro relativní závaznost soudního rozhodnutí je lhostejné, který soud vydal pravomocné rozhodnutí, avšak pro jeho význam jako součásti judikatury je údaj o instanci zcela zásadní.

Vnější forma soudního rozhodnutí podstatná pro jeho roli v rámci judikatury zahrnuje celou řadu parametrů, přičemž řada z nich je zcela mimo kontrolu soudu, který toto rozhodnutí vydal. Typicky pasivní citace které významně promlouvají do výsledné praktické důležitosti soudního rozhodnutí, jsou výsledkem činnosti soudů často odlišných od toho, který odkazované rozhodnutí původně vydal. Podobně třeba zařazení soudního rozhodnutí do některé ze zákonných sbírek nemusí být v gesci vydávajícího soudu jako celku ale nějakého jeho zvláštního grémia.[21]

---

[20] Pro vady interní formy se v našem právním prostředí vžila, především v důsledku judikatury nejvyšších soudů a Ústavního soudu, různá typická označení, jako například nepřezkoumatelnost nebo opomenutý důkaz.

[21] Srovnání způsobů, jimiž proces výběru a editace judikatury k publikaci probíhá na nejvyšších evropských správních instancích, viz v publikaci Molek, P., Polčák, R. Poskytnout nebo chránit? Brno: Nejvyšší správní soud, 2017, str. 53.

Praktickou důležitost soudního rozhodnutí mohou dokonce často definovat i prvky vnější jeho formy, jejichž původci nedisponují žádnou vrchnostenskou legitimitou. Příkladem mohou být třeba anotace nebo citace, pozitivní či negativní, odbornou literaturou.

Nikoli přímo praktickou důležitost, ale samotnou dohledatelnost soudního rozhodnutí mohou zásadním způsobem ovlivňovat též jiné více či méně arbitrární prvky vnější formy, jako například právní věty nebo indexy. Neadekvátní a téměř až posvátných charakter právních vět[22] svádí v našem právním prostředí k dojmu, že tyto jsou součástí vnitřní formy soudního rozhodnutí a v procesu editace judikatury dochází pouze k jejich zdůraznění. Soudci sami pak často trpí pod tíhou odpovědnosti, když se snaží cizelovat formulace v odůvodnění s vidinou toho, že se příslušná věta může, to právě kvůli neadekvátnímu jejímu užití, stát v důsledku jejího „právního zvětnění" čímsi jako apendixem zákonného práva.

Ve skutečnosti je však právní věta pouze indikátorem potenciálního významu soudního rozhodnutí pro judikaturu a je součástí jeho vnější formy. Může samozřejmě jít o vhodně formulovanou součást odůvodnění příslušného rozhodnutí. Může ji ale legitimně formulovat, dokonce zcela nezávisle na vnitřní formě příslušného soudního rozhodnutí, též nezávislý editor, anotátor nebo komentátor. Klidně pak může dojít k situaci, kdy je k jednomu soudnímu rozhodnutí formulováno více právních vět v závislosti na tom, jakého konkrétního aspektu aplikace práva si příslušný editor, anotátor nebo komentátor všímal.

Podobnou funkci jako právní věty mají též různé dodatečně doplňované indexy. Ty mohou například indikovat vztah k zákonné úpravě nebo k judikatuře, tuzemské nebo zahraniční – to dokonce i v případech, kdy tento vztah není součástí vnitřní formy soudního rozhodnutí. Informační systém zpracovávající judikaturu, ať jde o systém soudu nebo nějaké komerční řešení, tedy může soudní rozhodnutí označit i vztahovými atributy, které soud původně nevyjádřil, nebo o nich dokonce ani neuvažoval.

[22] Srov. Bobek, M., Kühn, Z. a kol. Judikatura a právní argumentace, 2. vyd. Praha: Auditorium 2013, str. 238.

Především dopad externí formy na výslednou praktickou důležitost judikatury může vypadat pochybně vzhledem k legitimitě jednotlivých původců. Zatímco soud je alespoň legitimován k původnímu rozhodnutí, nedisponuje nezávislý editor informačního systému nebo autor právnické publikace žádným typem oficiální legitimace. Dokonce ani v případě, pokud je externí forma soudního rozhodnutí důsledkem aktivity samotného soudce (tj. soudce třeba formuluje právní větu nebo doplňuje indexy), není tato výrazem původní legitimace soudu k rozhodnutí ve věci.

Právě v tomto ohledu je však třeba zdůraznit shora konstatovaný rozdíl mezi relativní závazností soudního rozhodnutí a jeho praktickou důležitostí jakožto součásti judikatury. Soud je totiž v kontinentální právní kultuře přímo legitimován pouze k relativnímu zavazování, nikoli k tvorbě práva.[23] Praktická důležitost judikatury tedy v tomto případě nevychází z autority soudu, ale z obecných principů rovnosti a právní jistoty. Intenzita těchto principů pak není pro další případy otázkou autority soudu a z ní odvozené právní moci rozhodnutí, ale je dána situační koherencí všech možných relevantních vlivů, včetně arbitrární pozornosti právní doktríny, kvality nástrojů pro automatizované zpracování judikatury nebo dokonce souvislostí se zahraniční právní úpravou či judikaturou.

Právě uvedené samozřejmě neznamená, že by měl kontinentální soudce s klapkami na očích ostentativně odmítat cizí nebo i vlastní úvahy o tom, jak se jeho rozhodnutí dál obecně projeví v právní praxi. Právě provedený kategorický soud snad až příliš příkře připomínající roli soudce v systému založeném na dělbě moci vzešlé z francouzské revoluce, je zde spíš reakcí na realitu českého souzení. V ní soudce vrcholného soudu, nikoli výjimečně a nikoli důvodně, sužuje sám sebe palčivými myšlenkami na všechny možné eventuality různých možných budoucích interpretací svého rozhodnutí nebo dokonce jeho právních vět. V horších případech pak tím, co soudce autonomně staví do nepříslušné role tvůrce práva, může dokonce být jeho vlastní touha po zanechání vlastní stopy v právním řádu hnaná

[23] Srov. Bobek, M., Kühn, Z. a kol. Judikatura a právní argumentace, 2. vyd. Praha: Auditorium 2013, str. 66.

navíc vědomím, že případ, který mu to aktuálně umožnil, už třeba nemusí nikdy dostat na stůl.

3. INFORMAČNÍ EFEKTY VNĚJŠÍ FORMY SOUDNÍHO ROZHODNUTÍ

Informační efekt různých formálních důsledků následného zpracování soudního rozhodnutí se samozřejmě neomezuje pouze na jeho roli jako součásti judikatury. Odborná publikace nebo jiná forma přiblížení soudního rozhodnutí odborné veřejnosti může i vyvolat veřejný zájem o určitý problém nebo třeba zvýšit známost nebo odbornou reputaci příslušného soudce. I v případě problematického nebo dokonce vyloženě vadného soudního rozhodnutí může mít ve výsledku odborná publikace i pozitivní informační efekt – to například v případě, kdy je součástí vnější formy argumentovaná identifikace vady, případně ještě doplněná o návod k řešení.[24] Přestože tedy problematické soudní rozhodnutí chaotizuje svůj primární cílový systém tím, že vadně upraví právní poměry účastníků řízení, může v důsledku jeho adekvátního následného zpracování (včetně publikace) dojít k obecnému informačnímu efektu spočívajícímu třeba v následné korekci vadného procesního postupu nebo vyjasnění adekvátní interpretace hmotného práva.

K informačnímu efektu může vedle odborné externí formy soudního rozhodnutí vést i jeho populární užití. Typickým příkladem je v tomto směru mediální prezentace soudního rozhodnutí. Na rozdíl od odborné publikace nemá mediální prezentace vliv na praktickou důležitost soudního rozhodnutí ani na jeho dostupnost (dohledatelnost). Soudní rozhodnutí totiž samozřejmě nezíská na odborném uznání tím, že si je jako obecně zajímavé vybere nějaké populární médium. Podobně ani populární publikace obvykle nevede k tomu, že by se zvýšila dohledatelnost soudního rozhodnutí. Mediálně zajímavé případy se totiž obvykle dotýkají věcí, které by byly dostupné odbornému publiku i bez mediální pozornosti.

[24] Srov. Bogoch, B., Peleg, A. Carping, Criticizing and Circumventing: Judges, the Supreme Court and the Media in Israel, in Davis, R., Taras, D. (eds.) Justices and Journalists, Cambdridge: Cambridge University Press, 2017, str. 164.

Informační či naopak entropický efekt zpracování soudního rozhodnutí v takovém případě samozřejmě odpovídá kvalitě novináře a nátuře publika.[25] V porovnání s odbornou publikací nebo jinou externí formalizací soudního rozhodnutí je nutno předložit je veřejnosti v atraktivním zpracování nevyžadujícím rozsáhlé předvědění ohledně okolností příslušného případu ani platného práva. Takové zjednodušení s sebou samozřejmě nese úskalí zkratky a jeho důsledkem může docela snadno být i neúmyslná nebo dokonce záměrná manipulace publika. Zvláštním případem jsou v tomto směru případy soudů, které se z různých důvodů snaží různými nástroji zprostředkovaně ovlivňovat svůj mediální obraz.[26]

Relativně novým druhem populární publikace soudního rozhodnutí je, podobně jako v jiných mediálně vděčných oblastech typu zdravotnictví nebo školství, justiční verze takzvané datové žurnalistiky.[27] Jedná se o publikaci různých analýz vzniklých zpracováním primárních dat, tj. zejm. rozhodovací praxe a různých metadat generovaných justičními orgány. Tyto empiricky se tvářící sekundární statistiky se mohou týkat kvality rozhodovací činnosti, efektivity nebo jiných snadno srozumitelných atributů justiční aktivity. Vcelku snadno tak lze například ukazovat různé korelace, které díky velikosti zdrojových datových souborů mohou dokonce působit dosti věrohodným dojmem.[28]

Typickým příkladem může být třeba korelace mezi denní dobou a výší ukládaných trestů. Na tisících případů z české právní praxe lze empiricky doložit, že tresty ukládané při jednáních konaných před obědem jsou

[25] Komplexní srovnávací pohled na problematiku populárního referování o rozhodovací činnosti soudů přinesl sborník Davis, R., Taras, D. (eds.) Justices and Journalists, Cambdridge: Cambridge University Press, 2017.

[26] Srov. Harada, S. The „Uncomfortable Embrace“: The Supreme Court and the Media in Canada, in Davis, R., Taras, D. (eds.) Justices and Journalists, Cambdridge: Cambridge University Press, 2017, str. 81.

[27] K pojmu datové žurnalistiky a jejím právním souvislostem viz Baranetsky, V. Data Journalism and the Law, Tow/Knight Report, Columbia Journalism School, 2018, dostupné ze cjr.org.

[28] Obtížnost úkolu informovat v mediální zkratce o soudním rozhodování dokládá mimo jiné i existence celosemestrálního speciální kursu, který na toto téma pořádá Shorenseinovo centrum Harvardské univerzity nebo rozsáhlý portál „ A Journalist’s Guide to the Federal Courts“ provozovaný americkým ministerstvem spravedlnosti.

nepoměrně tvrdší než ty, které soudy ukládají v odpoledních hodinách. Důvodem v tomto případě samozřejmě není frustrace hladových soudců, ale skutečnost, že ráno a dopoledne se obvykle projednávají tzv. vazební věci, tj. zpravidla závažnější trestné činy, jejichž obžalovaní pachatelé jsou k soudu předváděni z vazby. Tato podstatná informace však z mediální zkratky může vypadnout stejně snadno, jako z ní pravidelně vypadávají důležité faktory třeba u různých populárních žebříčků úspěšnosti advokátů nebo úmrtnosti ve zdravotnických zařízeních.

Justiční datová žurnalistika samozřejmě nemusí vést pouze k manipulaci publika. Vhodně zvolená statistika může ukazovat též na reálně existující problémy rozhodovací činnosti soudů. Díky dostupnosti judikatury a dalších justičních dat lze na základě analýzy odhalit třeba i neefektivní procesy nebo podezřelé anomálie. Vše v tomto případě záleží, ostatně jako kdekoli jinde, na schopnostech a vůli novináře posoudit adekvátnost příslušných statistických korelací.[29]

Zvláštním typem vnějšího informační efektu hromadného zpracování soudních rozhodnutí je kontrola rozhodovací činnosti soudů. V demokratickém právním státě je samozřejmě tato kontrola svěřena instančně nadřazenému soudu a ve vybraných specifických otázkách mimo vlastní rozhodovací činnost případně též orgánu justičního dozoru. V režimech se zamlženou nebo otevřeně neexistující dělbou moci však může automatizované zpracování soudních rozhodnutí poskytnout vysoce efektivní nástroj k plošné autoritativní kontrole rozhodovací činnosti soudů.

Efektivní kontrola soudnictví stála i za rozvojem právní informatiky v justičním systému komunistického Československa. Zakladatel československé právní informatiky, Viktor Knapp, k tomu v roce 1963 píše[30]: *„Logická kontrola tedy přes omezenost svých možností je důležitým prostředkem nejenk přesnění statistických údajů, ale může být, jak již uvedeno, dost významným prostředkem kontroly dodržování socialistické zákonnosti.*

[29] Blíže viz např. Bradshaw, P. Data Journalism, in Zion, L. Craig, D. Ethics for Digital Journalists: Emerging Best Practices, New York: Routledge, 2015, str. 202.

[30] Viz Knapp, V. O možnosti použití kybernetických metod v právu. Praha : Nakladatelství Československé akademie věd, 1963, str. 20.

Poněvadž pak logická kontrola, byť zatím nebyla prováděna kybernetickými stroji, nepochybně náleží k celkovému procesu použití kybernetické metody v soudní statistice, lze jistě bez nadsázky říci, že praxe a zkušenosti v justiční statistice ukázaly pozoruhodnou novou stránku použití kybernetických metod v právu a ukázaly zejména i to, že rozvážné jejich použití na vhodném místě může sloužit i velmi důležitým cílům politickým, jakým je bez jakékoli pochybnosti kontrola zachovávání socialistické zákonnosti."

Knapp od svých původních vizí automatizace ideologické kontroly justice postupně ustoupil. Ještě v půli osmdesátých let se však vyskytovaly publikace připomínající využitelnost právních informačních technologií a informačních metod pro aktivní distribuci komunistické ideologie v justici. O dvacet let později, než Knapp nastínil vizi automatizované logické kontroly jako metody plnění politického zadání, tak píše tehdejší ředitelka Odboru řízení a justiční informatiky Ministerstva spravedlnosti SSR v časopise Socialistické súdnictvo, že: „*…sa zabezpečí riešenie a realizácia podsystému úloh vyplývajúcich z usnesení najvyšších straníckych a štátnych orgánov ČSSR a SSR, týkajúcich sa činnosti justicie v SSR a vytvorí sa automatizovaný informačný systém spracúvania a vyhodnocovania verbálnych informácií pre potrebu riadiaciej činnosti Ministerstva spravedlivosti SSR.*[31]"

4. LEGITIMITA TLAKU NA KONZISTENCI SOUDNÍHO ROZHODOVÁNÍ

V důsledku technických možností hromadného zpracování dat z rozhodovací činnosti soudů se v posledních letech začíná i v demokratickém právním státě objevovat kvalitativně nový problém tlaku na nezávislost soudního rozhodování. Na rozdíl od shora popsané autoritářské kontroly rozhodovací činnosti však jde v tomto případě spíše o autonomní motivaci soudce indukovanou technologicky determinovanou reflexí dosavadní rozhodovací praxe.

[31] Viz Colotková, Z. Rozvoj automatizovanej sústavy justičnëj informatiky. Socialistické súdnictvo, roč. 37,č. 9, 1985, str. 1.

Typově tento tlak odpovídá shora zmíněnému břemeni, kterému čelí soudce rozhodující v případě, o němž lze důvodně předpokládat, že výrazným způsobem promluví do judikatury. Soudce je v takovém případě autonomně motivován k tomu nepřemýšlet jen o předmětném případě, ale anticipovat i další užití svého rozhodnutí v obecných souvislostech principů rovnosti a právní jistoty.

Efekt anticipované praktické důležitosti soudního rozhodnutí samozřejmě nemá, resp. nesmí, ovlivnit výrok. Pokud by totiž byl výrok rozhodnutí určen namísto okolností konkrétního případu spíše anticipovanou budoucí aplikací příslušného rozhodnutí, jednalo by se o evidentní rozpor s právem na zákonného soudce a obecně s právem na spravedlivý proces (k obecnému problému s principem dělby moci viz výše). Účastníci řízení by totiž v takovém případě mohli oprávněně namítat, že soudce zde ve skutečnosti nerozhodoval o jejich právech, ale o nějakých hypotetických budoucích případech. Zprostředkovaný tlak principů rovnosti a právní jistoty projevuje se zde spíš v konstrukci odůvodnění, jehož zamýšleným adresátem nemusí být jen účastníci řízení nebo nadřízený soud, ale může jím být též okruh všech možných potenciálních adresátů příslušných právních pravidel.

Výše zmíněný nový typ tlaku působený hromadným zpracováním dat produkovaných soudy jde v tomto směru ještě dál a může se, i přes veškerou snahu soudce, reálně projevit dokonce i v samotném rozhodování o právech, tj. v konstrukci výroků. Velmi snadno se totiž dají zpracovat např. data mapující různé souvislosti rozhodovací činnosti každého jednotlivého soudce, a to za libovolně dlouhou dobu. Vedle víceméně jednoduchých statistik ukazujících třeba na výkonnost soudce, mohou být předmětem datové analýzy i velmi komplexní otázky samotného rozhodovací činnosti včetně vývoje jeho právních názorů, inspirace odbornou či jinou literaturou, způsobů reakce na rušící rozhodnutí vyšší instance apod.

V soudcovské profesi, kde je osobní i profesní konzistentnost brána za ultimativní ctnost, může mít tento typ datové transparentnosti fatální

důsledky.[32] Může totiž vést k vědomému nebo podvědomému potlačování těch složek soudcovského rozhodování, které, přestože se staví jakoby na odpor vůči shora opakovaně zmiňovaným principům rovnosti a právní jistoty, mají v systému justice a práva jako takového nezastupitelné místo – kreativity a intuice.[33]

Problém vztahu mezi konzistentností soudce na jedné straně a jeho kreativitou a intuicí na straně druhé samozřejmě není v právu ničím novým. Jedná se o standardní projev generického konfliktu mezi dvěma ze tří fundamentálních účelů práva, tj. Jistotou a spravedlností. V kontinentální evropské právní kultuře je regulatorní kreativita a intuice svěřena do rukou zákonodárce a až jeho prostřednictvím (resp. prostřednictvím neurčitého pojmu) pak je k realizaci jejích projevů vyzván soudce. Neznamená to však, že by se měl soudce zabývat jen „slepou dedukcí" vedoucí k „mechanické jurisprudenci.[34]"

Je z podstaty vadné domnívat se, že evropský soudce musí být při výkladu neurčitého pojmu nebo jiné právní metafory v čase dokonale konzistentní. Pokud by časová konzistentnost výkladu byla vůlí zákonodárce, vyžádal by si ji přeci autoritativně konkrétním pojmem nebo jeho legální definicí. Užití neurčitého pojmu naproti tomu dokonce přímo zakládá povinnost soudce průběžně posuzovat, i na základě vlastní zkušenosti a intuice, zda není důvod přehodnotit kvůli (nikoli nutně objektivně evidentním) měnícím se okolnostem jeho význam. Soudce, který na základě toho, že v čase nabývá životní zkušenost či odborné znalosti nebo sleduje vývoj společnosti, průběžně mění názor na adekvátní

[32] Z jiného úhlu pohledu se problémem motivace soudce konzistentností zabývají William Richman a William Reynolds v kritické práci Richman, W. M., Reynolds, W. L. Injustice on Appeal, Oxford: Oxford University Press, 2013, str. 95.

[33] Mariusz Golecki píše o projevech kreativity a intuice jako o „emocích" a argumentuje jejich nezastupitelnost v soudcovském rozhodování v kapitole Golecki, M. J. Between Nomos and Pathos: Emotions in Aristotelian Theory of Adjudication and the Dual Process Theory, in Huppes-Cluysenauer, L., Coelho, N. (eds.) Aristotle on Emotions in Law and Politics, Springer, 2018, str. 435.

[34] Tento pojem užívá v souvislosti s kritikou přehnaného tlaku na logickou konzistentnost soudního rozhodování Roger Cotterrell v práci Cotterrell, R. B. M., The Politics of Jurisprudence: A Critical Introduction to Legal Philosophy, Philadelphia: University of Pennsylvania Press, 1992, str. 158.

interpretaci právních metafor, přitom samozřejmě nejedná ani v nějakém neproporcionálním rozporu s požadavkem právní jistoty nebo rovnosti před zákonem.

Přese všechno výše uvedené ale není žádnému normálně myslícímu soudci příjemná představa, že bude ve svém rozhodování evidentně nekonzistentní. Nejde v tomto případě ani tak o nějakou zásadní změnu názoru na otázky života a smrti, k níž by zřejmě u soudce skutečně nemělo dojít, ale o konzistentnost v partikulárních záležitostech marginálního významu, které však se přímo projevují při každodenním rozhodování konkrétních případů. Dostupnost dat o předchozí rozhodovací činnosti soudce a všech možných více či méně souvisejících metadat ve spojení se stále dokonalejšími analytickými nástroji totiž umožňují stavět soudce před zrcadlo vlastní konzistentnosti i v sebemenší drobnosti. Pod vlivem takového tlaku pak může racionalita, tj. Konzistentnost, u soudce vcelku snadno zvítězit nad jeho intuicí či kreativitou.

Technologií motivované vítězství konzistentnosti nad intuicí nemusí se jevit na první pohled nijak problematicky. Ve fungování mechanismu právní regulace však jde o přinejmenším diskutabilní systémové vychýlení rovnováhy mezi třemi Radbruchovými účely ve prospěch jistoty na úkor (nejisté) spravedlnosti a (rovněž nejisté) praktické užitečnosti.[35] Pohledem výše zmíněných základních premis právní informatiky pak je omezení intuice či kreativity ve prospěch konzistentnosti dokonce jednoznačně vadné, protože brání přirozenému projevu unikátní schopnosti života reagovat na změnu (aktuální nebo očekávanou) produkcí originální informace.[36]

Shora popsaný vysoce problematický charakter hloubkové analýzy rozhodovací činnosti soudů jdoucí na úroveň jednotlivých soudců reflektuje z demokratických právních států jako první na světě aktuální francouzská zákonná úprava.[37]Ta zakazuje takovou práci s daty pocházejícími ze soudní rozhodovací praxe (tj. se soudními rozhodnutími a dalšími

[35] Srov. Schmidt, A. Radbruch in Cyberspace: About Law-System Quality and ICT Innovation. Masaryk University Journal of Law and Technology, 2009,č. 3(2), str. 195.

[36] Srov. Wiener, N. Cybernetics: Or the Control and Communication in the Animal and the Machine. Cambridge : MIT Press, 1961, str. 11.

metadaty), která ve výsledku vede k profilování soudců za účelem předvídání budoucího jejich rozhodování. Příslušné ustanovení má následující podobu (překlad RP): „*Zpracování osobních údajů soudců nebo soudních úředníků za účelem srovnávání nebo předvídání jejich skutečné nebo domnělé úřední činnosti se zakazuje.*“

Tento kategorický zákaz, stíhaný dokonce trestní sankcí, se stal předmětem rozhořčené kritické debaty v Evropě i USA.[38] Kritici této úpravě nejčastěji vyčítají fatální neproporcionalitu vzhledem k právu na svobodu informací (včetně práva získávat a zpracovávat údaje o činnosti orgánů veřejné moci) a právu na svobodu projevu. Pohledem právní informatiky však k takovému zákazu profilování existuje docela dobrý důvod, a to shora popsané neadekvátní zesílení tlaku principů rovnosti a právní jistoty a omezení možnosti a povinnosti soudce zapojit do rozhodování též z podstaty nejistou a nepředvídatelnou spravedlnostní intuici. Čím kvalitnější totiž bude systém predikující z dosavadních údajů budoucí rozhodovací praxi (ve smyslu komplexnosti dat a sledovaných parametrů), tím složitěji bude muset soudce vůči tomu, kdo nebude spokojen s příslušným rozhodnutím, argumentovat odchýlení se od jeho predikce založené výlučně na empirické analýze a logické extrapolaci stávající rozhodovací praxe.

Nabízí se v tomto směru srovnání například s diagnostickými systémy užívanými v medicíně. Zde se autonomní algoritmy vcelku úspěšně používají například v oblasti diagnostiky nádorových onemocnění. Platí ale přitom, že i špičkový systém založený na rozsáhlé datové základně a vyspělé autonomní technologii nikdy nedosáhne kvality špičkového lidského diagnostika, který vedle empirických poznatků a zkušenosti používá též počítači nedostupnou metodu originální (kreativní) tvorby diagnostické informace.[39]

---

[37] Viz čl. 33 zákona o reformě justice ze dne 23. března 2019 (LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice), dostupný na www.legifrance.gouv.fr.

[38] Viz např. Langford, M. Madsen, M. R. France Criminalises Research on Judges, verfassungsblog.de, 22 červen 2019.

Dosavadní zkušenost s použitím této technologie ukazuje, že její nasazení tam, kde je k dispozici kvalitní lékař, může být ze statistického hlediska kontraproduktivní – lidský lékař je totiž nucen zdůvodňovat pacientovi případnou svoji odchylnou diagnózu, to dokonce pod tíhou vlastní odpovědnosti. Ve výsledku pak může dokonce dojít k tomu, že se role vymění, lékař rezignuje na kreativitu a pouze kontroluje, zda úsudek systému nevykazuje nějaké fatální nedostatky.

Je-li francouzský zákaz diskutabilní, není to dle našeho názoru problém premisy ale přinejhorším jen použité metody řešení neadekvátního tlaku na nezávislost soudce. Francouzský právotvůrce zde zakázal zpracování justičních údajů a publikaci rozhodovacích predikcí, tj. vydal se cestou absolutního omezení dostupnosti empirických dat hodnotících konzistentnost rozhodovací činnosti soudce. Jinou možností, vyžadující však změnu chápání principu rovnosti a právní jistoty ve spojení s pragmatickou reflexí adekvátního významu neurčitého pojmu a jeho vývoje v čase, je akceptace určité míry explicitně nezdůvodněné nekonzistence. To se může týkat samotného rozhodování nebo i jen jeho odůvodňování.

V tomto případě francouzský právotvůrce naznal, že adekvátním řešením problému technologicky determinovaného tlaku na nezávislost soudu je eliminace příslušné technologie, což je diskutabilní přístup typově podobný prohibici. Na druhou stranu jde však v tomto případě o pochopitelnou snahu reagovat, byť možná až příliš opatrně, na hrozbu nezávislosti justice, o jejíž závažnosti, resp. toxicitě, zatím nemáme odpovídající poznatky. Vcelku pochopitelná je v tomto případě též zjevná nedůvěra francouzského právotvůrce v instantní evoluci relativně tradicionalistické francouzské právní kultury ve smyslu shora zmíněné změny chápání principů rovnosti a právní jistoty, resp. možností jejich oslabení pouze v důsledku běhu času. Pokud zde tedy francouzský právotvůrce dospěl k pragmatickému závěru, že dostupnost nástrojů

[39] Viz např. Miller, D. D., Brown, E. W. Artificial Intelligence in Medical Practice: The Question to the Answer? The American Journal of Medicine, roč. 131,č. 2, str. 129 nebo Krittanawong, C. The rise of artificial intelligence and the uncertain future for physicians, European Journal of Internal Medicine,č. 48, str. 13.

profilujících soudy a soudce vzhledem k jejich rozhodovací činnosti přinese víc škody (shora popsaným neadekvátním tlakem na nezávislost soudního rozhodování) než užitku (ten by zde zřejmě spočíval v těžko předem definovatelném zvýšení míry transparentnosti justice), těžko lze tomuto závěru něco zásadního vytknout.

5. SHRNUTÍ

V tomto příspěvku jsme se zabývali problematikou informačního efektu automatizovaného zpracování judikatury. Dospěli jsme zde k nikoli překvapivému závěru, že informační efekt judikatury je dán kombinací informační kvality příslušných soudních rozhodnutí a mechanismu jejich následného zpracování.

Konkrétně jsme se věnovali informační analýze podstatných rozdílů mezi soudním rozhodnutím (judikátem) a judikaturou jakožto pramenem práva. Upozornili jsme v tomto ohledu na problém legitimního primárního účelu soudního rozhodnutí, kterým je organizovat systém účastníků řízení. Informační efekt judikatury jako pramene práva je pak až sekundárním projevem nikoli přímo soudního rozhodnutí jako takového (nebo dokonce jeho právní věty), ale informačního komplexu ustálené rozhodovací praxe a různých aspektů její informační expozice veřejnosti.

Zvláštní pozornost jsme věnovali též novým vysoce přesným metodám hloubkové prediktivní analýzy rozhodovací činnosti konkrétního soudce nebo úřední osoby. Všímali jsme si potenciálního informačního, resp. entropického, efektu této relativně nové technologie, která se již stala předmětem vysoce diskutabilní zákonné restrikce. Dospěli jsme v tomto směru k závěru, který úplně nekoresponduje s aktuální mezinárodní kritikou, a to že tato restrikce nepředstavuje evidentní regulatorní exces a může být pragmaticky důvodná a právně legitimní.

6. SEZNAM POUŽITÉ LITERATURY

[1] Alexy, R. On the Structure of Legal Principles. Ratio Iuris. 2000, roč. 13, č. 3.

[2] Baranetsky, V. Data Journalism and the Law, Tow/Knight Report, Columbia Journalism School, 2018, dostupné ze cjr.org.

[3] Bobek, M., Kühn, Z. a kol. Judikatura a právní argumentace, 2. vyd. Praha: Auditorium 2013.

[4] Bogoch, B., Peleg, A. Carping, Criticizing and Circumventing: Judges, the Supreme Court and the Media in Israel, in Davis, R., Taras, D. (eds.) Justices and Journalists, Cambdridge: Cambridge University Press, 2017.

[5] Bradshaw, P. Data Journalism, in Zion, L. Craig, D. Ethics for Digital Journalists: Emerging Best Practices, New York: Routledge, 2015.

[1] Cole, B. Shepardizing: A Comparison of the Printed Citators and On-Line Shepardizing Services. Legal Reference Services Quarterly. 1988, roč. 7, č. 2-4.

[2] Colotková, Z. Rozvoj automatizovanej sústavy justičněj informatiky. Socialistické súdnictvo, roč. 37, č. 9, 1985.

[3] Cotterrell, R. B. M., The Politics of Jurisprudence: A Critical Introduction to Legal Philosophy, Philadelphia: University of Pennsylvania Press, 1992.

[4] Davis, R., Taras, D. (eds.) Justices and Journalists, Cambdridge: Cambridge University Press, 2017.

[5] Golecki, M. J. Between Nomos and Pathos: Emotions in Aristotelian Theory of Adjudication and the Dual Process Theory, in Huppes-Cluysenauer, L., Coelho, N. (eds.) Aristotle on Emotions in Law and Politics, Springer, 2018.

[6] Harada, S. The „Uncomfortable Embrace“: The Supreme Court and the Media in Canada, in Davis, R., Taras, D. (eds.) Justices and Journalists, Cambdridge: Cambridge University Press, 2017.

[7] Holländer, P. Filosofie práva. Plzeň : Aleš Čeněk, 2006.

[8] Kelsen, H. Pure theory of Law, New Jersey: The Lawbook Exchange, 2005.

[9] Knapp, V. O možnosti použití kybernetických metod v právu. Praha: Nakladatelství Československé akademie věd, 1963.

[10] Knapp, V. Teorie práva. Praha: C.H. Beck, 1991.

[11] Krittanawong, C. The rise of artificial intelligence and the uncertain future for physicians, European Journal of Internal Medicine, č. 48.

[12] Langford, M. Madsen, M. R. France Criminalises Research on Judges, verfassungsblog.de, 22 červen 2019.

[13] Miller, D. D., Brown, E. W. Artificial Intelligence in Medical Practice: The Question to the Answer? The American Journal of Medicine, roč. 131, č. 2.

[14] Molek, P., Polčák, R. Poskytnout nebo chránit? Brno: Nejvyšší správní soud, 2017.

[15] Neff, V. Filozofický slovník pro samouky aneb Antigorgias. Praha: Mladá fronta, 1993.

[16] Paliwala, A. A History of Legal Informatics. Zaragoza : Prensas de Universitarias de Zaragoza, 2010.

[17] Polčák, R. Informační teorie práva, in Bobek, M., Molek, P., Šimíček, V. Komunistické právo v Československu, Brno: Masarykova univerzita, 2009.

[18] Polčák, R. Internet a proměny práva, Praha: Auditorium, 2012, str. 23.

[19] Richman, W. M., Reynolds, W. L. Injustice on Appeal, Oxford: Oxford University Press, 2013.

[20] Schmidt, A. Radbruch in Cyberspace: About Law-System Quality and ICT Innovation. Masaryk University Journal of Law and Technology, 2009, č. 3(2).

[21] Schrödinger, E. What is Life. Cambridge : Cambridge University Press, 1992.

[22] Wiener, N. Cybernetics: Or the Control and Communication in the Animal and the Machine. Cambridge : MIT Press, 1961.

---

https://doi.org/10.5817/RPT2019-2-3

OTÁZKY ODPOVĚDNOSTI UMĚLÉ INTELIGENCE ZA ZÁSAH DO AUTORSKÉHO PRÁVA

JAN ZIBNER[1]

ABSTRAKT

Příspěvek se soustředí na otázky, které vyvstávají v oblasti umělé inteligence při zkoumání odpovědnosti za zásah do autorského práva. S ohledem na nárůst využití umělé inteligence při vytváření autorských děl je v této souvislosti podstatné analyzovat potenciální zásah do autorského práva v procesu tvorby a odpovědnostní režim, který by se v takovém případě uplatnil. V rámci toho je důležité zkoumat jak druh odpovědnosti, odpovědné entity, tak i stávající řešení náhrady škody při dostatečné reflexi vlastností a potenciálu umělé inteligence, jakož i případné návrhy pro futuro v dané oblasti. Příspěvek v první části představí hlavní otázky, které v této problematice vyvstávají. Ve druhé části pak příspěvek představí stávající řešení dříve uvozených otázek, na což naváže třetí část věnovaná návrhům na vhodnější právní úpravu de lege ferenda.

KLÍČOVÁ SLOVA

Odpovědnost, umělá inteligence, zásah do autorského práva

[1] JUDr. Jan Zibner – prezenční doktorský student na Ústavu práva a technologií (školitel JUDr. Matěj Myška, Ph.D.). Téma disertační práce *Umělá inteligence jako technologická výzva autorskému právu*. Příspěvek je podpořen projektem specifického výzkumu MUNI/A/1339/2018, e-mail: jan.zibner@mail.muni.cz.

ABSTRACT

The paper focuses on the issues in the area of artificial intelligence when examining the liability for the copyright infringement. Since the use of artificial intelligence in the creation of copyrighted works is increasing, it is essential to analyze the potential copyright infringement in the process of creating as well as the liability regime that would apply in such a case. Moreover, it is important to examine the type of liability, the liable entities and the solutions of compensation, with a reflection of the characteristics and potential of artificial intelligence, as well as possible proposals pro futuro. In the first part, the paper presents the main questions that arise in this area. In the second part, the paper will present the existing solutions to the previously raised questions, which will be followed by the third part devoted to proposals de lege ferenda.

KEYWORDS

Artificial Intelligence, Copyright Infringement, Liability

1. UMĚLÁ INTELIGENCE JAKO SOUČÁST TVŮRČÍHO PROCESU

Umělá inteligence je stále více zapojována do tvůrčího procesu autorských děl.[2] Díky možnostem a potenciálu, které umělá inteligence skýtá, je v oblasti literární či umělecké umělá inteligence využívána pro vytváření autorských děl nejrůznějšího druhu i kvality bez ohledu na účel či následné využití takových děl. Obecně vzato, umělá inteligence (coby software s tvůrčími možnostmi)[3] je v rámci daného procesu využívána ve dvojí podobě, a to jako specializovaný software, nebo v rámci interaktivních platforem s intenzivní rolí vlastních uživatelů takových

[2] K otázce výtvorů umělé inteligence jako autorských děl obecně srov. GINSBURG, Jane C; BUDIARDJO, Luke A. Auhors and Machines [online]. *Berkeley Technology Law Journal*. 2019, roč. 34, č. 2. Columbia Public Law Research Paper No. 14-597; *SSRN*, publikováno 20. 8. 2018, 116 s [cit. 10. 3. 2019].

[3] Vnímání umělé inteligence jako softwaru je jen jedním z mnoha významů, se kterými odborná veřejnost pracuje (srov. SCHAFER, Burkhard a kol. A Fourth Law of Robotics? Copyright and the Law and Ethics of Machine Coproduction. *Artificial Intelligence and Law*, 2015, č. 23, s. 217-240). K tvůrčím možnostem umělé inteligence srov. ZIBNER, Jan. *Tvůrčí činnost autora v kontextu technologického vývoje* [online]. Rigorózní práce. Masarykova univerzita, Právnická fakulta, 2018, s. 75 a násl. [cit. 10. 3. 2019].

platforem.[4] Co je těmto způsobům zapojení umělé inteligence do tvůrčího procesu společné, je „funkční" závislost na již existující bázi autorských děl, případně i dalších výtvorů bez autorskoprávní ochrany. Tyto datasety jsou různými způsoby využívány pro tvorbu výstupů umělé inteligence v podobě autorských děl, a to skrze modelování tzv. tvůrčího rámce sloužícího jako mezistupeň ve tvůrčím procesu, od kterého se odvíjí výsledná podoba autorských děl vytvořených umělou inteligencí.[5] Užívání takových datasetů však zejména v rozsahu předmětů autorskoprávní ochrany podléhá legálním pravidlům a mechanismům vztahujícím se k nakládání s autorskými díly. S tím se potažmo pojí i jednotlivé otázky z oblasti odpovědnosti za případný zásah do autorských práv dotčených autorů, které jsou v dnešní době stále více relevantní.[6]

Příspěvek se proto věnuje analýze odpovědnosti za případný zásah do autorských práv v případech, kdy umělá inteligence představuje jeden z pilířů tvůrčího procesu při vytváření autorských děl, ať už skrze fungování umělé inteligence jako specializovaného softwaru, nebo integrované součásti interaktivních platforem. V první části se příspěvek soustředí na vymezení základních otázek z oblasti odpovědnosti za zásah do autorského práva, které poté řeší *de lege lata*. V poslední části se

[4] K tomuto dělení obecně srov. ZIBNER, Jan. Subjects' Relevance Within an AI-included Creative Process. In: SCHWEIGHOFER, Erich a kol. (eds.). *Internet of Things: Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019*. Bern: Editions Weblaw, 2019. s. 401-406 (vč. zde uvedených zdrojů).

[5] Umělá inteligence je v dnešní době založena zejména na kombinačním či analogickém postupu tvůrčího procesu při současné nemožnosti tvořit mimo předem definovaný rámec. Tato myšlenka tvoří základní pilíř fungování umělé inteligence (obecně srov. DREYFUS, Hubert L. *What Computers Still Can't Do: A Critique of Artificial Reason*. Revised edition. Cambridge: The MIT Press, 1992, 429 s; POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 171).

[6] S ohledem na nárůst využití umělé inteligence vznikají postupně např. národní výzkumné zprávy upozorňující (směrem k orgánům Evropské unie) na takový nárůst a snažící se více či méně vhodným způsobem představit řešení nejpalčivějších otázek. V České republice byla taková zpráva publikována v roce 2018 (obecně srov. KRAUSOVÁ, Alžběta a kol. Výzkum potenciálu rozvoje umělé inteligence v České republice Analýza právně-etických aspektů rozvoje umělé inteligence a jejích aplikací v ČR [online]. *Úřad vlády České republiky*, publikováno 10. 12. 2018, 72 [cit. 10. 3. 2019]). Stejně tak se objevují tendence o nastavení funkčního autorskoprávního rámce pro tuto situaci (srov. AIPPI. Resolution 2019 - Study Question: Copyright in Artificially Generated Works [online]. *AIPPI*, publikováno 18. 9. 2019 [cit. 10. 3. 2019]).

příspěvek soustředí na případnou vhodnou úpravu daných otázek *de lege ferenda* na základě dříve dovozených závěrů.

Příspěvek mimo jiné navazuje na předcházející výzkum a jednotlivé závěry autora v dané oblasti a na vybraných místech na ně odkazuje. S ohledem na teritorialitu autorského práva se příspěvek soustředí na právní řád České republiky, potažmo právní řád Evropské unie, který do značné míry ovlivňuje podobu autorského práva v České republice. V teoretických aspektech se příspěvek opírá též o obecnou právní doktrínu.

1.1 OTÁZKY ODPOVĚDNOSTI UMĚLÉ INTELIGENCE ZA ZÁSAH DO AUTORSKÝCH PRÁV

Hovoříme-li o interaktivních platformách,[7] dá se tvůrčí proces demonstrovat následujícím způsobem. Poté, co je vytvořena umělá inteligence (software), je potřeba definovat formu výstupů, tedy autorských děl, která jsou s její pomocí a s využitím dat jednotlivých uživatelů vytvářena. Za tímto účelem je umělá inteligence „trénována" jednou z mnoha technik[8] na již existujících datasetech v podobě autorských děl či jiných výtvorů. Na základě nich umělá inteligence vytváří generický předobraz budoucího výstupu, jakýsi tvůrčí rámec (jak uvedeno shora), v jehož rámci jsou vytvářena výsledná autorská díla. Tento tvůrčí rámec poté slouží v rozsahu interaktivních platforem pro nahrávání uživatelských dat, která jsou přetvářena v jeho mezích. I v případě umělé inteligence jako specializovaného softwaru je takový tvůrčí rámec využíván, nicméně s ohledem na tvůrčí proces v takovém případě již rámec nekooperuje s uživatelskými daty, nýbrž je přetvářen pro potřeby konkrétního výstupu.[9] Přístup umělé inteligence k datasetům a jejich zpracování je však v obou případech stejný.

---

[7] Mezi příklady takových platforem patří *Humtap* (dostupné z: https://humtap.com/); *Amper Music* (dostupné z: https://ampermusic.com/); *Shelley* (dostupné z: http://shelley.ai/); *DeepArt* (dostupné z: https://deepart.io/).

[8] K povedenému přehledu základních technik „trénování" umělé inteligence obecně srov. LE, James. The 10 Deep Learning Methods AI Practitioners Need to Apply [online]. *Medium*, publikováno 17. 11. 2017 [cit. 10. 3. 2019].

[9] Srov. ZIBNER, 2019, op. cit., s. 402.

Při užívání autorských děl cizích autorů jako datasetů nebo báze pro vytváření zmíněného tvůrčího rámce a pro následnou tvorbu autorských děl lze (v souladu s naukou o právní odpovědnosti a jejích prvcích)[10] obecně identifikovat následující problematické otázky, které je potřeba postupně zodpovědět při snaze o nalezení konkrétního řešení odpovědnosti za zásah do autorského práva.

Způsob zásahu do autorského práva. Primárně je potřeba dobrat se závěru ohledně vlastního způsobu zásahu do autorského práva. Ať už nahlédneme do vlastních ochranných ustanovení autorského zákona[11],[12] či mezi jednotlivé výjimky a omezení autorského práva coby legální tituly užití díla,[13] samotný zásah do autorského práva je podmíněn relevantním užitím díla, popř. specifickým nakládáním s dílem. Primárně je proto potřeba určit, jakým způsobem dochází k relevantnímu užití autorských děl v rámci vytváření tvůrčího rámce, popř. jakým způsobem je s autorskými díly nakládáno. Dospějeme-li v tomto kroku k závěru, že k žádnému způsobu užití díla nedochází, popř. nedochází k zásahu do autorského práva, není třeba věnovat se otázkám dalším, které jsou existencí zásahu do autorského práva nutně podmíněny, neboť při neexistenci zásahu do autorského práva nelze založit za takový zásah odpovědnost.

Odpovědná entita. Do samotného tvůrčího procesu je vedle umělé inteligence jako jedné z potenciálně odpovědných entit zapojeno nemalé množství subjektů s víceméně jasnou úlohou; od tvůrců, programátorů a dalších společných autorů dané umělé inteligence na jedné straně, kteří definují rozsah autorských děl v rámci zmíněných datasetů, přes operátory umělé inteligence, kteří se mohou z první skupiny subjektů vydělit, až po případné uživatele, kteří mohou daný tvůrčí proces iniciovat, popř. určovat výslednou formu autorských děl vytvářených umělou inteligencí. V rámci

[10] Srov. GERLOCH, Aleš. *Teorie práva*, 4. upravené vydání. Plzeň: Aleš Čeněk, 2007, s. 178 a násl.; HARVÁNEK, Jaromír a kol. *Teorie práva*. Plzeň: Aleš Čeněk, 2013, s. 355 a násl.; KNAPP, Viktor. *Teorie práva*, 1. vydání. Praha: C.H. Beck, 1995, s. 200 a násl.

[11] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“ či jen „AZ“).

[12] Srov. § 11 odst. 3 AZ, § 40 a násl. AZ.

[13] Srov. § 29 a násl. AZ.

této otázky je potřeba zkoumat podíl daných entit na tvůrčím procesu a jejich legitimní postavení v rámci obecného i odpovědnostního právního vztahu, a to jak ve vztahu k dotčeným autorským dílům, tak ve vztahu k jednotlivým způsobům užití.

Odpovědnostní režim. Odpovědnost za zásah do autorského práva je jistě odpovědností deliktní; *Gerloch* i *Harvánek* v rámci takové odpovědnosti explicitně zmiňuje i odpovědnost za zásah do nehmotného statku.[14] Tato deliktní odpovědnost poté může být rozdělena na základě typu deliktu na trestněprávní, správněprávní, i civilněprávní, neboť ve všech třech oblastech se lze standardně setkat s postihy za zásah do autorského práva.[15] Podle odpovědí na předchozí dva body je na tomto místě nutno zkoumat řešení v rámci jednotlivých režimů a posoudit případné specifické pojmové znaky pro aplikaci adekvátních odpovědnostních institutů.

Odpovědnost k náhradě škody a vydání bezdůvodného obohacení. S ohledem na jednotlivé funkce právní odpovědnosti[16] a s ohledem na pragmatické tendence autorů usilovat především o zadostiučinění v podobě finančního odškodnění je třeba zabývat se též řešením odpovědnosti k náhradě škody a vydání bezdůvodného obohacení, které standardně sekundují odpovědnosti za zásah do autorského práva a jsou autorským zákonem předpokládané jako jedny z hlavních kompenzačních mechanismů.

2. MOŽNÉ ŘEŠENÍ DE LEGE LATA

Na tomto místě je nutno soustředit se na zodpovězení výše stanovených otázek dle aktuálně účinné právní úpravy. Postupně jsou proto analyzovány dané otázky a představeno aktuální řešení v závislosti na příslušných argumentačních tendencích. Analýza zároveň předpokládá zásah do autorského práva, tj. nepočítá s datasety a *priori* skládajícími se

[14] Srov. GERLOCH, 2007, op. cit., s. 182; HARVÁNEK, 2013, op. cit., s. 356.

[15] Odpovědnost plynoucí z disciplinárního deliktu (která se mnohdy řadí k civilněprávní, správněprávní a trestněprávní větvi odpovědnosti) lze ponechat pro svou povahu a význam při dalším rozboru stranou pro přílišnou vzdálenost autorskému právu.

[16] Srov. ŠKOP, Martin; MACHÁČ, Petr. *Základy právní nauky*. Praha: Wolters Kluwer ČR, 2011, s. 165.

z volných děl nebo děl užitých na základě licence v adekvátním rozsahu, kde k autorskoprávnímu zásahu nedochází.

2.1 ZPŮSOB ZÁSAHU DO AUTORSKÉHO PRÁVA

Autorské právo je v obou svých integrálních součástech, osobnostní a majetkové, právem výlučným náležejícím autorovi, popř. vykonavateli práv v určitém rozsahu. Výkon těchto práv je kromě osoby autora, popř. vykonavatele práv teoreticky možný jen na základě adekvátního právního titulu v podobě zákonné, či smluvní. V opačném případě platí limity nastavené jak v rámci osobnostních, tak majetkových práv. Zatímco osobnostní práva autora pamatují na zásah do díla tak, že jej podmiňují svolením, popř. je zakázáno užívat dílo způsobem nesnižujícím hodnotu díla,[17] majetková práva jsou podmíněna jen autorskoprávně relevantním způsobem užití díla.[18] Na toto právo jsou pak navázána jiná autorským zákonem předpokládaná a stanovená majetková práva finančního charakteru, tzv. jiná majetková práva.[19]

Analýza osobnostních práv v našem případě je relevantní zejména co do ochrany integrity díla. Jak uvádí doktrína, i zařazování díla do souboru či jiná tvůrčí činnost v kontextu daných děl může být zásahem do integrity díla.[20] Nicméně taková tvůrčí činnost musí zároveň nutně představovat zásah do formálního či obsahového pojetí díla, tj. do charakteru literárního, uměleckého nebo vědeckého daného díla.[21] Zatímco zásahy, které se tohoto charakteru dotknou jen minimálně, nelze za takový zásah považovat pro

[17] Srov. § 11 odst. 3 AZ. Na tomto místě je navíc nutno upozornit na odlišnost *svolení* a *licence* v rámci autorského práva. Zatímco *svolení* se týká možnosti zásahu do osobnostních práv, *licence* dle § 2358 a násl., resp. § 2371 a násl. Zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“ nebo „OZ“) se týká majetkových práv, když explicitně pokrývá právo dílo užít. Dle doktríny svolení není a nemůže být pro svou povahu integrální součástí licence a je třeba udělovat je zvlášť (srov. TELEC, Ivo; TŮMA, Pavel. *Autorský zákon: komentář*. 2. vydání. Praha: C.H. Beck, 2019, s. 150).

[18] Srov. § 12 a násl. AZ.

[19] Srov. § 24 a násl. AZ.

[20] Srov. TELEC; TŮMA, 2019, op. cit., s. 150.

[21] Odborná literatura se v tomto názoru opírá zejména o rozsudek Městského soudu v Praze sp. zn. 13 Co 216/90. K charakteru tvůrčí činnosti srov. ZIBNER, 2018, op. cit., s. 13 a násl.

kvalitativní nedostatek tvůrčí činnosti.[22] Uvedené se navíc týká i případné fragmentace díla v rámci „trénování“ umělé inteligence, jakož i doplňování díla o případné nutné prvky pro umožnění takového „trénování“ a pro nutnou indexaci pro vytváření tvůrčího rámce.[23] Stejně tak uvedené dopadá i na případné adaptace formátů daných děl při zachování shora uvedených podmínek v rozsahu charakteru díla.[24] Od zásahu do hodnoty díla se pak bude odvíjet i posuzování, zda je dílo užíváno dehonestujícím způsobem, což v našem případě nejspíš naplněno nebude.

Co se týče zařazování do díla souborného, které by bylo zásahem do osobnostních práv bez řádného svolení či jiného právního titulu, na tomto místě je nutno podotknout, že ač nelze takový způsob vytváření tvůrčího rámce a *priori* vyloučit, nejedná se o standardní postup. Tvůrčí rámec je vytvářen spíše na základě metadat, která umělá inteligence získává z jednotlivých autorských děl, nikoliv vytvářením díla souborného.

Majetková práva stojí na autorskoprávně relevantním způsobu užití díla. Autorský zákon aktuálně operuje s demonstrativním výčtem způsobů užití díla, které postupně reagují na technologický vývoj.[25] Základní aspekt, který je v tomto kontextu třeba zkoumat, je, zda užívání autorských děl pro potřeby vytváření tvůrčího rámce je užitím autorskoprávně relevantním, tj. takovým, které přísluší výlučně autorovi a které může v případě existence bez adekvátního právního titulu znamenat zásah do autorského práva. Na tomto místě lze odkázat na předchozí závěry autora a shrnout následující.[26] Aktuální otevřený výčet jednotlivých způsobů užití díla v autorském zákoně není uspokojivým řešením, neboť ponechává až přílišný prostor interpretaci; zejména s nástupem a rozšiřováním možností umělé

[22] Srov. TELEC; TŮMA, 2019, op. cit., s. 151.

[23] Srov. TELEC; TŮMA, 2019, op. cit., s. 151 a násl.

[24] Srov. TELEC; TŮMA, 2019, op. cit., s. 152.

[25] Srov. § 12 AZ a například *právo na sdělování veřejnosti*, které na svém významu nabylo zejména až s příchodem rozhlasového a televizního vysílání, vlivem čehož byl s rekodifikací autorského práva výčet způsobů užití díla rozšířen, aby držel krok s technologickým vývojem.

[26] Srov. ZIBNER, Jan. Dopady digitalizace do autorského práva. In: BEJČEK, Josef a kol. (eds.). *Dny práva 2018: Část IV. Dopady digitalizace do oblasti soukromého práva*. 2019, 1. vydání. Edice Scientia, sv. č. 653, s. 120 a násl.

inteligence jako relativně nové technologie.[27] Taková interpretace může totiž vést ke dvěma odlišným závěrům. Pokud budeme argumentovat vytěžováním dat a zpracováním metadat daných autorských děl jako dalším ze způsobů užití díla (autorským zákonem nezmíněným, nicméně s účinností směrnice o autorském právu na digitálním trhu[28] předpokládaným)[29], bude se jednat o takové užití díla, které je podmíněno smluvním titulem či titulem, jenž nabízejí případné výjimky a omezení. Pokud však shoda na vytěžování dat coby užití díla panovat nebude (např. s poukazem na zjišťování a užívání myšlenky, nikoliv vyjádření díla), pak se v případě vytváření tvůrčího rámce o užití díla jednat nebude a ač se budou jednotlivá autorská díla užívat za účelem vytváření tvůrčího rámce, nebude mít takové počínání autorskoprávní relevanci.[30] O zásah do výlučného práva dílo užít se tak jednat nebude. V rámci této argumentace je však nutno vyloučit jak argument užívání hudebního stylu, který je v daných autorských dílech zachycen, popř. napodobeniny takového hudebního stylu v autorských dílech vytvořených umělou inteligencí,[31] tak i teoretický koncept užití díla bez reprodukce či zobrazení vyjádření (*non-display use of work*), který v tomto případě selže pro nedostatek legitimity.[32]

---

[27] Na problematickou interpretaci upozorňují například *Telec a Tůma* (srov. TELEC; TŮMA, 2019, op. cit., s. 171 a násl.).

[28] Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES.

[29] Samotná směrnice zakotvuje mandatorní výjimku pro vytěžování textu a dat při zachování specifických stanovených podmínek. Z charakteru výjimek a omezení coby základního autorskoprávního institutu je však nutno dovozovat, že tyto výjimky a omezení nové způsoby užití autorského díla nezakládají, nýbrž jen poskytují právní titul při nedostatku smluvního oprávnění u již existujících způsobů užití děl a mnohdy se specifickým účelem (srov. PRCHAL, Petr. Výjimky a omezení práva autorského, náhradní odměny. In: SRSTKA, Jiří a kol. *Autorské právo a práva související.* Vysokoškolská učebnice. Praha: Leges, 2017, s. 124 a násl.).

[30] V takovém případě však postrádá smyslu zakotvování specifické výjimky pro vytěžování textu a dat, který předpokládá shora uvedená směrnice, neboť je bezvýznamné zavádět právní titul k jednání bez právní relevance.

[31] Neboť tzv. pastiš primárně není zásahem do autorského práva.

[32] Srov. BORGHI, Maurizio; KARAPAPA, Stavroula. Non-display Uses of Copyright Works: Google Books and Beyond. *Queen Mary Journal of Intellectual Property*. 2011, roč. 1, č. 1, s. 52.

2.2 ODPOVĚDNÁ ENTITA

Budeme-li odpovídat na předešlou otázku tak, že se v daném případě bude jednat o zásah do autorského práva, je nutno hledat odpovědnou entitu, popř. odpovědné entity za takový zásah. Jak výše uvedeno, takových entit se k úspěšné odpovědi nabízí celá řada, a to teoreticky včetně umělé inteligence. Pokud je totiž umělá inteligence nadaná jistou volností a skrze hluboké učení a podobné metody „trénování" může v rámci předem definovaného prostředí dospívat k neočekávaným závěrům či ke kombinaci známých závěrů, může být vina na straně umělé inteligence, resp. nemusí být vina nutně na straně operujícího subjektu.[33] V tomto kontextu se jedná o skutečně nový regulatorní fenomén, jak podotýkají *Grimmellmann*[34] či *Polčák*[35]. S ohledem na komplexitu umělé inteligence, užitých systémů, jakož i vazeb na jednotlivé subjekty v tvůrčím procesu může být odpověď složitější.

Co do samotné umělé inteligence, *de lege lata* u ní odpovědnost hledat nelze, a to z toho důvodu, že odpovědnost je právní vztah, který k určení „viníka" potřebuje subjekt, který bude shledán odpovědným a ponese odpovídající následky.[36] Umělá inteligence však subjektem dle aktuálních možností českého právního řádu není pro nedostatek právní osobnosti jakožto pasivní stránky právní způsobilosti,[37] ač by *pro futuro* teoreticky být nositelem právní osobnosti mohla s oporou v institutu svěřenského fondu či tzv. jiných právnických osob, se kterými český právní řád na několika

[33] K diferenciaci počítačové tvůrčí činnosti srov. ZIBNER, 2018, op. cit., s. 85 a násl. (vč. uvedených zdrojů); ZIBNER, Jan. Artificial Intelligence: A Creative Player in the Game of Copyright. *European Journal of Law and Technology*. 2019, roč. 10, č. 1, s. 1-20.

[34] Srov. GRIMMELMANN, James. Copyright for Literare Robots. *Iowa Law Review.* 2016, roč. 101, č. 2, s. 657.

[35] Srov. POLČÁK, Radim. Odpovědnost umělé inteligence a informační útvary bez právní subjektivity. *Bulletin advokacie*. 2018, č. 11, s. 23.

[36] Srov. GERLOCH, 2007, op. cit., s. 178 a násl.; HARVÁNEK, 2013, op. cit., s. 355; KNAPP, 1995, op. cit., s. 200.

[37] Obecně srov. ZIBNER, Jan. Akceptace právní osobnosti v případě umělé inteligence. *Revue pro právo a technologie* [online]. 2018, roč. 9, č. 17, s. 19-49 [cit. 10. 3. 2019].

místech počítá. Umělá inteligence je prozatím stále objektem právního vztahu, který odpovědným shledán být z povahy věci nemůže.[38]

Co se aktuálních subjektů odpovědnostního vztahu týče, tam, kde interaktivní platformy operují s uživatelskými daty, teoreticky lze počítat se skupinou uživatelů, která se na tvůrčím procesu podílejí do jisté míry srovnatelně se skupinou autorů, popř. operátorů umělé inteligence. Nicméně ačkoliv se v jejich případě jedná o iniciátory konkrétního tvůrčího procesu směřujícího k výslednému autorskému dílu a subjekty, které dotvářejí samotný tvůrčí rámec, čímž je jejich role ve tvůrčím procesu podstatná, na vytváření samotného rámce se nepodílejí. Výjimkou mohou být platformy či modely, kde by uživatelé nejprve vytvářeli daný rámec na základě vlastních preferencí s využitím přednastavených možností umělé inteligence k jeho vyhledávání a následnému užívání.[39] Se stejným argumentem je třeba odmítnout i podíl uživatelů na případném dehonestujícím užívání autorských děl, neboť přicházejí-li uživatelé daných platforem do styku až s tvůrčím rámcem, neužívají autorská díla užitá k jeho vytvoření, nýbrž generický obraz v něm zachycený, a nelze proto odpovědnost shledávat u takových subjektů. Uvedené platí zejména z důvodu přílišné vzdálenosti jednání uživatelů od škodlivého následku v podobě vytvoření tvůrčího rámce, od kterého se odpovědnostní vztah odvíjí.

Podstatnou složku této otázky představují autoři umělé inteligence, kteří konkretizují obsah vytvářeného tvůrčího rámce konkrétně (vybírání konkrétních děl a cílových datasetů, např. skladeb konkrétního autora), popř. obecně (sběr takových autorských děl bez ohledu na konkrétní obsah). I když bychom mohli argumentovat tím, že při dostatečné míře volnosti umělé inteligence (např. při vytváření tvůrčího rámce na základě vágního a obecně určeného datasetu složeného např. z hudebních děl vzniklých v letech 1991-2000, či z hudebních děl, které odpovídají určitému hudebnímu žánru) neexistuje zaměření autora či operátora umělé inteligence k zásahu do autorských práv, či že to je právě až umělá

[38] Srov. GRIMMELMANN, 2016, op. cit., s. 658.

[39] Takových platforem si však autor aktuálně není vědom.

inteligence, která skrze hluboké učení vybírá v několika následných fázích konkrétní díla, autoři umělé inteligence budou stále odpovědni, a to vlivem institutu přičitatelnosti. Občanský zákoník zde totiž upozorňuje na to, že jen osoba může mít a vykonávat práva předpokládaná právním řádem;[40] pokud někdo zřídí právo nebo uloží povinnost tomu, co není osoba, pak se takové prvky přičítají osobě, které podle povahy právního případu náleží.[41] Podle doktríny takovou osobou bude většinou vlastník umělé inteligence,[42] resp. v našem případě příhodnější osoba autora či operátor umělé inteligence jakožto osoba, která iniciovala vytváření tvůrčího rámce, bude-li se taková osoba lišit od osoby autora.[43] Uvedené platí zejména s důrazem na blízkost subjektu k umělé inteligenci, škodlivému jednání a vyvolanému následku, jakož i s důrazem na adekvátní reakci odpovědnostního schématu.

Taková osoba však většinou nebude vystupovat sama, nýbrž bude s ohledem na komplexnost umělé inteligence spolupracovat s dalšími osobami. V rámci takových „společenství" pak bude potřeba dle míry účasti na závadném jednání určit odpovědný subjekt, popř. odpovědné subjekty dle proporcí jednotlivých dále stanovených odpovědnostních režimů, a to s apelem na právní jistotu, jakož i alokaci rizika. Primární nastavení odpovědnosti v takovém případě je solidární, tj. škůdci odpovídají společně a nerozdílně, přičemž jsou-li přítomny důvody zvláštního zřetele hodné (např. při oddělitelnosti jednotlivých jednání v rámci vytváření tvůrčího rámce), může soud rozhodnout, že daný škůdce nahradí škodu podle své účasti na škodlivém následku, popř. dle míry pravděpodobné účasti na škodlivém následku; při vědomé účasti na způsobení škody či při

[40] Srov. § 17 OZ.

[41] Srov. § 17 odst. 2 OZ.

[42] Srov. LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1-654). Komentář*. 1. vydání. Praha: C.H. Beck, 2014, s. 145.

[43] Na tomto místě nelze si nepovšimnout jisté podobnosti s určováním autorství k výslednému autorskému dílu vytvořenému umělou inteligencí, jak je aplikují ve Velké Británii (srov. čl. 9 odst. 3 Copyright, Designs and Patents Act 1988, as amended, 1988 c. 48).

podněcování však taková mitigace neplatí.[44] Mezi danými škůdci pak působí jakýsi regres dle § 2916 občanského zákoníku.

2.3 ODPOVĚDNOSTNÍ REŽIM

V návaznosti na shora uvedené můžeme rozlišovat při zásahu do autorského práva tři druhy odpovědnosti (odpovědnostní režimy), a to civilněprávní, trestněprávní a správněprávní. Při společné aplikaci pouze na fyzické a právnické osoby se civilněprávní odpovědnost odvíjí od § 40 a násl. autorského zákona (doprovázená odpovědností k náhradě škody a k vydání bezdůvodného obohacení dle občanského zákoníku), což poté doplňuje standardní správněprávní odpovědnost dle § 105a a § 105b autorského zákona. Trestněprávní odpovědnost je konstituována zejména skutkovou podstatou zakotvenou v § 270 trestního zákoníku[45]. Všechny tři odpovědnostní režimy si pro komisivní povahu zásahu do autorského práva lze v našem případě představit.

Civilněprávní odpovědnost je založena na (potenciálním) neoprávněném zásahu do autorského práva, jak je o něm pojednáno výše (srov. bod 2.1 příspěvku). Jednotlivé nároky jsou pak upraveny autorským zákonem. Tato objektivní odpovědnost je pak doprovázena nároky z titulu odpovědnosti k náhradě škody a vydání bezdůvodného obohacení podle občanského zákoníku.[46] V rámci odpovědnosti za zásah do autorského práva lze oprávněnou osobou (tedy originárním nositelem práv, popř. adekvátních vykonavatelů autorských práv) aktivně uplatňovat veškeré nároky, které předpokládá § 40 autorského zákona,[47] protože jak shora uvedeno, o zásah do autorského práva se může jednat, stejně jako existuje možnost určení odpovědných subjektů. V tomto rozsahu odpovědnost nepředstavuje větší výzvu. Problematické však mohou být aspekty odpovědnosti k náhradě

[44] Srov. § 2915 OZ.

[45] Zákon č. 40/2009, trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník" nebo „TZ").

[46] Plyne tak z § 40 odst. 4 AZ.

[47] *Leška* v této souvislosti zdůrazňuje komplexní úpravu autorského zákona v otázce nároků (srov. LEŠKA, Rudolf. Ochrana práva autorského. In: SRSTKA, Jiří a kol. *Autorské právo a práva související.* Vysokoškolská učebnice. Praha: Leges, 2017, s. 242).

škody a vydání bezdůvodného obohacení. O těch je pojednáno v rámci následující otázky. Jak upozorňuje *Leška*, odpovědnost za zásah do osobnostních práv (i s ohledem na výše uvedené) je však budována na subjektivním principu a je třeba hledat zavinění obdobně jako je tomu obecně v rámci odpovědnosti k náhradě škody.[48]

Nutno navíc zdůraznit, že formulace § 40 autorského zákona je vágní co do samotné definice škůdce, jelikož samotné ustanovení počítá jen s tím, že dané nároky se aktivizují ve chvíli, kdy je do práva autora potenciálně zasaženo, a neurčuje přitom, jakým způsobem, kým či z jakého důvodu. S ohledem na to je pak možné i v rámci konstituování tohoto druhu odpovědnosti shledávat nejrůznější (níže uvedené) modely odpovědnosti umělé inteligence za použitelné i zde v rozsahu způsobení škodlivého následku.

Správněprávní odpovědnost je v tomto případě opřená explicitně o neoprávněné užití autorského díla se sankcí v podobě pokuty, která v případě fyzických i právnických a podnikajících fyzických osob činí až 150.000,- Kč.[49] Takto vybrané pokuty jsou přitom příjmem *Státního fondu kultury České republiky*.[50] S ohledem na charakter sankce lze mít za to, že pokuta bude ukládána zejména ve vztahu k vlastníkovi umělé inteligence, resp. autorovi softwaru či platformy, v rámci kterých se umělá inteligence takovým závadným způsobem bude užívat. Správní orgán totiž s ohledem na právní jistotu i evidentní snahu o promptní řešení bude nejspíše hledat subjekt, který bude nejjistějším a zjevným způsobem spojen s tvůrčím procesem a neprokáže-li tento subjekt, že operátorem umělé inteligence a tím, kdo iniciuje tvorbu tvůrčího rámce, bude místo něj jiná osoba, bude to právě tento subjekt, který bude shledán odpovědným.

Správněprávní odpovědnost na rozdíl od civilněprávní nedopadá na neoprávněný zásah jakožto širší pojem, jak je o něm pojednáno výše.[51] Je tak činěno zejména z důvodu odlišné funkce a zájmu správněprávní

[48] *Leška* tak činí s odkazem na § 2894 odst. 2 OZ (srov. LEŠKA, 2017, op. cit., s. 247).

[49] Srov. § 105a odst. 2 a § 105b odst. 2 AZ.

[50] Srov. § 105c AZ.

[51] § 105a a § 105b AZ totiž odkazují na neoprávněný zásah jen v intencích § 43 a § 44 AZ.

odpovědnosti, která cílí na odstranění závadného stavu a reparaci škůdce spíše než na kompenzaci nositele práv. Z toho důvodu je výčet povinností restriktivní ve vztahu k civilněprávní odpovědnosti. Navíc aplikace odpovědnosti civilněprávní a uplatnění nároků plynoucích z takové odpovědnosti nevylučuje nikterak odpovědnost správněprávní.

V případě trestní odpovědnosti je třeba naplnit základní kvalifikační předpoklady pro aplikaci skutkové podstaty zmíněné v § 270 trestního zákoníku. Navíc je třeba upozornit na to, že se může jednat dokonce o kvalifikovanou skutkovou podstatu,[52] a to z důvodu charakteru obchodní činnosti či podnikání, které se s provozem daného softwaru, platformy či nakládáním s autorským dílem vytvořeným umělou inteligencí bude pojit;[53] o značném či velkém prospěchu, škodě či rozsahu a dalších možnostech pro naplnění znaků kvalifikované skutkové podstaty nemluvě. Samotná skutková podstata *porušení autorského práva, práv souvisejících s právem autorským a práv k databázi* chrání danou tvůrčí činnost ztělesněnou v autorském díle, přičemž svou dispozicí odkazuje do autorského zákona, a to jak do sféry osobnostních, tak majetkových práv autora.[54] Podstatné je v tomto případě sledovat subjektivní stránku, která je založena na úmyslné formě zavinění a pachatelova vědomí, že jde skutečně o autorské dílo.[55] Navíc, jak uvádí odborná literatura, není nutné, aby pachatel znal dokonale přesný rozsah práv konkrétního autora, neboť stačí vědomí nakládání s dílem (bez ohledu na záměr).[56] V pojednávaném případě si proto lze takovou odpovědnost přestavit.

Kritické se však mohou ukázat dva okamžiky aplikace trestněprávní odpovědnosti. Zatímco v případě správněprávní odpovědnosti je správním trestem „jen“ pokuta, u které prakticky nebude větší snaha správních

[52] Ve smyslu § 270 odst. 2 TZ.

[53] Srov. ŠÁMAL, Pavel a kol. *Trestní zákoník*, 2. vydání. Praha: C.H. Beck, 2012, s. 2731 a násl.

[54] Srov. ŠÁMAL, 2012, op. cit., s. 2737; PÚRY, František. Trestněprávní aspekty autorského práva a práv souvisejících s autorským právem. In: SRSTKA, Jiří a kol. *Autorské právo a práva související*. Vysokoškolská učebnice. Praha: Leges, 2017, s. 354.

[55] Srov. ŠÁMAL, 2012, op. cit., s. 2753.

[56] Ibid.

orgánů o přesnou lokalizaci škůdce, trestní právo působí subsidiárně jako *ultima ratio* a dopady do soukromé sféry jsou s ohledem na charakter ukládaného trestu razantně vyšší. Právě z toho důvodu bude potřeba odpovědný subjekt lokalizovat přesně a s podrobnou argumentací, což se může ukázat jako problém. S ohledem na mnohdy intenzivní spolupráci autorů a případných operátorů umělé inteligence ve tvůrčím procesu bude nejspíše uplatňován režim spolupachatelů trestného činu, popř. odpovídající režim účastenství[57] s e zohledněním individuální role jednotlivých subjektů, jakož i konkrétního podílu na tvůrčím procesu ve vztahu k vytváření tvůrčího rámce. Druhým kritickým okamžikem může být teoreticky materiální stránka trestného činu. Podle trestního zákoníku je trestní odpovědnost založena jen v případech společensky škodlivých (podle dřívější terminologie společensky nebezpečných) dle povahy a závažnosti trestného činu.[58] Je otázkou, do jaké míry bude společenská škodlivost shledávána v jednání spočívajícím v „užívání" autorských děl pro vytváření tvůrčího rámce. Stejně tak je otázkou, do jaké míry bude takové posuzování závislé na komerčních aspektech interaktivních platforem nebo vědeckém charakteru softwaru pracujícího s umělou inteligencí, či na kvalitě výsledných autorských děl a jejich případné podobě s díly „užívanými" při vytváření rámce. Aktuálně lze mít za to, že na závěr o společenské nebezpečnosti bude mít vliv rozsah užívaných autorských děl stejně jako povaha tvůrčího rámce a následné operativnosti softwaru (ať už v podobě interaktivní platformy, či v podobě specializovaného softwaru).

2.4 ODPOVĚDNOST K NÁHRADĚ ŠKODY A VYDÁNÍ BEZDŮVODNÉHO OBOHACENÍ

Nárok na náhradu škody a na vydání bezdůvodného obohacení je sekundární složkou odpovědnosti za zásah do autorského práva. Na rozdíl od výše popsané objektivní složky odpovědnosti a odpovědnosti k vydání

[57] Srov. § 23 a násl., jakož i § 22 odst. 2 TZ.

[58] Srov. § 12 odst. 2 TZ. Navíc tento materiální korektiv trestných činů a trestní odpovědnosti je mohutně zdůrazňován judikaturou (mezi všemi srov. usnesení Nejvyššího soudu ze dne 17. 8. 2011, sp. zn. 5 Tdo 751/2011).

bezdůvodného obohacení je ale odpovědnost k náhradě škody obecně stižena principem subjektivní odpovědnosti a je třeba hledat zavinění obdobně jako v případě trestněprávního postihu, tam, kde není stanoveno jinak.[59] Autorský zákon stanovuje, že nositel práv se místo skutečně ušlého zisku[60] může domáhat náhrady ušlého zisku ve výši odměny, která by byla obvyklá za získání licence v době neoprávněného nakládání s dílem a na bezdůvodném obohacení se může domáhat vydání dvojnásobku licenční odměny, která by byla obvyklá za užití předmětu ochrany takovým způsobem (jelikož jak upozorňuje odborná literatura, obvykle se při kalkulaci nevychází z ušlého zisku, neboť je složité prokázat, že by při neexistenci neoprávněného užití skutečně došlo k užití na základě licence)[61]. Blíže však není stanoven režim náhrady škody ani konkrétní odpovědnostní titul, resp. aplikovatelnost zvláštních ustanovení občanského zákoníku, které se jednotlivými druhy odpovědnosti za škodu zabývají. Z těchto zvláštních ustanovení přicházejí v potaz teoreticky dvě možnosti, a to aplikace škody z provozní činnosti[62] či aplikace škody způsobené věcí[63].

Škoda z provozní činnosti se při bližším prozkoumání jeví jako nevhodná, a to s ohledem na provoz k výdělečné činnosti (tj. obchodní a podnikatelskou činnost)[64] a náhradu škody, kterou právě až vlastní provozní činnost způsobí. S ohledem na konstrukci platforem či specializovaného softwaru s umělou inteligencí ale škoda nevzniká až činností provozu platformy nebo softwaru, ale již dříve při jejich vytváření. Argumentovat by se dalo provozem umělé inteligence jako do jisté míry autonomního systému, nicméně v takovém okamžiku argumentace selže nepřítomností výdělečné činnosti, která je přítomna až při inkorporaci tvůrčího rámce do výsledku, neboť se odvíjí až od výsledku a příslušných

[59] Srov. § 2895 OZ.

[60] V kontextu § 2952 OZ, podle kterého se hradí skutečná škoda a to, co poškozenému ušlo (ušlý zisk).

[61] Srov. LEŠKA, 2017, op. cit., s. 246.

[62] Srov. § 2924 OZ.

[63] Srov. § 2936 a násl. OZ.

[64] Srov. HULMÁK, Milan a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055-3014). Komentář*. 1. vydání. Praha: C.H. Beck, 2014, s. 1601.

aktivit subjektů ve vztahu k němu. Jak navíc uvádí *Vojtek*, škoda musí mít podstatu v samotné činnosti (a to bez ohledu na zavinění v takovém případě, neboť daný druh odpovědnosti je vystaven jen na základě protiprávního následku),[65] což další aplikaci vylučuje. Není proto třeba zkoumat ani liberačně/exkulpační možnosti daného ustanovení, ani případný zvlášť nebezpečný charakter provozu.[66]

Druhou možností je aplikace odpovědnosti k náhradě škody způsobené věcí. Podle § 2937 občanského zákoníku platí, že pokud škodu způsobí věc sama od sebe (což se s ohledem na autonomní charakter umělé inteligence může stát), nahradí škodu ten, kdo nad věcí měl mít dohled, popř. vlastník věci. Touto konstrukcí se blížíme k přičitatelnosti dle § 17 občanského zákoníku. Část odborné veřejnosti se k tomuto řešení přiklání v kontextu obecné odpovědnosti za provoz umělé inteligence a autonomních systémů zejména s poukazem na obecnou známost tohoto institutu a celkovou jednoduchost řešení, což lze jen kvitovat.[67] Na druhou stranu je tomuto řešení vytýkána obecně vágní formulace povinného dohledu a nerozlišování iniciátoru podnětů, na základě kterého umělá inteligence jedná a působí škodu. Zde však problematická aplikace tohoto institutu nekončí, neboť terminologické problémy může způsobovat podřazení umělé inteligence pod samotný rozsah věci, na kterou se ustanovení váže, resp. pod vlastnictví. Při analýze relevantních ustanovení[68] a adekvátní odborné literatury[69] totiž odpověď na tuto otázku může být přinejmenším sporná. Ačkoliv podle autora je možno umělou inteligenci považovat za věc, problém může být s určováním vlastníka, jelikož vlastnické právo k nehmotným statkům je s novou koncepcí pojetí věci v občanském

[65] Srov. TOMÍŠEK, Jan. Jaký je ideální model odpovědnosti za autonomní systém? *Revue pro právo a technologie* [online]. 2018, roč. 9, č. 18, s. 42 [cit. 10. 3. 2019]; VOJTEK, Pavel. Náhrada újmy z provozních činností (vybrané otázky). *Soudní rozhledy*. 2015, č. 6, s. 202 a násl.

[66] Srov. § 2925 OZ.

[67] Srov. TOMÍŠEK, 2018, op. cit., s. 44 a zde uvedení autoři.

[68] Srov. § 489, § 495, § 496, § 977 a § 1011 OZ.

[69] Obecně srov. LAVICKÝ, 2014, op. cit., s. 1750-1753 (§ 495), s. 1753-1759 (§ 496); HORÁK, Ondřej; DOSTALÍK, Petr. Věc v právním slova smyslu v novém občanském zákoníku z právněhistorické perspektivy. *Časopis pro právní vědu a praxi*. 2013, č. 1, s. 14-21.

zákoníku nejasné a spíše nebude akceptovatelné. Na druhou stranu tyto prvotní interpretační potíže daného ustanovení lze dle přesvědčení autora překonat teleologickým výkladem, neboť účelem vykládaného ustanovení je chránit před rizikem, které může věc představovat, jakož i umožnit poškozenému kompenzaci vůči osobě, která porušila povinnost dohledu nad věcí.[70] I v tomto případě se pak jedná o objektivní odpovědnosti při současné možnosti liberace/exkulpace prokázáním nezanedbaného náležitého dohledu. Co může být dalším problematickým aspektem v tomto případě, je evidentní aplikovatelnost ustanovení v případech, kdy je škoda způsobena vlivem povahy věci a nikoliv tam, kde věc slouží jen jako prostředek ke způsobení škody jejím uživatelem (tj. v našem případě spoluautory umělé inteligence a subjekty vytvářejícími tvůrčí rámec).

Další možností aplikovanou při odpovědnosti k náhradě škody tedy může být jen obecný odpovědnostní režim ve smyslu § 2915 v návaznosti na § 2910 občanského zákoníku, který bude uplatněn při nemožnosti podřadit nastalou situaci pod jedno ze speciálních ustanovení. Tento režim již předpokládá zavinění a počítá explicitně i s mnohostí osob potenciálně odpovědných, jak výše uvedeno.

Co do bezdůvodného obohacení, literatura upozorňuje, že standardně může pro výpočet výše bezdůvodného obohacení sloužit minimální distribuční odměna, běžně účtovaná vůbec za možnost zařadit dílo do nabídky elektronické služby.[71] Takový teoretický model je dost podobný vytváření tvůrčího rámce, ačkoliv neodpovídá celkově. Při aplikaci fikce dvojnásobku však již nelze současně ze stejného titulu požadovat též paušalizovanou náhradu škody, jelikož kompenzační princip je již v takové kalkulaci zahrnut.[72] Ustanovení občanského zákoníku ohledně bezdůvodného obohacení se pak v našem případě použijí standardním způsobem a není třeba věnovat jim na tomto místě více pozornosti.

---

[70] Srov. HULMÁK, 2014, op. cit., s. 1640.

[71] Srov. LEŠKA, 2017, op. cit., s. 247.

[72] Ibid. Plyne tak mimo jiné z rozsudku Soudního dvora Evropské unie (pátého senátu) ze dne 25. 1. 2017. Věc C-367/15. *Stowarzyszenie „Oławska Telewizja Kablowa" proti Stowarzyszenie Filmowców Polskich*.

3. NÁVRHY DE LEGE FERENDA

Ačkoliv se nastíněné aktuální řešení může jevit při troše vůle jako dostatečné a adekvátní situaci, právní řád se neustále vyvíjí v reakci na technologický pokrok. V tomto ohledu je třeba zamýšlet se nad tím, zda i představený rámec je skutečně dostatečný s ohledem například na právní jistotu, spravedlnost a další základní premisy práva.

Již první otázka ukázala, že je třeba vyřešit bližší identifikaci zásahu do autorského práva, neboť užití díla v tomto případě, byť se na první pohled může zdát jako jasné, nemusí být nutně naplnitelné s ohledem na proces vytváření tvůrčího rámce. Podle aktuálního výkladu lze spíše usuzovat, že o užití díla v daném případě nepůjde, ergo nebude zasaženo do výlučného majetkového práva autora dílo užít a další odpovědnostní aspekty není třeba zkoumat. S odkazem na demonstrativní výčet a nešťastný legislativní mechanismus lze do budoucna v této otázce doporučit explicitní zařazení takového užití děl mezi legální výčet, popř. dovozovat v odborné literatuře či v judikatuře takové užití za autorskoprávně relevantní, leč nezmíněné v zákonném výčtu v § 12 autorského zákona. Ať už však bude tento výčet obohacen, či nikoliv, obě možnosti s sebou ponesou nutný přesah do zajetých interpretačních kolejí, které budou muset být změněny, jako tomu bylo například při nastavení práva na sdělování veřejnosti v návaznosti na nástup rozhlasového a televizního vysílání. Stejně tak obě možnosti ovlivní odpovědi na navazující otázky v rámci posuzování odpovědnosti, ať již v pozitivním, či negativním slova smyslu, což je potřeba před zvolenou pozicí řádně zhodnotit. Autor se kloní k tomu, aby užití díla tímto způsobem bylo užitím autorskoprávně relevantním, pro které je třeba smluvní či zákonný právní titul, s případnými odpovědnostními peripetiemi, a doporučuje jeho adekvátní reflexi v autorském zákoně.

Ani druhá otázka není podle přesvědčení autora uspokojující, neboť s ohledem na právní jistotu neposkytuje jednoznačnou odpověď na hledání odpovědné entity. Ano, můžeme vyloučit z okruhu odpovědných entit samotnou umělou inteligenci, nicméně zbývající okruh subjektů je stále příliš široký, což vede například k problémovému dokazování zavinění tam,

kde je potřeba k naplnění předpokladů odpovědnosti,[73] což jednak stěžuje postavení poškozeného nositele práv, jednak může umocňovat nechtěné praktiky ze strany těch, kteří daný tvůrčí rámec vytvářejí. V souvislosti s třetí otázkou, která se zaměřuje na vlastní odpovědnostní režim je pak záhodnou explicitně stanovit v tomto smyslu odpovědnou osobu napříč jednotlivými režimy. Ideálním řešením se jeví kolektiv autorů umělé inteligence v případě, kdy nelze přesně určit subjekt dávající příkaz umělé inteligenci k vytváření tvůrčího rámce. Na druhou stranu, ani v případě, kdy bude možno takový subjekt lokalizovat, neměl by být takový subjekt odpovědný za zásah do autorského práva i k náhradě škody či k vydání bezdůvodného obohacení sám, neboť interaktivní platforma či specializovaný software jsou vždy dílem více autorů a odpovědnost by se měla dělit dle podílu na vytváření umělé inteligence. Nelze totiž mít za to, že ten, kdo nedá příkaz k vytváření tvůrčího rámce, leč podílí se na vytváření umělé inteligence, nemá a *priori* vztah k zahrnutí datasetů do takového rámce. Umělá inteligence je v takových případech již od počátku vytvářena s takovým cílem.

Odpovědnostní režimy a odpovědnost k náhradě škody a vydání bezdůvodného obohacení jsou pak další výzvou. Ačkoliv se jejich hodnocení odvíjí od jasných odpovědí na předchozí dvě otázky, v rámci civilněprávní odpovědnosti lze shledávat jistou potíž. Režim odpovědnosti za škodu způsobenou věcí nemusí vždy vyhovovat. Stejně tak obecný odpovědnostní režim v kontextu prevenční povinnosti[74] nemusí reflektovat specifika umělé inteligence a vytváření tvůrčího rámce, zejména v rozsahu autonomie a možností, které umělá inteligence představuje. Obecný odpovědnostní režim slouží jako „pojistka“ a obecný rámec pro otázky, které nelze hojit skrze speciální ustanovení. Ta se vlivem společenského či jiného vývoje dostávají do občanského zákoníku, a stejně tak by tomu mělo být i v tomto případě.[75] S ohledem na komplexnost mechanismů umělé inteligence a strukturu subjektového aparátu se totiž problematickou jeví

[73] Srov. HUBBARD, F. Patrick. "Sophisticated Robots": Balancing Liability, Regulation, and Innovation. *Florida Law Review* [online]. 2014, roč. 66, č. 5, s. 1828 [cit. 10. 3. 2019].

[74] Srov. § 2900 a násl. OZ.

[75] Na uvedené upozorňuje i *Grimmelmann* (srov. GRIMMELMANN, 2016, op. cit., s. 661).

zejména neurčité dokazování souvislostí a jednotlivých jednání vedoucích k zásahu do autorského práva, v čemž lze vidět argumentační a interpretační slabinu. Do budoucna proto autor navrhuje specifické řešení této situace v rozsahu odpovědnosti za užívání autorských děl či obecně předmětů duševního vlastnictví v rámci vytváření tvůrčího rámce (stejně jako se odborná veřejnost snaží navrhovat více či méně schůdná řešení např. v oblasti autonomních zařízení a vozidel)[76]. Specifickou otázkou je pak odbornou veřejností často diskutované pojištění v případech zahrnujících umělou inteligenci, které má zhojit do jisté míry nejistotu poškozených a usměrnit jejich složitou důkazní pozici ve vztahu k nejrůznějším škodám. V tomto případě stejně jako v ostatních případech odpovědnosti za umělou inteligenci může pojištění pomoci co do finanční kompenzace, nicméně na rozdíl od provozů a obchodních činností, kde se mnohdy pojištění dá realizovat s ohledem na finanční možnosti daných subjektů, v případě interaktivních platforem je otázkou, nakolik je povinné pojištění těchto specifických případech adekvátní hodnotě výstupů umělé inteligence a možnostem provozovatelů platforem. Autor soudí, že při správném uchopení specifické odpovědnosti v takovýchto případech není institut pojištění potřebný.

4. ZÁVĚR

Příspěvek se snažil přispět k diskuzi na téma odpovědnosti umělé inteligence v případě zásahu do autorského práva a snažil se předestřít řešení vymezených otázek odpovědnosti *de lege lata* a *de lege ferenda* s možnostmi úprav dotčených ustanovení. V případě, že dojde k zásahu do autorského práva činností, která zahrnuje umělou inteligenci, je podstatné zejména určit čtyři otázky, které pomohou v určení vhodného odpovědnostního režimu. První z nich je identifikace vlastního zásahu do autorského práva vč. správného zhodnocení autorskoprávně relevantního způsobu užití díla. Na to pak navazuje otázka určení odpovědné entity, kterých v daném případě může být více a mohou odpovídat společně a nerozdílně, popř. dle míry účasti na způsobené škodě. Po určení

[76] Obecně srov. TOMÍŠEK, 2018, op. cit.; POLČÁK, 2018, op. cit.

odpovědné entity pak přichází na řadu samotná kvalifikace odpovědnostního režimu, který v daném případě lze spatřovat jak civilněprávní, správněprávní, tak i trestněprávní se svými specifiky a možnostmi, které nabízejí pro poškozeného nositele práv. Zejména s civilněprávním odpovědnostním režimem se pak pojí odpovědnost k náhradě škody a vydání bezdůvodného obohacení, kde se jako problematický aktuálně jeví zejména aspekt odpovědnosti k náhradě škody pro spornou aplikovatelnost speciálních ustanovení, které v souvislosti s odpovědností umělé inteligence často skloňuje odborná veřejnost.

Příspěvek se snažil poukázat na argumentační možnosti při hledání odpovědí na dané otázky stejně jako navrhnout adekvátní úpravu problematických fází analýzy odpovědnosti a příslušných ustanovení. Aktuální právní úprava totiž sice poskytuje relativně komplexní možnosti v otázce odpovědnosti v případech, jako je ten, který posloužil k analýze, avšak nenabízí explicitní řešení problematických aspektů a dává prostor více či méně širokým interpretacím, které nejen, že nepřidávají právní jistotě, ale mohou též vést ke špatnému zhodnocení situace. Takový stav ale nelze shledávat uspokojivým.

5. SEZNAM ZDROJŮ

5.1 MONOGRAFIE

[1] DREYFUS, Hubert L. *What Computers Still Can't Do: A Critique of Artificial Reason*. Revised edition. Cambridge: The MIT Press, 1992, 429 s. ISBN 9780262540674.

[2] GERLOCH, Aleš. *Teorie práva*. 4. upravené vydání. Plzeň: Aleš Čeněk, 2007, 344 s. ISBN 978-80-7380-023-9.

[3] HARVÁNEK, Jaromír a kol. *Teorie práva*. Plzeň: Aleš Čeněk, 2013, 439 s. ISBN 978-80-7390-458-9.

[4] HULMÁK, Milan a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055-3014). Komentář*. 1. vydání. Praha: C.H. Beck, 2014, 2072 s. ISBN 978-80-7400-287-8.

[5] KNAPP, Viktor. *Teorie práva*, 1. vydání. Praha: C.H. Beck, 1995, 247 s. ISBN 80-7179-028-1.

[6] LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1-654). Komentář*. 1. vydání. Praha: C.H. Beck, 2014, 2400 s. ISBN 978-80-7400-529-9.

[7] LEŠKA, Rudolf. Ochrana práva autorského. In: SRSTKA, Jiří a kol. *Autorské právo a práva související*. Vysokoškolská učebnice. Praha: Leges, 2017, 416 s (s. 242-250). ISBN 978-80-7502-240-0.

[8] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, 392 s. ISBN 978-80-87284-22-3.

[9] PRCHAL, Petr. Výjimky a omezení práva autorského, náhradní odměny. In: SRSTKA, Jiří a kol. *Autorské právo a práva související*. Vysokoškolská učebnice. Praha: Leges, 2017, 416 s (s. 124-157). ISBN 978-80-7502-240-0.

[10] PÚRY, František. Trestněprávní aspekty autorského práva a práv souvisejících s autorským právem. In: SRSTKA, Jiří a kol. *Autorské právo a práva související*. Vysokoškolská učebnice. Praha: Leges, 2017, 416 s (s. 341-368). ISBN 978-80-7502-240-0.

[11] ŠÁMAL, Pavel a kol. *Trestní zákoník*. 2. vydání. Praha: C.H. Beck, 2012, 3614 s. ISBN 978-80-7400-428-5.

[12] ŠKOP, Martin; MACHÁČ, Petr. *Základy právní nauky*. Praha: Wolters Kluwer ČR, 2011, 196 s. ISBN 978-80-7357-709-4.

[13] TELEC, Ivo; TŮMA, Pavel. *Autorský zákon: komentář*. 2. vydání. Praha: C.H. Beck, 2019, 1295 s. ISBN 978-80-7400-748-4.

5.2 ČLÁNKY, PŘÍSPĚVKY VE SBORNÍCÍCH

[14] BORGHI, Maurizio; KARAPAPA, Stavroula. Non-display Uses of Copyright Works: Google Books and Beyond. *Queen Mary Journal of Intellectual Property*. 2011, roč. 1, č. 1, s. 21-52. ISSN 2045-9807.

[15] GINSBURG, Jane C; BUDIARDJO, Luke A. Auhors and Machines [online]. *Berkeley Technology Law Journal*. 2019, roč. 34, č. 2. Columbia Public Law Research Paper No. 14-597; *SSRN*, publikováno 20. 8. 2018, 116 s [cit. 10. 3. 2019]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3233885

[16] GRIMMELMANN, James. Copyright for Literare Robots. *Iowa Law Review*. 2016, roč. 101,č. 2, s. 657-681. ISSN 0021-0552.

[17] HORÁK, Ondřej; DOSTALÍK, Petr. Věc v právním slova smyslu v novém občanském zákoníku z právněhistorické perspektivy. *Časopis pro právní vědu a praxi*. 2013, č. 1, s. 14-21. ISSN 1210-9126.

[18] HUBBARD, F. Patrick. "Sophisticated Robots": Balancing Liability, Regulation, and Innovation. *Florida Law Review* [online]. 2014, roč. 66, č. 5, s. 1803-1872. ISSN 1045-4241 [cit. 10. 3. 2019]. Dostupné z: https://scholarship.law.ufl.edu/flr/vol66/iss5/1/

[19] POLČÁK, Radim. Odpovědnost umělé inteligence a informační útvary bez právní subjektivity. *Bulletin advokacie*. 2018, č. 11, s. 21-28. ISSN 1210-6348.

[20] SCHAFER, Burkhard a kol. A Fourth Law of Robotics? Copyright and the Law and Ethics of Machine Coproduction. *Artificial Intelligence and Law*, 2015 ,č. 23, s. 217-240. ISSN 0924-8463.

[21] TOMÍŠEK, Jan. Jaký je ideální model odpovědnosti za autonomní systém? *Revue pro právo a technologie* [online]. 2018, roč. 9, č. 18, 29-54 [cit. 10. 3. 2019]. Dostupné z: https://journals.muni.cz/revue/article/view/10452

[22] VOJTEK, Pavel. Náhrada újmy z provozních činností (vybrané otázky). *Soudní rozhledy*. 2015,č. 6, s. 202-206. ISSN 1211-4405.

[23] ZIBNER, Jan. Akceptace právní osobnosti v případě umělé inteligence. *Revue pro právo a technologie* [online]. 2018, roč. 9, č. 17, s. 19-49 [cit. 10. 3. 2019]. Dostupné z: https://journals.muni.cz/revue/article/view/9067

[24] ZIBNER, Jan. Artificial Intelligence: A Creative Player in the Game of Copyright. *European Journal of Law and Technology*. 2019, roč. 10, č. 1, s. 1-20. ISSN 2042-115X.

[25] ZIBNER, Jan. Dopady digitalizace do autorského práva. In: BEJČEK, Josef a kol. (eds.). *Dny práva 2018: Část IV. Dopady digitalizace do oblasti soukromého práva*. 2019, 1. vydání. Edice Scientia, sv. č. 653, s. 120-134. ISBN 978-80-210-9328-7.

[26] ZIBNER, Jan. Subjects' Relevance Within an AI-included Creative Process. In: SCHWEIGHOFER, Erich a kol. (eds.). *Internet of Things: Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019*. Bern: Editions Weblaw, 2019, 673 s (s. 401-406). ISBN 978-3-96443-724-2.

5.3 OSTATNÍ ZDROJE

[27] AIPPI. Resolution 2019 - Study Question: Copyright in Artificially Generated Works [online]. *AIPPI*, publikováno 18. 9. 2019 [cit. 10. 3. 2019]. Dostupné z: https://aippi.org/wp-content/uploads/2019/10/Resolution_Copyright_in_artificially_generated_works_English.pdf?fbclid=IwAR0mPqjCn-0dfnNBYcF7RLcLa3Pcs6m3RFA_g_VYsD7eL9j20j9xapA6Q94

[28] KRAUSOVÁ, Alžběta a kol. Výzkum potenciálu rozvoje umělé inteligence v České republice: Analýza právně-etických aspektů rozvoje umělé inteligence a jejích aplikací v Č R [online] . *Úřad vlády České republiky*, publikováno 10. 12. 2018, 72 s. [cit. 10. 3. 2019]. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/AI-pravne-eticka-zprava-2018_final.pdf

[29] LE, James. The 10 Deep Learning Methods AI Practitioners Need to Apply [online] . *Medium*, publikováno 17. 11. 2017 [cit. 10. 3. 2019]. Dostupné z: https://medium.com/
cracking-the-data-science-interview/the-10-deep-learning-methods-ai-practitioners-need-to-apply-885259f402c1

[30] ZIBNER, Jan. *Tvůrčí činnost autora v kontextu technologického vývoje* [online]. Rigorózní práce. Masarykova univerzita, Právnická fakulta, 2018, 120 s [cit. 10. 3. 2019]. Dostupné z: https://is.muni.cz/auth/th/g6t5k/

5.4 SOUDNÍ ROZHODNUTÍ

[31] EVROPSKÁ UNIE. Rozsudek Soudního dvora Evropské unie (pátého senátu) ze dne 25. 1. 2017. Věc C-367/15. *Stowarzyszenie „Oławska Telewizja Kablowa“ proti Stowarzyszenie Filmowców Polskich.*

[32] Rozsudek Městského soudu v Praze sp. zn. 13 Co 216/90.

[33] Usnesení Nejvyššího soudu ze dne 17. 8. 2011, sp. zn. 5 Tdo 751/2011.

5.5 PRÁVNÍ PŘEDPISY A JINÉ DOKUMENTY

[34] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES.

[35] VELKÁ BRITÁNIE. Copyright, Designs and Patents Act 1988, as amended, 1988 c. 48.

[36] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

[37] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

[38] Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

https://doi.org/10.5817/RPT2019-2-4

PŘEHLED AKTUÁLNÍ JUDIKATURY II/2019

DOMINIKA COLLETT, FRANTIŠEK KASL, JAKUB KLODWIG, IVANA KUDLÁČKOVÁ, PAVEL LOUTOCKÝ, JAKUB MÍŠEK, TEREZA NOVOTNÁ, ANNA STÁRKOVÁ, JAN SVOBODA, PETRA VYDROVÁ, JAN ZIBNER

ELEKTRONICKÉ KOMUNIKACE & ISP

SLUŽBA VOLÁNÍ PŘES INTERNETOVÝ PROTOKOL (VOIP) JAKO SLUŽBA ELEKTRONICKÝCH KOMUNIKACÍ

Soud: Soudní dvůr Evropské unie
Věc: C-142/18 (Skype)
Datum: 5. 6. 2019
Dostupnost: curia.europa.eu

Společnost Skype zavedla funkci SkypeOut umožňující uskutečňovat telefonní volání z koncového zařízení na pevnou linku nebo na mobilní telefon za použití internetového protokolu (IP), a to technikou zvanou „Voice over IP“ (VoIP). Belgický úřad pro poštovní a telekomunikační služby uložil společnosti Skype správní pokutu, protože se Skype řádně neoznámil poskytovanou službu elektronických komunikací. Skype podal návrh na zrušení rozhodnutí a domáhal se určení, že SkypeOut není službou elektronických komunikací a Skype tak není poskytovatelem služeb elektronických komunikací.

Soudní dvůr byl tázán, zda musí být čl. 2 písm. c) směrnice 2002/21/ES („rámcová směrnice“), vykládán v tom smyslu, že poskytuje-li výrobce

softwaru funkci nabízející službu VoIP, musí být tato služba kvalifikována jako služba elektronických komunikací.

Soudní dvůr uvedl, že pro kvalifikaci služby jako služby elektronických komunikací není rozhodující, že k přenosu signálu dochází prostřednictvím infrastruktury, která poskytovateli služeb nepatří.[1] Soudní dvůr došel k závěru, že společnost Skype nabízí službu VoIP, pobírá od uživatelů služby úplatu a je vůči nim odpovědná za přenos hlasových signálů, a to na základě smluv uzavřených s poskytovateli telekomunikačních služeb.[2] Dále uvedl, že i když má uživatel funkce SkypeOut přístup ke službě prostřednictvím připojení na Internet, kterou poskytuje ISP a která je sama o sobě službou elektronických komunikací, neznamená to, že služba VoIP nemůže být kvalifikována jako služba elektronických komunikací.[3] Přestože služba VoIP předpokládá dvě různé služby, kdy jedna spadá do odpovědnosti ISP volajícího uživatele a druhá do společné odpovědnosti poskytovatelů telekomunikačních služeb volaných osob a společnosti Skype,[4] odpovědnost za službu VoIP nese společnost Skype, neboť ji poskytuje za úplatu svým zákazníkům.[5] Skutečnost, že SkypeOut je jednou z funkcí softwaru Skype není pro kvalifikaci služby VoIP jako služby elektronických komunikací rozhodující, neboť Skype a SkypeOut se jasně liší co do svého předmětu a ve svém fungování jsou navzájem zcela autonomní.[6] Klauzule ve všeobecných obchodních podmínkách o nenesení odpovědnosti za přenos signálů, nemůže mít vliv na kvalifikaci služby VoIP jako služby elektronických komunikací.[7] Též skutečnost, že služba VoIP poskytovaná funkcí SkypeOut spadá rovněž pod pojem služba informační společnosti, neznamená, že by nemohla být kvalifikována jako služba elektronických komunikací.[8]

---

1 Srov. bod 29 anotovaného rozhodnutí.

2 Srov. bod 31, 33 a 35 anotovaného rozhodnutí.

3 Srov. 37 anotovaného rozhodnutí.

4 Srov. bod 38 anotovaného rozhodnutí.

5 Srov. bod 40 anotovaného rozhodnutí.

6 Srov. bod 43 anotovaného rozhodnutí.

7 Srov. bod 44 anotovaného rozhodnutí.

8 Srov. bod 46 anotovaného rozhodnutí.

Soudní dvůr tedy dospěl k závěru, že poskytuje-li výrobce softwaru funkci nabízející službu VoIP, která uživateli umožňuje volat z koncového zařízení na číslo pevné linky nebo mobilního telefonu prostřednictvím veřejné telefonní sítě některého členského státu, jedná se o službu elektronických komunikací ve smyslu rámcové směrnice, pokud výrobce pobírá za poskytování uvedené služby úplatu a pokud poskytování této služby předpokládá uzavření smluv mezi tímto výrobcem a poskytovateli telekomunikačních služeb.

Autorka: IK

GMAIL JAKO SLUŽBA ELEKTRONICKÝCH KOMUNIKACÍ

Soud: Soudní dvůr Evropské unie
Věc: C-193/18 (Google)
Datum: 13. 6. 2019
Dostupnost: curia.europa.eu

V původním sporu proti sobě stála německá Spolková agentura pro elektrické, plynofikační, telekomunikační, poštovní a železniční sítě (dále jen „spolková agentura“) a společnost Google, která provozuje elektronickou službu Gmail soužící k emailové komunikaci. Spolková agentura měla za to, že služba Gmail je službou elektronických komunikací dle platných německých i unijních předpisů, a tudíž na ni dopadá ohlašovací povinnost. Proti tomuto správnímu rozhodnutí podal Google stížnost, a následně správní žalobu. Správní soud žalobu zamítl s tím, že přenos emailů (odesílání a doručování), který poskytuje společnost Google, je přenosem signálů i přesto, že tento přenos probíhá přes internetové připojení, které poskytuje jiná služba ISP a ne Google samotný. Google se odvolal k německému Nejvyššímu správnímu soudu spolkové země Severní Porýní-Vestfálsko (dále jen „předkládající soud“) s hlavním argumentem, že nezařizuje přenos signálů, který zařizuje jiná ISP, a tudíž na něj nespadá ohlašovací povinnost.

SDEU se zabýval předběžnou otázkou, která se týkala výkladu pojmu přenos signálů jako definičního znaku služby elektronických komunikací.

SDEU posuzoval, zda je přenosem signálů internetová emailová služba, která je založena na odesílání a přijímaní signálů skrz otevřený internet, ale sama nezajišťuje přístup k internetu, a tudíž faktický přenos těchto signálů.

Služba elektronických komunikací je definována zejména v čl. 2 písm. c) směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), kde je uvedeno *„[…] ‚službou elektronických komunikací' se rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací […]"*.

SDEU dovozuje, že provozování internetové emailové služby je nesporně přenosem signálů, nicméně nejedná se o službu elektronických komunikací ve smyslu čl. 2 písm. c) rámcové směrnice, neboť se tato služba nespočívá *„zcela nebo převážně v přenosu signálů"*.[9] Odpovědnost za přenos signálů mají dle Soudního dvora poskytovatelé zejména *„správci různých sítí tvořících otevřený Internet"*[10] a ani to, že má Google vliv na přijímání a odesílání emailových zpráv není dostatečným pro zařazení této společnosti mezi službu elektronických komunikací.[11]

SDEU shrnul, že internetová emailová služba, která nezajišťuje přístup k internetu, ale pouze poskytuje odesílání a přijímání emailů přes internet pak nespočívá *„zcela či převážně v přenosu signálů"* a nemůže se tedy jednat o službu elektronické komunikace a Google tedy nemá ohlašovací povinnost.[12]

Autorka: TN

[9] Odst. 34 a 35 anotovaného rozhodnutí.

[10] Odst. 36 anotovaného rozhodnutí.

[11] Odst. 37 anotovaného rozhodnutí.

[12] Odst. 41 a 43 anotovaného rozhodnutí.

MOŽNOST SOUDU ULOŽIT PŘEDBĚŽNÝM OPATŘENÍM POSKYTOVATELI HOSTINGU POVINNOST ODSTRANĚNÍ STEJNÉHO ČI ROVNOCENNÉHO OBSAHU FORMOU DOHLEDU A VYHLEDÁVÁNÍ V CELOSVĚTOVÉM ROZSAHU

Soud: Soudní dvůr Evropské unie
Věc: C-18/18 (Glawischnig-Piesczek)
Datum: 3. 10. 2019
Dostupnost: curia.europa.eu

Podkladem případu byl příspěvek uživatele na sociální síti Facebook z dubna 2016, kterým byl sdílen odkaz na článek na rakouském portálu oe24.at o kontroverzním politickém postoji die Grünen (Zelení), pod kterým algoritmus Facebooku v rámci shrnutí obsahu článku zobrazil fotografii Evy Glawischnig-Piesczek, která je předsedkyní jejich poslaneckého klubu.[13] Ta toto její propojení s daným postojem vnímala jako urážku na cti a po bezvýsledné komunikaci se společností Facebook podala žalobu u rakouského soudu.

Soud vydal v prosinci 2016 předběžné opatření, aby se společnost Facebook do pravomocného rozsudku zdržela zveřejňování fotografie žalobkyně ve spojení s příspěvky stejného či rovnocenného obsahu.[14] Odvolacím soudem byl rozsah povinnosti omezen pouze na stejné či ohlášené příspěvky. Spor tak doputoval před Oberster Gerichtshof (Nejvyšší soud), který položil předběžné otázky SDEU.[15]

Ty se týkaly přípustného obsahového a teritoriálního rozsahu povinnosti na odstranění obsahu, která může být uložena soudem poskytovateli hostingu, zde společnosti Facebook, s přihlédnutím k vyloučení obecné povinnosti poskytovatelů hostingu dohlížet na přenášený a ukládaný obsah skrze čl. 15 směrnice o elektronickém obchodu.[16]

[13] Body 10-12 anotovaného rozhodnutí.

[14] Bod 14 anotovaného rozhodnutí.

[15] Body 16-19 anotovaného rozhodnutí.

SDEU předně podotkl, že je přípustnost uložení soudních příkazů v podobě předběžného opatření na základě vnitrostátního práva předvídána čl. 14 odst. 3 a čl. 18 směrnice o elektronickém obchodu.[17] Dále pak potvrdil, že posuzovací pravomoc ohledně provádění těchto prostředků soudní ochrany přísluší v souladu s čl. 18 odst. 1 směrnice členským státům a některá jazyková znění zde obsahují velmi otevřenou formulaci přípustného rozsahu daných opatření.[18] SDEU pak výsledně dovodil, že zákaz obecné povinnosti dohlížet na hostovaný obsah se v souladu s bodem 47 odůvodnění směrnice netýká povinnosti uložené v konkrétním případě ve vztahu ke konkrétní informaci.[19] V případě příspěvků se stejným obsahem je pak soud takto oprávněn po poskytovateli požadovat odstranění bez ohledu na to, kdo požádal o její uložení,[20] tedy celosvětově.[21] Shodný závěr Soudní dvůr dovodil i pro příspěvky s informací rovnocenného obsahu, ačkoliv daný soudní příkaz musí být dostatečně specifikován.[22] Pokud tedy dané soudní opatření ukládá dostatečně konkrétně vymezený stejný či rovnocenný obsah, který má být odstraněn, tak aby poskytovatel nebyl nucen uvedený obsah samostatně posuzovat, není nepřiměřené soudem požadovat, aby poskytovatel hostingu v tomto rozsahu prováděl dohled a vyhledávání daného obsahu v rámci svých (automatizovaných) kapacit.[23]

Rozhodnutí ve svém důsledku posiluje soudní ochranu proti zásahům do práv skrze obsah na sociálních sítích či jiných hostingových službách, jelikož jednoznačně zakotvuje plnou šíři opatření, ke kterým je soud v tomto směru oprávněn.

Autor: FK

---

[16] 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.

[17] Body 24-27 anotovaného rozhodnutí.

[18] Body 29-30 anotovaného rozhodnutí.

[19] Body 34-35 anotovaného rozhodnutí.

[20] Bod 37 anotovaného rozhodnutí.

[21] Bod 50 anotovaného rozhodnutí.

[22] Body 38-47 anotovaného rozhodnutí.

[23] Body 45-46 anotovaného rozhodnutí.

EGOVERNMENT

ZAŘAZENÍ IP ADRESY SPRÁVNÍM ORGÁNEM NA *BLACK-LIST*

Soud: Nejvyšší správní soud České republiky
Věc: 2 As 153/2018 - 31
Datum: 6. 3. 2019
Dostupnost: nssoud.cz

Stěžovatel se v původním sporu domáhal ochrany před nezákonným zásahem žalovaného – Městského úřadu Domažlice. Stěžovatel se domníval, že žalovaný nezákonně zasáhl do jeho práv tím, že se jeho emailová adresa, kterou využil k podání k žalovanému, objevila na tzv. *black-listu* žalovaného a kvůli tomu mu podání nebylo vůbec doručeno, o čemž byl stěžovatel informován prostřednictvím svého poskytovatele emailové služby (email s podáním nebyl doručen adresátovi). Ačkoliv byl stěžovatel informován, jiné podání už neučinil a tím promeškal procesní lhůtu.

Stěžovatel nejprve reagoval na situaci podáním žaloby na ochranu před nezákonnými zásahy žalovaného ke Krajskému soudu v Plzni. Stěžovatel se domáhal určení, že zařazení jeho emailové adresy na tzv. *black-list* je nezákonným postupem Městského úřadu a domáhal se zdržení a zrušení rozhodnutí žalovaného.[24]

Nejvyšší správní soud se zabýval otázkou, zda zařazení emailové adresy správním orgánem na tzv. *black-list*, který navíc spravuje externí soukromá společnost, je postup v souladu se zákonem.

Podání učiněné elektronicky ve správním řízení upravuje § 19 odst. 4, 9 a 10 zákona č. 500/2004 Sb., správního řádu.

Stěžovatel argumentuje především tím, že správní orgán *de facto* odmítnul přijmout jeho podání, ovšem tím, že mohl vůbec vykonat akt „odmítnutí“ tak je prokázáno, že podání bylo doručeno, tedy dostalo se do dispoziční sféry adresáta (odmítnutí je také disponováním s podáním)

[24] Odst. 1 anotovaného rozhodnutí.

a lhůta tedy byla dodržena.[25] Druhým nosným argumentem stěžovatele bylo to, že jde na vrub správního orgánu, pokud se rozhodne pověřit zabezpečením své emailové schránky externí soukromou společnost a kvůli tomu nepřijme včasné a řádně odeslané podání. Není možné, aby taková situace šla na vrub stěžovateli, který podal své podání včas a řádným způsobem (skrz emailovou schránku správního orgánu).[26] NSS jeho argumentaci odmítl a zamítl kasační stížnost jako nedůvodnou.[27] Dle NSS zařazení emailové adresy na tzv. *black-list* znamená, že rozhodnutí ani nedorazí do dispoziční sféry orgánu, protože je zastaveno a vráceno ještě před doručením, o čemž je odesílatel také řádně informován.[28] Dle NSS je dále naopak žádané, aby správní orgány využívaly pro zabezpečení elektronických schránek služeb soukromých profesionálních společností, a dále také jde na vrub stěžovatele, že zvolil tento způsob podání, který je méně privilegovaný než datová schránka či podání doručení poštou a jedná se o jeho volbu využít soukromou společnost, jejíž server byl správním orgánem zablokován pro doručování.[29]

Autorka: TN

E-MAIL A PÍSEMNÁ FORMA

Soud:	Nejvyšší soud České republiky
Věc:	23 Cdo 3439/2018
Datum:	16. 5. 2019
Dostupnost:	nsoud.cz

Žalobce (česká obchodní korporace) sjednala se španělskou společností (žalovanou) e-mailem smlouvu o dílo, jejíž součástí byla rovněž rozhodčí doložka. Žalovaná společnost nicméně nerespektovala platnost rozhodčí doložky v rámci vzniklého sporu a nebyla ochotna se tak účastnit

[25] Odst. 6 anotovaného rozhodnutí.

[26] Odst. 7 anotovaného rozhodnutí.

[27] Odst. 18 anotovaného rozhodnutí.

[28] Odst. 14 anotovaného rozhodnutí.

[29] Odst. 15, 16 a 17 anotovaného rozhodnutí.

rozhodčího řízení. Namítala, že nedošlo k platnému sjednání rozhodčí smlouvy, když nebyla podepsána kvalifikovaným elektronickým podpisem.

Spor projednávaly místně příslušné české soudy a jak prvostupňový, tak odvolací soud rozhodly, že se v daném případě jednalo o platně uzavřenou rozhodčí doložku. Proto se žalovaná dovolala k Nejvyššímu soudu.

Nejvyšší soud posuzoval, jestli uzavřením e-mailem došlo k naplnění podmínky pro uzavření rozhodčí smlouvy písemnou formou. Toto Nejvyšší soud posuzoval zejména v souvislosti s požadavkem, který je jednak kladen zákonem č. 216/1994 Sb., o rozhodčím řízení a o výkonu rozhodčích nálezů, ve znění pozdějších předpisů, ale rovněž Newyorkskou úmluvou[30] a Evropskou úmluvou o mezinárodní obchodní arbitráži.[31] Ve všech těchto závazných pramenech práva je stanoveno velmi obdobně,[32] že „*písemná forma je zachována i tehdy, je-li rozhodčí smlouva sjednána telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení jejich obsahu a určení osob, které rozhodčí smlouvu sjednaly*".[33] Postupným zkoumáním podstaty soud nejprve určil, že se na danou věc bude aplikovat Newyorkská úmluva, poté odkázal na UNCITRAL Recommendation ze dne 7. 7. 2006, které jednoznačně shrnuje, že daný výčet ("*dálnopisem, telegraficky*") je demonstrativní a v době tvorby Newyorské úmluvy nebyla předpokládána existence internetu. To ale neznamená, že by nemohla být daným způsobem rozhodčí smlouva uzavřena. Newyorská úmluva tak dle Nejvyššího soudu zahrnuje i výměnu komunikace prostřednictvím e-mailu. Soud dále ještě zdůraznil, že pro platné uzavření rozhodčí smlouvy by požadavek na využití kvalifikovaného elektronického podpisu byl excesivní.

Soud tak dovolání španělské žalované zamítl.

Autor: PL

---

[30] Vyhláška č. 74/1959 Sb. ze dne 6. listopadu 1959 o Úmluvě o uznání a výkonu cizích rozhodčích nálezů (Newyorská úmluva).

[31] Vyhláška č. 176/1964 Sb., vyhláška ministra zahraničních věcí o Evropské úmluvě o obchodní arbitráži.

[32] Faktická textace je v rámci těchto uvedených pramenů jiná, význam a požadavky jsou ale stejné.

[33] Viz anotované rozhodnutí.

E-MAIL A PÍSEMNÁ FORMA (OPĚT, ALE ŠPATNĚ)

Soud: Nejvyšší soud České republiky
Věc: 26 Cdo 1230/2019
Datum: 22. 5. 2019
Dostupnost: nsoud.cz

Toto vcelku krátké usnesení se zabývalo podmínkami, které je nutno splnit pro dodržení písemné formy kladené zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ“) při využití e-mailu.

Žalobkyně proti výpovědi z nájmu podala námitky e-mailem, odvolací soud však zdůraznil, že takovéto podání námitek nesplnilo požadavek na písemnou formu dle § 2314 OZ. Zdůraznil pak, že pro zachování písemné formy (dle § 562 OZ) by bylo nutno doplnit e-mail o elektronický podpis.

Nejvyšší soud se tak zabýval tím, jestli byly v daném případě splněny dvě náležitosti pro zachování formy, a to písemnost a podpis. Podmínku písemnosti soud shrnul jen ve smyslu, že dané jednání je zachyceno v písemném textu listiny. Nezabýval se již ale nijak tím, co znamená pojem „písemné“ (jedná se rovněž o elektronickou formu – pozn. autor) a pojem „listina“ (zde se může ve spojení s § 3016 odst. 1 OZ jednat opět o elektronickou formu). Jediným argumentem soudu k podpisu bylo, že *„vznesla-li žalobkyně Námitky e-mailem […], který nebyl opatřen elektronickým podpisem, je závěr odvolacího soudu, že nedodržela písemnou formu Námitek, v souladu s judikaturou Nejvyššího soudu.“*[34] Judikaturu soud pak jen obecně shrnuje bez jakékoli analýzy konkrétních aspektů.

Soud tak shrnul, že e-mail, který nebyl podepsán elektronickým podpisem nemůže naplnit písemnou formu.

Na rozhodnutí je nutno pohlížet kriticky zejména v souvislosti s tím, že se soud nijak nezabýval otázkou, co elektronický podpis je a zejména nezjišťoval, jestli žalovaná námitku neopatřila „prostým“ elektronickým podpisem. Už v tom případě by dané naplnilo podmínku podpisu.[35] Rovněž je možné rozhodnutí kritizovat i pro jeho rigidní výklad, jelikož tímto

[34] Anotované rozhodnutí.

rozhodnutím bylo žalované následně *de facto* upřeno právo na spravedlivý přístup k soudu. Rozhodnutí je tak nutno považovat za špatné a matoucí. Anotované rozhodnutí ukazuje, že v některých případech v problematice elektronické identifikace a kontraktace stále tápou i vyšší soudy.

Autor: PL

ELEKTRONICKÝ PODPIS A ÚŘEDNÍ OVĚŘENÍ PODPISU

Soud:	Nejvyšší soud České republiky
Věc:	KSPH 64 INS 26339/2015, 29 NSČR 133/2017-B-36
Datum:	30. 7. 2019
Dostupnost:	isir.justice.cz

Anotované rozhodnutí se zabývalo velmi zajímavou otázkou vzájemné souvislosti elektronického podpisu (resp. některého z jeho typů) s úředním ověřením podpisu.

Věřitel v rámci insolvenčního řízení podal hlasovací lístek pro oddlužení zpeněžením majetkové podstaty prostřednictvím datové schránky (lístek byl podepsán zaručeným (*sic!*) elektronickým podpisem). Dle nižších soudů ale v souvislosti s § 97 odst. 2 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění od 1. 1. 2014 do 18. 9. 2016 (dále jen „IZ“) nedošlo takovým podáním k naplnění podmínky požadované zákonem – hlasovací lístek je nutno opatřit úředně ověřeným podpisem nebo elektronicky s využitím uznávaného elektronického podpisu (v současné chvíli je ekvivalentem kvalifikovaný elektronický podpis).

Nejvyšší soud se tak v daném případě zabýval otázkou, jestli je možné, aby vůbec nějaký typ elektronického podpisu (ať už se jedná o zaručený nebo kvalifikovaný elektronický podpis) naplnil požadavek úředního ověření a za jakých podmínek.

[35] K tomu částečně viz například LOUTOCKÝ, Pavel. *Ochrana spotřebitele při uzavírání smluv na internetu a možnost řešení vzniklých sporů online*. In: POLČÁK, Radim et al. Právo informačních technologií. 2018. Praha: Wolters Kluwer. S. 307 a násl. nebo POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoněč. 89/2012 Sb. *Bulletin advokacie*. 2014, č. 13, s. 34–41.

Nejvyšší soud zdůraznil, že úřední ověření je úzce vymezeným institutem, který je zákonem jasně definován.[36] Soud dále poměrně vhodně rozvedl jednotlivé druhy podpisů, správně identifikoval, že zaručený elektronický podpis je jen předstupněm kvalifikovaného elektronického podpisu (rozebral poměrně kvalitně i dopady nařízení eIDAS, které upravuje problematiku elektronické identifikace), odkázal na odbornou literaturu a shrnul, že požadavek úředního ověření podpisu obecně vylučuje možnost využít elektronický podpis, jelikož chybí v českém právu takové zákonné propojení.[37] To bylo ale explicitně zakotveno v určitou dobu IZ.

Nejvyšší soud tak uzavřel, že v daném případě nebyly požadavky na formu podání splněny, jelikož nebylo využito adekvátního typu elektronického podpisu.

Dané rozhodnutí je zajímavé tím, že poměrně přehledně vymezuje jednotlivé druhy podpisu a rozebírá je do detailu. Je dále nutno upozornit, že fakticky není důvod, aby kvalifikovaný elektronický podpis nemohl být kladen na roveň úřednímu ověření. Přestože daná úprava v IZ již není bohužel účinná, připravovaný zákon o právu na digitální služby[38] by měl obecně zakotvit předpoklad, že úřední ověření bude moci být nahrazeno právě kvalifikovaným elektronickým podpisem.

Autor: PL

PRÁVO DUŠEVNÍHO VLASTNICTVÍ

LOCUS DELICTI PŘI UŽITÍ OCHRANNÉ ZNÁMKY NA INTERNETU

Soud: Soudní dvůr Evropské unie

Věc: C-172/18 (AMS Neve)

Datum: 5. 9. 2019

Dostupnost: curia.europa.eu

[36] Strana 10 anotovaného rozhodnutí.

[37] Strana 8 anotovaného rozhodnutí.

[38] Sněmovní tisk 447. N.z. o právu na digitální služby [online]. Poslanecká sněmovna České republiky [vid. 16. 11. 2019]. Dostupné z: http://www.psp.cz/sqw/historie.sqw?o=8&t=447.

Žádost o předběžné otázky byla předložena v rámci sporu mezi britskými společnostmi AMS Neve Ltd, Barnett Waddingham Trustees a Markem Crabtreem na straně jedné (dále jen „žalobci“) a španělskou společností Heritage Audio SL a Pedrem Rodríguez Arribasem na straně druhé (dále jen „žalovaní). Dne 15. října 2015 podali žalobci u soudu pro duševní vlastnictví a podnikání ve Spojeném království žalobu pro porušení práv plynoucích z ochranné známky EU. Žalovaným bylo vytýkáno, že nabízeli k prodeji spotřebitelům ve Spojeném království napodobeniny výrobků společnosti AMS Neve označených totožnou nebo podobnou ochrannou známkou EU žalobců. Na podporu žaloby žalobci předložili různé dokumenty, mimo jiné screenshoty internetových stránek, účtů Facebook a Twitter společnosti Heritage Audio.

Žalovaní vznesli námitku nepříslušnosti soudu, kterému byla tato věc předložena. Soud pro duševní vlastnictví a podnikání určil, že není příslušný k projednání této žaloby pro porušení v rozsahu, v němž se zakládá na dotčené ochranné známce EU. Žalovaní podali proti tomuto rozsudku odvolání u odvolacího soudu pro Anglii a Wales.

Spor spočíval v otázce, jaké národní soudy jsou příslušné pro řešení daného případu. Předběžné otázky předložené Soudnímu dvoru se týkaly zejména výkladu čl. 97 odst. 5 nařízení č. 207/2009,[39] dle kterého řízení mohou být rovněž vedena před soudy členského státu, na jehož území k porušení došlo.

Soudní dvůr EU připomněl, že ustanovení čl. 97 odst. 5 nařízení č. 207/2009 působí pro případy žalob o ochranné známky EU jako *lex specialis* vůči nařízení 1215/2012.[40] Pro určení působnosti národního soudu proto bylo nezbytné vyložit formulaci „*[členský stát], na jehož území k porušení došlo*“. V případě, že vytýkané jednání spočívá jako v projednávaném případě v reklamách a nabídkách k prodeji zobrazovaných elektronickými prostředky (například na webových

[39] Nařízení Rady (ES) č. 207/2009 ze dne 26. února 2009 o ochranné známce Společenství (dále jen „nařízení č. 207/2009“).

[40] Bod 34 anotovaného rozhodnutí.

stránkách, a sítích Twitter a Facebook), je nutné dovodit,[41] zda k tomuto jednání došlo na území, kde se nacházejí spotřebitelé nebo podnikatelé, kterým jsou tyto reklamy a nabídky k prodeji určeny. Není přitom podstatné, že žalovaný má sídlo nebo bydliště na jiném území, že se server elektronické sítě, který žalovaný používá, nachází na jiném území[42] nebo že třetí osoba učinila rozhodnutí a opatření za účelem tohoto elektronického zobrazování v jiném členském státě.[43]

Autorka: DC

NEPLATNOST OCHRANNÉ ZNÁMKY TVOŘENÉ TVAREM RUBIKOVY KOSTKY

Soud: Soudní dvůr Evropské unie
Věc: T-601/17 (Rubik's Brand Ltd)
Datum: 24. 10. 2019
Dostupnost: curia.europa.eu

V roce 1999 byla registrována[44] evropská ochranná známka Rubikovy kostky.[45] Následně bylo společností Simba Toys GmbH & Co. KG („Simba Toys") postupně iniciováno několik pro tuto společnost neúspěšných řízení směřujících k prohlášení ochranné známky za neplatnou.[46] To mělo dle Simba Toys nastat z absolutních důvodů pro zamítnutí zápisu ochranné známky, mimo jiné s odkazem na skutečnost, že do rejstříku nemohou být zapsané takové známky, které jsou tvořeny výlučně tvarem nebo jinou vlastností výrobku, jež jsou nezbytné pro dosažení technického výsledku.[47]

Na základě kasačního opravného prostředku podaného Simba Toys v roce 2016 k Soudnímu dvoru tento napadené rozhodnutí odvolacího

[41] Soudní dvůr EU odkázal na předchozí judikaturu, srov. bod 63 rozsudku ze dne 12. července 2011, L'Oréal a další, C-324/09.

[42] Bod 47 anotovaného rozhodnutí.

[43] Bod 65 anotovaného rozhodnutí.

[44] Jejím vlastníkem se roku 2014 stala společnost Rubik's Brand Ltd.

[45] Viz bod 1-5 anotovaného rozhodnutí.

[46] Viz bod 6-14 anotovaného rozhodnutí.

[47] Viz bod 6, 8 a 10 anotovaného rozhodnutí.

senátu EUIPO zrušil pro nesprávný postup při posouzení toho, zda je dané označení tvořeno výlučně tvarem nebo jinou vlastní výrobku nutných pro dosažení technického výsledku.[48] Následně první odvolací senát EUIPO vydal rozhodnutí, v němž prohlásil dotčenou známku za neplatnou. Při posuzování výše uvedeného byla pozornost věnována kubickému tvaru Rubikovy kostky, černým liniím i čtverečkům na každé ze stran daného předmětu, jakožto prvkům tvořící dané označení. Všechny tyto prvky přitom byly shledány jakožto nezbytné pro dosažení daného technického výsledku Rubikovy kostky, vč. funkcionality rotace jejích jednotlivých částí.[49]

Posledně uvedené rozhodnutí bylo společností Rubik's Brand Ltd napadeno u Tribunálu. Ten, byť se neztotožnil s přístupem, který EUIPO zvolil vzhledem k jednotlivým čtverečkům na stranách Rubikovy kostky (resp. s jejich zohledněním v daném rozhodnutí),[50] napadené rozhodnutí potvrdil a žalobu zamítnul.[51] Uvedl mimo jiné, že černé linie Rubikovy kostky představují fyzické oddělení mezi jednotlivými kostkami, což hráči umožňuje otáčet každou řadu malých kostek nezávisle na sobě, aby tyto malé kostky shromáždil v požadovaném barevném schématu na šesti stranách krychle. Takové fyzické oddělení je nutné k rotaci, vertikálně a horizontálně.[52]

Daný rozsudek je tak jedním z těch potvrzujících, že institut ochranných známek nemůže bez dalšího vést k ochraně technických řešení, a to ani u notoricky známých tvarů.[53]

Autor: JS

[48] Bod 16-19 anotovaného rozhodnutí.

[49] Bod 19-30 anotovaného rozhodnutí.

[50] Dle bodu 99 anotovaného rozhodnutí tento přístup nikterak neovlivnil závěry rozhodnutí EUIPO.

[51] Bod 116 anotovaného rozhodnutí.

[52] Bod 86 anotovaného rozhodnutí.

[53] Srov. např. rozsudek Soudního dvora Evropské unie ze dne 14. 9. 2010 ve věci C-48/09 P.

AUTORSKÉ PRÁVO

KONFLIKT MEZI PRÁVY AUTORA A ZÁKLADNÍMI LIDSKÝMI PRÁVY

Soud: Soudní dvůr Evropské unie
Věc: C-469/17 (Funke Medien NRW)
Datum: 29. 7. 2019
Dostupnost: curia.europa.eu

Společnost Funke Medien dne 27. září 2012 požádala o přístup ke všem dokumentům označeným „Unterrichtung des Parlaments“ („informace pro Parlament“, dále jen „UdP“) vypracovaným v době od 1. září 2001 do 26. září 2012. Tyto dokumenty vypracovává každý týden německá vláda. Zprávy UdP jsou považovány za „utajované dokumenty – Vyhrazené“, kdy tato kvalifikace odpovídá nejnižšímu ze čtyř stupňů utajení dle německého práva. Příslušné orgány žádost společnosti Funke Medien zamítly. Společnost Funke Medien nicméně velkou část UdP získala neznámým způsobem a některé z těchto zpráv zveřejnila na jejích internetových stránkách v podobě jednotlivě naskenovaných stránek spolu s úvodní poznámkou, dalšími odkazy a výzvou k diskuzi.

Spolková republika Německo podala proti společnost Funke Medien pro porušení jejích autorských práva k UdP žalobu na zdržení se jednání, které zemský soud v Kolíně nad Rýnem vyhověl. Odvolání podané společností Funke Medien vrchní zemský soud v Kolíně nad Rýnem zamítl. V rámci opravného prostředku se společnost Funke Medien domáhala zamítnutí žaloby na zdržení se jednání.

Předmětem předběžných otázek je zejména otázka, jakým způsobem má být vykládán čl. 2 písm. a), čl. 3 odst. 1 a čl. 5 odst. 3 písm. c) a d) směrnice 2001/29,[54] ve spojení se základními právy, konkrétně svobodou informací a svobodou tisku.

[54] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

Soudní dvůr EU v rámci první předběžné otázky konstatoval, že ustanovení čl. 2 písm. a) a čl. 3 odst. 1 směrnice 2001/29 musí být vykládány v tom smyslu, že představují opatření úplné harmonizace věcného obsahu práv, která jsou v nich uvedena.[55] Naproti tomu ustanovení čl. 5 odst. 3 písm. c) druhého případu a písm. d) směrnice 2001/29 dle soudního dvora EU nepředstavují opatření úplné harmonizace rozsahu výjimek či omezení, které jsou v nich obsaženy.[56] Soudní dvůr EU se dále zabýval druhou a třetí předběžnou otázku, týkající se svobody informací a svobody tisku a jejich kolize s právy autorů. Soudní dvůr konstatoval, že svoboda informací a svoboda tisku nemohou nad rámec zakotvených výjimek a omezení v čl. 5 odst. 3 písm. c) druhého případu a písm. d) směrnice 2001/29 odůvodnit další výjimku z výlučného práva autora.[57] Vnitrostátní soud musí v rámci poměřování mezi výlučnými právy autora a právy uživatelů předmětů ochrany vycházet z výkladu těchto ustanovení, který respektuje jejich znění a zachovává jejich užitečný účinek a zároveň je v úplném souladu se základními právy zaručenými Listinou základních práv EU.[58]

Autorka: DC

VÝJIMKY A OMEZENÍ AUTORSKÉHO PRÁVA V KONTEXTU LIDSKÝCH PRÁV

Soud:	Soudní dvůr Evropské unie
Věc:	C-516/17 (Spiegel Online)
Datum:	29. 7. 2019
Dostupnost:	curia.europa.eu

Poslanec německého Spolkového sněmu, pan *Volker Beck*, byl autorem trestněprávního rukopisu. Tento rukopis byl postupem času zveřejněn s úpravami textu a názvu, které pozměnily smysl rukopisu. Při kandidování

[55] Bod 38 anotovaného rozhodnutí.

[56] Bod 40 anotovaného rozhodnutí.

[57] Bod 64 anotovaného rozhodnutí.

[58] Bod 76 anotovaného rozhodnutí.

do voleb v roce 2013 pan Beck obhajoval své jméno před médii a na důkaz změny smyslu rukopisu tento rukopis uvedeným médiím zpřístupnil. Média, včetně portálu *Spiegel Online*, bez jeho svolení rukopis bez dalšího zveřejnila. Spiegel Online navíc uvedl, že k žádné změně při dřívějším zveřejnění nedošlo.

Zemský soud v Německu vyhověl žalobě pana Becka na zásah do autorského práva. Po odvolání a po uplatnění dalších opravných prostředků pak Spolkový soudní dvůr tápal při výkladu čl. 5 směrnice InfoSoc v kontextu svobody informací a svobody tisku. Rozhodl se proto vznést předběžnou otázku.

Soudní dvůr byl tázán šesti otázkami na to, zda výjimky a omezení podle čl. 5 směrnice InfoSoc poskytují prostor pro uvážení; jak se zohledňují lidská práva podle Listiny základních práv EU; zda může katalog lidských práv rozšířit taxativní výčet výjimek a omezení či jaké jsou náležitosti zveřejnění pro účely citace.[59]

Soudní dvůr vyložil možnosti prostoru pro uvážení při aplikaci unijních norem s ohledem na charakter harmonizace,[60] která v tomto případě není plná.[61] Stejně tak apeloval na podstatu lidských práv zakotvených v Listině základních práv Evropské unie.[62] Soudní dvůr dále připomněl, že katalog výjimek a omezení v dané směrnici je taxativní,[63] což je plně v souladu s tradicemi a zaručenými lidskými právy.[64] Výklad jednotlivých výjimek a omezení přitom musí být plně v souladu s šetřením právě těchto práv.[65] Na adresu citace Soudní dvůr uvedl zejména její význam[66] a roli v informační společnosti v kontextu internetu.[67] V závěru pak Soudní dvůr

[59] Srov. bod 15 anotovaného rozhodnutí.

[60] Srov. bod 18 anotovaného rozhodnutí.

[61] Srov. body 26 a násl. anotovaného rozhodnutí.

[62] Srov. bod 20 anotovaného rozhodnutí.

[63] Srov. bod 41 anotovaného rozhodnutí.

[64] Srov. body 42 a násl. anotovaného rozhodnutí.

[65] Srov. body 52 a násl. anotovaného rozhodnutí.

[66] Srov. bod 78 anotovaného rozhodnutí.

[67] Srov. bod 81 anotovaného rozhodnutí.

uvedl, že podmínka vázanosti zpřístupnění díla veřejnosti na souhlas autora by byla příliš restriktivní.[68]

Soudní dvůr uzavřel, že čl. 5 směrnice InfoSoc nepředstavuje opatření plné harmonizace. Dále dodal, že svoboda informací ani svoboda tisku nemohou založit další výjimku či omezení, které by nebyly v katalogu této směrnice. Na druhou stranu však výklad již existujících výjimek a omezení musí respektovat lidská práva dle Listiny základních práv Evropské unie. Co do citace, Soudní dvůr uvedl, že i hypertextový odkaz může být citací, a že zpřístupnění veřejnosti není nutně podmíněno souhlasem autora.

Autor: JZ

METALL AUF METALL

Soud:	Soudní dvůr Evropské unie
Spojené věci:	C-476/17 (Pelham)
Datum:	29. 7. 2019
Dostupnost:	curia.europa.eu

Společnost *Pelham* pořídila zvukový záznam skladby *Nur mir*, která údajně obsahovala dvouvteřinový vzorek (sample) rytmické sekvence dříve zveřejněné skladby *Metall auf Metall*.

Výrobci záznamu skladby Metall auf Metall žalovali společnost Pelham pro porušení práv výrobce zvukového záznamu, jakož i práv výkonných umělců a práv autorských k dané skladbě. Zemský dvůr v Hamburku žalobě vyhověl. Odvolání společnosti Pelham pak bylo opakovaně zamítnuto, až se věc dostala ke Spolkovému ústavnímu soudu, který věc vrátil ke Spolkovému soudnímu dvoru a ten pro nejednotnou judikaturu předložil Soudnímu dvoru předběžné otázky.

Soudní dvůr měl zodpovědět, zda vynětí velmi krátkých zvukových úryvků může být zásahem do práva výrobce zvukových záznamů, zda se v takovém případě jedná o rozmnoženinu, či zda je takový akt krytý některou z výjimek a omezení. Soudní dvůr byl navíc tázán, jaká je v dané

[68] Srov. body 89 a násl. anotovaného rozhodnutí.

situaci aplikovatelnost citační výjimky, zda existuje alespoň minimální prostor pro uvážení při provádění výjimek a omezení a jaká je v daném kontextu role základních lidských práv.

Soudní dvůr připomněl rozsah práv výrobců zvukových záznamů[69] a stejně tak apeloval na nutný soulad a rovnováhu se základními lidskými právy katalogovanými v Listině základních práv Evropské unie.[70] Na základě toho uvedl, že samplování nemůže být chápáno jako rozmnožování ve smyslu čl. 2 směrnice InfoSoc.[71] Soudní dvůr dále vyzdvihnul nutnou návratnost investice do výroby zvukových záznamů a důležitost práva výrobce, jakož i nutnost boje proti pirátství a s tím spojenou analýzu dopadu ochrany rozmnoženin.[72] Soudní dvůr též vyložil tzv. právo na volné užití[73] a zdůraznil roli lidských práv při aplikaci základních výjimek a omezení.[74] Na adresu citace Soudní dvůr dodal, že citace se může týkat i hudebního díla,[75] bude záležet na kontextu užití takové citace, rozeznatelnosti v těle další skladby a obvyklém smyslu.[76]

Soudní dvůr proto uzavřel, že výrobce zvukových záznamů může bránit tomu, aby třetí osoba použila byť jen velmi krátký zvukový vzorek z onoho záznamu a začlenila ho do jiného zvukového záznamu, ledaže je do něj tento vzorek začleněn v pozměněné a při poslechu nerozpoznatelné podobě. Stejně tak uvedl, že záznam obsahující přenesené hudební vzorky není rozmnoženinou jako takovou, protože nepřebírá prvotní záznam nebo jeho podstatnou část. Dodal dále, že výčet výjimek a omezení dle čl. 5 směrnice InfoSoc je taxativní, pro použití citační výjimky musí být dílo, které je předmětem dotčené citace, rozeznatelné. Uzavřel, že čl. 2 této směrnice představuje opatření plné harmonizace.

Autor: JZ

[69] Srov. body 26 a násl. anotovaného rozhodnutí.

[70] Srov. body 32 a násl. anotovaného rozhodnutí.

[71] Srov. bod 37 anotovaného rozhodnutí.

[72] Srov. body 44 a násl. anotovaného rozhodnutí.

[73] Srov. bod 56 anotovaného rozhodnutí.

[74] Srov. body 60 a násl. anotovaného rozhodnutí.

[75] Srov. bod 68 anotovaného rozhodnutí.

[76] Srov. body 70 a násl. anotovaného rozhodnutí.

ZÁKON REGULUJÍCÍ ČINNOST VYHLEDÁVAČE JE „TECHNICKÝ PŘEDPIS“ VE SMYSLU SMĚRNICE 98/34

Soud: Soudní dvůr Evropské unie
Věc: C-299/17 (VG Media)
Datum: 12. 9. 2019
Dostupnost: curia.europa.eu

Při zadání vyhledávaného výrazu do vyhledavače provazovaného společností Google se zobrazí tzv. Snippet, což je krátký text nebo úryvek textu sloužící uživateli k posouzení relevantnosti zobrazeného výsledku pro jeho konkrétní potřebu. Společnost VG Media podala proti společnosti Google žalobu na náhradu škody způsobenou tím, že společnost Google od 1. 8. 2013 používá při zobrazení výsledků vyhledávání zpráv úryvky z textů, obrázky a pohyblivé obrázky, aniž za to platí poplatek. Tento závěr společnost VG Media dovodila z ustanovení autorského zákona, která Snippety regulují a která nabyla účinnosti právě 1. 8. 2013.

Soudní dvůr byl tázán, zda čl. 1 bod 11 směrnice 98/34 (o postupu při poskytování informací v oblasti norem a technických předpisů a předpisů pro služby informační společnosti) musí být vykládán v tom smyslu, že vnitrostátní ustanovení, které zakazuje pouze komerčním provozovatelům vyhledávačů a komerčním poskytovatelům služeb, kteří zpracovávají obsah obdobným způsobem, veřejně zpřístupňovat tiskoviny nebo jejich části (s výjimkou jednotlivých slov nebo velmi krátkých úryvků textu), představuje „technický předpis“, jehož návrh musí být pod rizikem sankce neaplikovatelnosti předem oznámen Komisi.[77]

Soudní dvůr v této souvislosti uvedl, že technický předpis představuje čtyři kategorie opatření, a to zaprvé technickou specifikaci, zadruhé jiný požadavek, zatřetí předpis pro služby nebo začtvrté právní a správní předpisy členských států zakazující výrobu, dovoz, prodej nebo používání určitého výrobku nebo zakazující poskytování nebo využívání určité služby

[77] Srov. bod 24 anotovaného rozhodnutí.

nebo usazování poskytovatele služeb.[78] Předmětné vnitrostátní ustanovení nelze považovat za technickou specifikaci, neboť se nevztahuje na výrobek nebo jeho obal,[79] nespadá ani do kategorie jiný požadavek, neboť se netýká spotřebního cyklu výrobku po jeho uvedení na trh.[80]

Aby byl technický předpis považován za předpis pro služby, musí být zaměřený specificky na služby informační společnosti.[81] Soudní dvůr konstatoval, že ačkoli tento cíl nevyplývá ze samotného znění vnitrostátního ustanovení, z jeho odůvodnění vyplývá, že jeho konkrétním záměrem je výslovně a cíleně regulovat služby informační společnosti a chránit oprávněné zájmy vydavatelů tisku před porušováním autorského práva prostřednictvím vyhledávačů on-line.[82]

Soudní dvůr tedy dospěl k závěru, že předmětné ustanovení představuje technický předpis a jeho návrh tak musí být v souladu s požadavkem vyplývajícím ze směrnice 98/34 předem oznámen Komisi.

Autorka: IK

OCHRANA DESIGNU AUTORSKÝM PRÁVEM

Soud: Soudní dvůr Evropské unie
Spojené věci: C-683/17 (Cofemel)
Datum: 12. 9. 2019
Dostupnost: curia.europa.eu

Společnost *Cofemel* navrhovala a vyráběla oděvy stejně jako společnost *G-Star*, která je držitelem několika ochranných známek užívaných v oděvním průmyslu, konkrétně v případě džín, mikin a triček. Společnost Cofemel se přitom měla dopustit užívání designu chráněného ochrannými známkami bez náležité licence.

[78] Srov. bod 25 anotovaného rozhodnutí.

[79] Srov. bod 26 anotovaného rozhodnutí.

[80] Srov. tamtéž.

[81] Srov. bod 31 anotovaného rozhodnutí.

[82] Srov. bod 35 a 36 anotovaného rozhodnutí.

Společnost G-Star podala proti uvedené společnosti Cofemel žalobu pro porušování autorských práv a nekalosoutěžní jednání, přičemž tvrdila, že jednotlivé modely oblečení jsou jejími autorskými díly. Právě tuto argumentaci společnost Cofemel rozporovala. Soud prvního stupně žalobě částečně vyhověl. Po odvolání společnosti Cofemel soud druhého stupně daný rozsudek potvrdil. V návaznosti na podané dovolání Nejvyšší soud Portugalska provedl výklad pojmových znaků autorského díla a pro nejasnou judikaturu položil Soudnímu dvoru předběžné otázky.

Soudní dvůr musel řešit, zda je originalita nutným pojmovým znakem i v případě děl užitého umění, průmyslových vzorů a designových děl, která mají vedle užitného účelu vlastní charakteristický vizuální efekt z estetického hlediska. Stejně tak měl posoudit, zda naplnění znaku uměleckého výtvoru není pro dosažení autorskoprávní ochrany díla postačující.

Soudní dvůr odkázal na svou bohatou judikaturu v oblasti pojmových znaků autorského díla[83] a připomněl podstatnou roli originality, která musí odrážet osobnost autora v mezích tvůrčí svobody,[84] jakož i roli objektivního zachycení.[85] Jedině při naplnění všech těchto Soudním dvorem dovozených znaků bude daná komodita dílem a bude chráněna autorským právem. Po odkazu na Bernskou úmluvu[86] Soudní dvůr zdůraznil souběh ochrany průmyslových vzorů a autorského práva[87] a připomněl zejména jejich odlišný charakter, cíl a odlišné režimy ochrany.[88] Po takovém rozboru Soudní dvůr naznal, že je bezpředmětné zodpovídat druhou položenou otázku.

Soudní dvůr dospěl k závěru, že autorskoprávní ochrana nemůže být přiznávána průmyslovým vzorům jen proto, že mají vedle vlastního užitného účelu i charakteristický vizuální efekt z hlediska estetického.

Autor: JZ

[83] Srov. body 28 a násl. anotovaného rozhodnutí.

[84] Srov. bod 30 anotovaného rozhodnutí.

[85] Srov. bod 32 anotovaného rozhodnutí.

[86] Srov. body 41 a násl. anotovaného rozhodnutí.

[87] Srov. body 45 a 48 anotovaného rozhodnutí.

[88] Srov. body 50 a násl. anotovaného rozhodnutí.

OSOBNÍ ÚDAJE A SOUKROMÍ

MOŽNOST TRESTAT PORUŠENÍ NAŘÍZENÍ 2016/679 V ŘÍZENÍ ZAHÁJENÝCH PŘED PŘIJETÍM ADAPTAČNÍ LEGISLATIVY

Soud: Nejvyšší správní soud
Věc: 9 As 380/2017 - 46
Datum: 31. 1. 2019
Dostupnost: nssoud.cz

Stavební bytové družstvo Praha se dopustilo neoprávněného shromažďování osobních údajů vlastníků, nájemců, podnájemců a dalších členů domácnosti všech bytových a nebytových jednotek, které jsou v jeho vlastnictví či správě.[89]

V roce 2016 mu byla za tento správní delikt podle zákona o ochraně osobních údajů[90] uložena pokuta Úřadem pro ochranu osobních údajů. Družstvo proti rozhodnutí podalo rozklad, jenž předsedkyně Úřadu zamítla. Věc dále pokračovala k Městskému soudu v Praze, jenž v roce 2017 žalobu proti rozhodnutí zamítl jako nedůvodnou. Tento rozsudek proto družstvo napadlo kasační stížností u Nejvyššího správního soudu, který ji rovněž shledal nedůvodnou a zamítl ji *in fine*.[91]

V průběhu řízení před Nejvyšším správním soudem družstvo namítalo, že dne 25. 5. 2018 účinnost nařízení 2016/679. Zákon o ochraně osobních údajů sice nebyl formálně zrušen, avšak účinností nařízení 2016/679 došlo k faktické derogaci hmotněprávních norem tohoto zákona a jejich nahrazení přímo aplikovatelným nařízením. Současně však tehdy ještě nebyl přijat adaptační zákon k jeho provedení.

Vzhledem k těmto skutečnostem, bylo družstvo toho názoru, že trestnost jeho jednání dnem účinnosti nařízení 2016/679 zanikla, jelikož se trestnost jeho činu posoudí a trest ukládá podle právní úpravy, která nabyla

[89] Bod 9 anotovaného rozhodnutí.

[90] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[91] Bod 1, 3, 11 a 57 anotovaného rozhodnutí.

účinnosti až poté, kdy byl trestný čin spáchán, je-li to pro pachatele příznivější. Opíral se přitom o názor, že nařízení 2016/679 nemůže formulovat univerzální skutkové podstaty deliktních jednání a přímo na jeho základě není možné trestat.[92] Nejvyšší správní soud se proto zabýval otázkou, zda není nutné na odpovědnost stěžovatele aplikovat novou právní úpravu nařízení 2016/679, přičemž na základě usneseníč. j. 5 As 104/2013 – 46 došel k tomu, že novou, pro pachatele příznivější úpravu lze použít pouze ve správním řízení, případně v řízení před krajským (zde městským) soudem. Soud se proto již dále nezabýval ani otázkou, zda by úprava byla pro pachatele skutečně příznivější.[93]

Z tohoto závěru vyplývá, že nařízení 2016/679 skutečně představuje „komplexní podklad pro ukládání sankcí", jak jej nazval Úřad[94] a bylo by podle něj možné trestat porušení nových povinností, které by nebylo možné postihnout podle zákona o ochraně osobních údajů. Přijetím zákona o zpracování osobních údajů[95] byla však tato mezera v právní úpravě již překlenuta.

Autorka: AS

PŘECHOD OD ZÁKONA 101/2000 SB. K OBECNÉMU NAŘÍZENÍ

Soud: Nejvyšší správní soud
Věc: 4 As 140/2019 - 27
Datum: 27. 6. 2019
Dostupnost: nssoud.cz

Ministerstvo vnitra (MV) od září 2014 do října 2014 umožnilo chybným nastavením informačního sytému neoprávněný přístup České televizi a Českému rozhlasu do Registru obyvatel, čímž došlo k porušení zabezpečení osobních údajů dohromady v přibližně 70 250 případech.[96]

[92] Bod 19 anotovaného rozhodnutí.

[93] Bod 56 anotovaného rozhodnutí.

[94] Bod 27 anotovaného rozhodnutí.

[95] Zákon č. 110/2019 Sb., o zpracování osobních údajů.

[96] Odst. 3 anotovaného rozhodnutí.

Úřad pro ochranu osobních údajů (ÚOOÚ) proto uložil MV pokutu v celkové výši 500 000 Kč. MV podalo správní žalobu a po potvrzení rozhodnutí ÚOOÚ rovněž kasační stížnost. MV svoji stížnost podložilo řadou argumentů, z nichž nejzajímavější je ten, dle kterého Obecné nařízení o ochraně osobních údajů (nařízení č. 2016/679, dále GDPR) klade na správce osobních údajů mírnější nároky než zákon č. 101/2000 Sb. (dále ZoOOÚ), protože jeho čl. 24 a 32 stanoví povinnosti pro správce mírněji, než rigidní § 13 ZoOOÚ. Vzhledem k tomu měl dle názoru MV ÚOOÚ i Městský soud v Praze přihlédnout k této mírnější úpravě a pokutu neudělit, nebo zrušit.

Hlavní řešenou otázkou je v tomto případě vztah § 13 odst. 1 ZoOOÚ a čl. 24 a 32 GDPR.

MV uvádí, že zatímco § 13 odst. 1 ZoOOÚ klade na správce údajů v podstatě absolutní nároky bez výjimky, nové čl. 24 a 32 GDPR požadují pouze „vhodná opatření“, případně „vhodnou úroveň bezpečnosti“, přičemž má být zhodnocena hlavně rizikovost daného zpracování.[97] Z toho důvodu je dle MV nová úprava pro správce příznivější.

NSS odmítl argumentaci MV a kasační stížnost zamítl. Dle NSS není možné vykládat ustanovení GDPR jako příznivější právní úpravu. Rozdíl mezi § 13 odst. 1 ZoOOÚ a čl. 24 a 32 GDPR není možné vykládat tak, že § 13 odst. 1 představuje absolutistický požadavek na zabezpečení, zatímco čl. 24 a 32 GDPR tento požadavek neobsahují. Dle NSS čl. 24 a 32 pouze výslovně konkretizují hlediska, k nimž správce musel přihlížet i při posuzovaní opatření dle § 13 odst. 1 ZoOOÚ.[98] Z argumentace stěžovatelky pak dle NSS nevyplynulo, že by její jednání nepředstavovalo správní delikt dle GDPR.[99] Neobstál ani argument MV, že riziko zpracování bylo nízké, protože neoprávněný přístup k údajům měly jen Česká televize a Český rozhlas.[100] NSS odmítl bagatelizaci vytýkaného porušení zabezpečení

[97] Odst. 9 anotovaného rozhodnutí.

[98] Odst. 26 anotovaného rozhodnutí.

[99] Odst. 28 anotovaného rozhodnutí.

[100] Odst. 12 anotovaného rozhodnutí.

a připomněl, že Česká republika je ústavně definována jako právní stát, a proto je nutné vyžadovat důsledné respektování zákonných povinností.[101]

Autor: JM

TLAČÍTKO „TO SE MI LÍBÍ“ A S NÍM SOUVISEJÍCÍ ROLE SPRÁVCŮ OSOBNÍCH ÚDAJŮ

Soud: Soudní dvůr Evropské unie
Věc: C-40/17 (Fashion ID)
Datum: 29. 7. 2019
Dostupnost: curia.europa.eu

Rozsudek Soudního dvora byl vydán na základě několika předběžných otázek, které tomuto byly předloženy v rámci sporu mezi společností Fashion ID GmnH & Co KG („Fashion ID“) a Verbraucherzentrale NRW eV ohledně začlenění pluginu pro propojení se sociální sítí Facebook. Ten společnost Fashion ID použila na svých webových stránkách.[102] Fashion ID do svých webových stránek konkrétně začlenila tlačítko „to se mi líbí“.[103] Na základě tohoto přitom měly být osobní údaje návštěvníků stránek Fashion ID předány společnosti Facebook Ireland Ltd.[104] Verbraucherzentrale NRW eV jakožto veřejně prospěšné sdružení na ochranu zájmů spotřebitelů podalo žalobu proti společnosti Fashion ID, aby ukončila svou praxi spočívající v onom předávání osobních údajů bez souhlasu subjektů údajů a za porušení informační povinnosti vůči těmto subjektům.[105] Zemský soud v Düsseldorfu této žalobě částečně vyhověl a společnost Fashion ID se proti danému rozhodnutí následně odvolala.[106]

[101] Odst. 33 anotovaného rozhodnutí.
[102] Bod 2 anotovaného rozhodnutí.
[103] Bod 25 anotovaného rozhodnutí.
[104] Bod 27 anotovaného rozhodnutí.
[105] Bod 28 a 29 anotovaného rozhodnutí.
[106] Bod 30 a 31 anotovaného rozhodnutí.

Odvolacím soudem je v dané věci vrchní zemský soud v Düsseldorfu, který je rovněž předkladatelem předběžných otázek.[107]

V rámci odpovědí došel Soudní dvůr k tomu, že články 22 až 24 směrnice 95/96 nebrání vnitrostátní právní úpravě umožňující sdružením na ochranu spotřebitelů podat žalobu proti údajnému rušiteli ochrany osobních údajů.[108]

Soudní dvůr v rámci odpovědí na předběžné otázky konstatoval, že Fashion ID je možné (stejně jako druhou ze zmíněných společností) považovat za správce osobních údajů sbíraných a následně předávaných společnosti Facebook Ireland Ltd.[109] To proto, že společně s Facebook Ireland Ltd. určuje účel a prostředky zpracování osobních údajů.[110] Výše uvedené Soudní dvůr dovodil i přesto, že k těmto osobním údajům Fashion ID nemá přístup.[111]

Následně Soudní dvůr mimo jiné konstatoval, že povinnost získání souhlasu v dané věci, stejně jako výkon informační povinnosti, leží na prvním ze správců, tedy Fashion ID, avšak logicky pouze pro operace nebo soubory operací, u nichž skutečně určuje účely a prostředky zpracování.[112]

Anotované rozhodnutí vnáší větší jistotu do vztahů mezi provozovateli internetových stránek a poskytovateli služeb využívající tlačítka typu „to se mi líbí“, a to nejen ve smyslu již zrušené směrnice 95/46/ES, ale i ve smyslu v současné době účinného nařízení (EU) 2016/279. Závěry z anotovaného rozhodnutí jsou totiž obecně aplikovatelné i při výkladu jeho ustanovení.

Autor: JS

[107] Bod 31 anotovaného rozhodnutí.

[108] Bod 43 až 63 anotovaného rozhodnutí.

[109] Bod 85 anotovaného rozhodnutí.

[110] Viz bod 65-71 anotovaného rozhodnutí. V souvislosti s tímto je vhodné upozornit na zakotvení institutu společného správcovství v čl. 26 nařízení (EU) 2016/279, které směrnici 95/46/ES zrušilo. To však neznamená, že by závěry z anotovaného rozhodnutí nebyly použitelné i dle současné právní úpravy.

[111] Bod 82 anotovaného rozhodnutí.

[112] Bod 98-106 anotovaného rozhodnutí.

POVINNOST PROVOZOVATELE VYHLEDÁVAČE ODSTRANIT ODKAZY VEDOUCÍ KE ZVLÁŠTNÍM KATEGORIÍM OSOBNÍCH ÚDAJŮ Z VÝSLEDKŮ VYHLEDÁVÁNÍ

Soud: Soudní dvůr Evropské unie
Věc: C-136/17 (GC a další)
Datum: 24. 9. 2019
Dostupnost: curia.europa.eu

Předmětem sporu v původním řízení byly na sobě nezávislé žádosti subjektů údajů GC, AF, BH a ED o výmaz odkazů z výsledků vyhledávání, které se ve vyhledávači společnosti Google zobrazily po zadání jejich jmen. Od politických názorů přes náboženská přesvědčení až po údaje týkající se protiprávního jednání – ve všech případech se jednalo o odkazy vedoucí ke zvláštním kategoriím údajů.[113]

Poté, co společnost Google odmítla těmto žádostem o výmaz vyhovět, se subjekty údajů obrátily na CNIL (francouzský dozorový úřad), který však řízení o stížnostech zastavil. Stěžovatelé proto podali žaloby ke Conseil d'État (Státní rada), která je spojila a dospěla k závěru, že v rámci argumentace vyvstalo několik problematických otázek, které je nutné adresovat Soudnímu dvoru.[114]

Tyto otázky se týkaly výkladu čl. 8 směrnice o ochraně osobních údajů[115], jakož i čl. 9 a 10 nařízení 2016/679[116], konkrétně rozsahu povinností provozovatele vyhledávače jako správce osobních údajů respektovat zákaz zpracování zvláštních kategorií osobních údajů, jsou-li takové údaje součástí obsahu umístěném na internetu třetími osobami,

[113] Bod 25-28 anotovaného rozhodnutí.

[114] Bod 29-31 anotovaného rozhodnutí.

[115] 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.

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

a umožnit výkon práva subjektu údajů na výmaz při vyvážení s ostatními základními právy, zejm. svobodou informací.

V rozsudku Soudní dvůr navazuje na své závěry z věci *Google Spain*[117] *a* dodává, že s přihlédnutím ke zvláštnostem zpracování vyhledávače se jeho provozovatel jakožto správce musí řídit zákazem zpracování zvláštních kategorií údajů, a to když tento provozovatel pod dohledem příslušných vnitrostátních orgánů provádí ověření na základě žádosti subjektu údajů.[118] Provozovatel vyhledávače je přitom na základě těchto ustanovení povinen až na stanovené výjimky vyhovět žádostem o odstranění odkazů na internetové stránky, které obsahují zvláštní kategorie osobních údajů. V případě, kdy je některá z výjimek aplikovatelná, provozovatel musí vyvážit základní práva na základě všech relevantních okolností věci a s ohledem na závažnost zásahu do základního práva subjektu údajů na soukromí a na ochranu osobních údajů ověřit, zda je uvedení tohoto odkazu nezbytně nutné k tomu, aby bylo chráněno právo uživatelů internetu na svobodu informací.[119] V případě zpracování zvláštní kategorie údajů týkajících se protiprávního jednání či rozsudků v trestních věcech, provozovatel vyhledávače je povinen vyvážit základní práva a zpravidla vyhovět žádosti o odstranění odkazů, pokud se informace týkají dřívější fáze dotčeného soudního řízení, již neodpovídající současnému stavu.

Ač Soudní dvůr potvrdil obecný zákaz zpracování zvláštních kategorií údajů, rozhodnutí ve svém důsledku zohledňuje zvláštní povahu zpracování prováděném provozovatelem vyhledávače a přibližuje za těchto okolností výkon práva na výmaz institutu notice-and-action, čímž zároveň dochází k přenosu větší odpovědnost za vyvažování základních práv na samotné povinné subjekty.

Autorka: AS

[117] Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014, ve věci C 131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

[118] Bod 45-48 anotovaného rozhodnutí.

[119] Bod 69 anotovaného rozhodnutí.

TERITORIÁLNA PÔSOBNOSŤ PRÁVA „NA ZABUDNUTIE“

Soud: Súdny dvor Európskéj Únie
Věc: C-507/17 (Google v CNIL)
Datum: 24.9.2019
Dostupnost: curia.europa.eu

Francúzsky úrad na ochranu osobných údajov CNIL vydal voči spoločnosti Google rozhodnutie, v ktorom nariadil Google odstrániť zo svojho vyhľadávača odkazy vedúce na webové stránky, ktoré sa zobrazili ako výsledky vyhľadávania mena dotknutej osoby, pričom toto odstránenie odkazov malo byť vykonané na všetkých koncovkách doménového mena vyhľadávača. Google tejto výzve odmietol vyhovieť a odstránil predmetné odkazy iba z výsledkov zobrazených vo verziách svojho vyhľadávača, ktoré mali doménové meno členského štátu EÚ. CNIL mu na základe neuposlúchnutia výzvy uložil pokutu 100 000 EUR.[120]

Google podal proti rozhodnutiu, ktorým mu CNIL uložil pokutu, žalobu na francúzsky súd. Ten inicioval konanie o predbežnej otázke pred SDEÚ.[121]

Hlavnou predbežnou otázkou posudzovanou SDEÚ bolo, či má poskytovateľ vyhľadávača v prípade, ak vyhovie žiadosti dotknutej osoby o odstránenie odkazov, vykonať toto odstránenie na všetkých doménach svojho vyhľadávača a v prípade, že nie, z ktorých verzií domén má toto odstránenie vykonať. Súd zároveň riešil aj povinnosť vyhľadávačov v týchto prípadoch využiť tzv. geoblokáciu.[122]

SDEÚ vychádzal zo svojho predchádzajúceho rozhodnutia vo veci *Google Spain*,[123] pričom podobne ako v tomto prípade vykladal článok 12 b) a článok 14 a) smernice o ochrane osobných údajov,[124] avšak do výkladu

[120] Body 30-33 anotovaného rozhodnutia.

[121] Bod 39 anotovaného rozhodnutia.

[122] Tamtiež.

[123] Rozsudok SDEÚ vo veci C-131/12 z 13. mája 2014, Google Spain a Google (ďalej len „Google Spain“).

[124] Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov.

začlenil aj článok 17 ods. 1 GDPR.[125] Podľa SDEÚ treba právo na zabudnutie, ktoré nie je absolútnym právom, vyvažovať aj s inými právami, najmä s právom na informácie. Nakoľko rôzne štáty sveta majú rôzny prístup k vyváženiu týchto práv prípadne právo na zabudnutie ani nepoznajú a nakoľko zákonodarca v predmetných predpisoch nepredpokladal, že by právo na zabudnutie malo mať pôsobnosť mimo EÚ, poskytovateľ vyhľadávača nie je povinný vykonať odstránenie odkazu vo všetkých verziách vyhľadávača.[126] Ak však vyhovie žiadosti o odstránenie odkazu, je povinný ho odstrániť vo verziách vyhľadávača zodpovedajúcich všetkým členským štátom, vzhľadom na skutočnosť, že právo byť zabudnutý je upravené v GDPR ako v norme s priamou pôsobnosťou v celej EÚ.[127] Zároveň je vyhľadávač v prípade potreby povinný vykonať opatrenia, ktoré sú v súlade so zákonom a ktoré zabránia používateľom z EÚ (resp. ich účinne odradia) pristúpiť k odstráneným odkazom cez doménu vyhľadávača určenú pre používateľov z iného ako členského štátu EÚ.[128]

Rozsudok bližšie upresňuje teritoriálnú pôsobnosť právo na zabudnutie a obmedzuje tak právo fyzických osôb z členských štátov EÚ požadovať globálne odstránenie odkazu vo výsledkoch vyhľadávania zobrazených po vyhľadaní ich mena.

Autorka: PV

PŘEDZAŠKRTNUTÉ POLÍČKO NENÍ PLATNÉ VYJÁDŘENÍ SOUHLASU

Soud:	Soudní dvůr Evropské unie
Věc:	C-673/17 (Planet49)
Datum:	1. 10. 2019
Dostupnost:	curia.europa.eu

[125] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

[126] Body 59-65 anotovaného rozhodnutia.

[127] Bod 66 anotovaného rozhodnutia.

[128] Bod 70 anotovaného rozhodnutia.

Německá společnost žalovala Planet 49, za používání předzaškrtnutého políčka pro souhlas s používáním cookies a následné předávání údajů třetím stranám.[129] Zemský soud žalobě částečně vyhověl, načež vyšší zemský soud rozhodl opačně.[130] Až Spolkový soudní dvůr podal předběžné otázky SDEU, kterých se ptal, zda je je předzaškrtnuté políčko platným souhlasem dle čl. 5 odst. 3 směrnice 2002/58/ES, zda při použití čl. 5 odst. 3 směrnice 2002/58/ES hraje roli, pokud jsou zpracované informace osobními údaji a jaké informace musí poskytovatel služby podle čl. 5. odst. 3 směrnice 2002/58/ES poskytnout.[131]

Spor bylo nutné posoudit dle původní i nové legislativy.[132] SDEU se zabýval vývojem čl. 5 odst. 3 směrnice 2002/58/ES, jež původně požadoval pro ukládání souborů do koncových zařízení možnost takové ukládání odmítnout (opt-out) a po novelizaci byl zpřísněn požadavek na explicitní souhlas (opt-in).[133] Novelizace v německém právním řádu však zvýšený nárok nereflektovala a ponechala režim opt-out.[134]

Pokud souhlas uživatele spočívá v absenci vyjádření námitky proti předzaškrtnutému políčku, pak dle SDEU nelze s jistotou říci, zda bude uživatel před-zaškrtnutému políčku věnovat pozornost. Nečinnost ani nedbalost proto dostatečně nevypovídá o vůli uživatele.[135] SDEU konstatoval, že pro platný souhlas, musí být uživatel schopný posoudit vlastní situaci natolik, aby znal efekt udělení souhlasu.[136] K tomuto rozhodnutí je nezbytné mít kvalitní a dostupné informace, jakými je: doba funkčnosti cookies a možnost přístupu třetích osob.[137]

[129] Bod 24 anotovaného rozhodnutí.

[130] Bod 30-31 anotovaného rozhodnutí.

[131] Bod 32 anotovaného rozhodnutí.

[132] Bod 49 anotovaného rozhodnutí.

[133] Bod 54 anotovaného rozhodnutí.

[134] Stejně jako v českém § 89 odst. 3 zákona o elektronických komunikacích č. 127/2005 Sb.

[135] Bod 62 anotovaného rozhodnutí.

[136] Bod 67 anotovaného rozhodnutí.

[137] Body 117-120 anotovaného rozhodnutí.

SDEU na základě výše uvedeného uzavřel, že předzaškrtnuté políčko není dostatečným projevem vůle pro nesplnění nároku na aktivní a informovaný souhlas. Souhlas s přístupem do koncového zařízení přitom nijak nekvalifikuje takto ukládané údaje,[138] a tudíž není relevantní, zda se jedná o osobní údaje. Vždy však subjekt údajů musí dostat informaci o době uchování cookies a zda k souborům cookies mají přístup třetí osoby.[139]

Autor: JK

ZÁSAH DO PRÁVA NA OCHRANU OSOBNÝCH ÚDAJOV ZAKLADÁ NÁROK NA NÁHRADU ŠKODY SÁM OSEBE, BEZ NUTNOSTI PREUKAZOVAŤ FINANČNÚ ŠKODU ALEBO NEMAJETKOVÚ UJMU

Soud: Britský odvolací súd
Věc: Lloyd v Google [2019] EWCA Civ 1599
Datum: 2.10.2019
Dostupnost: judiciary.uk

Pán Lloyd, obhajca práv spotrebiteľov, podal na britský súd hromadnú žalobu v mene 4 miliónov používateľov telefónov iPhone na spoločnosť Google, ktorá tajne monitorovala ich internetové aktivity medzi augustom 2011 a februárom 2012.[140] Google v tomto čase implementoval tzv. *Safari Workaround,* ktorý mu umožnil uložiť do prehliadačov Safari na iPhone svoj *DoubleClick* cookie bez vedomia používateľa či bez jeho súhlasu. Google tak mohol sledovať aktivity používateľov naprieč webstránkami a zbierať či vyvodzovať o týchto používateľoch mnohé informácie, na základe ktorých jednotlivé kategórie používateľov ponúkal svojim zákazníkom na cielenú reklamu.[141]

[138] Bod 108 anotovaného rozhodnutí.

[139] Bod 122 anotovaného rozhodnutí.

[140] Bod 1 anotovaného rozhodnutia.

[141] Body 10-12 anotovaného rozhodnutia.

V novembri 2017 požiadal p. Lloyd britský súd o povolenie, aby boli spoločnosti Google doručené procesné dokumenty mimo jurisdikcie súdu, teda v USA, kde má Google sídlo. Táto žiadosť bola zamietnutá, avšak z dôvodu novosti žaloby ako aj žalobcom zvolenej procedúry bolo odvolacím súdu umožnené voči tomuto rozhodnutiu podať odvolanie.[142]

Hlavnou otázkou, ktorú skúmal odvolací súd bolo, či môže žalobca získať náhradu škody za stratu kontroly nad vlastnými osobnými údajmi podľa čl. 13 ods. 1 britského zákona o ochrane osobných údajov (ďalej len „DPA"),[143] ktorým bol implementovaný článok 23 ods. 1 smernice o ochrane osobných údajov,[144] a to bez toho, aby musel preukazovať peňažnú škodu alebo inú ujmu.

Súd dovodil, že zákon o ochrane osobných údajov bol prijatý na vykonanie smernice o ochrane osobných údajov a keďže táto smernica bola vydaná na vykonanie čl. 8 Charty základných práv EÚ, ktorý ustanovuje právo na ochranu osobných údajov, čl. 13 DPA je potrebné vykladať v kontexte tejto Charty. Charta pritom ustanovuje, že ktokoľvek, koho práva z Charty sú porušené, má právo na účinný opravný prostriedok.[145] Zároveň sa súd oprel o rozhodnutie vo veci *Gulati*,[146] podľa ktorého má žalobca právo na náhradu škody bez dokazovania peňažnej straty alebo inej ujmy za civilný delikt zneužitia súkromných informácií. Podľa súdu tak môže byť žalobcovi priznaný nárok na náhradu škody za stratu kontroly nad osobnými údajmi, a to aj v prípade, že mu nebola spôsobená finančná ani nemajetková ujma. Iba týmto spôsobom získajú jednotlivci efektívnu ochranu pred porušením ich práv garantovanú Chartou.[147]

Rozsudok výrazne posilňuje pozíciu fyzických osôb, ktorých právo na ochranu osobných údajov bolo porušené, nakoľko pri uplatňovaní svojich nárokov za stratu kontroly nad svojimi osobnými údajmi na britských

[142] Bod 14 anotovaného rozhodnutia.

[143] The Data Protection Act 1998.

[144] Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov.

[145] Bod 42 anotovaného rozhodnutia.

[146] Gulati v MGN Limited [2015] EWCA Civ 1291.

[147] Bod 70 anotovaného rozhodnutia.

súdoch už nebudú musieť preukazovať škodu alebo inú nemajetkovú ujmu, na druhej strane však uvedené znamená vyššie riziko litigácii a následných nákladov pre prevádzkovateľov, ktorí porušili svoju povinnosť v zmysle DPA.

Autorka: PV

GRIFFIN, JAMES. *THE STATE OF CREATIVITY, THE FUTURE OF 3D PRINTING, 4D PRINTING AND AUGMENTED REALITY*

DOMINIKA COLLETT[1]

GRIFFIN, James. *The State of Creativity, The Future of 3D Printing, 4D Printing and Augmented Reality*. Cheltenham: Edward Elgar Publishing, 2019. 304 str.

Publikace přináší vyčerpávající teoretické pojednání o základním pilíři práva duševního vlastnictví jimž, je tvůrčí činnost. Text monografie v mnoha místech reflektuje jednak závěry humanitních věd, zejména filosofie a sociologie, tak i poznání v oblasti technických věd. Monografii lze pak rozdělit na část, která se zabývá současnou právní úpravou a jejím historickým vývojem a část, která předkládá návrhy nové právní úpravy, které je založena primárně na regulaci tvůrčí činnosti.

První kapitola monografie se věnuje historickému vývoji lidské tvořivosti. Tvůrčí schopnost je prezentována jako imanentní lidská vlastnost, která je neodmyslitelně spjata s vývojem člověka samotného i s vývojem společnosti.[2] Autor se zaměřuje na tvořivost v jejich širších souvislostech, kdy mimo jiné identifikuje její biologickou podmíněnost. S biologickou podmíněností tvořivosti pak souvisí i přítomný prvek spolupráce a konfliktu.[3] Dalším důležitým prvkem pro schopnost tvořit je vnímání okolí a získávání poznatků. Autor se v této části opírá o významné

[1] Mgr. Dominika Collett, doktorská studentka na Ústavu práva a technologií, Právnická fakulta Masarykovy univerzity, e-mail: dominika.collett@law.muni.cz.

[2] Viz str. 1-2 knihy.

[3] Viz str. 5 knihy.

práce z oblasti filozofie.[4] Zároveň se autor zamýšlí nad budoucí regulací tvůrčí činnosti skrze autorské právo a ochranu literárních děl na základě rozvoje technologie, kdy základním argumentem je možnost digitalizace jednotlivých výtvorů. V tomto místě lze s autorem polemizovat nad otázkou předmětu právní ochrany, neboť přestože je daný výtvor zachycen v digitální podobě (ve formě kódu), může být povaha tohoto předmětu od literárních děl v tradičním smyslu odlišná.[5]

Druhá kapitola se zabývá analýzou tvůrčí činnosti a otázkou její centrální role pro společnost. Hlavní důraz je v této kapitole kladen na vztah jednotlivce a státu v souvislosti s tvůrčí činností. V úvodu této kapitoly se však text věnuje obecnému vymezení tvůrčí činnosti. V této souvislosti autor rozlišuje tzv. vnitřní a vnější tvůrčí činnost. Vnitřní tvůrčí činnost jako taková je spojená s biologickým procesem odehrávajícím se uvnitř jednotlivce z čehož vyplývá, že jakákoliv regulace tohoto procesu je nemožná, neboť by se toliko jednalo o regulaci myšlenek, které nebyly vyjádřeny.[6] Vnější tvůrčí činnost je na druhou stranu dlouhodobě předmětem právní regulace a je spojena s principem vlastnictví, který tento vnější projev tvůrčí činnosti limituje. Kapitola následně obsahuje úvahu, jak tvůrčí schopnost jednotlivce ovlivnila vznik státu a považuje ji za základní předpoklad jeho vzniku.[7] Prostor je dán také úvaze, jaký vliv má na jednotlivce vyjádření tvůrčí činnosti jiné osoby. V této souvislosti se autor odvolává na úvahy Platona[8] a Nietzscheho[9] týkající se tvůrčí činnosti.

---

[4] LOCKE, John. *An Essay Concerning Human Understanding*. Londýn: Penguin Classics, 1998. 816 str.; Hegel, G. Philosophy of Right. Mineola: Dover Publications, 2005. 272 str.; Kant, I. Critique of Reason. Cambridge: Cambridge University Press, 1999. 785 str.

[5] V této souvislosti lze poukázat i na nevyhovující ochranu počítačových programů prostřednictvím autorského práva. Srov. GALAJDOVÁ, Dominika, ZIBNER, Jan. Nedostatky autorskoprávní ochrany počítačového programu. Právní rozhledy. Praha: Beck online, 2018, str. 784.

[6] Autor knihy v této souvislosti poukazuje pouze na koncept „push-button order“. Srov. Bronowski, J. *The Ascent of Man*. London: Ebury Publishing, 2011. 352 str.

[7] Viz str. 39 knihy.

[8] PLATO. *The Republic*. Cambridge: Cambridge University Press, 2000. 436 str.

[9] NIETZSCHE, Friedrich. *The Gay Science*. Manhattan: Random House Publishing, 1974. 95 str.

Následující kapitola se soustředí na důležitost prostoru, který je ponechán kreativitě ze strany právní regulace. V úvodní části této kapitoly se autor věnuje historickému vývoji prostoru tvůrčí svobody jednotlivce.[10] V této souvislosti je pak vyzdvihnut i význam jednotlivých nástrojů pro tvůrčí činnost jednotlivce. Následně se výklad detailně věnuje vlivu právní úpravy vytvářené státem na prostor tvůrčí svobody jednotlivce. Tato část přibližuje vývoj právní regulace jednotlivců a jejich tvůrčí svobody v historii, a to zejména na území Velké Británie. Na základě tohoto popisu pak autor demonstruje proměnu jednotlivých přístupů k právní regulace, kdy se předmětem regulace stává zejména vnější projev tvůrčí činnosti.[11]

Text čtvrté kapitoly se zabývá zvětšujícím se rozdílem mezi teoretickým výkladem zabývajícím se tvůrčí činností a zakotvením tvůrčí činnosti v právní úpravě. Právě soulad právní úpravy s podstatou tvůrčí činností je ze strany autora považován za významný pro opodstatnění právní úpravy.[12] Autor demonstruje, že přestože v počátcích byla právní regulace tvůrčí činnosti navázána na pochopení a podstatu tvůrčí činnosti od 14. století dochází k odchýlení se právní regulace. Právě postupný vývoj vedl k zakotvení vlastnického práva a kapitalismu jakožto hlavnímu odůvodnění právní úpravy tvůrčí činnosti.[13] Toto pojetí je však ze strany autora knihy kritizováno, neboť je v rozporu se samotnou schopností tvůrčí činnosti, která je na základě zakotvení konceptu vlastnického práva mylně pojímána.

Následující kapitola se zabývá zejména teoretickým pojetím vymáhání duševního práva a jeho vlivu na jednotlivce i stát. V úvodu se výklad obecně zaměřuje na význam hrozby negativních právních následků, které může aplikace práva vyvolat. Právě skrze hrozbu právního postihu dochází k formování chování jednotlivce a vývoji společnosti. Hrozby právním postihem jsou chápány jako prostředek, který vede k souladu mezi právní úpravou a každodenním životem společnosti.[14] V další části kapitoly je

[10] Viz str. 58 knihy.

[11] Viz str. 83 knihy.

[12] Viz str. 93 knihy.

[13] Viz str. 99 knihy.

[14] Viz str. 111 knihy.

popsáno, jaký má pak hrozící právní postih význam pro právní regulaci vytvářenou státem a jak má být tento případný postih právně zakotven, tak aby neohrozil tvůrčí činnost. Výklad zvažuje i možnost nové úpravy vymáhání práva v oblasti duševního vlastnictví. Autor navrhuje, aby případná právní regulace obsahovala[15]: a) vymezení jasného účelu v právní úpravě, který stanovuje, kdy může použití hrozby právní sankce negativně dopadnout na tvůrčí činnost, b) soubor zásad, které upravují, kdy se jedná o porušení právní úpravy a kdy se jedná o dovolené užití, c) systém, který umožňuje uživateli zjistit, kdo je autor.

Šestá kapitola se věnuje vlivu reprodukce ve společnosti. V první části kapitola pojednává obecně o jednotlivých předpokladech týkajících se reprodukce[16] a vývoje konceptu toku reprodukovaných myšlenek. Následně se výklad věnuje otázce vztahu mezi právní úpravou reprodukce ze strany státu a ze strany jednotlivce a obecně právní úpravě toku reprodukovaných myšlenek ve společnosti. V závěru této kapitoly pak autor pojednává o spojení reprodukčního toku s technologiemi. Na základě analýzy obsažené v této kapitole pak autor dospívá ke svým vlastním závěrům a návrhům nové právní regulace. V této souvislosti autor mimo jiné připomíná koncepty, jako jsou tzv. memes[17] nebo teorii informačního toku (z ang. information flow)[18], které však dostatečně nezohledňují vliv reprodukce ve společnosti. Je také zdůrazněna koncepce tzv. romantického autora, která spočívá na předpokladu, že autor tvoří v izolaci, tedy není

[15] Viz str. 130 knihy.

[16] Autor v anglickém originále používá výraz *reproduction*, který lze volně přeložit jako reprodukce. Tento výraz je v textu používán v obecné rovině a proto i v textu recenze je používáno toliko obecného pojmu, nikoliv např. pojmu pořízení rozmnoženiny, který má specifický význam v textu zákona č. 121/2000 Sb., autorských zákon.

[17] Srov. Dawkins, R. *The Selfish Gene: 40th Anniversary edition*. Oxford: Oxford University Press, 2018. 464 str. Dawkins definuje pojem „meme" jako jednotku replikace, která má určitě kulturní aspekty, které mohou ostatní tvůrci či uživatelé napodobovat nebo opakovat. Jako příklady memů uvádí Dawkins melodie, nápady, fráze nebo módní styl.

[18] Svůj původ má teorie zabývající se tokem informací má v pracích Platona, který konstatuje, že s myšlenkami by mělo být zacházeno jako s „tekoucím proudem vody". Obecně toto pojetí upouští od spojení procesu tvůrčí činnosti s vlastnictvím. Srov. Plato, *Timaeus*. Cambridge: Hackett Publishing Co, 2000. 112 str.

ovlivněn již existujícími výtvory.[19] Tento koncept však autor vyvrací a konstatuje, že obecně je proces reprodukce u lidí inherentně dán už tím, že vnímáme prostředí svými smysly.

Sedmá kapitola se následně soustřeďuje na samotnou tvůrčí činnost a problém jejího odlišení od následného užití jednotlivých výtvorů. V úvodní části je označen jako hlavní důvod nejasného rozlišení mezi tvůrčí činností a následným užitím děl skutečnost, že při zrodu dané právní úpravy byla možnost dalšího užití děl minimální.[20] Následně se kapitola zaměřuje na srovnání tvůrčí činnosti s konceptem kapitalizace výsledků tvůrčí činnosti, jež je základem stávající právní úpravy.[21] Závěr kapitoly se věnuje návrhu nového systému regulujícímu tvůrčí činnost.[22] Autor dále navrhuje zavedení paralelní právní úpravy pro tvůrčí činnost, která bude doplňovat stávající úpravu užití konečných výtvorů.[23] Dílčí části nově návrhovaného systému jsou pak obsahem následných kapitol, které lze považovat za nejzajímavější částí knihy. Hlavními základy tohoto systému by se měl stát tzv. kreativní fond a systém povinného licencování děl pro účely jejich dalšího užití.[24] Závěr sedmé kapitoly se věnuje právě obecně kreativnímu fondu a jeho zavedení. Fungování kreativní fondu autor přirovnává k digitální knihovně, která zajistí autorům přístup, k již existujícím dílům a jejich dalšímu tvůrčímu užití. Tento fond by dle návrhu měl být vytvořen a financován ze strany státu. Přestože se jedná o koncept, který si zaslouží pozornost není jasné, jak by tento fond obstál v současné situaci, kdy na poli tvůrčí činnosti již existují platformy a systémy, které umožňují přístup a další tvůrčí užití již existující děl. Mezi nejznámější můžeme pak zařadit Creative Commons. Z tohoto důvodu se návrh tohoto fondu nemusí za současné situace jevit jako pragmatický.

---

[19] Viz str. 135 knihy.

[20] Viz str. 164 knihy.

[21] Viz str. 167 knihy.

[22] Viz str. 168 knihy.

[23] Viz str. 182 knihy.

[24] Autor knihy předkládá své návrhy ve vztahu k autorskoprávní úpravě, avšak dodává, že by daná změna právní úpravy mohla být převzata i dalších právních předpisech upravujících duševní vlastnictví.

Osmá kapitola se konkrétně věnuje navrhovanému systému povinného licencování a v úvodu popisuje jeho jednotlivé základní prvky. Systém povinného licencování by byl zaměřen zejména na další komerční užití již existujících děl. Jako základní je zde hledisko dalšího užití díla, které by mělo být založeno na principu transparentnosti[25] a další užití díla by se mělo posuzovat zejména dle kvantitativního hlediska. Významným aspektem, bez něhož by celý systém nemohl fungovat, je pak zapojení technologie do povinného licencování pro potřeby identifikace rozsahu dalšího užití. Co zde již autor výslovně nezvažuje je však stávající úprava odvozených děl ve vztahu k dalšímu užití již existujících děl.[26] Zachování právní úpravy odvozených děl při zavedení tohoto nového systému se toliko zdá nadbytečné. Zajímavým je dále také návrh, kdy poplatek za užití díla by byl placen až jednotlivými uživateli, kteří by nově vytvořené dílo užili.[27] V rámci kapitoly lze za nejslabší část považovat analýzu souladu navrhovaného systému s osobnostními právy autorskými, kdy se závěry analýzy zaměřují na pouhé konstatování malého významu osobnostních práv v praxi. Z tohoto důvodu tak osobnostní práva v případě přijetí navrhovaného systému nepředstavují pro autora žádnou překážku.[28] Avšak osobnostní práva jsou nadále zakotvena jak na mezinárodní[29], tak i národní úrovni[30] a nic nenasvědčuje tomu, že by mělo být upuštěno od jejich právní ochrany.

Text předposlední kapitoly se pak zaměřuje na právní úpravu nového orgánu, jež by navrhovaný systém implementoval a zajistil jeho další fungování. Autor se v této souvislosti inspiruje návrhem na zavedení „digitální burzy děl“ (z angl. Digital Copyright Exchange).[31] V této souvislosti autor posuzuje možnost využít již existující britský

[25] Viz str. 193 knihy.

[26] Srov. GOLDSTEIN, Paul. Derivative rights and derivative works in copyright. *J. Copyright Soc'y USA*, 1982, roč. 30, str. 209.

[27] Viz str. 202 knihy.

[28] LEWINSKI, Silke von. *International copyright law and policy*. Oxford: Oxford University Press, 2008. p. 33

[29] Srov. čl. 6bis Bernské úmluvy o ochraně literárních a uměleckých děl v revidovaném znění.

[30] Srov. např. § 11 autorského zákona.

Autorskoprávní soud (z angl. Copyright Tribunal) a Autorskoprávní centrum (z angl. Copyright Hub) pro potřeby zavedení nového systému. Již v současné době je Autorskoprávní soud příslušný k administrativnímu zajištění a monitorování jednotlivých subjektů, které licencují jednotlivá díla. Překážkou tohoto orgánu je, že zde chybí jasné zastoupení zájmů uživatelů. Autorskoprávní centrum svou činnost zaměřilo zejména na vydávání jednotlivých příkladů dobré praxe v oblasti licencování digitálního obsahu. Autor v závěru navrhuje vytvoření nového orgánu, který by byl kombinací obou uvedených a zároveň by zajišťoval i fungování kreativního fondu.

Závěrečná kapitola obsahuje shrnutí knihy a doplňující úvahy nad budoucností tvůrčí činnosti, kdy bude nejvýznamnější využití technologií pro účely její právní regulace. Monografie je nepochybně přínosem pro oblast práva duševního vlastnictví, neboť podává ucelený výklad o základním předmětu právní úpravy v této oblasti, a to o tvůrčí činnosti. Jestli by se dalo textu něco vytknout, tak je to soustředěnost pouze na oblast právní úpravy v zemích *common law*, kdy však následné závěry autor často bez dalšího aplikuje i v zemích kontinentálního práva. Zároveň jak bylo uvedeno výše některé návrhy autora může být problematické zavést do praxe. Závěrem lze okrajově vytknout, že samotný název monografie může navozovat dojem, že se text bude uceleně zabývat i právní úpravou 3D, 4D tisku a rozšířenou realitou, kdy však monografie na žádném místě nepodává ucelený popis těchto technologií pouze na ně skrze text odkazuje. Tyto drobné výtky však nesnižují kvalitu publikace, která bude i v budoucnu nadále pro potřeby teorie i praxe aktuální.

[31] Tento návrh byl zveřejněn v nezávislé zprávě o stavu duševního vlastnictví a jeho dalšího růstu. Srov. HARGREAVES, Ian. *Digital Opportunity–A Review of Intellectual Property and Growth*. UK Intellectual Property Office. 2011.

MATES, PAVEL A KOL. OCHRANA OSOBNOSTI, SOUKROMÍ A OSOBNÍCH ÚDAJŮ

PETRA VYDROVÁ[1]

MATES, Pavel (ed.); VALOUŠEK, Martin; FIALOVÁ, Eva; LECHNER, Tomáš; HÁLOVÁ, Markéta; SIVÁK, Jakub; SOVOVÁ, Olga; BRUNA, Eduard; BRUNOVÁ, Markéta. *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges, 2019. 427 s. ISBN 978-80-7502-346-9.

V auguste tohto roka bola vydaná odborná publikácia širšieho autorského kolektívu zaoberajúca sa ochranou osobnosti, súkromia a osobných údajov. Spoluautormi tejto kolektívnej monografie sú nielen odborníci z akademického prostredia ale aj praktizujúci advokáti. Cieľom autorov tejto kolektívnej monografie bolo vytvoriť praktickú príručkou nielen pre odbornú ale aj širšiu verejnosť, ktorej chceli priblížiť problematiku ochrany osobnosti v českom právnom prostredí, s osobitným dôrazom na ochranu súkromia. Autori navyše v publikácii špeciálne pojednávajú aj o ochrane osobnostných práv v kybernetickom priestore a reagujú tak na posledný vývoj moderných informačno-komunikačných technológií. Nakoľko takáto publikácia, ktorá by pojednávala o problematike ochrany osobnosti a zároveň brala do úvahy nové fenomény „internetovej doby“ či sa venovala problematike v špecifických sektoroch ako bankovníctvo

[1] Mgr. Petra Vydrová, LL.M., doktorandka na Ústave práva a technológií Právnickej fakulty Masarykovej univerzity. E-mail : petra.vydrova@mail.muni.cz.

a zdravotníctvo na českom trhu chýba, takúto iniciatívu je možné určite privítať.

Kniha je rozdelená na osem kapitol, ktoré tvoria oddelené celky a je ich tak možné čítať samostatne. Nakoľko sa z publikácie nedá zistiť, ktorý z autorov napísal konkrétnu kapitolu alebo podkapitolu, bude v tejto recenzii pri jednotlivých kapitolách používaný všeobecný pojem „autor“, nie konkrétne meno autora. Z hľadiska systematiky predstavujú prvá dve kapitoly s názvom *„I. Pojem soukromí“* a *„II. Ochrana osobnosti“* úvod do problematiky. Je možné diskutovať vhodnosti zvoleného poradia týchto kapitol, z ktorých prvá sa venuje výkladu pojmu súkromie, pričom následne je tento pojem samostatne rozoberaný aj v druhej kapitole ako súčasť, resp. podkategória konceptu ochrany osobnosti. Za úvahu by teda určite stálo včlenenie tejto prvej kapitoly a v nej obsiahnutého výkladu do kapitoly druhej, aby čitateľ získal viac systematický výklad a teda aj pohľad na predmetnú problematiku. Nasledujú kapitoly, o ktorých by sa súhrnne dalo povedať, že sa venujú ochrane osobnosti, súkromia, resp. osobných údajov v špecifických kontextoch.

Prvá kapitola z názvom „*Pojem soukromí*“ pojednáva o práve na súkromie. V krátkosti rozoberá pôvod tohto práva, jeho základné charakteristiky a pramene na úrovni medzinárodných dohovorov, na ústavnej úrovni a tiež koncept súkromia. Čitateľ sa v nej zoznámi s problematikou hraníc tohto práva z hľadiska jeho obmedzení definovanými na úrovni ústavy a dohovorov vo vzťahu k iným základným právam ako aj s problematikou stretu práva na súkromie s modernými technológiami. Autor v tejto kapitole skôr naznačuje, avšak systematickejšie či podrobnejšie nerozoberá uvedené aspekty práva na súkromie, skôr ich ilustruje na individuálnych príkladoch. Túto kapitolu je preto určite vhodné považovať najmä za všeobecný úvod do problematiky práva na súkromie.

V druhej kapitole s názvom „*Ochrana osobnosti*“ je následne rozoberaná problematika ochrany osobnosti, ktorá je systematicky rozdelená na výklad

o ochrane cti a dôstojnosti[2], podoby a podobizne[3] a na záver o ochrane súkromia[4]. Autor oboznámi čitateľa s prameňmi práva týkajúcimi sa ochrany osobnosti, následne svoj výklad v jednotlivých podkapitolách zameriava primárne na relevantné ustanovenia Občianskeho zákonníka. Tie sú vo väčšine prípadov vykladané samotným autorom a tiež na základe judikatúry českých súdov, prípadne Európskeho súdu pre ľudské práva a Súdneho dvora EÚ.[5] Je škoda, že autor len minimálne odkazuje na inú odbornú literatúru - vystačuje si s jedným odkazom na komentár k Občianskemu zákonníku a s jediným odkazom na odbornú monografiu,[6] čo sa vzhľadom na tému kapitoly, ktorá nie je úplne nová a dosiaľ nepreskúmaná, nejaví ako úplne dostatočné.

Tretia kapitola nesie názov „*Ochrana osobnosti ve zvláštních případech*“ a aj keď je rozčlenená do 11-tich podkapitol, zaoberá sa v podstate tromi témami: automatizovaným individuálnym rozhodovaním podľa čl. 22 GDPR[7] (podkapitoly 3.1 až 3.4), právom byť zabudnutý podľa čl. 17 GDPR (podkapitoly 3.5 až 3.7) a následne zodpovednosťou poskytovateľov v kontexte ochrany osobnosti (podkapitoly 3.8 až 3.11). Nakoľko teda niektoré podkapitoly na seba tematický nadväzujú a pojednávajú o rovnakej téme kým ďalšie podkapitoly s rovnakou úrovňou číslovania pojednávajú o téme odlišnej, zvolené rozdelenie kapitoly na jedenásť podkapitol namiesto troch je pre čitateľa mätúce. Zo systematického hľadiska stojí za zmienku aj skutočnosť, že kapitola pojednáva o dvoch špecifických právach z GDPR, v knihe ju však nepredchádza žiadna kapitola vysvetľujúca základné pojmy, ktoré sú v nej používané, čo môže byť problematické pre čitateľa, ktorý sa v problematike chce zorientovať.

[2] Porov. podkapitola 2.1.

[3] Porov. podkapitola 2.2.

[4] Porov. podkapitola 2.3.

[5] Autor sa tiež v texte odvoláva na ustálenú judikatúru v určitej oblasti bez odkazu na jediný konkrétny judikát, napr. pri definovaní pojmu „súkromné priestory“.

[6] Obidva odkazy na inú odbornú literatúru sú v poznámke pod čiarou na strane 57, iné odkazy kapitola neobsahuje.

[7] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „GDPR“).

Zároveň je otázne, či rozobratie problematiky zodpovednosti poskytovateľov by malo byť súčasťou kapitoly pojednávajúcej o ochrane osobnosti v zvláštnych prípadoch (zaoberajúcou sa dvoma právami z GDPR) a nie samostatnou kapitolou, prípadne či nemalo byť včlenené do kapitoly pojednávajúcej o všeobecných aspektoch problematiky ochrany osobnosti.

V kapitole samotnej má čitateľ možnosť zoznámiť sa s vykladanými témami čitateľsky prístupným spôsobom. Kapitola začína rozborom problematiky automatizovaného individuálneho rozhodovania, ktorý pozostáva najmä z výkladu čl. 22 GDPR. Autor tu upozorňuje na zaujímavý interpretačný problém, ktorý spôsobila formulácia tohto ustanovenia a ktorý spôsobil nejasnosti ohľadom jeho samotnej povahy – je toto ustanovenie zákazom takéhoto automatizovaného rozhodovania s formulovanými výnimkami alebo upravuje skôr právo dotknutej osoby namietať proti takémuto spracúvaniu? Autor ďalej rozoberá problémy automatizovaného rozhodovania, ktoré vyplývajú zo skutočnosti, že je založené na prediktívnych modeloch, problém s jeho transparentnosťou či povahu práva na ľudský zásah a práva vyjadriť svoj názor voči automatizovanému rozhodovaniu. V ďalších troch podkapitolách tretej kapitoly sa autor venuje právu byť zabudnutý a to najmä vo vzťahu k právu na informácie. Autor najskôr rozoberá rozsudok Súdneho dvora EÚ vo veci *Google Spain*[8] a teoretické dôvody, pre ktoré je toto právo v digitálnej spoločnosti potrebné.[9] Následne prechádza k výkladu právnej úpravy tohto práva v GDPR[10] a rozoberá právo byť zabudnutý vo vzťahu k právu na informácie, a to najmä vo svetle rozsudku *Google Spain*. Posledné štyri podkapitoly sú venované zodpovednosti poskytovateľov v kontexte ochrany osobnosti. Autor na úvod v krátkosti zhŕňa konflikt medzi právom na informácie a právom na ochranu osobnosti ako aj základne nástroje v českom práve, ktoré je možné využiť proti porušiteľovi osobnostných práv. Následne rozoberá podmienky zodpovednosti poskytovateľov služieb

[8] Rozsudok SDEÚ vo veci C-131/12 z 13. mája 2014, Google Spain a Google (ďalej len „Google Spain“).

[9] Podkapitola 3.5.

[10] Podkapitola 3.6.

informačnej spoločnosti v súlade so Smernicou o elektronickom obchode.[11] V kapitole by bolo vhodné výraznejšie zdôraznenie skutočnosti, že čl. 14 Smernice o elektronickom obchode upravuje výnimku zo zodpovednosti poskytovateľov týchto služieb a že zároveň ide o výnimku zo zodpovednosti sekundárnej, teda nie z primárnej zodpovednosti,[12] čo by čitateľovi pomohlo túto problematiku pochopiť v širších súvislostiach. Autor napokon informuje o posledných politických dokumentoch Európskej komisie, ktoré naznačujú budúce smerovanie regulácie zodpovednosti poskytovateľov služieb informačnej spoločnosti.

Štvrtá kapitola s názvom „*Ochrana osobních údajů v praxi*" tvorí ucelenú kapitolu, ktorá je výsledkom výskumu Vysoké školy ekonomické. Je písaná veľmi prakticky a zrozumiteľne - okrem všeobecnejšieho úvodu, ktorý vysvetľuje kto je to prevádzkovateľ (z češtiny *správce*) a sprostredkovateľ (z češtiny *zpracovatel*) a ich základné povinnosti všeobecne obsahuje väčšina kapitoly najmä konkrétne rady pre prevádzkovateľov a sprostredkovateľov. Popisuje tak napr. potrebné kroky a opatrenia, ktoré by mali vykonať obce a školy na to, aby ich spracúvanie osobných údajov bolo v súlade s GDPR, praktické rady ako získať súhlas[13] či ako spracúvať osobné údaje ako zamestnávateľ spôsobom, ktorý bude v súlade s týmto predpisom. Pri všeobecnejšom výklade o povinnostiach prevádzkovateľov

[11] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (ďalej len „Smernica o elektronickom obchode").

[12] Viď napr. KOHL, Uta. 2012. The rise and rise of online intermediaries in the governance of the Internet and beyond – connectivity intermediaries. In: International Review of Law, Computers &Technology, 26:2-3, 185-210, s. 189.

[13] V kapitole pojednávajúcej o výslovnom súhlase je problematické odporúčanie, že získanie výslovného súhlasu „*vyžaduje opatřit prohlášení kvalifikovaným elektronickým podpisem*". Aj keď autor uvedené tvrdenie následne zmierňuje dovetkom, že je možné použiť aj iné prostriedky, podľa neho sa tým však prevádzkovateľ môže vystaviť riziku, že nebude vedieť „výslovnosť" súhlasu dostatočne preukázať. Výklad Pracovnej skupiny 29, na ktorý sa autor odvoláva, pritom interpretuje požiadavky na „explicitnosť" súhlasu tým, že má ísť o výslovné vyhlásenie dotknutej osoby, v protiklade s tým, že by jej súhlas bol iba odvodený zo správania subjektu a teda „implicitný". Nikde vo výklade Pracovnej skupiny sa nepožaduje konkrétny spôsob autorizácie súhlasu, a tak výslovný súhlas by malo byť možné získať aj na základe zakliknutia políčka, pri ktorom bude vyhlásenie uvedené. V takomto prípade by podľa môjho názoru mohol byť do budúcna problém preukázať, či súhlas bol vôbec udelený, nie však to, že bol „výslovný".

a sprostredkovateľov[14] by pre jeho úplnosť bola vhodná zmienka aj o iných typoch právnych vzťahov, ktoré môžu vzniknúť pri spracúvaných osobných údajov ako iba vzťah prevádzkovateľ - sprostredkovateľ, napr. o spoločných prevádzkovateľoch v zmysle čl. 26 GDPR alebo o vzťahu medzi dvoma prevádzkovateľmi (z ktorých niektorý napr. iba poskytuje osobné údaje druhému) a o povinnostiach, ktoré z nich vyplývajú. Následne sa kapitola venuje ochrane súkromia a informácii v bankovníctve a platobnom styku.[15] Okrem informácií o spracovaní osobných údajov bankami a platobnými inštitúciami a o tom čo sú platobné služby, je v nej obsiahnutý výklad právnej úpravy bankového tajomstva a odlišností v povinnosti mlčanlivosti pri poskytovaní platobných a bankových služieb. Na záver kapitoly sa autor venuje aj ochrane informácií Českou národnou bankou pri výkone dohľadu v oblasti bankovníctva a platobného styku.[16]

V piatej kapitole nazvanej „*Ochrana osobnosti v kybernetickém prostoru*“ sa autor venuje špecifikám ochrany osobnosti v kybernetickom priestore. Na začiatok vymedzuje čo myslí samotným kyberpriestorom[17] a tiež popisuje jednotlivé predmety ochrany v prípade práva na ochranu osobnosti, ako dôstojnosť, česť, súkromie a pod.[18] Následne autor deskriptívnym spôsobom popisuje niektoré spôsoby narušenia osobnosti v kybernetickom priestore,[19] napr. sexting[20], cyberstalking, kyberšikana, útok na osobnosť v hromadnej konverzácii alebo diskusii či cybergrooming.[21] V ďalších podkapitolách autor rozoberá trestné činy proti

[14] Porov. podkapitola 4.2.

[15] Porov. podkapitola 4.3.

[16] Porov. podkapitola 4.4.

[17] Porov. podkapitola 5.1.

[18] Porov. podkapitola 5.2.

[19] Porov. podkapitola 5.3.

[20] Je otázne, do akej miery je sexting vôbec spôsobom narušenia ochrany osobnosti, nakoľko k porušeniu práv by malo dôjsť až samotnou publikáciou citlivého obsahu.

[21] Autorovi sa dá vytknúť skutočnosť, že sa zaoberá výlučne týmito špecifickými fenoménmi reprezentovanými určitými „buzzwords“, k narušeniu osobnosti v kybernetickom priestore však môže dôjsť prostou publikáciou určitého obsahu (porušujúceho právo na ochranu osobnosti) na webovej stránke, či už v rámci novinového článku, blogu alebo komentára v diskusii, viď napr. rozhodnutie SDEÚ v spojených vecech C-509/09 a C-161/10 z 25. októbra 2011, eDate Advertising a Martinez a Martinez.

osobnosti človeka, ktoré sú v kybernetickom priestore najbežnejšie[22] a venuje sa tak nielen občianskoprávnym ale aj trestnoprávnym aspektom ochrany osobnosti, následne popisuje špecifiká použitia elektronických dôkazných prostriedkov pre dokazovanie v civilnom konaní. V kapitole však absentuje komplexnejšie a ucelenejšie uchopenie problematiky, najmä vysvetlenie, v čom je vlastne ochrana osobnosti v kybernetickom priestore špecifická či aké špecifické prostriedky ochrany môže mať poškodený k dispozícii.[23] Práve zo skutočnosti, že k určitému porušeniu práv na ochranu osobnosti dochádza v kybernetickom priestore totiž často vyplývajú nové výzvy a problémy, napr. s určením identity škodcu či problémy s určením rozhodného práva a jurisdikcie.[24] Posledná podkapitola s názvom *Ochrana společnosti v kybernetickém prostoru*,[25] sa venuje niektorým nebezpečenstvám na internete (najmä propagácii teroristických útokov, rekrutovaniu teroristov, kybernetickým útokom) či kvalite kybernetickej ochrany v ČR. Prepojenie obsahu tejto podkapitoly na tému ochrany osobnosti, resp. ich súvislosť však čitateľovi nebolo vysvetlené, nie je ani zrejmé a tak sa jej začlenenie do tejto kapitoly javí ako nadbytočné.

Siedma kapitola je venovaná problematike „*Soukromí při poskytování zdravotní peče*“. V kapitole sa autor zaoberá špecifikami ochrany súkromia a osobnosti v segmente poskytovania zdravotnej starostlivosti, pričom sa odvoláva nielen na relevantné predpisy a dostupnú judikatúru, ale aj na príklady z praxe, ktoré často používa pre lepšie vysvetlenie popisovanej problematiky. Na úvod detailne rozoberá otázku mlčanlivosti v zdravotníctve, a to najmä predpoklady jej prelomenia či podmienky, za

[22] Porov. podkapitola 5.4.

[23] Napr. možnosť uplatniť si právo vyplývajúce z tzv. *notice and takedown* procedúry vyplývajúcej z čl. 14 Smernice o elektronickom obchode a teda uplatniť si svoje právo nielen priamo u škodcu, ale u osoby, ktorá mu poskytuje hosting.

[24] V prostredí internetu sa totiž do právnych vzťahov často dostáva cudzí prvok (obsah je zverejnený na serveri lokalizovanom v zahraničí, osoba zverejňujúca obsah alebo osoba poskytujúca hosting má sídlo v zahraničí a pod.), navyše obsah je rozširovaný a dostupný po celom svete, čo ochranu týchto práv komplikuje – viď napr. OSTER, Jan. 2012. Rethinking Shevill. Conceptualizing the EU Private International Law of Internet torts against personality rights. In: International Review of Law, Computers & Technology. Vol. 26, Nos. 2-3, 113-128, s. 113-114.

[25] Porov. podkapitola 5.6.

ktorých majú zdravotné zariadenia možnosť alebo povinnosť poskytovať informácie zdravotnej povahy (napr. orgánom činným v trestnom konaní). V kapitole sa čitateľ oboznámi s problematikou informovaného súhlasu a nesúhlasu pacienta či s problematikou ochrany zdravotníckej dokumentácie, čo obsahuje či kto do nej okrem vyšetrujúcich lekárov môže nahliadať. Následne po popise týchto špecifických modifikácií práva na súkromie v zdravotníctve prechádza autor k výkladu zodpovednosti za jeho porušenie. V závere autor v krátkosti zhŕňa české reálie týkajúce sa elektronizácie poskytovania zdravotnej starostlivosti.

Ôsma kapitola s názvom *„Prokazovaní a zjišťováni totožnosti“* sa zaoberá, ako to vyplýva z jej názvu, problematikou zisťovania a preukazovania totožnosti. Autor tak v prvej podkapitole zhŕňa a popisuje právne predpisy, ktoré ukladajú niektorej zmluvnej strane povinnosť zistiť totožnosť druhej zmluvnej strany ako aj právne následky v prípadoch nedodržania týchto povinností a ilustruje ich na konkrétnych príkladoch. Nasledujúce podkapitoly sú krátkym zhrnutím pravidiel týkajúcich sa preukazovania totožnosti vo vzťahu k orgánom verejnej moci, pri výkone kontroly či vo vzťahu k príslušníkom verejných zborov, spôsobov preukazovania totožnosti a tiež právnych následkov, ktoré nastanú v prípade, že povinný subjekt svoju totožnosť nepreukáže či odmietne preukázať.

Posledná, deviata kapitola nesie názov „*Ochrana soukromí z pohledu tresněprávní úpravy*“. Autor sa v nej venuje predovšetkým deskriptívnemu výkladu trestných činov uvedených v II. hlave 2. časti Trestního zákoníka,[26] teda trestných činov proti slobode a právam na ochranu osobnosti, súkromia a listového tajomstva ako aj pojmom používaných pri jednotlivých skutkových podstatách týchto trestných činov. Aj keď autor sám v úvode poznamenáva dôležitosť vysvetlenia pojmu súkromie tak, aby ho bolo možné podradiť pod predmetné trestné činy, ktorých účelom je v mnohých prípadoch ochrana nielen súkromia, ale aj osobnej slobody či ľudskej dôstojnosti,[27] toto vysvetlenie v kapitole de facto absentuje.[28] Táto skutočnosť tak môže v čitateľovi budiť odôvodnenú otázku, prečo autor

[26] Zákon č. 40/2009 Sb. Trestní zákoník.

[27] Porov. podkapitoly 8.1 a 8.2, s. 395.

popisuje úplne všetky trestné činy II. hlavy Trestního zákoníka, vrátane trestných činov proti slobode (napr. vydieranie, lúpež) a ako tieto trestné činy vôbec súvisia s ochranou súkromia. Je tiež vhodné poznamenať, že autor si v tejto kapitole vystačuje s odkazom na jedinú odbornú monografiu a nepomáha si ani ustálenou judikatúrou, čo v čitateľovi môže budiť pochybnosti o odbornej kvalite v nej uvedeného výkladu.

Ako vyplýva aj z vyššie uvedeného popisu obsahu jednotlivých kapitol, kapitoly samotné je možné čítať úplne samostatne, nie sú obsahovo nadväzné ani na seba navzájom nijako neodkazujú, práve naopak, niektoré základné pojmy ako napr. „súkromie“ či „dôstojnosť“ sú popisované, resp. definované samostatne v každej kapitole, ktorá s daným pojmom narába.[29] Je tak možné odôvodnene predpokladať, že boli jednotlivými autormi napísané samostatne, bez väčšej koordinácie autorského kolektívu. Zároveň celková systematika publikácie pôsobí veľmi nesúrodo a nekoncepčne, kapitoly sa striedavo venujú ochrane osobnosti, súkromia alebo osobných údajov a teda majú v určitom zmysle spoločnú tému, avšak bez jasnejšej a pochopiteľnejšej štruktúry či zvoleného poradia týchto kapitol.[30] Vzhľadom na túto skutočnosť nepreviazanosti jednotlivých kapitol, celkovú nesúrodosť systematického členenia publikácie či neúplnosť výkladu týkajúceho sa problematiky ochrany osobných údajov[31] je na mieste položiť otázku, či uvedená publikácia je skutočne kolektívnou monografiou (ako je

[28] Autor v podstate konštatuje, že ide o práva, ktoré chránia človeka a ktoré spolu súvisia, pričom ich výklad je závislý vždy od konkrétneho autora, čo sa javí ako nie úplne postačujúce vymedzenie.

[29] Napr. v kapitole I., II., aj V.

[30] Pre ilustráciu nahodilosti usporiadania kapitol: I. kapitola pojednáva o súkromí, II. o ochrane osobnosti a opäť o súkromí ako o jednom z jeho prvkov, III. sa venuje špecifickým právam v GDPR (kde používa pojmy z GDPR, z ktorých niektoré sú vysvetlené až v IV. kapitole a niektoré nie sú v knihe vysvetlené vôbec) a zároveň otázkou zodpovednosti poskytovateľov, IV. sa venuje ochrane osobných údajov a následne publikácia prechádza opäť k výkladu problematiky ochrany osobnosti (v kyberpriestore) v V. kapitole, VI. kapitola sa vracia k ochrane súkromia (pri poskytovaní zdravotnej starostlivosti), VII. Kapitola pojednáva o zisťovaní totožnosti a VIII. o trestnoprávnej ochrane súkromia (pritom trestnoprávne aspekty ochrany osobnosti už boli riešené aj v V. kapitole pri výklade ochrany osobnosti v kybernetickom priestore).

[31] V publikácii absentuje kapitola, ktorá by komplexne pojednávala o problematike ochrany osobných údajov, IV. kapitola hlbšie neanalyzuje relevantné základné pojmy používané v publikácii, napr. pojem „osobné údaje“.

uvedené v jej klasifikácii) vypracovanou viacerými spolupracujúcimi autormi, alebo skôr zborníkom nezávisle vypracovaných odborných článkov, ktoré spája iba spoločná téma ochrany osobnosti, súkromia a ochrany osobných údajov.[32]

Ďalším problémom predmetnej publikácie je skutočnosť, že autori v nej explicitne nevysvetlili aký je vlastne vzťah medzi ochranou súkromia (resp. ochranou osobnosti) a osobných údajov, ani aké stanovisko k tejto problematike zaujímajú. Zo systematického členenia publikácie[33] ako aj z niektorých tvrdení v nej uvedených[34] je možné odvodiť, že väčšina autorského kolektívu vníma ochranu osobných údajov ako rozšírenie práva na súkromie, resp. ochranu osobnosti, a teda ako ich podmnožinu. Až na jeden prípad[35] však toto chápanie vzťahu týchto dvoch konceptov v publikácii nebolo verbalizované. Nakoľko je ochrana osobných údajov jedna z hlavných tém publikácie a uvedená publikácia je kolektívnou monografiou, vysvetlenie vzájomného vzťahu týchto základných konceptov bolo určite odôvodnené očakávať. Taktiež by bolo vhodné uvedený postoj autorského kolektívu odôvodniť, a to v rámci konfrontácie s ďalšou odbornou literatúrou, ktorá sa vzťahom týchto konceptov zaoberala. Uvedené chápanie vzťahu medzi právom na súkromie a ochranu osobných

[32] Podľa České terminologické databáze knihovnictví a informační vědy České národní knihovny je kolektívna monografia: „*Neseriálová publikace, která systematicky, všestranně a podrobně pojednává o jednom, zpravidla úzce vymezeném tématu a která je dílem více autorů. Jednotlivé části publikace na sebe navzájem tematicky navazují a jejich zpracování je předem pečlivě naplánováno a svěřeno jednotlivým autorům, popř. skupinám autorů. (Sborník se liší od kolektivní monografie tím, že u něj se nelze setkat s tak všestranně a podrobně zpracovaným tématem. Jednotlivé části či příspěvky jsou zpravidla pouze rámcově tematicky příbuzné a mohly by existovat samy o sobě. Nejedná se o společné dílo více autorů, nýbrž o soubor článků nespolupracujících autorů.)*“ Porov. Kolektivní monografie. *KTD - Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Národní knihovna ČR, © 2012 [cit. 30. 11. 2019]. Dostupné z: http://aleph.nkp.cz/publ/ktd/00001/46/000014657.htm.

[33] Napr. III. kapitola pojednáva o právach obsiahnutých v GDPR avšak jej nadpis znie *„Ochrana osobnosti ve zvláštních případech“*.

[34] Napr. v I. kapitole, na str. 26 autor uvádza, že právo byť zabudnutý upravené GDPR je jedným z prostriedkov ochrany súkromia, alebo v III. kapitole na str. 84 autor spomína, že právo na ľudský zásah a vyjadrenie svojho názoru pri automatizovanom spracovaní sa dá subsumovať pod právo na ochranu osobnosti podľa Občianskeho zákonníka.

[35] Autor V. kapitoly na str. 269 hovorí, že súkromie a súkromné informácie sú *„natolik esenciální, že dále na jejich ochranu existují mimo občanský zákoník i další, jemu speciální právní předpisy. Z nich bych zmínil zejména GDPR.“*

údajov ako vzťahu nadriadenosti a podriadenosti totiž nie je univerzálne prijímané. Časť odbornej literatúry sa prikláňa k záveru, že aj keď sa tieto práva v určitom rozsahu prekrývajú, nie sú obsahovo rovnaké, slúžia na ochranu odlišnej a nie vždy sa prekrývajúcej množiny prípadov a odlišné sú aj právne nástroje na ich ochranu, preto právo na ochranu osobných údajov nemá byť chápané ako podmnožina práva na ochranu súkromia či osobnosti.[36]

Na záver je vhodné zhrnúť, že publikácia samotná spracúva zaujímavé a v súčasnosti stále aktuálne témy, a to aj v špecifických kontextoch, ktoré dosiaľ boli v českom právnom prostredí len málo rozpracované. Bohužiaľ však má viacero nedostatkov rozobratých v tejto recenzii, ktoré zhoršujú jej čitateľnosť a žiaľ uberajú aj jej odbornej kvalite.

---

[36] Porovn. napr. KOKOTT, Juliane a SOBOTA, Christoph. 2013. The Distinction between Privacy and Data Protection. In: International Data Privacy Law, Vol. 3, No. 4. Oxford University Press, s. 223; KUNER, Christopher. 2007. European Data Protection Law: Corporate Compliance and Regulation. Second Edition. Oxford University Press, s. 2; POLČÁK, R. a kol. 2018. Právo informačních technologií. Praha: Wolters Kluwer ČR, s. 400-401.

https://doi.org/10.5817/RPT2019-2-5

CERTIFIKACE KYBERBEZPEČNOSTNÍCH TECHNOLOGIÍ[1]

JAKUB VOSTOUPAL[2]

ABSTRAKT

Tento článek pojednává o certifikaci jako o jednom z nástrojů posuzování shody v oblasti technologií kybernetické bezpečnosti. V článku je vysvětlena problematika compliance a jejích výhod oproti obecnému odpovědnostnímu režimu, vysvětlena funkce posuzování shody a certifikace jak obecně, tak v kyberbezpečnostním prostředí, shrnutý stav současné úpravy certifikace kyberbezpečnostních technologií v ČR a EU a představení nadcházející úpravy jednotného evropského certifikačního rámce. V druhé části příspěvku autor představuje konkrétní certifikační systémy včetně institucionálního, organizačního a procesního zabezpečení. Pozornost je přitom zaměřena na systém Common Criteria a chystanou evropskou úpravu podle Aktu o kybernetické bezpečnosti. Pro úplnost jsou stručně rozebrány i vnitrostátní certifikační schémata z vybraných evropských států.

[1] Tento článek vznikl za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" reg.č.: CZ.02.1.01/0.0/0.0/16_019/0000822 financovaného z EFRR. Článek vychází z autorovy diplomové práce "Certifikace kyberbezpečnostních technologií" (dostupná z: https://is.muni.cz/th/ggumu/). Autor děkuje za podnětné připomínky anonymním recenzentům článku.

[2] Mgr. Jakub Vostoupal je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a studentem bakalářského studia psychologie na Fakultě sociálních studií Masarykovy univerzity. Vedle toho působí v rámci několika projektů pod Právnickou fakultou a Fakultou informatiky Masarykovy univerzity, e-mail: Jakvost@gmail.com.

KLÍČOVÁ SLOVA:

Kybernetická bezpečnost, posuzování shody, certifikace, compliance, Common Criteria, Akt o kybernetické bezpečnosti

ABSTRACT

This article deals with certification as one of the instruments of conformity assessment in the area of cybersecurity technologies. The article explains the issue of compliance and its advantages over general liability regime. The text continues with an explanation of conformity assessment and certification both in general and in cybersecurity environment, followed by a summarization of the current state of regulation of certification of cybersecurity technologies in the Czech Republic and the EU and by an introduction of the forthcoming regulation of the unified European certification framework. In the second part of the article, the author presents specific certification systems including their institutional, organizational and procedural aspects. Attention is primarily given to the system of Common Criteria and the European regulation – the Cyber-Security Act. The author completes the comparison by introducing national certification schemes from selected European countries.

KEYWORDS:

Cyber-security, conformance assessment, certification, compliance, Common Criteria, the Cybersecurity Act

SEZNAM NEJDŮLEŽITĚJŠÍCH POJMŮ A ZKRATEK

Agentura	Evropská agentura pro bezpečnost sítí a informací, také jako „*ENISA*“
Akt	Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („*Agentuře Evropské unie pro kybernetickou bezpečnost*“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013
ANSSI	Agence nationale de la sécurité des systémes d’information

BSPA	Baseline Security Product Assessment
CAB	Conformance Assessment Body
CC	Common Criteria for Information Technology Security Evaluation
CCRA	Common Criteria Recognition Agreement
CEM	Common Evaluation Methodology
CPA	Commercial Product Assurance
CSPN	Certification Sécuritaure de Premier Niveau
ČIA	Český institut pro akreditaci, o.p.s.
EAL	Evaluation Assurance Level
eIDAS	Nařízení Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
GDPR	General Data Protection Regulation, Obecné nařízení o ochraně osobních údajů
ICT	Informační a komunikační technologie
ISMS	Information Security Management System (Systém řízení bezpečnosti informací)
ISO	International Standards Organization (Mezinárodní organizace pro standardizaci)
MRA	Mutual Recognition Agreement/Arrangement (Dohoda o vzájemném uznávání)
NBÚ	Národní bezpečnostní úřad
NCCA	National Cybersecurity Certification Authority (Národní autorita pro certifikaci kybernetické bezpečnosti)
NIS	Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
NLCSA	Nationaal Bureau voor Verbindingsbeveiliging
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PP	Protection Profile, Profil ochrany

Program	Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti
SFEU	Smlouva o fungování EU
Skupina	Evropská skupina pro certifikaci kybernetické bezpečnosti
SOG-IS	Senior Officials Group Information Systems Security
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
ST	Security Target, Bezpečnostní cíl
TOE	Target of Evaluation, Předmět posuzování
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

1. ÚVOD

S příchodem internetu věcí se každým rokem rapidně zvyšuje počet zařízení, která jsou připojena k internetu.[3] V rámci kyberprostoru je však již delší dobu patrný trend oslabení bezpečnosti, a přestože dle Europolu byl v roce 2019 zaznamenán určitý pokles v množství útoků provedených online, ekonomický dopad kyberkriminality se dále zvyšuje.[4] Připojování nezabezpečených technologií pozici útočníků jenom zjednodušuje.

Ke zvýšení důvěry uživatelů v nové technologie je v takovém prostředí nutné začít řešit kybernetickou bezpečnost, a to i v případě jednotlivých „stavebních kamenů“ informačních systémů. Jednou z cest jak posílit důvěru i bezpečnost je pak právě certifikace.

Na téma kybernetické bezpečnosti bylo již napsáno mnoho vědeckých prací, přesto však zůstává problematika certifikace kyberbezpečnostních

[3] Dle předběžných odhadů Komise z roku 2016 se počet zařízení připojených k internetu měl zvýšit z přibližně 1,8 milionu v roce 2013 na téměř šest miliard v roce 2020. Více viz Commission Staff Working Document: Advancing the Internet of Things in Europe [online]. B.m.: European Commission. 2016. Tento trend bude pravděpodobně ještě dále umocněn nástupem 5G sítí, které dané připojování značně zjednoduší. Více viz např. Report: EU coordinated risk assessment of the cybersecurity of 5G networks [online]. B.m.: NIS Cooperation Group. 2019.

[4] To je způsobeno zejména tím, že útočníci se začínají soustředit na ekonomicky výnosnější cíle než třeba na plošný dopad ransomwaru. Více viz IOCTA: Internet Organised Crime Threat Assessment 2019 [online]. B.m.: Europol – European Cybercrime Centre. 2019.

technologií tématem nepříliš známým. Cílem tohoto článku je tak úkol zmapovat tuto problematiku a představit ji čtenáři. K naplnění tohoto cíle si kladu dvě výzkumné otázky:

Jak fungují stávající certifikační systémy?

Jak tuto funkci zlepší Akt o kybernetické bezpečnosti[5]?

Pozornost přitom věnuji srovnání certifikačního systému Common Criteria[6] a připravovaného evropského certifikačního rámce podle Aktu o kybernetické bezpečnosti. Dílčím cílem článku bude i vyhodnocení slabin obou zmíněných systémů.

Vzhledem k tomu, že téma je nesmírně živé a část Aktu o kybernetické bezpečnosti věnující se certifikaci stále není účinná, byla teoretická (statická) materie zakonzervována ke dni 25. 12. 2018 a části, u kterých došlo k výraznějším změnám, byly aktualizovány ke dni 12. 10. 2019.

K tomu, abych dokázal odpovědět na výše zmíněné otázky, přistoupím v obecné části článku nejdříve k představení pojmu compliance a certifikace, která je jedním z typů posuzování shody (tedy compliance). Dále se budu věnovat druhům regulatorních požadavků, neboť je nutné pochopit, jakým způsobem se pravidla, se kterými se shoda posuzuje, formulují a kdy je certifikace vůbec třeba.

V další kapitole budou představena bezpečnostní opatření, jejichž implementace se v rámci procesu certifikace posuzuje, popíšu stávající úpravu certifikace v ČR a pokusím se o její teoretické zasazení do systému kybernetické bezpečnosti v České republice. Na závěr kapitoly rozeberu stav, který panuje v Evropské unii.

---

[5] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (dále také jako „*Akt o kybernetické bezpečnosti*" nebo „*Akt*")

[6] Přestože Výkladový slovník kybernetické bezpečnosti zná Common Criteria pod oficiálním českým překladem „*Společná kritéria*" (viz JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. 3., aktualiz. vyd. Praha, Česká republika: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2015, s. 155), je v českém prostředí možné používat i originální anglickou verzi (činí tak např. Národní bezpečnostní úřad v níže citovaném informačním materiálu o Common Criteria), čehož v celém příspěvku využívám.

Ve čtvrté kapitole věnuji pozornost teoretické stránce a vývoji Aktu, přičemž se soustředím na jeho nejvíce problematické aspekty v průběhu vyjednávání. Touto kapitolou končí obecná část, která ve svém celku má sloužit jako teoretický základ pro pochopení, jak fungují certifikační systémy a rámcově i jaký typ změny s sebou přináší Akt o kybernetické bezpečnosti.

Článek ve zvláštní části přechází ke konkrétnímu popisu a analýze organizační, institucionální a procesní struktury aktuálních certifikačních schémat v prostředí mezinárodních iniciativ, národních úprav v prostředí vybraných evropských států a nakonec i v rámci Aktu samotného. V páté kapitole se věnuji aktivitě Mezinárodní společnosti pro standardizaci, rodině standardů ISO 27K a největšímu stávajícímu certifikačnímu systému – Common Criteria. Standardy ISO 27K sice nedopadají na certifikaci kyberbezpečnostních technologií, ale Akt vtahuje do své úpravy i materii upravenou těmito standardy, a tak je vhodné se s nimi seznámit, aby byla lépe pochopena povaha Aktu.

V šesté kapitole rozebírám národní schémata čtyř evropských certifikačních velikánů – Velké Británie, Francie, Nizozemí a Německa.[7,8] Jejich schémata jsou nejpokročilejší reakcí na slabiny systému Common Criteria a je tak možné je využít ke kritickému zhodnocení jak CC, tak Aktu (což je provedeno v kapitole sedmé).

Článek čerpá zejména z článků zahraničních odborných časopisů a monografií, a to hlavně pro značný nedostatek českých zdrojů[9] (díla českých autorů jsou využita hlavně v teoretické části). Neméně důležitou

[7] Toto je patrné z výzkumů a pracovních dokumentů Komise doplňujících prvotní návrh Aktu o kybernetické bezpečnosti (viz State of the Union 2017: Cybersecurity - EU Agency and Certification Framework. B.m.: European Commission). Explicitně byly tyto státy takto označeny na worshopu o budoucnosti ICT certifikace v Evropě, viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014 [vid. 24. srpen 2018].

[8] Více viz DROGKARIS, Prokopios. *Considerations on ICT security certification in EU - Survey Report* [online]. B.m.: European Union Agency for Network and Information Security. 2017 [vid. 9. září 2018]; Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu *aktu o kybernetické bezpečnosti* [online]. B.m.: Evropská komise. 2017 [vid. 12. červenec 2018].

roli zastávají prezentace z odborných konferencí, zprávy a výzkumy unijních orgánů, znění normativních předpisů a konzultace s odborníky.

2. COMPLIANCE A CERTIFIKACE

Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku upozornila[10] dne 13. 9. 2017 na studie,[11] ze kterých vyplývá, že hospodářský dopad kyberkriminality se mezi lety 2013 až 2017 zvýšil pětinásobně a do roku 2019 by se mohl ještě dále zčtyřnásobit.[12] Mezi kybernetickou kriminalitou a kybernetickou bezpečností existuje úzká vazba a provázanost,[13] a s narůstající kyberkriminalitou se tak zhoršuje bezpečnostní situace kyberprostoru celé Unie, přičemž rizika rostou téměř exponenciálně. To zároveň snižuje důvěru uživatelů v nové technologie a zpomaluje technologický postup (včetně negativního dopadu na zavádění internetu věcí).[14]

Aby byla bezpečnost v kyberprostoru posílena a tento znepokojivý trend zastaven (nebo přinejmenším zpomalen), politické reprezentace mnohých zemí se začaly kybernetickou bezpečností zabývat důkladněji. Příkladem

---

[9] Tuto skutečnost si autor příspěvku potvrdil nejen při samotném hledání pramenů, ale i konzultacemi s odborníky. O problematice kyberbezpečnostní certifikace je stručně pojednáno např. v POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti* [online]. 1. vydání. Brno: Masarykova univerzita, 2016 [vid. 10. srpen 2018].

[10] Učinila tak ve Společném sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017 „*Odolnost, odrazování a obrana: Budování silné kybernetické bezpečnosti pro EU*"

[11] V prohlášení citují jako jednu z použitých studií například „*Net losses: Estimating the Global Cost of Cybercrime*" (Čisté ztráty: Odhad globálních nákladů způsobených kyberkriminalitou), McAfee & Centre for Strategic and International Studies, 2014.

[12] To ve výsledku potvrzuje i zmiňovaná studie IOCTA. Více viz IOCTA: Internet Organised Crime Threat Assessment 2019 [online]. B.m.: Europol – European Cybercrime Centre. 2019.

[13] Boj proti kyberkriminalitě je součástí strategie národní kybernetické bezpečnosti na období let 2015-2020, a jako taková předpokládá mimo jiné přijímání legislativních kroků, které by vedly k minimalizaci škodlivého zneužívání ICT technologií. Více viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 125.

[14] V i z VYSOKÁ PŘEDSTAVITELKA UNIE PRO ZAHRANIČNÍ VĚCI A BEZPEČNOSTNÍ POLITIKU. *Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU* [online]. 2017 [vid. 11. říjen 2018].

může být Česká republika se svým zákonem o kybernetické bezpečnosti, Unie a směrnice NIS, Spojené státy americké, které se obdobnými otázkami zabývají již od roku 1991, nebo Ruská federace, jejíž hlavní kyberbezpečnostní regulace byla vytvořena mezi roky 2006 a 2014 a která do roku 2020 plánuje kapacity v této oblasti dále významně rozvíjet.[15,16]

Regulatorní zátěž povinných subjektů, stanovená jednotlivými národními úpravami kybernetické bezpečnosti, se pro mnohé z nich může ukázat jako prakticky nezvladatelná, a to nejen kvůli náročné orientaci v pravidlech samotných, ale též kvůli např. „*risk-managementu*“,[17] ke kterému je nutná značná orientace v praxi. Analýza rizik, jakožto základní kámen „*risk-managementu*“, může být v praxi lidově řečeno kámen úrazu. Přitom je nezbytnou i pro vyhovění dalším regulatorním požadavkům, jako je tomu např. u institutu varování podle českého zákona o kybernetické bezpečnosti.[18]

2.1 OBECNĚ O COMPLIANCE

Pokud povinné subjekty nechtějí riskovat pokutu či trest, musí se regulatorními požadavky, které na ně klade normotvůrce, řídit a být s nimi v souladu, tedy dosáhnout stavu compliance. Compliance je v takové situaci určitým zvláštním druhem povinnosti, která může stát samostatně, bez závislosti na splnění či nesplnění jiných povinností. Za porušení compliance povinností tak může hrozit sankce, aniž by předtím došlo k reálnému ohrožení chráněných zájmů.[19,20]

---

[15] V i z TSAKANYAN, V.T. The role of cybersecurity in world politics. *Vestnik Rudn. International Relations* [online]. 2017, roč. 17, č. 2, s. 4–8 [vid. 25. únor 2019].

[16] Naopak třeba v Německu byl s přijetím kybernetické bezpečnosti jako politické priority po dlouhou dobu problém. Viz tamtéž.

[17] Zvládání rizik. Jedná se o proces, při kterém povinný subjekt musí vyhodnotit rizika, která mu hrozí, a stanovit ta, která jsou neakceptovatelná, a to buď podle interních předpisů a metodiky, nebo podle vnější regulace.

[18] Aféra Huawei mimo jiné ukázala, že mnoho subjektů není vůbec schopno varování zapracovat, neboť žádnou analýzu rizik nemají.

[19] Čímž se liší od standardní odpovědnosti. Podrobnější porovnání compliance povinností a obecného odpovědnostního modelu je provedeno v kapitole 2.2.

[20] Získáno na základě konzultací s doc. JUDr. Radimem Polčákem, Ph.D.

Základ anglického pojmu „*compliance*“ je ve slově „*to comply*“, což znamená podřídit se, být v souladu či ve shodě. Tento pojem vzešel z angloamerické právní a ekonomické terminologie (přesněji řečeno vzešel tento pojem ze Spojených států amerických). Nejedná se sice o pojem čistě právní, spíše korporátní, ale s tímto pojmem pracuje jak odborná literatura, tak judikatura (případně se vyskytuje i v právních předpisech). Doposud pro něj však nebyl nalezen dostatečně vhodný český ekvivalent.[21] Pro účely tohoto článku tedy budu používat jak pojem „*compliance*“, tak i „*shoda*“ nebo „*soulad*“.

Hurychová a Sýkora dále uvádějí, že „*za podstatu compliance je považováno zajištění souladu mezi společností vykonávanou (podnikatelskou) činností a obecně závaznými právními i jinými předpisy (včetně předpisů interních) a etickými standardy.*“[22] Tyto předpisy mohou být různé povahy a úrovně (úprava evropská, národní atd.), což podnikatelům a investorům situaci nezjednodušuje.

Compliance je kontinuální stav, povinný subjekt se musí regulatorními požadavky řídit neustále. Není tak dostačující konstatovat, že shody bylo dosaženo v určitém časovém bodě, ale je naopak nezbytné neustále monitorovat naplňování požadavků a činit příslušná opatření k zachování takového stavu.[23]

Dodržování stavu compliance představuje z pohledu společnosti určitý typ podnikatelského rizika, se kterým musí kalkulovat. Při vytváření regulatorních požadavků je tak nutné počítat s tím, že pokud budou celkové náklady na zavedení a udržení shody podstatně vyšší než případné postihy, je naivní očekávat od společností, že by pravidla hromadně dodržovaly. Nesmí se ovšem zapomenout, že do následků non-compliance se nezapočítávají pouze případné veřejnoprávní pokuty či tresty (od zavedení trestní odpovědnosti právnických osob je toto plně relevantní

[21] Viz HURYCHOVÁ, Klára; SÝKORA, Michal. *Compliance programy (nejen) v České republice*. Praha, Česká republika: Wolters Kluwer, 2018, s. 4–7.

[22] Viz tamtéž, s. 7.

[23] Viz tamtéž.

i pro právnické osoby), ale stejně tak i poškození pověsti, omezení pojistného plnění či soukromoprávní nároky na náhradu škody.[24]

K dosažení shody nestačí formalistická implementace jakýchsi prázdných pokynů, kterými se nikdo nebude řídit. Je nezbytné, aby společnost, na kterou dopadá regulatorní požadavek (dále také jako „*povinný subjekt*"), skutečně přijala nezbytná opatření, která budou mít potenciál k naplnění kýženého pozitivního stavu. Jen takové řešení totiž dokáže v případě kontroly nebo soudního sporu aktivovat pozitivní účinky stavu compliance (viz níže).[25] Tento aspekt je jedním z nejdůležitějších a zároveň nejzrádnějších. Jak bude níže popsáno, míra potenciálu, která je pro zmíněnou aktivaci dostatečná, nemusí být vždy explicitně a přesně stanovená, a působí tak nejistotu.

2.2 COMPLIANCE VS. STANDARDNÍ MODEL ODPOVĚDNOSTI (LIABILITY)

Standardní odpovědnostní model je, zjednodušeně řečeno, založen na vzniku sekundární povinnosti při porušení povinnosti primární. Pokud tedy povinný subjekt nesplní ať už komisivně nebo omisivně určitý regulatorní požadavek, vzniká mu sekundární povinnost, obvykle v podobě povinnosti nahradit škodu nebo strpět jiný druh trestu. Odpovědnostní sekundární povinnosti jsou tak úzce a neoddělitelně navázány na povinnosti primární a nemohou stát samy o sobě. Na stav naplnění primární povinnosti se pohlíží ex post, tedy až poté, co dojde k nějakému incidentu zasahujícího do právem chráněného objektu.

V momentě, kdy je pravidlo regulující chování povinného subjektu nastaveno obecněji (zvláště performativní pravidla, viz níže), způsobuje tento režim značné snížení právní jistoty povinných subjektů, neboť z důvodu absence oficiálních implementačních postupů a návodů neví, jestli mohou považovat svůj způsob naplnění povinnosti za dostatečný.

[24] Viz ČERMÁK, Miroslav. Regulatorní požadavky představují jen další riziko, a tak je s nimi třeba i zacházet. *CleverAndSmart* [online]. 20. říjen 2018 [vid. 8. listopad 2018]; POLČÁK; HARAŠTA; STUPKA, op. cit., s. 77.

[25] Srov. HURYCHOVÁ; SÝKORA, op. cit., s. 7–13.

Tyto informace mají možnost získat až z činnosti regulátora, kontrolora nebo soudu v jejich případě. Takto nejistě nastavené pravidlo jim nedovoluje funkčně plánovat, nemohou předvídat kroky správních orgánů ani soudů. Těm naopak tato nejistota neúnosně zvětšuje vlastní míru diskrece.[26] Toto představuje značné podnikatelské riziko a je problémem zvláště pro střední a velké podniky i pro veřejnoprávní společnosti. Jsou totiž nuceny fungovat v nejistotě a své podnikatelské chování zakládat na a priori neznámé výši nákladů. Velikost sekundární povinnosti se dá v komplexních situacích jen stěží odhadnout do všech možných důsledků.[27]

Paradoxně největším *„strašákem“* pro společnosti nejsou veřejnoprávní sankce, ale zmíněné soukromoprávní nároky na náhradu škody a omezení pojistného plnění (což jim v případě porušení primární povinnosti hrozí). S veřejnoprávní sankcí se dá dopředu kalkulovat, neboť je alespoň rámcově předepsaná v právních předpisech. Kvůli této skutečnosti může být v určitých situacích pro společnost i výhodnější porušit primární povinnost, pokud bude zisk vyšší než sankce. Ovšem s rozsahem poškozených zájmů a způsobené škody se už ve všech případech dobře kalkulovat nedá. Škoda může dosáhnout až několikanásobně větší výše než veřejnoprávní sankce.[28] Zvláště pak je tento dosah citelný, pokud by škodlivé jednání společnosti vedlo k odepření pojistného plnění.[29]

Když je pro určitý regulatorní požadavek zavedena oficiální compliance procedura (a priori aprobování určitého postupu), tak se tento tradiční odpovědnostní model v případě compliance povinností nemusí uplatnit. Místo něj se nabízí možnost, aby splnění primární povinnosti posoudil oficiální certifikační subjekt ex ante, tedy předtím, než k nějakému incidentu vůbec dojde. Pokud je povinný subjekt shledán v souladu s regulatorním požadavkem, předpokládá se, že učinil všechna rozumná

[26] Viz D'AMATO, Anthony. Legal Uncertainty. *California Law Review* [online]. 1983, roč. 71, č. 1, s. 1–4 [vid. 25. únor 2019].

[27] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 76–77.

[28] Příkladem může být situace, kdy provozovatel celosvětově využívané služby bude odpovědným za škodu na majetku uživatelů způsobenou právě provozem této služby – tedy kdyby např. návštěva internetové stránky www.google.com způsobovala zničení pevného disku počítače.

[29] Viz tamtéž, s. 34 až 37 a 76.

opatření, aby předešel porušení primární compliance povinnosti. Může tak být zaštítěn před právní odpovědností za naplnění stavu compliance.[30]

V takovém režimu pak odpadá podstatná část z výše zmíněných nebezpečí, která hrozí povinným subjektům. Je tím pádem zřejmé, že po takových procedurách bude velká poptávka, zvláště pak ze strany veřejnoprávních společností a velkých podniků. Střední a malé podniky sice mohou žít a fungovat při využívání compliance procedur ve větší jistotě, ale v jejich případě je rizikovost spojená s uplatněním odpovědnosti podstatně nižší, než je tomu u podniků velkých, a kvůli tomu se může stát, že náklady na zajištění stavu shody mohou být pro malé a střední společnosti i podstatně vyšší než ty, vzniklé z povinnosti nahradit škodu.

Oficiální compliance procedury mají oproti odpovědnosti i několik faktických nevýhod. Zvlášť v bezpečnostních odvětvích dávají vzniknout stavu, kdy si povinné subjekty (i spotřebitelé) přijdou „*falešně v bezpečí*“[31] a značně to snižuje jejich touhu starat se o bezpečí nad rámec stavu compliance. Snižuje to pak míru investic věnovaných vývoji nových ochranných opatření. Ty se tak mohou postupně stát nedostatečnými a neaktuálními. Způsob, jakým by se dal dosah tohoto negativního důsledku compliance částečně minimalizovat, je dostatečná aktualizace regulatorních požadavků tak, aby úroveň ochrany a zabezpečení byla stále objektivně dostačující.[32] Nevyžadovala by pak inovaci od povinných subjektů. Takové řešení by se ale mohlo ukázat jako neunesitelné pro regulátora.[33]

Se zavedením compliance procedur souvisí i opačný problém, který se též týká neefektivity, tentokrát však způsobené nadužíváním povinnosti inovovat a zavádět bezpečnostní opatření. Vzhledem k tomu, že compliance

[30] Při splnění compliance povinností se ovšem subjekt nemusí zbavit odpovědnosti za incident.

[31] Tedy kdy se mylně domnívají, že implementace compliance procedury je uchrání před jakoukoliv hrozbou.

[32] Regulátor by např. jedenkrát za měsíc vydával aktualizované předpisy, se kterými by se posuzovala compliance. Tyto předpisy by počítaly s vývojem nových technologií, zranitelností a předepisovaly by modifikované bezpečnější chování. Tento přístup však dle mého názoru nemůže prakticky fungovat, a to zejména kvůli značné rigiditě a kauzálnosti.

[33] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 36–37.

procedura nemůže dopadnout na všechny případy stejně, neodvratně dojde k tomu, že prevence bude muset být prováděna i v situacích, kdy jí nebude reálně potřeba.[34]

Je zároveň možné, že naplnění compliance procedury by v případě její zjevné nedostatečnosti a zastaralosti již nemuselo vést k uplatnění domněnky *„naplnění všech rozumných opatření proti vzniku újmy“* a neochránilo by tak povinný subjekt před vznikem sekundární povinnosti úplně. V takové situaci by část škody možná mohla být požadována i po regulátorovi, např. státu, v případě, že by svým jednáním, případně zjevným opomenutím způsobil ohrožení či poškození cizích zájmů. Ovšem posuzování dostatečnosti compliance procedur je nebezpečná myšlenka vedoucí opět k velké právní nejistotě.

Obecně vzato budou mít compliance procedury tendence zvyšovat byrokratickou zátěž pro povinné subjekty, neboť oproti standardnímu režimu posuzování splnění primární odpovědnosti ex post (tedy posuzují se jenom ty, u kterých došlo k nějakému incidentu) budou posuzována úplně všechna konkrétní řešení povinných subjektů, na které pravidlo dopadne, ex ante. Takové zvýšení byrokratické zátěže v sobě skýtá i nebezpečí vysokého korupčního potenciálu a zvýšení korupčního tlaku na subjekty shodu posuzující.[35]

2.3 STANDARD

Vzhledem k tomu, že bezpečnostní požadavky byly málokdy nadefinovány přesně, vzniklo za dlouholeté absence oficiálních compliance procedur velké množství tzv. standardů, které obsahovaly specifickou úpravu toho,

[34] Příklad: Povinný subjekt A se pohybuje ve vysoce rizikovém prostředí, denně čelí několika incidentům a útoky vedené proti němu jsou vedeny za použití nejmodernějších technologií. Potřeba inovovat a zavádět nejmodernější bezpečnostní opatření tak, jak by si žádala hypotetická compliance povinnost, je tedy v souladu s jeho vlastním zájmem. Povinný subjekt B se pobyhuje v málo rizikovém prostředí a s útoky se musí vypořádávat pouze ojediněle. Pokud by měl tedy povinnost inovovat a investovat do bezpečnostních opatření na stejné úrovni jako povinný subjekt A, dosažení compliance pro něj bude představovat až zbytečnou zátěž.

[35] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 77–78.

jak dosáhnout shody. Tyto standardy byly vytvářeny různými tělesy, ať už národními, mezinárodními, obecnými nebo speciálními odvětvovými.[36]

Mezinárodní organizace pro standardizaci (dále jen jako „ISO"), která zaštiťuje standardizační instituty celkem ze 162 zemí a je tak jednou z nejvýznamnějších institucí v oboru (podrobněji bude představena ve čtvrté kapitole), vyložila pojem standard následovně: „*Zdokumentované dohody obsahující technické specifikace či jiná konkrétní kritéria, kterých má být soustavně užíváno jako pravidel, vodítek nebo definic charakteristik, a to k zajištění toho, aby materiály, produkty, procesy a služby byly vhodné pro daný účel.*"[37]

Standardy nebývají založeny na využití specifických technologií, neboť by tak byly značně neohebné z pohledu schopnosti reakce na technologický vývoj, častěji se tak definuje styl a smysl implementačních postupů. S množstvím organizací a jiných subjektů pracujících na vytváření standardů (a to i v oblasti kybernetické bezpečnosti) však vznikl problém nesourodého názvosloví. Každá organizace si do standardu nadefinovala určité pojmy, a bohužel ne vždy v souladu s ostatními. Odborné debaty jsou pak zatížené více slovíčkařením než přínosnou rozpravou.[38]

Jakmile povinný subjekt naplní kritéria, která standard stanoví, může prohlásit compliance s tímto standardem. Ovšem vzhledem k tomu, že takové prohlášení učiní sám, bez jakéhokoliv dohledu či kontroly, neponese takové prohlášení samo o sobě u informovaných účastníků trhu velkou váhu.[39]

ISO samotné varuje, že dosažení shody s mezinárodním standardem nemůže sloužit k zaštítění povinného subjektu před právní odpovědností.

---

[36] Pro příklad, jak se vytvářejí standardy, viz https://www.iso.org/developing-standards.html.

[37] Autorův překlad z anglického originálu: „*Documented agreements containing technical specification or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose*". Více viz MEHAN, Julie E. *CyberWar, CyberTerror, CyberCrime.* [online]. 2nd ed. Ely, Cambridge, UK: IT Governance Publishing, 2014, s. 162 [vid. 19. srpen 2018].

[38] Viz MEHAN, op. cit., s.162.

[39] Viz ALKALBANI, Ahmed et al. Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management* [online]. 2017, roč. 1, č. 2, s. 106 [vid. 23. červenec 2018].

Takovou schopnost získá standard až při oficiálním uznání státem a pouze ve vztahu ke compliance povinnostem (např. Japonsko ve vztahu ke standardu ISO 27001).[40] Některé standardy či certifikační řešení umožňují postup, který stojí mezi prohlášením compliance a oficiální certifikační procedurou → tzv. sebe-certifikaci (angl. self-certification) použitelnou většinou v nízko-rizikovém prostředí. V tomto případě si regulovaný subjekt samotný vyhodnotí, zdali určená kritéria splňuje. Může pak vydat prohlášení o souladu, kterým informuje potenciální zákazníky, že dodržování regulatorního požadavku bylo v souladu s určitou metodikou zkontrolováno. Povinný subjekt ale většinou přebírá plnou odpovědnost za řádné provedení kontroly, nebo rovnou za celý proces.[41] Vlastní posouzení je tak sice rychlejší a podstatně levnější variantou k certifikaci, ale zároveň tak podnikatel přichází o mnoho výhod spojených s certifikovaným stavem compliance.[42]

Snaha o dosažení shody se standardy je obecně založena na dobrovolné bázi. Povinný subjekt se může svobodně rozhodnout, jestli standard využije a získá tak určitou výhodu, či nikoliv a dosáhne souladu s pravidly po své vlastní ose. To samozřejmě značně snižuje harmonizační (a v bezpečnostních odvětvích i zabezpečovací) účinky takového řešení, ale zase nedochází k ohýbání trhu, které by při vysokých nákladech na dosažení shody mohlo menší společnosti ze soutěže úplně vyloučit. Snahy o vytvoření závazných standardů narážejí opakovaně jak na nedostatek mezinárodní vůle (státy mají stále v některých odvětvích, zvláště týkajících se národní bezpečnosti, tendence preferovat protekcionismus), tak i na mnoho praktických komplikací, jako přílišná obecnost formulací (na těch je sice možné dosáhnout konsensu, ale zase takový standard nic neřeší) nebo absence vymahatelnosti a kontroly. Vedle toho některé státy vypracovaly

[40] Viz SMEDINGHOFF, Thomas J. *Information Security Law* [online]. Ely, Cambridge, UK: IT Governance Publishing, 2008, s. 129 [vid. 11. říjen 2018].

[41] Sebe-certifikace tak v tomto bodě nepředstavuje pouze limitaci odpovědnosti, ale zároveň i prohlášení, přijímající odpovědnost za určité typizované škody. Povinný subjekt totiž zaručuje, že určitá skutečnost nenastane.

[42] Viz AXELROD, C. Warren. The creation and certification of software cybersecurity standards. In: *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* [online]. Farmingdale, NY, USA: IEEE, 2016, s. 1–2 [vid. 22. červenec 2018].

národní řešení, která jsou sice konkrétní, ale naprosto nevhodná k širší, či dokonce celosvětové aplikaci, neboť pochopitelně vůbec nereflektují specifika úpravy v dalších státech, a úprava je tak kompletně rozdrobená.[43] Na tyto problémy narazila i Common Criteria, která představují nejrozsáhleji akceptovaný mezinárodně uznávaný standard pro kyberbezpečnostní technologie. V jejich případě se ani po mnoha letech vyjednávání a úprav nepodařilo upravit tento model natolik, aby byl vhodný pro certifikaci služeb (např. služby typu Software as a Service, primárně z důvodu, že testovat jednotlivé části systému nepostačuje k tomu, aby bylo možné prohlásit bezpečnost celku).[44] O tom svědčí i fakt, že přestože bylo v roce 2013 certifikováno podle Common Criteria více jak 1500 produktů, nebyla certifikována ani jedna služba.[45] Do dne 12. 10. 2019 prošlo certifikačním procesem (včetně archivovaných) 4059 produktů, a služba stále žádná.[46]

Vzhledem k tomu, že standardizace vzniká nejčastěji díky spolupráci v rámci určitého odvětví, dochází tím mezi podniky k šíření tzv. best practice (společnosti se dělí o postupy, které se jim nejvíce osvědčily), což pozitivně ovlivňuje trh, vývoj i spotřebitele.[47] Se standardy často souvisí ještě různé pomocné dokumenty (angl. „*guidelines*“, tedy vodítka, návody, manuály, které demonstrují, jak mohou být standardy splněny). Ty jsou obvykle vydávány orgánem, který spravuje daný standard, za účelem výkladu problematických či neurčitých pojmů v praxi a fungují jako určitá forma soft law.[48]

---

[43] Viz AXELROD, op. cit., s. 1–3.

[44] Viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014 [vid. 24. srpen 2018].

[45] Viz KALUVURI, Samuel Paul; BEZZI, Michele; ROUDIER, Yves. Bringing Common Criteria Certification to Web Services. In: *2013 IEEE Ninth World Congress on Services (SERVICES)* [online]. Santa Clara, CA, USA: IEEE, 2013, s. 1 [vid. 22. červenec 2018].

[46] Jedná se o součet 1401 certifikovaných produktů a 2658 archivovaných. Více viz Certified Products List - Statistics. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/products/stats/.

[47] Viz HURYCHOVÁ; SÝKORA, op. cit., s. 8–14.

[48] Srovnej s HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti* [online]. Brno, 2017, s. 36 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta.

2.4 CERTIFIKACE

Shodu s určitým regulatorním požadavkem, případně se standardem, pokud ten k naplnění takového požadavku směřuje (v odborné literatuře se vyskytuje i pojem „*conformance*“, který je svým významem compliance podobný, ač není úplně totožný[49]), může prohlásit subjekt sám o sobě. Vyšší úroveň důvěry však zakládá proces označovaný jako „*certifikace*“. Ten značí, že produkt, služba, proces (či obecně cokoliv, co by mohlo být předmětem regulačních aktivit a certifikace) výrobce byl otestován subjektem akreditovaným k udílení certifikací. V obecném certifikačním režimu je nezbytné, aby mezi hodnoceným a akreditovaným subjektem neexistoval žádný vztah (jako např. mateřská – dceřiná společnost), aby bylo posuzování skutečně nestranné a objektivní.[50] Jedná se o formalizované posouzení naplnění určitého setu požadavků (označovaných obvykle jako certifikační schéma) hodnotitelem, který se označuje jako certifikační autorita. Na konci certifikačního procesu bude povinnému subjektu vydán oficiální certifikát (do nějž by nemělo být možné zasáhnout, ani ho zfalšovat), který potvrzuje naplnění požadavků do určité úrovně. Certifikační autorita se tak zaručuje za naplnění požadavků standardu nebo práva a propůjčuje důvěru, kterou mají zákazníci v její jméno, prostřednictvím certifikátu produktu povinného subjektu.[51]

K tomu, aby mohlo k hodnocení vůbec dojít, je nezbytné, aby byla certifikační autorita spojena s dostatečně vyspělými testovacími laboratořemi. V nich je produkt (služba atd.) otestován, zdali splňuje veškeré compliance požadavky, a to podstoupením rozličné materie testů. Vybavení takových laboratoří představuje enormní finanční zátěž, a proto před vznikem podobné laboratoře investoři zevrubně mapují trh

[49] Srovnej s SCORM Compliant, SCORM Conformant, SCORM Certified. *SCORM.com* [online]. [vid. 27. říjen 2018]. Získáno z: https://scorm.com/scorm-explained/scorm-resources/conformance-vs-compliance/.

[50] Vyskytují se i compliance modely, ve kterých není naplnění této podmínky zapotřebí. Příkladem může být metoda vlastního posouzení, kterou upravuje Akt (viz kapitola 7.4.3), kdy se subjekt certifikuje sám.

[51] Viz What's the Difference Series: Compliance vs. Certification. *Mireaux Management Solutions* [online]. 14. leden 2013 [vid. 27. říjen 2018]; AXELROD, op. cit., s. 1–3.

a vyhodnocují, jaká bude po certifikačních službách poptávka (návratnost investice). V případě kybernetické bezpečnosti mnohé z menších evropských států zatím nepředstavují dostatečně zajímavý trh, a tak na jejich území certifikační laboratoře a autority zatím vůbec nevznikly (tomuto trendu napomáhá i mnohdy chybějící vnitrostátní právní úprava kyberbezpečnostní certifikace). Z právě uvedeného je patrné, že neexistuje a ani prakticky nemůže existovat laboratoř, která by byla schopna testovat univerzálně všechno. Z ekonomických důvodů dochází vždy k určité profilaci.[52]

Úprava možnosti vytvářet nová certifikační schémata může být buď rigidní (např. ISO 27001) nebo uvolněná (např. Common Criteria, kde si povinný subjekt může schéma nadefinovat i sám). Se schopností adaptace certifikačního schématu však rostou i náklady na výbavu laboratoří jak z pohledu technologického, tak personálního. Proto je výhodou, když i nově vytvářená schémata jsou založena na univerzálně přijímaných základech, díky čemu je snadnější najít laboratoř schopnou provedení testů. Certifikační proces může být zároveň i různě přísný podle toho, jak důkladnému testování bude produkt podroben před udělením certifikátu.

U testování obecně nastává problém prostředí, ve kterém k testování dochází. Pokud totiž dojde k aplikaci testovaného objektu v jiném prostředí, než v jakém byl testován, bude certifikát de facto (mnohdy i de iure) k ničemu, neboť v takovém prostředí se můžou vyskytovat úplně jiné hrozby. Zároveň je u certifikace velký problém s životním cyklem produktu/služby atd. Mezi teoretiky nepanuje shoda, jestli úpravy a aktualizace činí certifikát neplatným v celém jeho rozsahu a je tak nutné provést plnou recertifikaci, jestli se mají testovat jenom samotné úpravy, či jestli je správná jakási verze kompromisu mezi zmíněnými.[53]

U certifikace je důležité rozlišovat, zdali se jedná o certifikaci komerční, o certifikaci státem uznávanou nebo přímo o certifikaci státní. S povahou certifikace může právotvůrce spojit různé právní následky. Státní certifikace je prováděna státním orgánem a stát tak nad ní má kompletní

[52] Viz AXELROD, op. cit., s. 5.

[53] Viz AXELROD, op. cit., s. 5.

dohled a moc, tudíž bude získání takového certifikátu podmínkou pro splnění nějakého ze zákonných požadavků. Státem uznaná certifikace je vykonávaná sice samostatným subjektem, ale stát s takovouto procedurou pojí určité pozitivní následky. Poněkud na pomezí zmíněných modelů stojí certifikace prováděná sice samostatným subjektem, ovšem akreditovaným k takové činnosti akreditačním orgánem. Čistě komerční systém je prováděn toliko na podnikatelské bázi soukromým subjektem, kdy stát certifikaci nepřiznává žádné účinky. Posledně zmíněný model je pro podnikatele nevýhodný (i přes pozitiva, která spolupráce a šíření nejlepších praktik přináší), a proto jsou tendence zvrátit čistě komerční certifikace alespoň do modelu certifikace uznávané státem.[54]

Pokud povinný subjekt získá státem uznávaný certifikát, může žít a priori v jistotě, že dosáhl compliance se všemi jejími pozitivními efekty (nebo by se compliance alespoň předpokládala a bylo by nutné ji vyvrátit). S náklady na získání certifikátu se dá dopředu kalkulovat a taková situace je tak pro povinné subjekty podstatně jednodušší a výhodnější. Mimo jiné je tím odstraněna podnikatelská nejistota spojená s neurčitou úrovní dostatečnosti příslušné implementace compliance procedur a s výší nákladů.[55]

2.5 DRUHY REGULATORNÍCH PRAVIDEL

Složitost procesu k dosažení shody je základní otázkou, která určuje, zda je pro určitou regulaci potřebný specificky upravený compliance proces. Složitost je ovlivňována jak specifickou povahou regulace technologií, tak i samotným způsobem stanovení regulačního požadavku. V případě naprosto konkrétní úpravy požadavku bude potřeba compliance procedur minimální, s rostoucí obecností pak poroste i potřeba zjistit, jak shody uspokojivě dosáhnout. V této podkapitole tak rozeberu tři druhy regulatorních pravidel, kterých může být využito v certifikačních schématech, o nichž bude řeč v dalších kapitolách. Smyslem této

[54] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 80.

[55] Viz tamtéž, s. 30.

podkapitoly je objasnit, „*jak*“ mohou být formulovány požadavky, proti kterým má být shoda certifikována.

Normotvůrce stojí při rozhodování o metodě formulování regulatorního požadavku před problematikou poměřování čtyř důležitých principů – konzistence a jistoty proti flexibilitě a inovaci.[56] Nadměrná a nepragmatická obliba konzistence a rigidních úprav má dnes již mnoho kritiků, přestože se v minulosti jednalo o přístup víceméně jediný. Tito kritici poukazují na fakt, že mnohé regulace jsou tak úzce nadefinované a tak silně preskriptivní, že jejich účinky jsou po čase nedostatečně a až nelogicky zbytečně zatěžující společnosti, které musí na dosažení shody vynaložit příliš mnoho prostředků s minimální efektivitou výstupu (toto se děje zvláště v některých odvětvích, např. ochrana životního prostředí).[57]

Podle toho, na jakou fázi aktivit společnosti regulace dopadá,[58] rozlišujeme tři režimy pravidel – technologická pravidla (která můžou být též řazena jako podkategorie pravidel deskriptivních či behaviorálních,[59] z angl. Technology-based, resp. Descriptive rules) dopadající na fázi realizační, performativní pravidla (z angl. Performance-based rules) dopadající na fázi výslednou a pravidla řízení (z angl. Management-based rules) dopadající na fázi plánování.[60]

---

[56] Viz MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy* [online]. 2003, roč. 25, č. 4, s. 382–383 [vid. 22. září 2018].

[57] Viz HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti* [online]. Brno, 2017, s. 52–54 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta; MAY, op. cit., s. 382-383.

[58] Rozlišujeme celkem tři fáze každé regulované aktivity a tři způsoby, jak na ně mohou pravidla dopadnout: plánovací fáze (pravidla zde regulují, jakým způsobem se má plánovat a jak se má chovat společnost od počátku projektu, aby směřovala k určitému cíli), realizační fázi (regulují konkrétně, jakým způsobem a za použití jakých prostředků má být činnost vykonávána) a na fázi výslednou či fázi výsledků, z ang. Output stage (pravidla regulující tuto fázi stanoví, k čemu má chování společnosti směřovat).

[59] Viz KNEEPKENS, Jules. Performance Based Regulation. In: *EASA Safety Conference* [online]. B.m. 10. říjen 2012 [vid. 20. září 2018].

[60] Viz COGLIANESE, Cary; LAZER, David. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals. *Law & Society Review* [online]. 2003, roč. 37, č. 4, s. 694 [vid. 12. září 2018].

2.5.1 DESKRIPTIVNÍ PRAVIDLA

Pravidla, která jsou vystavěna na deskriptivním principu, jsou pravidla nejstarší. Stanovují konkrétně definované povinnosti subjektům. Jedná se např. stanovení výše daní nebo nejvyšší dovolené rychlosti na silnici. Tato pravidla nezmiňují přímo, k jakému cíli se má dospět (přestože je to z nich často pochopitelné), ale předepisují konkrétní chování, které má tento cíl naplnit. Normotvůrce tak přebírá povinnost vyhodnotit, jaké chování je v dané situaci žádoucí. V minulosti byl tento model používán nejvíce, nyní se ovšem ukazuje, že v mnohých oblastech úpravy (zvláště těch, ve kterých dochází ke střetu technologií a práva) má značné slabiny.[61]

Deskriptivní pravidla nejvíce trpí slabinou, která v různé míře postihuje všechny druhy regulatorních požadavků. Tato slabina se v angličtině označuje jako problém „*One size to fit them all*“.[62] Nabízí se sice řešení v podobě větší míry obecnosti, ale ani toto není žádoucí, neboť obecnost nevyhnutelně snižuje právní jistotu a způsobuje nutnost extenzivního výkladu normy, případně i vytvoření compliance procedur.[63]

Zůstává tedy faktem, že není možné zohlednit okolnosti každého určitého případu při vytváření normy, a tudíž může v mnoha případech dojít k tomu, že výsledný stav je buď nesmyslně přeregulován či podregulován. Tím myslím, že v takové situaci je po povinném subjektu pravidlem vyžadováno buď daleko víc, nebo podstatně méně, než je nezbytně nutné. Tím narůstají investice společností na dosažení shody s regulací či se naopak zvyšuje míra rizika, že se projeví negativní následek, kterému chce regulace zabránit. Buď tedy dochází k nesmyslnému ohýbání trhu, nebo regulace nepostačuje ani ke splnění svého vlastního cíle, čímž se stává de facto zbytečnou.[64]

Dalším negativem deskriptivních pravidel je skutečnost, že mohou efektivně vyřadit touhu společností inovovat „*žádoucím*“ způsobem. Oproti

[61] Viz tamtéž, s. 701.

[62] Po regulaci se chce, aby dopadla na všechny unikátní případy, a to s optimálními účinky.

[63] V i z COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform* [online]. 2016, roč. 50, č. 3, s. 527 [vid. 12. září 2018].

[64] Viz tamtéž.

tomu se u společností může rozvinout touha inovací směřujících k úniku z dosahu regulace. Pokud je pevně stanoveno, jaké technologie má provozovatel služby používat, nemá pak tento provozovatel důvod nacházet efektivnější řešení, kromě lepšího poměru cena/výkon. Chybějící inovativnost subjektů musí nahrazovat normotvůrce, což samozřejmě vede ke zvýšení nákladů normotvorného procesu. Je možné tento „*aktualizační proces*“ provést buď neustálou novelizací textu zákona, nebo využitím neurčitých pojmů, které následně definuje správní cestou regulátor k tomu určený.[65] V českém prostředí vystupuje jako takový regulátor např. Český telekomunikační úřad.[66]

2.5.2 PERFORMATIVNÍ PRAVIDLA

Performativní pravidla jsou relativně novým konceptem regulace (přestože pravděpodobně první pravidlo tohoto druhu se vyskytlo již v Chamurappiho zákoníku[67]) a bude jim zde věnována větší pozornost kvůli jejich vhodnosti k použití regulace technologií. Performativní pravidlo je takové, které vymezí určitý cíl, určitý chtěný stav a nechá na regulovaném subjektu, jakým způsobem tohoto stavu dosáhne.[68] Pro příklad – „*Řidič motorového vozidla je povinen jet pouze tak rychle, aby jeho jízda byla bezpečná*“. Pro regulovaný subjekt není předepsané, jakým konkrétním způsobem se má zachovat, důležité je, aby naplnil stav požadovaný normou. Pravidlo tak přizpůsobí své individuální potřebě a do značné míry tím limituje dosah již zmíněného problému „*One size to fit them all*“, neboť si každý regulovaný subjekt své chování reguluje sám ad hoc.[69]

---

[65] Viz HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti* [online]. Brno, 2017, s. 33 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta.

[66] Jako regulátor, alespoň v určitém smyslu slova, může vystupovat i NÚKIB v oblasti kybernetické bezpečnosti. Povaha jeho aktivit je ovšem v tomto ohledu méně jednoznačná, a je tak spíše „*kvaziregulátorem*“.

[67] Viz MAY, op. cit., s. 390.

[68] Viz COGLIANESE, Cary; NASH, Jennifer; OLMSTEAD, Todd. Performance-Based Regulation: Prospects and Limitations in Health, Safety and Environmental Protection. *Administrative Law Review* [online]. 2003, roč. 55, č. 4, s. 14 [vid. 20. září 2018].

[69] Viz tamtéž, s. 14–15.

Performativní pravidla se tak stávají, spíše než pravidly o chování, pravidly o vytváření pravidel chování. Nabízejí flexibilitu a mohou rozproudit touhu po „*dobré*“ inovaci a nacházení nových řešení, jak efektivněji plnit povinnost.[70] V praxi pak jeden subjekt, který se bude řídit výše zmíněným performativně-konstruovaným rychlostním limitem, může bez problémů jet rychlostí 150 km/h, protože se jedná o zkušeného řidiče na bezproblémovém úseku, a druhý subjekt pojede rychlostí 30 km/h, neboť se jedná o začátečníka a na více si nevěří. Oba dva jsou v souladu s pravidly, přesto každý jiným způsobem.

Performativní pravidla nabízejí velkou svobodu normotvůrci. Je možné je nadefinovat úzce či široce (určuje míru diskrece, která je ponechána subjektu, pokud regulace naformuluje, jakého výkonu má dosáhnout motor, tak je možnost diskrece očividně nízká).[71]

Tato pravidla operují s velkou mírou obecnosti, případně až volnosti povinných subjektů.[72] Pozitiva těchto pravidel, plynoucí z využívání velké volnosti subjektů, jsou velká, mají však i své slabiny. Ty vychází z téměř absolutní absence empirického výzkumu, který by jakkoliv vyhodnotil jejich reálné účinky. Přestože nad povahou performativních pravidel byly vedeny rozsáhlé vědecké debaty, mnohé vědění o těchto pravidlech zůstává na čistě teoretické úrovni. Problémem pak je i otázka vymáhání – většina států tuto otázku ignoruje nebo se jí z důvodu nedostatku zkušeností či prostředků věnuje naprosto nedostatečně a pravidla pak nefungují (jak ukázal i debakl Volkswagenu ohledně dodržování emisních limitů[73]).[74]

Performativní pravidla mají na první pohled velkou ekonomickou výhodu pro stát, neboť pro jejich vývoj není nutné vynaložit tolik prostředků, ani není nutné tak hluboké pochopení problematiky jako pro

[70] Viz COGLIANESE, 2016, op. cit., s. 543.

[71] Viz COGLIANESE; NASH; OLMSTEAD, op. cit., s. 14–15.

[72] Ale zvláště menší a začínající subjekty často nemají prostředky, kapacity nebo zkušenosti na to, aby mohly svobodu poskytovanou performativními pravidly efektivně využívat. To vytváří potřebu alespoň rámcových návodů, jak shody dosáhnout.

[73] Tento skandál vypukl v roce 2015, kdy vyšlo najevo, že Volkswagen více jak 7 let ignoroval performativně nastavená pravidla na limitaci vypouštěných emisí.

[74] Viz COGLIANESE, 2016, op. cit., s. 529–531.

zkonstruování funkčního pravidla deskriptivního. Ve skutečnosti se však jedná o částečné přesunutí finanční zátěže do oblasti vynucování pravidel. Svoboda v dosahování shody pro stát představuje daleko náročnější vyhodnocování, jestli subjekty dodržují právo.[75,76]

Snížení ekonomické zátěže státu se zároveň pojí se zvýšením nákladů pro povinné subjekty. Regulátor využívající tohoto modelu spoléhá na fakt, že regulované subjekty samotné ví nejlépe, co a jak mají dělat. Tak tomu bude často v případě velkých konglomerátů, ale pro malé podniky tato situace platit nebude. Ty budou muset vynaložit velké prostředky, aby zjistily, který z postupů je pro dosažení shody nejlepší. Tyto náklady mohou být dokonce tak vysoké, že ve spojení s absencí dostatečné jistoty, že tento postup bude pro dosažení shody dostatečný (tedy v případě absence oficiálních compliance procedur), povede taková situace k vytvoření blokády na trhu proti malým podnikům. Pro velké podniky dojde ke značné finanční úlevě, protože si budou moci stanovit limity a pravidla efektivněji a náklady na výzkum a inovace u nich nebudou tak znatelně zvýšeny.

Performativní pravidla mohou plně fungovat pouze tehdy, pokud se zájmy regulátora a regulovaných subjektů alespoň rámcově shodují. Pokud jsou v přímém rozporu, jako je tomu např. u daní, není prakticky možné, aby byla výše daní upravena performativně. Je jasné, že příkaz ve stylu „*Platte daně v takové výši, aby to státu vystačilo*“ by regulované subjekty k placení moc nemotivoval.

2.5.3 PRAVIDLA ŘÍZENÍ

Management-based rules, tedy pravidla řízení, regulují fázi plánování, procesů a operací, a to tak, že předepíšou, jak by plánování a celkově chování řídících orgánů společnosti mělo vypadat, aby mělo potenciál naplnit cílový stav. Mohou tedy stanovit, že součástí plánování musí být

[75] Nadále se totiž nevyskytuje jednoduchý stav „*splňuje/nesplňuje konkrétní normu*“, ale je nutné vyhodnotit celý proces i s jeho dopady, tedy – „*Byl tímto cíl naplněn?*“. I pro stát samotný tak může být výhodné vytvořit oficiální compliance proceduru, která sice nemusí být závazná pro všechny, ale mnohé subjekty by jí mohly využít a navíc poskytne i rámcový návod pro postup při kontrolách.

[76] Viz MAY, op. cit., s. 388.

hodnocení rizik, procedury pro monitorování problémů či zavedení jiných typů procesu do chování subjektu.[77] Procesy implementované do plánovací fáze pak ovlivňují celý život projektu, často v něm i celou dobu vystupují. Tyto procesy se musí dobře dokumentovat a zanést i do plánů, které v počátečních fázích života projektu vznikají, aby bylo možné kontrolovat a posuzovat shodu.[78] I tato pravidla má však smysl využívat pouze v případě, že stát dokáže dohlížet na jejich naplňování a případně shodu vynucovat, stejně jako u pravidel performativních.[79]

Ani pravidla řídící, ani pravidla performativní se v praxi téměř nevyskytují v čisté podobě. Je často nutné, aby byla zkombinována s modelem deskriptivním.

2.5.4 CHARAKTER PRAVIDEL KYBERNETICKÉ BEZPEČNOSTI

V oblasti kybernetické bezpečnosti je většina pravidel vystavěna na principu povinnosti subjektu provést rozumná či přiměřená opatření k ochraně dat. Cíle těchto regulací bývají většinou vyjádřeny pozitivním stavem, kterého je zapotřebí dosáhnout, např. zajištění dostupnosti. Vhodné by tak mohlo být použít performativní pravidla. Ta by byla vhodná i z jiného důvodu. Zákonodárci často pravidla o kybernetické bezpečnosti formulují s užitím neurčitých pojmů pro lepší flexibilitu pravidla. Občas je to však způsobené i tím, že nemají k dispozici dostatečné informace či vědomosti o problematice kybernetické bezpečnosti, a pravidla jsou tak konstruována ve stylu povinné implementace „*dostatečných procedu*r“ či „r*ozumných pojistek*“ kvůli tomu, že zákonodárce správné řešení nezná a bylo by pro něj jednodušší toto břímě přesunout na povinný subjekt.[80] I to ukazuje na větší vhodnost performativních pravidel, v některých případech i pravidel řízení. Tím však nechci bagatelizovat výhody využití neurčitých pojmů, pouze podotýkám, že je zapotřebí skutečně odborného regulátora.[81]

---

[77] Viz COGLIANESE; LAZER, op. cit., s. 694.

[78] Viz COGLIANESE; LAZER, op. cit., s. 694.

[79] Viz tamtéž, s. 711.

[80] Viz SMEDINGHOFF, op. cit., s. 61–62.

[81] Příkladem performativního pravidla v českém zákoně o kybernetické bezpečnosti je bezpečnostní opatření (§ 4 odst. 1 zákona č. 181/2014 Sb.)

3. CERTIFIKACE V SYSTÉMU KYBERNETICKÉ BEZPEČNOSTI

Na začátku této kapitoly stručně popíšu fungování zabezpečování v kybernetické bezpečnosti, aby bylo možné si představit konkrétní bezpečnostní opatření, která jsou v průběhu certifikačního procesu testována, a nezůstalo jen u prázdných pojmů. Cílem a posláním kybernetické bezpečnosti je zabezpečení a ochrana prostředí pro realizaci práv člověka (pro potřeby tohoto článku si vystačíme i s ochranou informací a informační infrastruktury před hrozbami). Zájem na tom, aby v rámci informačních systémů byla zachována důvěrnost, integrita a dostupnost dat (tzv. CIA triáda, vycházející z anglického Confidentiality, Integrity a Availability; tato triáda je pravidelně využívána k definování toho, jaké vlastnosti mají mít „*zabezpečené informace*“[82]) je hnán snahou zabezpečit zájmy jak soukromých, tak veřejnoprávních subjektů. Výsledkem tohoto zájmu je pak určité regulované chování v kyberprostoru. Jako regulátor může vystupovat jak stát (výsledkem je právní předpis), tak i sdružení soukromých subjektů. Ti se mohou dohodnout na sdílení a plošném užívání osvědčené praxe, které pak mohou vynucovat i proti menším nebo začínajícím subjektům na trhu (tato pravidla tak budou mít podobu soft law). De facto tak vznikne standardizované bezpečné chování, které může být následně trhem vyžadované.[83]

Hrozby ohrožující bezpečnost a integritu informací se obecně dělí do tří kategorií podle oblastí, z nichž pocházejí – fyzické, technické a lidské. Fyzické v sobě zahrnují incidenty, jako jsou krádež nebo povodně. Technické hrozby jsou takové, které se provádějí za pomocí škodlivého počítačového kódu nebo jiného zautomatizovaného systému. A lidskými hrozbami jsou myšlena rizika mající svůj původ v operačním personálu (typicky zaměstnanec s lístečkem přilepeným na monitoru, a na lístečku má napsané heslo) a ti, kteří se snaží informační systém či část infrastruktury

[82] Viz BASKERVILLE, Richard; STRAUB, Detmar W; GOODMAN, Seymour E. *Information Security* [online]. Armonk, NY, USA: Routledge, 2008, s. 57 [vid. 11. listopad 2018]. Advances in Management Information Systems.

[83] Viz SMEDINGHOFF, op. cit., s. 15–17 a 61-63.

napadnout, zničit nebo zneužít.[84] Kybernetická bezpečnost implementuje bezpečnostní řešení, která mají za cíl minimalizovat dosah jednotlivých hrozeb, a zároveň lidově řečeno „*zacpávat bezpečnostní díry*“. Tento systém by měl ideálně fungovat tak, že se útočníkovi nepovede využít dvakrát stejné zranitelnosti (bezpečnostní díry).

Bezpečnosti je v této oblasti dosahováno nejen za pomoci různých technických prvků v podobě hardwarových a softwarových řešení (např. firewall), ale stejně tak i za pomoci různých interních předpisů, organizačních struktur či bezpečnostních politik. Jedním z nejdůležitějších prvků kontrování hrozeb jsou analýzy a analytické dokumenty (např. analýza rizik), které slouží k odhalení slabin a incidentů. Proškolení vlastního personálu ohledně pravidel bezpečnosti a zmíněných bezpečnostních procedur (v případě, že jsou reálně a dobře nastaveny) může také značně přispět ke zvýšení bezpečnosti prostředí (v praxi jsou pokyny pro zaměstnance často vytvářeny jako pouhá formalita, takže jim nikdo ve výsledku nerozumí).[85]

Bezpečnostní řešení se dělí, kromě druhu kontrované hrozby, i z pohledu času, a to na preventivní a reaktivní. Preventivní mají hrozbám předcházet (působit ex ante na základě již vyřešeného kybernetického bezpečnostního incidentu; český zákon o kybernetické bezpečnosti s nimi počítá v případě ochranných opatření[86]) a reaktivní opatření (tak je zná i český zákon[87]) se aktivují až při probíhajícím incidentu, kdy jejich účelem je minimalizace škod a zastavení útoku/incidentu.[88] Příkladem preventivního opatření kontrujícího hrozbu fyzické povahy je zámek na vstupních dveřích. Preventivní ochranou před technologickou hrozbou můžou být firewall, hesla, PIN kódy nebo šifrování, a před lidskou hrozbou zase důkladné proškolení zaměstnanců o bezpečnosti a kyber-hygieně.[89]

---

[84] Viz SMEDINGHOFF, op. cit., s. 26–28.

[85] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 37; SMEDINGHOFF, op. cit., s. 29–30.

[86] Viz § 14 zákona o kybernetické bezpečnosti.

[87] Viz § 13 zákona o kybernetické bezpečnosti.

[88] Viz KYSELOVSKÁ, Tereza et al. *Cofola 2015: Sborník z konference* [online]. Edice Scientia. Brno: Masarykova univerzita, 2015, s. 20 [vid. 22. listopad 2018].

[89] Viz SMEDINGHOFF, op. cit., s. 30–34.

3.1 SPECIFIKA CERTIFIKACE V KYBERNETICKÉ BEZPEČNOSTI

Oblast kybernetické bezpečnosti a celkově IT prostředí se vyznačuje vysokou mírou inovativnosti a rychlostí technologického pokroku a nutí tak zabezpečovací opatření do převážně reaktivní polohy (výše zmíněné „*zacpávání děr*“). To je patrné zvlášť v momentě, kdy je v procesu certifikace testováno, jestli objekt neobsahuje známé zranitelnosti.

V oblasti kybernetické bezpečnosti je hned několik objektů, u kterých je možné certifikovat soulad – jedná se o technologie (produkty a služby), bezpečnostní procesy (např. systém řízení bezpečnosti informací), zabezpečení organizační struktury společností, případně i osoby ad. Pro účely tohoto článku je důležitá zejména certifikace technologií, ale nový Akt o kybernetické bezpečnosti, který bude rozebrán v dalších kapitolách, obsahuje i úpravu certifikace procesů, tudíž by mohl zasáhnout i do certifikace systémů řízení bezpečnosti informací (také jako „ISMS“), a tak je nutné zde vysvětlit i tento pojem.

Certifikace ISMS je primárně prováděna podle mezinárodního standardu ISO/IEC 27001:2013. Mezinárodní organizace pro standardizaci označuje ISMS za „*systematický přístup ke správě citlivých informací společnosti za účelem zachování bezpečnosti těchto informací. Tento přístup zahrnuje užití procesu zvládání rizik na personální složku, procesy i IT systémy společnosti*“.[90] ISMS zná i český zákon o kybernetické bezpečnosti včetně (nové) vyhlášky o kybernetické bezpečnosti. Ta ISMS definuje v § 2 písm. j) jako „*část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat*“.[91] Jedná se o komplexní řídící proces sloužící k zabezpečení informací, který je založen na hodnocení rizik hrozících subjektu, a tudíž je možné jeho „*přísnost*“ přizpůsobit prostředí společnosti. Vedení subjektu

[90] Autorův překlad z anglického originálu: „*systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.*“ Více viz ISO/IEC 27001 Information security management. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/isoiec-27001-information-securit.html.

musí na základě zprávy o hodnocení rizik rozhodnout, která rizika jsou ještě tolerovatelná a která již nikoliv. Na základě tohoto rozhodnutí pak dochází k řízení rizik (tedy k odstranění či minimalizaci netolerovatelných hrozeb). Vzhledem k tomu, že ISMS je procesem, dochází k hodnocení rizik v pravidelných intervalech a nikoliv pouze jednou. Hodně zjednodušeně řečeno by se tedy dalo říci, že ISMS upravuje chování, organizační opatření a procesy probíhající ve společnosti. A pokud ISMS odpovídá bezpečnostním požadavkům nadefinovaným v určitém standardu, je možné, aby příslušná certifikační autorita takový soulad certifikovala, pokud takový postup standard umožňuje.[92]

Certifikace kyberbezpečnostních technologií je oproti tomu zaměřená na stavební prvky informačních systémů. Nejčastěji se těmito prvky myslí IT produkty (Common Criteria tímto myslí software, hardware i firmware). Méně často se mezi technologie řadí i služby. To je způsobené především tím, že Common Criteria, která jsou momentálně hlavním mezinárodním certifikačním rámcem pro ICT/kyberbezpečnostní produkty, nejsou vhodná ani žádaná k certifikaci služeb (ani procesů).[93] Když celou problematiku ještě více zjednoduším, certifikace kyberbezpečnostních technologií se bude týkat bezpečnosti věcí, jako je např. router, nebo služeb, jako je např. provoz autentizace klientů, ale nebude dopadat na úpravu vnitřních procesů povinného subjektu, nebude posuzovat, jak se subjekt, který tento

[91] Viz § 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *CODEXIS ACADEMIA* [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018]

[92] Viz BÂRSAN, Mihai. Aspects regarding the implementation of information security standards in organizations. *Revista Română de Biblioteconomie și Știința Informării = Romanian Journal of Library and Information Science* [online]. 2017, roč. 13, č. 1, s. 22–24 [vid. 29. říjen 2018].

[93] Certifikace je velice nákladný proces a zároveň i proces značně zdlouhavý, kdy jedno posouzení může zabrat až 12 měsíců. Zakonzervovat podobu poskytované služby na 12 měsíců je v prostředí, kde se služba musí neustále vyvíjet, aby zůstala schopná reagovat na nové trendy a hrozby, nemyslitelné. Takový styl certifikace by dokázal konstatovat pouze to, že před rokem byla tato služba bezpečná. Pro budoucí možnost certifikace služeb je příslibem nový model certifikace kyberbezpečnostních technologií v EU, ale o tom bude podrobněji pojednáno v dalších kapitolách. Dále viz KALUVURI; BEZZI; ROUDIER, op. cit., s. 1.

router vlastní, stará o bezpečnost informací obecně. To je doména certifikace ISMS. Je tak patrné, že oba zmíněné certifikační systémy nemají mnoho společného, přestože mohou dobře pracovat vedle sebe, a porovnávat je je účelné jenom kvůli Aktu.

Po provedeném srovnání se vrátím k obecnému pojednání, co vlastně certifikace kyberbezpečnostních technologií představuje. Technologie, o jejíž certifikaci výrobce usiluje, musí podstoupit sérii různě náročných testů, které prověří, jakým kyberbezpečnostním hrozbám je schopna tato technologie čelit.[94] To, jak náročné testy budou, závisí na tom, na jakou bezpečnostní úroveň chce investor technologii certifikovat. Pokud zůstane při testování i jen jediný bezpečnostní požadavek dané úrovně nenaplněn, technologie certifikát nezíská. Problematickým se může stát testovací prostředí. Není představitelné, že by bylo možné otestovat určitou technologii v nějakém *„univerzálním“* všeobjímajícím prostředí, které by obsahovalo všechny typy hrozeb. Proto si investor nebo v některých případech i spotřebitel musí/může nadefinovat, v jakém prostředí (jaký typ uživatelů bude technologii užívat, jaké fyzické podmínky budou v okolním světě, jaké hrozby jsou pro technologii relevantní, k čemu bude technologie využívána atd.) má být technologie testována. Pro takové prostředí pak bude vydán certifikát.

Pokud uživatel překročí poučení výrobce o specifickém prostředí užívání a užije technologii v rozporu s certifikátem, nedojde případnou škodou z bezpečnostní vady technologie k porušení certifikační záruky za bezpečný výkon technologie, neboť ta panuje toliko nad určitým prostředím. Zároveň nemusí dojít ani k uplatnění odpovědnosti výrobce. Investor totiž oficiálně proklamoval a informoval uživatele o určité úrovni zabezpečení, kterou uživatel navzdory tomu překročil a následek tak je zodpovědností uživatele.

[94] Některé hodnotící systémy (zvláště u testů na vyšší bezpečnostní úrovně) posuzují i výrobce/vývojáře – např. kde vyrábějí, zabezpečení výrobního procesu, ad.

3.2 AKTUÁLNÍ ÚPRAVA CERTIFIKACE V KYBERNETICKÉ BEZPEČNOSTI

3.2.1 STAV V ČESKÉ REPUBLICE

V České republice ke dni 12. 10. 2019 neexistuje žádná obecná vnitrostátní právní úprava certifikace kyberbezpečnostních technologií. Nezmiňuje se o ní ani zákon o kybernetické bezpečnosti, ani žádná z vyhlášek o kybernetické bezpečnosti. Tato absence oficiální compliance procedury způsobuje povinným subjektům značnou právní nejistotu ohledně zvoleného řešení, které požaduje český zákon o kybernetické bezpečnosti, a řadu dalších negativních důsledků, které byly již rozebrány v druhé kapitole.[95] Jedná se o příklad jednoho z největších problémů, se kterými se certifikace potýká – v mnoha odvětvích vůbec neexistuje. Přesto však na českém trhu existuje poptávka po certifikační proceduře, primárně mezi veřejnoprávními korporacemi a velkými soukromoprávními subjekty, které se dostanou pod dosah zákona o kybernetické bezpečnosti.

Polčák tento zarážející stav vysvětluje takto:

„Zavedení státní certifikace by 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 služeb státu. 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 zkušenostech připomenout, že nemá smysl uvádět v účinnost právní úpravu, na jejíž implementaci není státní exekutiva náležitě připravena).“[96]

Čistá varianta státní certifikační procedury tak podle něj není v momentálním rozložení trhu reálná. Jedinou variantou přímého zapojení státního aparátu je pak možnost státní akreditace nezávislého subjektu

[95] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 76.

[96] Viz tamtéž, s. 79-80.

(v podobě profesního či oborového sdružení, komerčního subjektu nebo i akademické instituce, případně kombinace všeho). Ten by k tomu, aby mohl sloužit jako certifikační autorita, musel samozřejmě vládnout požadovanou personální i technologickou kapacitou. Vzájemná spolupráce zájmových sdružení, působících v oblasti kybernetické bezpečnosti, je v tomto ohledu pozitivní kombinací transparentnosti, profesní specializace a společných podnikatelských zájmů.[97]

Je sice pravdou, že situace na českém trhu momentálně není k zavedení možnosti státem uznávané certifikace nejpříznivější,[98] ale Česká republika má již zkušenost s procedurou, která je obecné certifikaci kyberbezpečnostních technologií velice podobná, a to v oboru ochrany utajovaných informací. Jak Polčák dále uvádí, ani v této oblasti se kapacity pro provoz takového systému původně nevyskytovaly, ale byly postupně vytvořeny. Překvapením byla i příznivá situace ohledně korupčních tlaků, které zde nezaznamenaly výraznější úspěch (a to i přesto, že vzhledem k povaze této agendy není možné dosáhnout tak vysoké míry transparentnosti, jak by tomu bylo v případě kyberbezpečnostních technologií).[99]

Certifikace ISMS se v českém právním prostředí nachází v daleko lepším postavení, neboť s ní v podobě komerční certifikace podle standardu ISO/IEC 27001 právo přímo počítá a je státem uznána. Stará vyhláška o kybernetické bezpečnosti ji v § 29 stanovila jako podmínku presumpce naplnění zákonných požadavků (viz níže). Nová vyhláška již celá vychází ze stejných principů a pravidel jako standardy z rodiny ISO 27K, a přestože výslovná úprava vztahu certifikátu a povinností podle vyhlášky z textu předpisu zmizela, v důvodové zprávě k vyhlášce se o tomto vztahu píše v části vztahující se k § 3 následující:

---

[97] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 79-80.

[98] Je ovšem nutné jedním dechem zdůraznit, že se situace od roku 2016 přece jenom zlepšila a dle konzultačního emailu s doc. JUDr. Radimem Polčákem, Ph.D. z října 2019 se nyní v České republice vyskytují kapacity, soustředěné zejména na univerzitách, které provádějí certifikaci pro zahraniční certifikační autority.

[99] Viz tamtéž.

„Zmíněná norma (ISO/IEC 27001 – pozn. autora) po jejích uživatelích vyžaduje mimo jiné respektování zákonných závazků, u zákonem regulovaných subjektů, tedy i povinností vyplývajících ze zákona o kybernetické bezpečnosti. Z toho důvodu není potřeba zvyšovat administrativní zátěž, kterou by především znamenalo dodržování jak požadavků normy, tak požadavků na bezpečnostní opatření, daných touto vyhláškou. Je tedy možné respektovat certifikaci ISMS dle ISO/IEC 27001 jako adekvátní k dodržování bezpečnostních opatření daných touto vyhláškou. Výkon kontroly v oblasti kybernetické bezpečnosti není tímto ustanovením nijak dotčen, přičemž kontrola bude provedena pouze v rozsahu informačního a komunikačního systému.“[100]

Zmíněný standard je produktem práce Mezinárodní společnosti pro standardizaci, které je Česká republika plnoprávným členem. Na poli této organizace je reprezentována Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví (detailní pojednání o členství v ISO a mezinárodní organizaci samotné je v páté kapitole).[101] Dále je pak Česká republika tzv. konzumujícím členem dohody CCRA (Common Criteria Recognition Arrangement – jedná se o dohodu o vzájemném uznávání certifikátů systému Common Criteria). To znamená, že není oprávněná vytvářet nová Common Criteria schémata, ani vydávat certifikáty (takovou pravomoc má toliko 17 států), ale certifikáty, které jsou autorizačními členy vydávány, uznává. Je tedy možné mluvit o určitém nepřímém dosahu certifikace kyberbezpečnostních technologií na území České republiky.[102]

---

[100] Viz Důvodová zpráva k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

[101] Viz Členství v mezinárodních organizacích. *ÚNMZ* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.unmz.cz/urad/clenstvi-v-mezinarodnich-organizacich ; UNMZ. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/member/00/21/2133.html.

[102] Viz Common Criteria. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/ ; Members of the CCRA: *New CC Portal* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.commoncriteriaportal.org/ccra/members/

Důvodem k tomu, proč existuje tak málo autorizačních států, je vzájemná mezinárodně-bezpečnostní nedůvěra. Aby na poli kybernetické bezpečnosti vznikla spolupráce založená na vzájemném uznávání certifikátů, musí mezi těmito státy panovat skutečně vysoká míra důvěry ohledně svědomitosti, zodpovědnosti a dostatečné pokročilosti bezpečnostních testů a procedur prováděných dalšími členy. Česká republika, i kdyby měla politický potenciál na to, aby se stala autorizačním členem, nemá na tuto funkci zdaleka potřebné kapacity ani dostatečně vybavené laboratoře.

Česká republika není členem užší evropské spolupráce na poli Common Criteria, která je představována dohodou SOG-IS MRA (z angl. „Senior Officials Group Information Systems Security – Mutual Recognition Agreement“, o této dohodě viz níže).[103]

3.2.2 POTENCIÁLNÍ MÍSTO CERTIFIKACE KYBERBEZPEČNOSTNÍCH TECHNOLOGIÍ V ČESKÉM SYSTÉMU KYBERNETICKÉ BEZPEČNOSTI

Zákon o kybernetické bezpečnosti pracuje zejména s bezpečnostními opatřeními. Ta jsou definována jako „*souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.*“[104] Takováto opatření musí povinné subjekty provádět v rozsahu, který je nezbytný pro zajištění bezpečnosti informačního systému kritické informační infrastruktury. Dále zákon pracuje s institutem opatření, která definuje jako „*úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu*“.[105] Ta se dělí na varování, reaktivní opatření a ochranné opatření. Poslední zmíněná se vydávají ve formě

[103] Viz SOG-IS - Home. *SOG-IS* [online]. [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html.

[104] Viz § 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *CODEXIS ACADEMIA* [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

[105] Viz § 11 zákona č. 181/2014 Sb.

opatření obecné povahy a jsou svojí povahou daleko blíže normálnímu správnímu rozhodování než reaktivní opatření, která jsou spíše faktickým zásahem.[106] Pokud by tedy, čistě teoreticky, došlo k zavedení oficiální certifikační procedury kyberbezpečnostních technologií, je pravděpodobné, že by se její pozice pohybovala buď v okruhu bezpečnostních, nebo ochranných opatření,[107] případně pak by mohla fungovat stejně, jako fungovala certifikace podle ISO/IEC 27001 podle staré vyhlášky o kybernetické bezpečnosti. Určujícím je, jestli by certifikace byla vedena jako povinná nebo dobrovolná, případně smíšená.

Certifikace by sama o sobě nemusela být povinná (např. pro výkon určité činnosti nebo provoz kritické informační infrastruktury). Mohla by být formulována jako součást podmínek kvalifikace zadávacího řízení veřejných zakázek, zejména pak těch, které se týkají kritické informační infrastruktury, případně i dalších, bude-li tento požadavek shledán opodstatněným a v souladu se zásadami veřejného investování. V rámci veřejných zakázek si lze držení certifikace (v některých případech) představit rovněž jakožto jedno z kritérií hodnocení. Subjekty k ní také mohou přistoupit např. z tržních důvodů, kdy jim daná certifikace může poskytnout výhodu (zejména z hlediska zvýšení důvěryhodnosti v daný produkt) oproti ostatním konkurentům. Certifikace navíc může být pozitivním znamením pro potenciální investory daného subjektu. Získání certifikace totiž nejen ukazuje splnění určitých kvalitativních požadavků, ale i motivaci (a dispozici s potřebnými prostředky) projít časově a finančně nezanedbatelným procesem.[108] Podmínku certifikace by pak mohlo být možné stanovit jen dodavatelům (a jejich subdodavatelům), kteří by se chtěli účastnit soutěže, aniž by povinnost certifikovat dopadla na ostatní. Pokud by certifikace byla povinná bez dalšího, byla by dle mého názoru jedním z bezpečnostních technických opatření. Takovou certifikaci

[106] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 34.

[107] Dá se usuzovat, že užití certifikovaných technologií by bylo možné opatřením v případě potřeby nařídit.

[108] Certifikace může být ve vztahu k veřejným zakázkám realizována i vícero způsoby – např. jako podmínka akceptace (výsledné řešení získá certifikát). Certifikáty mohou být zároveň součástí i souvisejících povinností, jako např. kodexů podle nařízení GDPR.

by musel mít každý povinný subjekt, jinak by nemohl regulovanou činnost provozovat.

V případě, který jsem nazval jako „*smíšená závaznost*“, jsem měl na mysli obecnou dobrovolnost certifikace, kdy jenom v určitých případech by regulátor (pravděpodobně NÚKIB, případně Komise) stanovil povinnost pro určité subjekty si certifikaci obstarat, případně ji vyžadovat po svých dodavatelích. Tak by byla certifikace svým způsobem ochranným opatřením.

Jako fakultativní může certifikace fungovat buď jako výše zmíněná tržní výhoda, informace pro investory nebo i jen jako informace pro spotřebitele a důkaz, že subjekt naplnil, co mu právo ukládalo, a dosáhl tak stavu compliance. Míra hodnověrnosti certifikátu závisí na povaze certifikačního tělesa, ale pokud budou tato tělesa akreditována státem, neměl by problém s důvěrou nastat. V případě, že by povinný subjekt držel určitý certifikát, vycházelo by se při státní kontrole pravděpodobně z vyvratitelné domněnky, že povinný subjekt je v souladu s právem (bylo by tedy zapotřebí najít důkaz, že není).[109] To je pro povinný subjekt o hodně příznivější situace. Pokud by tedy certifikace byla zavedena jako dobrovolná, jasnou analogií by bylo fungování certifikace dle ISO 27001 ve staré vyhlášce o kybernetické bezpečnosti. Podle ustanovení § 29 této vyhlášky bylo na subjekt, jehož bezpečnostní řešení bylo certifikováno akreditovaným certifikačním orgánem a který vedl v tomto paragrafu specifikovanou dokumentaci, nahlíženo jako na subjekt *„splňující požadavky na zavedení bezpečnostních opatření podle zákona a této vyhlášky*“.[110]

3.2.3 STAV V EVROPSKÉ UNII

V Evropské unii ke dni 12. 10. 2019 neexistuje žádná plně účinná právní úprava unifikující nebo alespoň harmonizující materii obecné certifikace v oblasti kybernetické bezpečnosti (jak bylo zmíněno, část Aktu

[109] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 80.

[110] Viz § 2 9 vyhlášky 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). In: *CODEXIS ACADEMIA* [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

o kybernetické bezpečnosti věnující se jednotnému certifikačnímu rámci je stále ještě z velké části neúčinná a běží implementační lhůta, která končí 27. června 2021). Vyskytují se sice úpravy certifikací pro účely nařízení eIDAS (což je svým uspořádáním velice podobný a již fungující systém), téměř nepoužívaná úprava certifikací pro účely nařízení GDPR, ale v oblasti kybernetické bezpečnosti se vyskytuje pouze směrnice NIS a ta certifikaci neupravuje. Přitom se stav kybernetické bezpečnosti v rámci EU zhoršuje.[111]

Celý stav je ještě umocněn skutečností, že vnitřní kyberbezpečnostní trh Unie byl v absenci jednotného certifikačního systému plně roztříštěn. Je rozpadlý na jednotlivá národní a sektorová řešení bez možnosti vzájemného uznávání certifikátů mezi členskými státy, různé interní standardy, a nejvíce připomíná jakousi širší spolupráci dohoda SOG-IS MRA. Počet různých druhů certifikátů pohybujících se na vnitřním trhu je tím pádem nesmírný.[112] Takováto roztříštěnost trhu způsobuje až absurdní situaci, kdy výrobce, který chce svůj produkt prodávat ve Francii, Německu a Nizozemí, musí tento svůj produkt nechat certifikovat podle „*Certification Cécuritaire de Premier Niveau*" ve Francii, „*Baseline Product Assessment*" v Nizozemí a podle speciálně upraveného modelu Common Criteria v Německu (tzv. „*Německý certifikát*"). Je tak nucen podstoupit tři zdlouhavé a nákladné procedury, což před mnoho podnikatelů staví překážku, kterou nejsou ochotni/schopni překonat.[113]

Panující stav je opakem myšlenky jednotného digitálního trhu, o který Evropská unie usiluje. Již dříve zmíněná směrnice NIS nebo nařízení eIDAS byly významné kroky, které Unii posunuly směrem k unifikaci digitálního

[111] Ekonomický dopad kyber-incidentů se v roce 2016 pohyboval celosvětově okolo jedné miliardy dolarů. Podle Evropské komise se v roce 2016 uskutečnilo více než 4 000 ransomware-útoků denně, což je nárůst o víc jak 300 % oproti roku 2015. Viz NEGREIRO ACHIAGA, Maria Del Mar. *EU Legislation in Progress - Briefing: ENISA and a new cybersecurity act (stav ke dni 16. 1. 2018)* [online]. B.m.: European Parliament Research Service. [vid. 11. říjen 2018].

[112] Viz DROGKARIS, op. cit. ; Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu aktu o kybernetické bezpečnosti [online]. B.m.: Evropská komise. 2017 [vid. 12. červenec 2018].

[113] Viz NEGREIRO ACHIAGA, op. cit.

trhu, ale jak je ze stávající situace patrné, bez sjednocení kyberbezpečnostní certifikace nebude pokrok možný.[114] Členské státy nejsou bez dalšího schopny nebo ochotny hlubší kooperace, která by vedla ke zlepšení kyberbezpečnostní situace v rámci EU, což způsobuje částečnou neúčinnost výhod vnitřního trhu.[115]

Spolupráce v Evropské unii na poli certifikace kyberbezpečnostních technologií je alespoň částečně upravena dohodou SOG-IS, kterou mezi sebou uzavřely některé členské státy.[116] Toto seskupení bylo vytvořeno na základě rozhodnutí Rady ze dne 31. 3. 1992 č. 92/242/EEC, o bezpečnosti informačních systémů, a doporučení Rady ze dne 7. 4. 1995 č. 1995/144/EC, o obecných kritériích pro posuzování bezpečnosti informačních systémů. Jedná se o sdružení 14 členských států (zejména pokročilé státy s vlastními testovacími laboratořemi) a Norska. Toto sdružení mezi sebou úzce spolupracuje na vytváření nových CC schémat, koordinuje své standardizační a certifikační aktivity a členové vzájemně uznávají CC certifikáty až do bezpečnostní úrovně EAL 4.[117] Česká republika není členem dohody SOG-IS a ani nemá zájem se do budoucna jejím členem stát.[118]

Popsaný stav dlouho beze změny přetrvával nejen v České republice, ale především v Unii navzdory tomu, že poptávka po certifikaci byla a je značná,[119] a to zejména ze strany povinných subjektů. Pro ty, na které dopadly compliance povinnosti vycházející z regulace kybernetické

[114] Srovnej s JEŽOVÁ, Daniela. EU Digital Single Market - Are we there yet? *Ad Alta: Journal of Interdisciplinary Research* [online]. 2017, roč. 7, č. 2, s. 1–3.

[115] Viz Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu aktu o kybernetické bezpečnosti [online]. B.m.: Evropská komise. 2017 [vid. 12. červenec 2018].

[116] Viz SOG-IS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, verze 3.0 [online]. 2010 [vid. 27. říjen 2018].

[117] Viz MITRAKAS, Andreas. The emerging EU framework on cybersecurity certification. *Datenschutz und Datensicherheit* [online]. 2018, roč. 42, č. 7, s. 3–5 [vid. 11. září 2018].

[118] Získáno na základě konzultací s odborníky z NÚKIB. Dále viz SOG-IS - Home. *SOG-IS* [online]. [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html.

[119] To je patrné hlavně u vyspělejších kyberbezpečnostních trhů s velkým počtem povinných subjektů. Velice žádaný je např. Německý certifikát, stejně tak i některá další národní schémata, případně pak i certifikace podle CC v režimu schémat vytvořených spoluprací SOG-IS. Pro podrobnější informace, viz kapitoly 5 a 6.

bezpečnosti,[120] totiž představuje certifikace jedinou možnost spolehlivého řešení compliance. Větší zájem panuje samozřejmě ve státech, kde je dodržení určité compliance povinnosti navázané na možnost podnikání v určité oblasti. Tak je tomu např. ve Francii, kde je naplnění daného bezpečnostního standardu nutným předpokladem k obchodování se státním sektorem (v oblasti zařízení připojitelných na internet).[121] Pro veřejnoprávní subjekty má certifikát význam i kvůli tomu, že bezpečnostní opatření financují z nejrůznějších projektů (dotací). Jakmile drží certifikát, mohou fungovat bez obavy z toho, že by se později zjistilo nedodržení standardu (který většinou funguje jako závazná podmínka pro udělení dotace), což by dále vedlo k povinnosti dotaci vrátit. Pro členy statutárních orgánů jak soukromoprávních, tak veřejnoprávních subjektů mají certifikáty ještě jeden velice lákavý účinek – mohou posloužit jako štít před osobní odpovědností těchto členů.[122]

4. PERSPEKTIVNÍ ÚPRAVA V EU

4.1 CESTA K NOVÉMU NAŘÍZENÍ

Problematický stav popsaný v závěru minulé kapitoly však nebyl Evropskou unií úplně ignorován. Už v roce 2014 se intenzivně pracovalo na tom, jak tuto situaci změnit. Dne 6. 10. 2014 zorganizovala ENISA (Agentura Evropské unie pro bezpečnosti sítí a informací) společně s Evropskou komisí workshop na téma ICT certifikace a budoucnosti SOG-IS. Tohoto workshopu se zúčastnilo přibližně 60 expertů z různých oblastí představujících různé zájmové skupiny (zúčastnili se reprezentanti veřejných i soukromých certifikačních a standardizačních orgánů, výrobců, spotřebitelů, průmyslových asociací, testovacích laboratoří atd.). Účelem

[120] Např. v Nizozemí musí být povinné subjekty v souladu se standardem definovaným v *„Baseline Informatiebeveiliging Rijksdienst“*.

[121] Viz CSPN: What U.S. companies need to know about the security certification process [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process.

[122] Tyto informace byly získány z konzultací a konzultačních emailů s doc. JUDr. Radimem Polčákem, Ph.D.

setkání bylo uvést zúčastněné strany do myšlenky společného certifikačního rámce pro celou Evropskou unii, zjistit jejich názory a probrat s odborníky z oblasti kybernetické bezpečnosti výzvy, kterým bude muset takový rámec čelit. Zpočátku se uvažovalo o rozšíření dosahu dohody SOG-IS na celou Unii, ale tento záměr si nakonec nezískal dostatečnou podporu, a to hlavně kvůli nedostatkům, kterými je systém Common Criteria postižen.[123,124]

Zúčastněné strany (český překlad pro „*Stakeholders*“) vyzdvihly na tomto setkání potřebu společného evropského postupu, potřebu vzájemného uznávání certifikátů a odstranění roztříštěnosti způsobené národními přístupy, která nesmyslně zvyšuje podnikatelské náklady a mnohé z malých a středních podniků úplně vyřazuje z možnosti nechat si svůj produkt certifikovat. Zároveň není takový postup ani moc výhodný pro velké podniky, což ve svém důsledku znamená, že evropský ICT a kyberbezpečnostní průmysl ztrácí (zejména) na USA. Vzhledem k tomu, že mnohé ze zúčastněných stran jsou mezinárodně působící korporace, bylo zdůrazňováno, že nová evropská certifikace by neměla jít proti uznávaným mezinárodním standardům třetích zemí jako např. ISO/IEC a Common Criteria. Řešil se i vztah mezi SOG-IS a touto novou úpravou. Byl vyzdvižen přínos skupiny SOG-IS a prosazována pozitiva adopce jeho standardů a profilů.[125] Kromě tohoto workshopu byly dále svolány i velké veřejné konzultace, a to na konci roku 2015 a začátku roku 2016. Na nich byly provedeny průzkumy mínění zainteresovaných subjektů. Z těchto výzkumů vyšlo najevo, že optimálním řešením by byla obecná a dobrovolná verze

[123] Bez debat se jedná o dominantní certifikační systém na poli kybernetické bezpečnosti ICT produktů, ale má i mezery, u kterých již není pravděpodobné, že by došlo k jejich odstranění. Zvláště byl vyzdvižen naprosto nedostatečně nastavený režim pro certifikaci velkých systémových řešení a služeb, kdy Common Criteria jednoduše neumožňují testovat službu jako kontinuální proces zasazený do určitého prostředí různě interagující se svým okolím. Místo toho se soustředí na certifikaci jednotlivých jeho částí a výsledné chování služby nikdo nekontroluje.

[124] Viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014 [vid. 24. srpen 2018].

[125] Viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes *of the workshop* [online]. 6. říjen 2014 [vid. 24. srpen 2018].

certifikace, spravovaná agenturou ENISA, jíž by byl stanoven permanentní mandát a rozšířeny pravomoci.[126]

Na základě těchto výstupů tedy Komise ve spolupráci s ENISA začala pracovat na posílení kybernetické bezpečnosti a odolnosti v Unii. Se zhoršující se kyberbezpečnostní situací stoupala i priorita vyřešení společného postupu v této otázce. To se odrazilo např. v rezoluci Evropského parlamentu ze dne 3. 10. 2017, ve které byly členské státy vyzvány k boji proti kyber-zločinu a k urychlení budování kyberbezpečnostní infrastruktury, nebo na společném sdělení Evropskému parlamentu a Radě – „*Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU*“, které předložila Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku necelý měsíc předtím.[127]

Jednou z nejdůležitějších částí sdělení, které vydal téhož dne (13. 9. 2017) předseda Komise Jean-Claude Juncker ohledně zvyšování schopností Unie reagovat na kyber-útoky, bylo, že po zohlednění závěrů uvedených mimo jiné ve sdělení Komise o přezkumu naplňování strategie pro jednotný digitální trh,[128] byl Komisí toho samého dne předložen návrh nařízení na posílení mandátu a pravomocí agentury ENISA a o zavedení certifikace kybernetické bezpečnosti informačních a komunikačních technologií (anglicky „*The Cybersecurity Act*“) jako součást tzv.

[126] Viz NEGREIRO ACHIAGA, op. cit..

[127] Viz VYSOKÁ PŘEDSTAVITELKA UNIE PRO ZAHRANIČNÍ VĚCI A BEZPEČNOSTNÍ POLITIKU. *Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU* [online]. 2017 [vid. 11. říjen 2018].

[128] Viz Sdělení Komise Evropskému parlamentu, Radě, EHS-výboru a výboru regionů ze dne 10. 5. 2017 o přezkumu v polovině období provádění strategie pro jednotný digitální trh [online]. B.m.: Evropská komise. 10. květen 2017 [vid. 11. říjen 2018] .

Kyberbalíčku[129] a stává se jednou z priorit k naplnění jednotného digitálního trhu.[130]

4.2 AKT O KYBERNETICKÉ BEZPEČNOSTI

Náročná legislativní pouť tohoto revolučního návrhu, která započala dne 13. 9. 2017, byla dokončena dne 17. dubna 2019, přičemž část úpravy certifikačního rámce se použije až od 28. června 2021. Výsledné podoby Aktu se de facto podařilo dosáhnout již 10. prosince 2018, kdy podle tiskové zprávy Evropské komise byla po dlouhých a náročných vyjednáváních ukončena fáze trialogu, kdy Evropský parlament, Rada a Evropská komise konečně nalezly kompromis ohledně podoby Aktu. Od té doby již došlo toliko k oficiálnímu překladu[131] a podoba Aktu se téměř nezměnila, což utlo naděje, že dojde k napravení některých vad Aktu, které jsou zmíněné níže.

Akt má dvě části – 1) rozšíření pravomocí a mandátu ENISA, přičemž tato část není předmětem tohoto článku, 2) zavedení jednotného evropského certifikačního systému. Je vhodné zdůraznit, že Akt samotný nezavádí jednotlivá certifikační schémata, to by bylo legislativně i pragmaticky neúnosné (představa, že by se kvůli každé změně certifikačního schématu muselo měnit nařízení samo, je absurdní). Místo

[129] Kyberbalíček je soubor opatření (zvlášť Junckerova komise byla těmito balíčky známá), které mají vést k posílení bezpečnosti v kyberprostoru. Mimo jiné obsahuje několik opatření ke zlepšení informovanosti o bezpečném chování na internetu či opatření ke zlepšení kyber-hygieny uživatelů. Ostatně i v Aktu o kybernetické bezpečnosti je několikrát zmíněna nově vzniklá povinnost Agentury ENISA k péči o kyber-hygienu a šíření informací o kybernetické bezpečnosti. De facto dostala ENISA za úkol naučit uživatele v Unii, jak se chovat na internetu bezpečněji.

[130] Viz State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks [online]. B.m.: European Comission – Press release. 19. září 2017 [vid. 11. říjen 2018].

[131] Oficiální překlad do českého jazyka s sebou přinesl několik poněkud nešťastných řešení této problematiky. Příkladem budiž překlad anglického „*certification scheme*" do českého „*certifikační systém*". Tato volba je dle mého názoru nejen zbytečná, ale zároveň i matoucí. Certifikační systém je totiž např. Common Criteria, kdežto schéma (jak by se anglické „scheme" dalo jednoduše přeložit) označuje dílčí set kritérií, podmínek a požadavků vztahujících se k danému produktu, službě nebo procesu. Tento článek primárně vychází z anglické varianty a kdykoliv, kdy budu pojednávat o schématu, v řeči české verze Aktu mluvím o certifikačním systému.

toho vytváří rámec pro přijímání evropských certifikačních schémat, a to nejen pro ICT produkty, ale zároveň i pro služby, čímž by měl předčít systém Common Criteria, a pro procesy, čímž se stává vskutku revolučním, neboť dosud žádný mezinárodně přijímaný certifikační rámec nebyl tak ambiciózní, aby integroval všechny tři aspekty dohromady.[132] Svou materií tak může částečně zasáhnout i do oblasti upravené standardy ISO/IEC 27001 ad. Výstupem certifikačních procesů prováděných dle schválených schémat budou v celé Unii univerzálně uznávané certifikáty.[133]

4.2.1 PRÁVNÍ ZÁKLAD NAŘÍZENÍ

Za právní základ Aktu byl zvolen čl. 114 Smlouvy o fungování Evropské unie (dále jen jako „SFEU"), tedy „*oprávnění Evropského parlamentu a Rady přijímat řádným legislativním postupem po konzultaci s Hospodářským a sociálním výborem opatření ke sbližování ustanovení právních a správních předpisů členských států, jejichž účelem je vytvoření a fungování vnitřního trhu a naplňování tak cílů uvedených v článku 26 (který sám stanovuje cíl vytvoření a zajištění fungování vnitřního trhu – poznámka autora)*". Zdůrazněno bylo právě zajištění fungování vnitřního trhu, což vzhledem k tomu, co jsem psal na konci minulé kapitoly, je pochopitelné. Mitrakas k tomuto bodu dodává, že vhodnost užití tohoto ustanovení SFEU byla již v minulosti potvrzena Soudním dvorem Evropské unie v případu C-216/04 (autor dotyčného článku zde pravděpodobně myslel rozhodnutí ve věci C-217/04 Spojené království proti Evropskému parlamentu a Radě) a v Nařízení Parlamentu a Rady č. 526/2013 ze dne 21. 5. 2013 (dosavadní nařízení regulující působení ENISA).[134] Uvádí dále, že „*potenciální fragmentace a omezení možnosti Evropské unie vytvořit vnitřní trh pro kyberbezpečnostní produkty*

[132] Zmíněné tři „*oblasti certifikace*" představují velice rozdílné certifikační systémy, podmiňující si užívání jiných metodik a certifikačních procesů. Zároveň jsou rozdílné i z pohledu vyžadovaných kapacit (technických i personálních) pro provádění certifikace. Jak již bylo zmíněno, certifikační systém Common Criteria, který představuje jeden z nejvíce využívaných certifikačních systémů pro oblast kyberbezpečnostních technologií, je postaven toliko na certifikaci produktů. Měl umožňovat též certifikaci služeb, ale tento cíl se až dosud nepodařilo naplnit.

[133] Viz odstavec 10 článku 56 Aktu o kybernetické bezpečnosti.

[134] Viz MITRAKAS, op. cit., s. 4.

a služby je dostatečným důvodem pro spuštění legislativního procesu v souladu se subsidiaritou.“[135] V odůvodnění první verze návrhu nařízení je toto ještě dále rozvíjeno navázáním na cíle stanovené směrnicí NIS (směrnice o bezpečnosti sítí a informací, jejímž právním základem je též článek 114 SFEU).[136] Vzhledem k tomu, že cílem Aktu je odstranit roztříštěnost evropského trhu a že individuální opatření členských států se neukazují pro posílení společné kybernetické odolnosti Unie jako dostatečná, souhlasím, že opatření ve formě nařízení je vhodné, pochopitelné a potřebné.

Ovšem samotná volba právního základu nařízení může být trochu sporná, což cítili i právníci z Council Legal Service.[137] Proti vystavění Aktu na základech článku 114 SFEU však po celou dobu nikdo ze zúčastněných stran ani států nepodal žádnou zásadní námitku. Nařízení je výsledkem spojení zájmů jednotného a konkurenceschopného trhu, který skutečně je plně v pravomoci Unie, s kybernetickou bezpečností a obecně bezpečnostní politikou, která je stále pod většinovou pravomocí členských států. Dle mého osobního názoru je přinejmenším sporné, jaký efekt je v Aktu důležitější a v praxi se silněji projeví, jestli unifikace roztříštěného trhu a zvýhodnění situace spotřebitelů, nebo posílení kybernetické bezpečnosti a odolnosti Unie. Zvláště když přihlédnu ke skutečnosti, že u systému Common Criteria byl dopad na obyčejné spotřebitele minimální a certifikátů bylo využíváno primárně při interakci se státním sektorem (dodavatelé zabezpečených systémů, provozovatelé kritické informační infrastruktury).[138] Na druhou stranu je nepopiratelným faktem, že nařízení nezasahuje do samotných pravomocí bezpečnostních složek. Je tak pochopitelné zaštítění článkem 114 SFEU. Jednotného certifikačního systému jednoduše bylo na území Unie potřeba a jiná řešení bezpečnosti Unie nebyla dostatečná. A vzhledem k absenci námitek, i přestože je zde pro ně místo, je patrné, že i členské státy si tuto potřebu fakticky

[135] Viz tamtéž.

[136] Toto se zachovalo až do výsledné verze návrhu, přestože vliv NIS na spuštění jednotného certifikačního rámce byl podstatně snížen.

[137] Council Legal Service je právně-poradenský orgán spadající pod Sekretariát Komise.

[138] Viz HEARN, J. Does the common criteria paradigm have a future? *IEEE Security & Privacy Magazine* [online]. 2004, roč. 2, č. 1, s. 1 [vid. 18. říjen 2018].

uvědomovaly. V tomto ohledu jednoduše převážily politické důvody nad čistě formalisticky – právními.

4.2.2 PŘEDSTAVENÍ CERTIFIKAČNÍHO RÁMCE

Vzhledem k tomu, že podrobný rozbor certifikační procedury podle Aktu bude předmětem sedmé kapitoly, zde bude nařízení představeno jako celek.

Akt vytváří páteřní úpravu pro tvorbu dílčích certifikačních schémat – modelových podmínek, podle nichž bude následně certifikovaný produkt (nebo služba či proces) testován. Jedná se o organizační, procesní, technologickou a právní úpravu celého certifikačního procesu. Smyslem nařízení je kromě zvýšení kybernetické bezpečnosti i povzbuzení evropského trhu s kyberbezpečnostními produkty, procesy a službami k vytvoření celosvětově konkurenceschopných subjektů. Akt je naprosto revoluční v unifikaci certifikace produktů, služeb a procesů pod jeden obecný rámec a v případě, že se tento systém osvědčí, mohl by být následně přejímán i státy mimo EU (dle mého názoru je velice pravděpodobné, že prvním nečlenským státem přistoupivším k Aktu bude Norsko, které se již nyní podílí na spolupráci SOG-IS a velice pravděpodobně s ním bude sjednána speciální smlouva o přístupu k certifikačnímu rámci brzo po vstoupení celého Aktu v účinnost).

Unie se přístupem ke kybernetické bezpečnosti liší od toho v USA, mimo jiné také proto, že Unie je v oblasti kybernetické bezpečnosti stále nováčkem. Rychle se rozvíjejícím, ale stále nováčkem (zvláště je to poznat na vyspělosti trhů). Spojené státy americké vyzkoušely několik různých přístupů k regulaci kybernetické bezpečnosti, ale nakonec se rozhodly do standardizační a certifikační regulace tolik nezasahovat (přestože v oblasti pravomocí zpravodajských služeb jsou zásahy stále vcelku citelné) a přenechat ji průmyslu, trhu a soukromým subjektům samotným. Prostředí Států je tak na jednu stranu daleko uvolněnější a prosycené lobbingem, ale na stranu druhou se velice těžko reguluje, když je zapotřebí bezpečnostních opatření. Unie se oproti tomu vydala cestou veřejnoprávní regulace (nařízení je první veřejnoprávní úpravou mezinárodně uznávané

kyberbezpečnostní certifikace) celé materie.[139] Dle mého názoru je prostředí v Unii mimo jiné i kvůli nedostatku zkušeností s certifikací vhodnější právě k rigorózní úpravě. Nedostatek zkušeností by podle mého názoru způsoboval v uvolněném prostředí chaos, nejistotu nebo přebírání nápadů, a tím pádem závislost na jiných, vyspělejších trzích.

Produkty, procesy a služby se podle Aktu budou testovat na naplnění bezpečnostních požadavků, které na ně ukládají jednotlivá certifikační schémata. Náročnost testování se odvíjí od požadované bezpečnostní úrovně produktu, kterou si vybírá investor (schéma samotné může uvést jednu až tři možné úrovně, podrobněji v sedmé kapitole). Akt respektuje a zdůrazňuje skutečnost, že certifikát sám o sobě nemůže garantovat absolutní bezpečnost testovaného produktu, pouze přísnost testů a relativní bezpečnostní úroveň záruky.[140]

Testování v rámci certifikace budou provádět testovací laboratoře. To je subjekt, který vládne dostatečnými kapacitami na to, aby mohl posoudit zabezpečení jednotlivých produktů. Testovací laboratoře mohou být buď samostatné a s certifikační autoritou (subjekt, který posuzuje shodu), pouze spolupracují na základě smlouvy, nebo mohou být přímo její součástí.[141] Vybudování takové testovací laboratoře je finančně nesmírně náročná záležitost. K tomu, aby byli investoři k takovému vytvoření přilákáni, musí trh nabízet dostatečnou možnost návratnosti investice. Certifikační proces totiž samozřejmě nebude zadarmo a testovacím laboratořím se bude za provedení testů platit. Investoři tedy musí očekávat, že zájem o certifikace bude dostatečně velký, aby se jim vybudování testovací laboratoře komerčně vyplatilo. Celé toto schéma však bylo v průběhu vyjednávání o Aktu ohroženo. A dle mého názoru, mohl mít dále popsaný pozměňovací návrh katastrofální následky pro celé uplatnění certifikace v praxi.

---

[139] Viz BELLANTUONO, Giuseppe. Comparing Smart Grid Policies in the USA and EU. *Law, Innovation and Technology* [online]. 2014, roč. 6, č. 2, s. 234–241 [vid. 22. červenec 2018]; KOVÁCS, László. Cyber Security Policy and Strategy in the European Union and NATO. *Revista Academiei Fortelor Terestre* [online]. 2018, roč. 23, č. 1, s. 10–13 [vid. 22. červenec 2018].

[140] Viz body 77–86 odůvodnění Aktu o kybernetické bezpečnosti.

[141] Viz článek 60 a příloha k Aktu o kybernetické bezpečnosti.

Pozměňovací návrh, jednoduše řečeno, navrhoval, aby skutečná certifikace, tedy certifikační proces v testovacích laboratořích pod taktovkou subjektu pro posuzování shody, probíhala jenom v případech, že by si výrobce nechával svůj produkt certifikovat na nejvyšší (a nejpřísnější) bezpečnostní úroveň. Ve střední a nízké úrovni by byla certifikace nahrazena postupem tzv. vlastního posouzení („*conformance self-assessment*"), kdy si podnikatel sám posoudí naplnění stavu compliance. V takovém případě by samozřejmě nikomu nic neplatil (kromě zvýšených nákladů na posouzení bezpečnostních kritérií, což je proti certifikaci stále podstatně nižší částka). Subjekty pro posuzování shody (také jako „CAB") a testovací laboratoře by tak přišly o všechny zájemce o bezpečnostní posouzení nižší a střední úrovně. Očekává se ovšem, že největší zájem bude právě o tyto dvě úrovně, a tak je v nich také ukryt největší komerční potenciál. CAB a testovací laboratoře by tak byly odkázány na komerční potenciál nejvyšší úrovně, který by je na menších a mladších trzích vůbec neuživil. Přijetí tohoto pozměňovacího návrhu by tak vedlo k faktickému zabránění vytvoření CAB a testovacích laboratoří v některých členských státech.

Ani otázka samotných certifikačních autorit nebyla bezproblémová. Zjednodušeně řečeno, certifikační autorita má být nezávislým subjektem, který byl akreditační autoritou akreditován k provádění certifikačních procesů po splnění podmínek, které jsou stanoveny v příloze k tomuto nařízení.[142] Panovala (a domnívám se, že vcelku oprávněná) obava, že státy nebudou dodržovat podmínky akreditace a na vnitřním trhu tak budou vznikat certifikační autority, které nebudou splňovat podmínky nařízení. Je pak představitelné, že by produkty certifikované těmito autoritami nemusely fakticky mít proklamovanou bezpečnostní úroveň. To by mohlo vést až k tomu, že certifikáty z některých států budou mít jinou reálnou hodnotu než ze států jiných, resp. by některé nemusely být fakticky vůbec akceptované (tržní subjekty by si jednoduše vybíraly certifikáty udělené spolehlivějšími autoritami), přestože by byly automaticky uznatelné podle práva. Aby se tento scénář nenaplnil, bylo do Aktu zařazeno několik

[142] Viz tamtéž.

kontrolních opatření. Kontrolu nad subjekty pro posuzování shody budou vykonávat jak národní autority pro certifikaci kybernetické bezpečnosti, tak i akreditační autority, které v případě nesplňování podmínek mohou akreditaci zase odebrat. Navíc certifikační subjekt by se nezodpovědným výkonem certifikačního testování vystavoval riziku, že v případě vzniku újmy kvůli chybě v produktu, procesu nebo službě mu vznikne odpovědnost za tuto škodu.

Komise zpočátku přenechává členským státům moc rozhodnout, jestli učinit certifikaci podle určitého schématu pro povinné subjekty na jejich území obligatorní. Do Aktu byl ovšem s tímto ústupkem prosazen i mechanismus, který dovoluje Komisi po určité časové prodlevě zvážit účinky certifikace na vnitřní trh a učinit certifikaci podle zvoleného schématu obligatorní.[143] Obecně dobrovolný princip byl pro Českou republiku jedním z nejdůležitějších bodů při vyjednávání,[144] a to z důvodu obav z přílišné moci Komise (která si faktickou moc diktovat certifikaci víceméně ponechala, jenom ji časově odsunula) a zároveň kvůli obavám, že se na českém trhu nevyskytuje dostatek kapacit pro institucionální a organizační zabezpečení obligatorní certifikace. V případě, že by byla prosazena plošná povinnost certifikovat produkty kybernetické bezpečnosti, jak navrhovalo např. Nizozemí s odvoláním na lepší implementaci produktů spadajících pod internet věcí, hrozilo by jednotnému trhu soutěžní ohnutí. Evropské certifikační velmoci – Francie, Německo, Nizozemí – by mohly využívat svých stávajících kapacit a nemusely by investovat do zřizování nových testovacích laboratoří žádné prostředky, případně jen velmi málo v porovnání s tím, jaké prostředky by musely vynaložit členské státy, které jsou „*certifikačními nováčky*“. Mezi ty se řadí i Česká republika. Čekala by je buď honba za subjektem či sdružením subjektů, jež by se vybudování CAB a testovacích laboratoří ujaly, nebo by menší státy musely vytvoření laboratoří zafinancovat samy. Na to ovšem většina z nich nemá dostatek volných prostředků, příp. politické vůle, takže není nepředstavitelné, že by

[143] K prvnímu takovému hodnocení dojde do 31. prosince 2023 (tedy po pouhých dvou rocích fungování certifikačního rámce) a dále alespoň každé dva roky.

[144] Ještě na začátku prosince 2018 byla tato otázka otevřena a probíhala bouřlivá jednání, kdy Česká republika stála téměř jako jediná za tímto principem bezpodmínečné dobrovolnosti.

existoval stát bez certifikační autority a laboratoře. To se může stát samozřejmě i při využití dobrovolného principu, ale při takovém rozvržení zůstane na členských státech, aby samy dobře zvážily následky takového kroku a povinné subjekty by tak nemusely zbytečně podstupovat certifikační proces v jiném státu (což opět představuje zvýšení nákladů a přenáší finanční prostředky subjektu do jiného členského státu). S ohledem na dlouho neupravenou implementační dobu nařízení (mohlo se stát, že by Akt vstoupil v účinnost příliš brzo pro certifikační nováčky a vytvoření CAB a laboratoří na mladších trzích by se pak nestihlo) hrozilo, že povinnost certifikace by vedla až k certifikačnímu „*monopolu*" laboratoří Francie, Německa a Nizozemí (pokud nedojde k Brexitu, pravděpodobně by do tohoto uskupení zapadla i Velká Británie), a to podobně, jak je tomu ve zbrojním průmyslu. Riziko monopolu bohužel zůstává, i kvůli nastavení požadavků na CAB, ale kvůli dobrovolnému principu certifikace je nižší a navíc se dá očekávat, že menší státy budou velice tvrdě bojovat proti tomu, aby si trh mezi sebou rozdělily německé a francouzské CAB. Česká republika má v úmyslu využít této šance, zhodnotit tento velký investiční potenciál (zvláště pokud dojde k rychlé implementaci a vytvoření relevantních kapacit) a stát se též jednou z certifikačních velmocí, přestože začíná na pozici relativního certifikačního nováčka.

4.2.3 HARMONIZAČNÍ PŘÍSTUP VS. PŘÍSTUP NA ZÁKLADĚ HODNOCENÍ RIZIK

Při vyjednávání finální podoby nařízení byla dlouho otevřená otázka „*obsahu*" certifikátu, tedy co by vlastně certifikát měl proklamovat a na jakém principu vystavět testování. Harmonizační přístup říká, že není možné za pomoci testování spolehlivě konstatovat, jestli je nějaký produkt bezpečný či nikoliv, a to převážně kvůli neustále se vyvíjejícímu prostředí kyberprostoru (vlastně jediné, co můžeme konstatovat s jistotou, je, že nic není úplně bezpečné). Zastánci tohoto názoru prosazovali zavedení jediné společné úrovně záruky bezpečnosti, která by de facto proklamovala, že produkt byl otestován určitou sérií testů, ve kterých obstál, a tak by se v něm neměly opakovat chyby, které byly v minulosti zneužity.

Princip hodnocení rizik (z angl. „*Risk-based approach*") je oproti tomu založen na kontinuálním procesu vyhodnocování rizik a jejich zvládání, řízení, kontrování nebo alespoň minimalizaci. Subjekt tedy nejdříve stanoví hranici, pod kterou je již riziko přijatelné (může jít buď o riziko sice závažné, ale je velice nepravděpodobné, že by riziková událost nastala, nebo může být riziková událost naopak velice pravděpodobná, ale závažnost následků je minimální) a může se tedy dočasně ignorovat a posléze začne vyhodnocovat jednotlivá rizika na základě předem stanovených kritérií (ta můžou být stanovena externě nebo interně). Zvládání rizik (z angl. risk-management) je pak proces, který snižuje rizika na úroveň přijatelnosti.[145,146] V případě aktu o kybernetické bezpečnosti šlo o stanovení tří rozdílných úrovní záruky, kdy u každé další úrovně je hranice přijatelnosti rizik vyšší a tím pádem je testování na danou úroveň přísnější a požadovaná bezpečnostní protiopatření komplexnější. Produkty se pak hodnotí ad hoc podle toho, jaká rizika jim mohou reálně hrozit v určitém prostředí a též podle toho, na jakou úroveň je daný produkt certifikován. Tento přístup byl podporován i ze strany různých zainteresovaných stran, např. Schneider Electric[147] nebo TÜV SÜD a TÜV NORD[148] (jedná se o jednu z největších německých elektrotechnických inspekčních a certifikačních asociací), takže není divu, že nakonec převážil. V Aktu je však patrný i určitý průnik harmonizačního přístupu, zvlášť ve formulaci bezpečnostních úrovní. Princip hodnocení rizik má totiž sám o sobě jednu velkou slabinu – může způsobit pocit falešného bezpečí, a to zvláště ve spotřebitelích. Akt o kybernetické bezpečnosti však zvládl tuto

[145] Viz KRISTENSEN, V.; AVEN, T.; FORD, D. A new perspective on Renn and Klinke's approach to risk evaluation and management. *Reliability Engineering & System Safety* [online]. 2006, roč. 91, č. 4, s. 1–3 [vid. 11. listopad 2018].

[146] Srov. s KLINKE, Andreas; RENN, Ortwin. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Analysis* [online]. 2002, roč. 22, č. 6, s. 1–2 [vid. 11. listopad 2018].

[147] Viz STANTCHEV, Pentcho. Cybersecurity of Industrial Systems. In: *Effectively Implementing the EU Certification Framework: Market Perspectives* [online]. Brusel, Belgie. 2018 [vid. 25. září 2018].

[148] Viz PRILLER, Christian. Effectively Implementing the EU Certification Framework: Market Perspectives - TÜV-SÜD-AG. In: *Effectively Implementing the EU Certification Framework: Market Perspectives* [online]. Brusel, Belgie. 2018 [vid. 25. září 2018].

nevýhodu alespoň v teorii kontrovat povinností informovat o rozsahu bezpečnostních záruk. V praxi bude potřeba osvětové činnosti ENISA a ostatních k tomu, aby koncoví uživatelé a spotřebitelé tomuto negativnímu následku nepodléhali.

5. AKTUÁLNÍ CERTIFIKAČNÍ ŘEŠENÍ – MEZINÁRODNÍ INICIATIVY

V této kapitole přistoupím k prvnímu konkrétnímu pojednání o tom, jak fungují certifikační systémy v praxi. Představím Mezinárodní organizaci pro standardizaci (oficiálním českým překladem ISO je *„Mezinárodní organizace pro normalizaci*“, ale s ohledem na kulturně-historické důvody jsem toho názoru, že je tento způsob překladu poněkud nešťastný, a místo toho se tak přikláním k verzi „*Mezinárodní organizace pro standardizaci*“) jako největší a pravděpodobně nejvýznamnější mezinárodní organizaci působící v této oblasti a rodinu kyberbezpečnostních standardů ISO 27K, kterým dala vzniknout. Těmto standardům se budu věnovat kvůli výše zmíněnému rozsahu Aktu o kybernetické bezpečnosti. Hlavní pozornost této kapitoly bude však zaměřena na představení a detailní rozebrání certifikačního rámce Common Criteria.

5.1 ISO

5.1.1 HISTORIE

Mezinárodní organizace pro standardizaci vznikla v roce 1946. Stalo se tak na konferenci v Londýně spojením dvou jiných organizací – ISA (International Federation of the National Standardizing Associations, která byla založena v New Yorku v roce 1926 s ústředím ve Švýcarsku) a UNSCC (United Nations Standards Coordinating Committee, založená v roce 1944 s ústředím v Londýně). Na konferenci, která představovala začátek ISO, se sešlo 65 delegátů z celkem 25 zemí. Organizace oficiálně započala svoji činnost v roce 1947.[149]

[149] Viz INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; CENTRAL SECRETARIAT. *Friendship among equals: recollections from ISO's first fifty years.* [online]. Geneva: ISO Central Secretariat, 1997, s. 15–18 [vid. 25. prosinec 2018].

Svůj první standard (v té době označovaný jako doporučení) publikovalo ISO v roce 1951. Stal se prvním krokem směrem ke skutečně velkému úspěchu organizace – publikaci unifikovaného mezinárodního systému jednotek SI v roce 1960. V 60. letech minulého století zároveň vznikl nový typ členství v ISO (neboť organizace se začala rozrůstat o rozvojové země) – tzv. „*Correspondent membership*“. Rozvojové země si tak mohly udržet přehled o dění v této mezinárodní organizaci, aniž by musely platit plné členské poplatky. Velký rozmach a opravdovou internacionalizaci zažilo ISO v 80. letech a také později pod vedením Lawrence D. Eichera, po kterém je pojmenována cena za vynikající práci v oboru standardizace.[150]

5.1.2 ČLENSTVÍ

Členství v organizaci ISO získávají přímo standardizační orgány daných zemí (vždy ten nejvíce vlivný orgán, členství je omezeno na jeden orgán za stát), přičemž každý člen pak reprezentuje ISO ve své zemi. Členem se nemůže stát obchodní společnost ani fyzická osoba. Organizace se rozrostla až tak, že ke dni 12. 10. 2019 má celkem 164 členů. Členství se dělí na „*Full Member*“ s plnými členskými právy a možností vyjadřovat se k připravovaným standardům, „*Correspondent Member*“, který vývoj uvnitř ISO sice jenom sleduje a sám ovlivnit nemůže, ale připravené standardy může prodávat nebo sám adoptovat, a „*Subscriber Member*“, který je o dění v organizaci informován, ale nemůže se na ní nijak podílet (je jim znemožněno veškeré oficiální nakládání se standardy). Úrovni členství odpovídá výše členských příspěvků.[151]

Na přijímání standardů se kromě členů podílí více než 250 různých sektorových výborů. Členové ISO se mohou rozhodnout, jestli k určitému výboru vůbec přistoupí, a zároveň mohou nadefinovat míru své účasti – „*účastnící se*“ členové jsou nadáni hlasovacími právy, kdežto „*sledující*“ členové mohou zasahovat do dění pouze radami, kritikou nebo

[150] Viz The ISO Story. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/the-iso-story.html.

[151] Viz *Members ISO* [online]. [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/members.html.

připomínkami. Při vývoji standardů je vývoj konzultován se zástupci rozvojových zemí, kteří jsou členy ISO, i se zástupci zúčastněných stran. Samotný proces přijímání je založen na konsensu.[152]

5.1.3 CERTIFIKACE

ISO samo o sobě certifikace svých standardů neprovádí a výslovně na to upozorňuje. Uživatel by tak měl zpozornět, pokud by mu podnikatel tvrdil, že produkt byl certifikován Mezinárodní organizací pro standardizaci. Je možné certifikovat soulad s některým ze standardů ISO (poté se tedy uvádí, že je např. ISMS certifikován podle ISO/IEC 27001:2013, přičemž první číslo značí řadu standardu a druhé rok revidované verze standardu), posouzení shody však musí provést některá z externích společností – certifikačních autorit, které jsou k tomu akreditovány akreditačním orgánem. Proces akreditace, zjednodušeně řečeno, představuje oficiální uznání, že určitý subjekt (certifikační autorita) je způsobilý provádět certifikační proces a že funguje v souladu s určitými standardy, které obsahují podmínky provozu takového tělesa. Tyto standardy vydává i Výbor pro posuzování shody („*Committee on Conformity Assessment*“ nebo ve zkratce CASCO), který patří pod ISO a který se otázkou posuzování shody zabývá.[153] Akreditační autoritou v České republice je z pohledu ISO Český institut pro akreditaci, o. p. s.[154]

Vzhledem k tomu, že proces certifikace se nachází mimo působení a zájem ISO, není explicitně řešena ani otázka vzájemného uznávání certifikátů napříč jednotlivými státy. Zůstává tak na členech, aby mezi sebou uzavřely dohody (anglicky označovaných jako „Mutual Recognition Agreements”, krátce MRA), které by zaručovaly vzájemné uznávání

[152] Viz Developing standards. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards.html ; Who develops standards. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards/who-develops-standards.html.

[153] Viz *Certification.ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/certification--conformity/certification.html.

[154] Viz IAF MEMBERS: Czech Republic. *International Accreditation Forum* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.iaf.nu/articles/IAF_MEM_Czech_Republic/66.

vydávaných certifikátů. Ukázkou takovéto dohody je dohoda SOGIS-MRA, která zaručuje uznávání certifikátů Common Criteria mezi členy evropského sdružení SOGIS.[155]

5.1.4 IEC – MEZINÁRODNÍ ELEKTROTECHNICKÁ ORGANIZACE

Z pojmenování standardu ISO/IEC 27001:2013 je patrné, že ISO není jediná organizace, která se na tvorbě standardu podílela. IEC je zkratka z „*International Electrotechnical Commission*" – organizace založené v roce 1906. IEC je vedoucí světovou organizací pro standardizaci produktů v oboru elektrotechniky,[156] a není tak divu, že při přípravě standardů z oblasti IT a ICT spojily organizace ISO a IEC síly ve formě Společného Technického Výboru ISO/IEC JTC 1 (Joint Technical Committee ISO/IEC JTC 1). Jeho podvýbor pojmenovaný ISO/IEC JTC 1/SC 27, který funguje od roku 1989, se zabývá vytvářením standardů v oblasti informační bezpečnosti (ke dni 12. 10. 2019 byl přímo odpovědný za 187 funkčních a 74 připravovaných standardů, a to včetně rodiny ISO/IEC 27K). Česká republika (přesněji řečeno Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, dále jen jako „ÚNMZ") s tímto podvýborem aktivně spolupracuje na tvorbě standardů a je tak jedním z 49 členů ISO, kteří v tomto výboru působí.[157]

5.1.5 RODINA MEZINÁRODNÍCH STANDARDŮ O INFORMAČNÍ BEZPEČNOSTI ISO/IEC 27K

Nejznámějším členem této rodiny je již zmiňovaný standard ISO/IEC 27001:2013 (= jeho poslední revize pochází z roku 2013), který představuje poněkud rigidní úpravu vytvoření, zabezpečení a udržení funkčního ISMS. Jeho první verze vznikla v roce 2005 a byla založena na

[155] Viz HEAD, Katie Bird. ISO workshop on Mutual Recognition Agreements. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/1998/04/Ref749.html.

[156] Viz IEC - About the IEC [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.iec.ch/about/?ref=menu.

[157] Viz ISO/IEC JTC 1/SC 27 - IT Security techniques. *ISO* [online]. [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/04/53/45306.html.

bezpečnostním standardu z Velké Británie (BS 7799-2). Určený je primárně společnostem, které jakýmkoliv způsobem operují s informacemi, ale obecně řečeno není z možnosti implementace vyloučen žádný subjekt.[158] Ani tento standard nevládne sám o sobě žádnou právní závazností, ale i kvůli své kvalitě a širokému uznávání se v mnohých státech dočkal buď právního uznání (ČR), nebo je přímo právem vyžadován (Japonsko).[159]

Standard se skládá ze dvou částí – z obligatorních specifikací, podle kterých se hodnotí shoda v certifikačním procesu, a z „*Code of Practice*", což je návod, ve kterém je popsána osvědčená praxe („*Best Practice*"). Specifikem druhé části je používání slov jako „*should*" (oproti první části, která užívá „*shall*"), z čehož je patrný doporučující charakter druhé části. Shoda s ní není pro účely certifikace nutná. Společnosti tak mohou použít třeba jenom některé z praktik zde popsaných, případně vůbec žádné, aniž by to mělo jakýkoliv negativní dopad na shodu.[160]

ISO 27001 úzce souvisí s dalším standardem – ISO 27002:2013. Kde ISO 27001 popisuje nástroje (především tedy z přílohy A), ISO 27002 obsahuje návod, jak takové nástroje správně implementovat. Oba dva standardy pak pracují s charakteristikami, definicemi a názvoslovím, jež jsou zakotveny ve standardu ISO 27000. Posledně zmíněný standard snižuje riziko nedorozumění při komunikaci jak v rámci společnosti, tak i s certifikačním orgánem.[161]

Aby mohl proces implementace ve společnosti započít, je nutné si pořídit kopie zmíněných standardů, neboť ty (na rozdíl od dokumentace Common Criteria) nejsou zdarma přístupné. Aktuální text standardu ISO 27001:2013 je k dostání za 300-500,- Kč.[162] Ceny zbylých dvou standardů se pohybují v obdobné výši. Nejnáročnější část celého procesu (kromě samotného vytvoření ISMS) bude pro většinu společností komplexní posouzení a vyhodnocení rizik (jak interních, tak externích), které

[158] Viz BÂRSAN, op. cit., s. 21.

[159] Viz SMEDINGHOFF, op. cit., s. 44.

[160] Viz CALDER, Alan. *Nine steps to success an ISO27001:2013 implementation overview* [online]. Ely, Cambridgeshire, U.K.: IT Governance Pub., 2013, s. 9–17 [vid. 11. listopad 2018].

[161] Viz tamtéž.

[162] K dostání např. zde: https://shop.normy.biz/detail/95805.

provádějí v přípravné fázi samy. Identifikují tak relevantní hrozby i zranitelné oblasti. ISMS by mělo být uzpůsobeno právě tomuto hodnocení a schopno adekvátně reagovat. Mělo by být přizpůsobeno jednotlivým částem společnosti a jednotlivým typům osob, které s ním přijdou do styku (spotřebitelé i zaměstnanci). Zúžení záběru ISMS pouze na relevantní oblasti se však může ukázat jako nemožné, případně popírající smysl ISMS jako celku, a musí tak pokrýt celou aktivitu společnosti.[163]

Proces implementace pokračuje stanovením interní politiky společnosti integrující ISMS, pro jejíž obsah standard ISO 27001 stanovuje sérii minimálních požadavků. Mezi témata, která mohou být takto upravena, patří politika utajení informací, kontrola přístupu k informacím, politika hesel či politika využívání kryptografických nástrojů. Po stanovení politik a vyhodnocení rizik jsou na řadě opatření, která mají rizika vyhodnocená jako nepřijatelná kontrovat. Taková opatření mohou mít podobu „*krizových*" plánů a dalších prvků řízení (celkem jich standard uvádí 114 v příloze A). Nezávislá certifikační autorita poté kontroluje vymezení rozsahu ISMS, jeho interakce s prostředím a hodnotí efektivitu zavedených protiopatření. V případě, že subjekt splní minimální požadavky stanovené ve standardu (subjekt může implementovat i daleko přísnější opatření, případně inovativnější, které nemusí standard explicitně uvádět, a pak je čistě na certifikační autoritě, aby posoudila efektivitu takového opatření), udělí mu certifikační autorita certifikát.[164]

Rodina standardů ISO 27K momentálně obsahuje již víc než 30 standardů, které jsou zacíleny na informační bezpečnost (každý další standard se zabývá specifickou částí zabezpečení informací).[165] Např. ISO 27040 obsahuje doporučení pro bezpečné ukládání dat, ISO 27037 doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů, nebo standard ISO 27032, který obsahuje bezpečnostní doporučení týkající se kyberprostoru.[166]

[163] Viz BÂRSAN, op. cit., s. 21-22.

[164] Viz tamtéž, s. 22–26.

[165] Viz CALDER, op. cit., s. 9–17.

[166] Viz MEHAN, op. cit., s. 183–188.

5.2 COMMON CRITERIA

Common Criteria nejsou „*pouhým*“ certifikačním schématem jako je ISO/IEC 27001:2013. Jedná se o komplexní certifikační systém pro bezpečnost IT technologií, sestávající z mnoha dílčích certifikačních schémat pro jednotlivé produkty, které mají „*poskytovat záruky, že procesy specifikace, implementace a vyhodnocení prvku počítačové bezpečnosti bylo provedeno standardním rigorózním a opakovatelným postupem na úrovni odpovídající cílovému prostředí použití*“.[167] Common Criteria byla vytvořena k tomu, aby „*umožňovala srovnatelnost výsledků nezávislých bezpečnostních hodnocení (a odstraňovala vícekolejnost právních úprav certifikačních režimů – pozn. autora). Činí tak stanovením obecného souboru požadavků pro bezpečnostní funkčnost IT produktů a pro úrovně záruky za spolehlivost produktů, kdy tyto požadavky jsou pak v procesu hodnocení na produkt aplikovány. IT produkty zahrnují řešení hardwarová, softwarová i firmwarová. Hodnotící proces, splňující požadavky stanovené v CC, zajišťuje společnou úroveň důvěry ve funkčnost bezpečnostních řešení i záruky za jejich spolehlivost a výsledky takového procesu mohou pomoci spotřebitelům určit, zda IT produkty splňují jejich bezpečnostní požadavky.*“[168]

Jedná se tak o prostředek, který umožňuje mezinárodní spolupráci v oboru hodnocení bezpečnosti ICT produktů. Jeho cílem je zvyšovat bezpečnostní úroveň pomocí předvídání a ex ante kontrování rizik a zranitelností, stejně jako odstraňování známých zranitelností, tedy postup ex post. Nejedná se o rigidní řešení předepisující pevnou sadu minimálních požadavků na zabezpečení tak, jak to dělá ISO 27001, ale umožňuje i uživatelům, aby nadefinovali své vlastní požadavky na bezpečnost, funkčnost a spolehlivost produktů. Zároveň usnadňuje uživatelům orientaci v nabízených bezpečnostních řešeních a umožňuje porovnávat úrovně jejich faktické „*bezpečnosti*“. Common Criteria mohou využít i vývojáři ke

[167] Viz JIRÁSEK; NOVÁK; POŽÁR, op. cit., s. 35.

[168] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017, s. 11 [vid. 12. září 2018].

kvalitnější implementaci bezpečnostních řešení, která by zároveň vyhovovala přáním uživatelů, a to již v rámci vývoje produktu.[169]

5.2.1 HISTORIE

V roce 1993 započalo uskupení složené z reprezentantů společností operujících v oblasti IT bezpečnosti a standardizace z USA (založené na systému TCSEC), Kanady (CTCPEC) a Evropského společenství (ITSEC)[170] práci na vytvoření nového certifikačního rámce, který by kombinoval všechna tři zmíněná kritéria a odstranil tak roztříštěnost úprav. Na tento nově vzniklý rámec měla dohlížet Mezinárodní organizace pro standardizaci (ovšem naplnění tohoto cíle se v průběhu příprav kritérií trochu zkomplikovalo). Kritéria byla dokončena v roce 1996 (verze 1.0), ovšem oficiálně publikována byla až verze 2.0, která následovala v roce 1998 po rozsáhlých revizích. Systém „*Common Criteria for Information Technology Security Evaluation*" (jednoduše Common Criteria nebo též pod oficiální zkratkou CC) si získal od počátku neobvyklou oblibu. Po publikaci verze 2.0 společně uzavřely Kanada, Francie, Německo, Spojená království a USA dohodu o vzájemném uznávání certifikátů vzešlých ze systému CC (CCRA – CC Recognition Agreement), čímž byl projekt oficiálně spuštěn. Hned následujícího roku se k dohodě přidala Austrálie a Nový Zéland a další státy následovaly nedlouho poté. Ještě téhož roku (tj. 1999) byla vydána první úprava – verze 2.1, která byla po dohodě adoptována Mezinárodní organizací pro standardizaci a Common Criteria byla přejata do mezinárodního standardu ISO 15 408 (text CC je totožný se zněním standardu).[171]

---

[169] Srov. ISA, Mohd Anuar Mat et al. Finest authorizing member of common criteria certification. In: *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* [online]. Kuala Lumpur, Malaysia: IEEE, 2012, s. 156 [vid. 22. červenec 2018].

[170] TCSEC = Trusted Computer System Evaluation Criteria, CTCPEC = Canadian Trusted Computer Product Evaluation Criteria, ITSEC = Information Technology Security Evaluation Criteria.

[171] Viz TANTAWI, Randa. Common Criteria. *Salem Press Encyclopedia* [online]. 2013 [vid. 13. září 2018].

Common Criteria se dočkala napříč lety ještě několika přepracování a nejaktuálnější (vydaná v dubnu 2017) je verze 3.1, páté vydání.[172] Přepracovávání kritérií je v poslední době motivováno především snahou zjednodušit celý proces, dokumentaci, odstranit podvojnou úpravu z jednotlivých dokumentů a urychlit certifikační proces.

V roce 2003 došlo k pokusu ustanovit Common Criteria jako oficiální a povinný certifikační rámec pro organizaci NATO. Mezi členskými státy ovšem nebylo dosaženo shody, a tak byla vydána pouze směrnice NATO, podle které je certifikace podle CC sice doporučeným, ale nikoliv povinným bezpečnostním řešením. I přesto jsou schémata a certifikáty, které byly schváleny orgány členských států, uznávány v rámci celého NATO jako projev vzájemné důvěry.[173]

Ke dni 12. 10. 2019 bylo členem dohody CCRA 31 zemí světa. Největší událostí nedávné minulosti byla změna statusu Velké Británie, která odstoupila od statusu „*produkující certifikáty*" a stala se jen dalším z konzumentů (dle vyjádření pro nedostatečnou poptávku po certifikaci na území Velké Británie). Členství má dvě formy – 17 států má status „*produkují certifikáty*" (tj. ti, kteří mohou provádět certifikaci podle schémat CC) a 14 států „*uznávající certifikáty*".[174] Tzv. „*Consuming*" členové certifikáty vyprodukované první skupinou uznávají, ale jim samotným není umožněno certifikáty autorizovat. Tento typ členství vznikl po roce 2000, aby se mohly přidat k CCRA i státy, jejichž vnitrostátní kapacity neumožňují provádět certifikaci na požadované úrovni.[175] Česká republika je od roku 2004 jedním z těchto států a mezinárodní normě ISO/IEC 15408 byl udělen status české technické normy (tedy ČSN EN ISO/IEC 15408). Reprezentaci ČR v rámci CCRA zajišťuje podle oficiálních stránek CC

[172] Viz Common Criteria. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/.

[173] Viz Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019].

[174] Viz Common Criteria. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/.

[175] Viz TANTAWI, op. cit.

Národní bezpečnostní úřad,[176] ale jedná se dle mého názoru o zastaralou informaci, neboť působnost na poli kybernetické bezpečnosti měl převzít NÚKIB beze zbytku.

5.2.2 SYSTEMATIKA CC

Páteří celého systému Common Criteria je samotný dokument CC rozdělený do 3 částí – Úvod a obecný model, Požadavky na funkčnost zabezpečení (SFR) a Požadavky na spolehlivost (SAR). Tento ústřední dokument je pak v praxi doplněn řadou podpůrných či vysvětlujících dokumentů a zpráv, mezi kterými zastává výsostné postavení tzv. CEM – Common Evaluation Methodology. Jedná se o metodologii, která byla vyvinuta specificky pro provádění posuzování podle Common Criteria, aby bylo dosaženo maximálně jednotného postupu při provádění testů napříč různými státy.[177]

První část obsahuje zejména základní definice, principy a zásady hodnocení, a jak už název oddílu napovídá, je zde i představen naprosto nejzákladnější model hodnocení. Druhá část je de facto seznamem zabezpečovacích funkčních komponent, které jsou roztříděné do 11 tříd – např. třída využívání zdrojů, kryptografické podpory, správy bezpečnosti, komunikace či soukromí. Každá ze tříd se dále dělí na rodiny a ty dále na komponenty. Tyto komponenty jsou pak středobodem funkčního hodnocení produktů. Třetí část CC stanovuje soubor komponent pro formulaci a popis požadavků na záruku spolehlivosti, který je možné použít jako určitou formu základní šablony. Zároveň jsou zde stanoveny hodnotící kritéria pro profily ochrany a bezpečnostní cíle (vysvětleno níže). Jednotlivé komponenty jsou opět sdruženy do jednotlivých rodin a tříd podle obsahové sounáležitosti (např. třída zaměřující se na průvodní dokumentaci, vývoj, testování, správu konfigurace aj.). Oproti druhé části je řazení komponent v tomto oddíle přísně hierarchizováno s rostoucí

[176] Viz Members of the CCRA. *New CC Portal* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.commoncriteriaportal.org/ccra/members/#CZ.

[177] Viz *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model* [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017, s. 37 [vid. 12. září 2018]; Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019].

složitostí a úrovní formálnosti. Z tohoto uspořádání pak vychází 7 úrovní záruky spolehlivosti produktů (Evaluation Assurance Levels – EAL), což jsou již v samotných CC vytvořené balíčky komponent pro hodnocení záruky jednotlivých produktů. Pro složené produkty byla vytvořena obdoba EAL nazvaná „*Composed Assurance Packages*“ (nebo zkráceně jednoduše CAP).[178]

5.2.3 EALS

EAL 1-7 formulují různé úrovně záruky, že je produkt spolehlivý a bezpečný. Vyjadřují, jak přísným testováním produkt před udělením certifikátu prošel a jak vážným hrozbám by měl produkt odolat. Vývojář si sám vybírá, na jakou úroveň svůj výrobek nechá certifikovat (přitom obvykle vychází nejen z vlastního odhadu závažnosti hrozeb, ale i požadavků uživatelů a ostatních zúčastněných stran).

EAL 1 je nejnižší stupeň záruky, který je určen pro případy, kdy je potřeba určité minimální záruky za bezpečnost produktu, ovšem v prostředí, ve kterém je výskyt závažnějších hrozeb nepravděpodobný. Hodnocení probíhá neformálně a soustředí se primárně na dokumentaci. Není vyžadována zvláštní spolupráce vývojářů produktu a hodnocení probíhá bez funkčního testování produktu samotného. V případě EAL 2 vývojář již musí spolupracovat a dodat specifické informace o produktu a jeho bezpečnostních funkcích. Testování sice probíhá stále ještě primárně na základě dodané dokumentace, ale aspekty a zranitelnosti, které vyjdou najevo z prozkoumání dokumentace, se testují již přímo na produktu (analýza zřejmých zranitelností atp.). Příprava na testování na tento stupeň již vyžaduje speciální přípravu a vypracování bezpečnostních procedur, ale zásadně ještě nezvyšuje náklady, jako je tomu u dalších úrovní. EAL 3 již zahrnuje rozsáhlejší a podrobnější testování produktu, zároveň se v něm jako v prvním objevuje i kontrola vývojového prostředí. EAL 4 je poslední, kterého lze ze zásady dosáhnout bez speciálních znalostí a dovedností v oboru. Je zároveň poslední, kterého lze dosáhnout pro již existující

[178] Viz Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019].

produkt, vyšší úrovně již vyžadují promítnutí bezpečnostních opatření do celého životního cyklu produktu, tedy již od vývojového stádia („*Security by design*“). Pro standardní produkty již tato úroveň představuje střední až vysokou úroveň záruky bezpečnosti a pro vývojáře představuje vynaložení zvýšených nákladů na správu zabezpečení. Tato úroveň pracuje s detailní dokumentací doprovázející produkt (v některých případech se stále jedná o zkoumání neformální – např. u modelu bezpečnostní politiky). Zároveň často vyžaduje dodání alespoň části zdrojových kódů bezpečnostních opatření, což některým vývojářům nemusí být příjemné. Při hodnocení se testuje schopnost odolat útočníkům s nízkým útočným potenciálem (tzn., že takový útočník má značně omezené zdroje či vědomosti, příkladem může být útočník označovaný v hackerské komunitě jako „*Script kiddie*“ – využívající toliko hotových skriptů a aplikací, bez skutečné znalosti materie). Až do této úrovně včetně je metodika hodnocení upravena v CEM. U vyšších úrovní je testování již tak komplexní, že metodika pro tuto oblast zatím vyhotovena nebyla. Pro porovnání uvedu, jak vypadá nejvyšší úroveň EAL 7. Tato úroveň je určená pro extrémně rizikové prostředí nebo pro ochranu extrémně hodnotných aktiv. Zároveň není mnoho testovacích laboratoří, které by zvládly otestovat produkty na tuto úroveň. Vývojář již musí dodat plně formální dokumentaci v celé její šíři včetně modelů bezpečnostní politiky. Při testování produktu se využívá metody „*white-box*“ – testy jsou zaměřené na vnitřní strukturu produktu, na jeho kódování a design. V tomto typu testování je celý kód zpřístupněn testujícímu subjektu a jedná se tak o hloubkový test (oproti tomu stojí tzv. „*black-box*“ testování, kdy testovacímu subjektu kód zpřístupněn není, testování probíhá z pohledu konečných uživatelů a zaměřuje se na funkčnost produktu).[179]

5.2.4 ORGANIZAČNÍ STRUKTURA

Na fungování projektu Common Criteria dohlíží tzv. „*Common Criteria Management Committee*“ (dále také jako „CCMC“), výbor, který je složen ze

[179] Viz Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019]; ISA et al, op. cit., s. 156.

zástupců jednotlivých členských států. CCMC je nejvyšším orgánem, který řídí zejména politická rozhodnutí související se spoluprací na CC. Od roku 2000 navíc pravidelně pořádá Mezinárodní konference o Common Criteria (ICCC), které jsou pokaždé pořádány v jiném členském státě. Tyto konference slouží k šíření osvědčených praktik, představování nových výzev a technologií a zprostředkování dialogu mezi zúčastněnými stranami a organizačním aparátem Common Criteria. CCMC má dva pomocné orgány – CCDB („*Common Criteria Development Board*"), která se zabývá technickým vývojem kritérií a dohlíží na jejich správnou a zodpovědnou aplikaci v členských státech, a CCMB („*Common Criteria Maintenance Board*"), jejíž úkol spočívá v hodnocení návrhů na změnu kritérií a udržování dialogu s členskými státy a Mezinárodní organizací pro standardizaci.[180]

Kromě organizačního aparátu, dohlížejícího na stav kritérií samotných, spadají do organizační struktury i testovací laboratoře a certifikační autority, bez nichž by faktický provoz certifikace nebyl možný. Common Criteria, respektive CCRA specificky rozlišuje testovací laboratoře od certifikačních autorit a dává tak možnost komerčnímu vzniku testovacích laboratoří, které mohou sloužit pro vícero certifikačních autorit nebo naopak. Testovací laboratoře jsou vázané podmínkami provozu stanovenými v CCRA – tzn., že tyto podmínky čerpají svou závaznost z možnosti uznávání certifikátů. Bez naplnění těchto podmínek nebudou certifikáty uznány a subjekt dostane pouze hezký vnitrostátní certifikát s potenciálně špatnou reputací. Hlavní podmínkou je akreditace laboratoře v souladu se standardem ISO/IEC 17025 v aktuálním znění, případně jinou formu licencování laboratoře splňující požadavky uvedené v příloze B. Ta stanovuje v bodě B.3 podmínky pro licencování a akreditování laboratoře – primárně materiální podmínky ISO/IEC 17025, technickou vybavenost, nezávislost, nepodjatost a metodologickou a procesuální kompetentnost. Splnění těchto podmínek musí prokazovat hlavně certifikačnímu orgánu a k jeho spokojenosti. Podmínky pro výkon funkce samotné certifikační autority jsou uvedené v článku 5. Certifikační autorita musí být akreditována v souladu se standardem ISO/IEC 17065 v aktuálním znění,

[180] Viz TANTAWI, op. cit.

nebo obdobou splňující požadavky podle přílohy C. Zároveň k tomu, aby byly její certifikáty uznávány, musí vykonávat hodnocení nezávisle, přísně aplikovat CEM tam, kde to bude možné, a chránit utajované informace, které se při výkonu hodnocení dozvěděla. Příklady základních práv a povinností certifikačních orgánů jsou stanoveny v bodě B.2 přílohy – patří mezi ně možnost autorizovat účast testovací laboratoře na schématu (tedy že laboratoř může testovat produkty podle určitého schématu), dohled nad plněním podmínek pro výkon testování v laboratořích, vydávat podpůrné dokumenty k vydaným schématům, vydávat CC certifikáty nebo zprostředkovávat komunikaci mezi všemi zúčastněnými stranami.[181]

Celý organizační komplex je de facto doplněn i soukromými subjekty a spotřebiteli, neboť ti mohou definovat bezpečnostní požadavky na jednotlivé produkty (popsáno v dalším oddílu), proti kterým se pak produkty poměřují.

5.2.5 TOE, ST, PP A CERTIFIKAČNÍ SCHÉMA

Common Criteria operují ve své dokumentaci s mnoha pojmy, které je vhodné pro účely tohoto článku vysvětlit. Základním pojmem je TOE – „*Target of Evaluation*“, česky předmět posuzování. Může se jednat jak o softwarové, tak o hardwarové či firmwarové řešení. Na TOE jsou navázané pojmy PP a ST. PP je zkratkou pro „*Protection Profile*“ – profil ochrany, ST pro „*Security Target*“ – bezpečnostní cíl.[182]

Profily ochrany poskytují uživatelům možnost nadefinovat svá přání a požadavky na bezpečnost nevázaně na určitém produktu a jeho implementačním procesu (tedy se může jednat např. o bezpečnostní požadavky k blíže nespecifikovanému firewallu). Profil ochrany je tedy spíše šablonou pro skupinu produktů než konkrétním schématem, vyznačuje se obecností (tím se liší od ST) a může být použit opakovaně pro několik různých TOE. K tomu, aby mohl být PP používán jako základ pro

[181] Viz Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security [online]. 2. červenec 2014 [vid. 12. září 2018].

[182] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017 [vid. 12. září 2018].

ST, je nutné, aby sám prošel náležitým posouzením. Teprve PP, který je schválen, je zapsán do registru profilů ochrany a zveřejněn. Úplný profil ochrany může obsahovat následující kapitoly: úvod, popis TOE, definici bezpečnostního prostředí TOE (zasazení produktu do reálného světa a jaké relevantní hrozby mohou produktu hrozit), bezpečnostní cíle produktu a prostředí, bezpečnostní požadavky a zdůvodnění.[183]

Bezpečnostní cíle jsou oproti tomu definice, které vytvořili vývojáři, stanovující, jaké by měl mít produkt konkrétní bezpečnostní vlastnosti. Pravost těchto sdělení se pak bude při hodnocení testovat. Bezpečnostní cíle mohou být založené na jednom nebo i více profilech ochrany, aby vývojáři demonstrovali, že vyhověli přáním uživatelů. Jsou ovšem vázané na konkrétní produkt a implementaci bezpečnostních řešení. Pokud ST udá, že je založeno na více PP, musí dodržet požadavky všech těchto profilů. V rámci ST jsou definovány bezpečnostní rizika, problémy a zároveň i dílčí bezpečnostní cíle, kterých by měl hodnocený produkt dosáhnout. Oproti PP není v případě ST žádný registr, neboť se jedná o konkrétní, ve většině případů jednou použitelný set požadavků. I ST však musí projít posouzením a až prověřený může být použit k testování v samotném certifikačním procesu TOE.[184]

Posledním pojmem je hodnotící/certifikační schéma. Jedná se o regulatorní a administrativní rámec vytvořený na základě obecného modelu stanoveného v dokumentaci Common Criteria, podle kterého certifikační orgán hodnotí soulad s konkrétním druhem produktů. Může být výsledkem spojení uvedených PP a užívaných ST, zároveň se může jednat i o průmět určitých vnitrostátních regulatorních požadavků.[185]

Z výše uvedeného je patrné, že nová schémata mohou vzniknout v tomto systému na popud kohokoliv. Common Criteria se tak v teorii

[183] Viz tamtéž.

[184] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017 [vid. 12. září 2018].

[185] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017 [vid. 12. září 2018].

vyznačují neobyčejnou flexibilitou a otevřeností novým nápadům, technologiím a postupům.

5.2.6 PROCES CERTIFIKACE

Proces získání certifikátu Common Criteria zde bude popsán za pomoci dvou zdokumentovaných zkušeností s certifikačními procesy – v jednom případě certifikace chytré televize (LG SmartTV) na úroveň EAL 2,[186] v druhém případě certifikace distribuce operačního systému Linux.[187] Druhý případ ovšem zaznamenává zkušenosti ze získávání certifikátu ještě před velkou revizí dohody CCRA v roce 2015, která odklonila zaměření dohody od úrovní EAL a zároveň snížila obecně mezinárodně uznávaný stupeň záruky z EAL4 na EAL2, takže informací v této případové studii bylo využito jenom k doplnění informací z certifikačního procesu SmartTV. Překvapivé může být, že snížením vzájemného uznávání na úroveň EAL2 se zájem o certifikaci na vyšší úrovně snížil jen lehce,[188] a to přestože vyšší úrovně jsou nyní použitelné pouze pro vnitrostátní aplikaci.

Než celý proces započne, musí se vývojáři rozhodnout, na jakou úroveň je certifikace z hlediska potřebnosti a nákladovosti vhodná. Vývojáři LG SmartTV se rozhodli podstoupit proces certifikace na úroveň EAL 2. Prvním krokem je vypracování ST a dokumentace, která se na této úrovni neformálně posuzuje – manuál, design a popis TOE, zvláště pak jeho bezpečnostních funkcí. V případě chytré televize tedy byla popsána zejména architektura bezpečnostních řešení (např. instalace aplikací v režimu „*sand box*“) a dále rizika a jejich kontrování v celém procesu vývoje produktu. V případě bezpečnostní díry je nutné, aby došlo k odstranění vadné aplikace či kódu, a je třeba se ujistit, že zranitelnou oblast není možné obejít. Celý tento proces je vhodné zdokumentovat, aby

[186] Viz KANG, Sooyoung; KIM, Seungjoo. How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability. *Symmetry* [online]. 2017, roč. 9, č. 10 [vid. 22. červenec 2018].

[187] Viz RECCHIA, Luca et al. Security Evaluation of a Linux System: Common Criteria EAL4 + Certification Experience. In: *2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* [online]. Naples, Italy: IEEE, 2014 [vid. 22. červenec 2018].

[188] Viz https://www.commoncriteriaportal.org/products/stats/.

mohla být dostatečnost bezpečnostních protiopatření otestována i při certifikačním procesu.

V rámci ST je potřeba správně nadefinovat relevantní požadavky na funkčnost zabezpečení (SFR) z části druhé CC a popsat způsoby jejich naplnění a přijatá opatření (např. správa přístupu k informacím). To samé je nutné i u požadavků na spolehlivost (SAR) podle části třetí. Hotové ST tak obsahuje definici TOE pomocí SFR, SAR, bezpečnostních rizik a hrozeb, dílčích bezpečnostních úkolů, cílů a funkcí (obvykle ve formě nejrůznějších analýz mapujících chování produktu v rizikových situacích). Je důležité dbát o to, aby se TOE v průběhu vývoje od ST neodklonil, jinak je potřeba aktualizovat ST.

V případě, že existuje PP, je vhodné se alespoň pokusit ho zahrnout do bezpečnostního cíle. Pro chytrou televizi ovšem žádný zveřejněný oficiální PP neexistoval, tudíž ST byl v tomto případě vytvořen na základě analogických PP. Vývojáři při tvorbě ST zároveň připisují jednotlivým aktivům produktu různou důležitost a tím pádem i míru ochrany (k určení hodnoty aktiva slouží právě PP).

Jakmile je ST (i produkt samotný) hotový, přichází fáze testování. V případě nových technologií bývá problematické najít laboratoř schopnou testování[189], referenční materiály či testovací metody a nástroje. Ty musí vývojáři v takovém případě vyhledat a referenční materiály a testy případně sestavit. Pro zmíněnou chytrou televizi, protože na úroveň EAL2 musela projít i praktickým testováním, vytvořili vývojáři na základě žádosti certifikační autority 4 druhy testů: funkční testování (testuje, zda specifikované funkce pracují a pracují dobře a v souladu s bezpečnostními požadavky), testování zranitelností (testuje odolnost proti již známým hrozbám a slabinám), penetrační testování (testovací hackerské pokusy o převzetí vlády nad zařízením) a „*fuzz*“ testování (testující schopnost vypořádat se s chybovou hláškou na vstupu, čímž se testují zbylé zranitelnosti). Certifikační autorita si pak sama vybere, který typ testování bude proveden.

[189] Informace o licencovaných laboratořích je možné najít mimo jiné zde: https://www.commoncriteriaportal.org/labs/.

Pokud je certifikace produktu první svého druhu (tedy dosud nebylo testováno nic ani ze skupiny podobných produktů), musí certifikační orgán provést speciální verifikační proces ohledně schopnosti certifikovat. V jeho procesu si musí hodnotitel obstarat certifikát osvědčující, že je schopen certifikaci provést, a dále sehnat potřebné případové („*hacking*“)[190] studie, seznamy známých zranitelností, hodnotící metody atp. S mnohým mohou pomoci vývojáři samotní, proto se při nedostatku referenčních materiálů a postupů může stát, že hodnotitel požádá vývojáře produktu, aby takové materiály a testy vyvinul. Tento verifikační proces protáhl čekací dobu u certifikace chytré televize o 1,5 měsíce, tzn. 1,5 měsíce se čekalo, než se vůbec započne s testováním samotným. Pokud je produkt a ST komplexnějšího rázu, je pravděpodobné, že verifikační proces zabere ještě delší dobu.

Poté, co vývojáři naleznou a kontaktují testu-schopnou testovací laboratoř a odpovídající certifikační autoritu, případně skončí verifikační proces u certifikační autority, může započít testování samotné (v souladu s pravidly stanovenými v CEM). Testování je řízeno certifikační autoritou a prováděno testovací laboratoří. TOE se testuje podle specifik daných v ST a podpůrné dokumentaci (např. manuál) – nejdřív je prozkoumána dokumentace, design a funkce TOE a podle výsledků z tohoto průzkumu je následně předepsáno, jakým způsobem, co a v jakém prostředí bude testováno. Vývojáři v případu chytré televize podotýkali, že u společnosti, která poprvé absolvuje certifikační proces, je nepřítomnost bezpečnostního inženýra, který by dohlížel na rychlou implementaci bezpečnostních řešení, značně zdržující (navíc mnohé společnosti nemají dostatečné kapacity ani zdroje, aby jeho přítomnost materiálně nahradily). Tento problém se však projeví jen v případě, kdy není TOE nebo ST dostatečně důkladně a detailně připraveno a při certifikačním procesu se projeví neočekávaná situace nebo chyba, kterou je zapotřebí rychle odstranit.

[190] Tyty případové studie jsou často zdokumentovaným postupem penetračního testování, popisují tedy způsob provádění testu a to, jak využít známých zranitelností z podobných případů.

Jakmile je testování dokončeno, podá testovací laboratoř report certifikační autoritě, která na jeho základě (v případě, že je report pozitivní) vydá pro produkt certifikát, TOE zařadí do registru a certifikát zveřejní.[191]

5.2.7 MEZINÁRODNÍ UZNÁVÁNÍ CERTIFIKÁTŮ

Mezinárodní a vzájemné uznávání certifikátů je zaručeno primárně na základě dohody CCRA, která nyní zajišťuje automatické vzájemné uznávání jen do úrovně EAL2 (ve specifických případech do EAL4). Původně bylo zajištěno uznávání do úrovně EAL4 (a ve specifických oblastech až do úrovně EAL7). Omezení na úroveň 4 bylo způsobeno rozsahem CEM, který sahal právě jenom do čtvrté úrovně. Vyšší úrovně již neměly upravenou metodiku testování (kvůli komplexní povaze přísnějších testů bylo vytvoření takové úpravy přinejmenším velice nesnadné), a tím pádem neměly ostatní členské státy dohody CCRA záruku, že testování bude probíhat zodpovědně a podle jednotného klíče, který by mohl vytvářet důvěru ve výsledek. Přestože je nyní uznávání omezeno jenom do úrovně 2, jedná se o uznávání automatické a nositelé certifikátu tak nemusí podstupovat žádné další řízení o uznání.[192]

Dohoda SOG-IS MRA byla v tomto článku již představena. Zajišťuje uznávání certifikátů až do úrovně čtvrté, případně sedmé ve specifických technických oblastech.[193] Toto sdružení není sjednoceno jenom vzájemným uznáváním, ale úzce spolupracuje i na vytváření nových schémat a PP.[194] Stejně jako CCRA i SOG-IS MRA má dvě formy členství – země produkující certifikáty a země certifikáty akceptující. Pro připomenutí – ČR není

[191] Pro představu o počtech certifikovaných produktů viz https://www.commoncriteriaportal.org/products/stats/.

[192] Viz Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security - Ratifikováno 8. 9. 2014 [online]. 2014 [vid. 12. září 2018].

[193] To byl i jeden z důvodů, proč byl SOG-IS vytvořen – mělo dojít k limitaci vzájemného uznávání certifikátů na vyšších bezpečnostních úrovních na technické oblasti, kde je již nadefinována metodologie, požadavky na laboratoře a na testování samotné.

[194] Impulzem ke stvoření nového schématu je často moment, kdy Evropská komise vydá směrnici týkající se IT bezpečnosti, která by měla být vnitrostátně implementována určitým (nejlépe jednotným) způsobem.

členem této dohody a ani nemá na členství zájem. Slovensko oproti tomu je jedním ze států uznávajících certifikáty (a 17. září 2019 se stalo i konzumujícím členem dohody CCRA).[195]

5.2.8 SLABINY A NEVÝHODY SYSTÉMU COMMON CRITERIA

Jedna z největších slabin CC je závislost na mezistátní důvěře. Tato závislost bohužel není ze strany CC ani CCRA odstranitelná, je neochvějně spojená se spoluprací v oblasti bezpečnosti, neboť v takových chvílích sice samy sobě poskytují členské státy výhody a informace, ale zároveň poskytují informace o zabezpečení vlastní infrastruktury dalším státům. A to je potenciálně zneužitelné. V ideálním světě by důvěra samozřejmě mohla fungovat bez problémů i bez regionálních uskupení, jako je Evropská unie, ale realita je bohužel jiná a ani Unie není nedůvěry prosta. Princip fungování CC je založen na idealistické vizi, která rozevřela nůžky mezi právně-technickým vnímáním světa a jeho skutečným politickým fungováním. Vzájemné uznávání tak funguje bez problémů jen mezi spojenci, kdežto mezi potenciálními nepřáteli takové uznávání nikdy naplno fungovat nebude, resp. bude sloužit jako třecí plocha. Common Criteria vznikala v období po pádu SSSR, které se vyznačovalo umírněním celé mezinárodní situace a vzrůstající spoluprací mezi státy. To období však skončilo. Kvůli nedostatku vzájemné důvěry tak širší implementace systému Common Criteria patrně svědky nebudeme, přestože se stále ještě jedná o „*state of the art*“ světa certifikace kyberbezpečnostních technologií.[196]

Common Criteria se potýkají i s dalšími problémy, které jsou alespoň částečně mimo dosah samotných kritérií. Jedná se o hrubě neaktuální profily ochrany a další schémata, kdy některá PP, stále ještě v užívání, pocházejí z roku 1999. To způsobuje odtržení požadavků na bezpečnost od reálného světa a staví vývojáře do nelehkých pozic, ze kterých často uniknou rezignací na certifikaci. Zároveň se CC minula s plánovaným

[195] Viz SOG-IS - Home. *SOG-IS* [online]. [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html; SOG-IS - Status of participants. *SOG-IS* [online]. [vid. 25. prosinec 2018]. Získáno z: http://sogis.org/uk/status_participant_en.html.

[196] Viz KALLBERG, Jan. The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal. *IEEE Security & Privacy Magazine* [online]. 2012, roč. 10, č. 4, s. 50–52 [vid. 22. říjen 2018].

účinkem na trh. Většina certifikátů je vystavována pro produkty ve vládním nebo vojenském sektoru, co se ovšem týká soukromého – zde je výskyt minimální. To snižuje zapojení subjektů průmyslových odvětví a soukromého výzkumu do inovací schémat pod CC, a tak snižují relevanci CC v čase. CC tak nedokáží reagovat na chyby, případně na zranitelnosti přicházejí moc pozdě. Efektivita certifikace tím značně trpí.[197]

Problémem, který byl již v tomto článku rozebrán a který vychází z kritérií samotných, je nevhodnost tohoto systému pro hodnocení TOE, jako jsou big data, cloudové služby a služby celkově, o čemž vypovídá i počet certifikovaných služeb (0, viz výše). Zároveň další velkou slabinou tohoto systému je délka a nákladnost certifikačního procesu. Zvláště při certifikaci nových produktů je tento proces dlouhý až 12 měsíců a značně nákladný, což je naprosto tristní, zvláště u nižších úrovní EAL, a k zajištění funkčnosti certifikovaných produktů hrubě nedostatečné. Common Criteria mají značný problém i s údržbou certifikátu (trvanlivost má 5 let, pak je nutné ho obnovit) a aktualizačním procesem certifikovaných produktů (certifikát se pojí jen k určité verzi produktu). To mimo jiné vedlo ze strany nespokojených členských států k zakládání vlastních certifikačních řešení soustředících se na limitaci času a zdrojů potřebných k provedení certifikace a zároveň na vyřešení slabiny certifikátů v evolučním cyklu produktů.[198,199]

Poslední velkou slabinou ukrytou přímo v dokumentech CC je vnitřní rozpornost. Metodologie si s touto vnitřní rozporností povětšinou neumí poradit a v mnohých případech ji neumí ani zjistit. Jedná se o skutečnost, že CC sice vývojářům produktu mnohdy stanoví při implementaci prvku A povinnost zavést i prvek B, ovšem v celém systému se neřeší, že při zavedení prvku X se již nesmí zavést prvek Y. Systém tak vůbec nemapuje vztahy, kdy se jednotlivé prvky mohou kontrovat až do absolutní neúčinnosti. Tento problém je zvlášť patrný, jakmile je potřeba zaručit jak anonymitu, tak přezkoumatelnost v rámci daného produktu (např. online

[197] Viz HEARN, op. cit., s. 64–65; ISA et al, op. cit.; KALLBERG, op. cit., s. 50-52.

[198] Viz KALLBERG, op. cit., s. 52.

[199] Srov. ISA et al, op. cit.

volby). Požadavek anonymity zabraňuje užití dostatečných nástrojů na zajištění přezkoumatelnosti a požadavek přezkoumatelnosti zároveň vylučuje možnost efektivního zaručení anonymity.[200]

6. AKTUÁLNÍ CERTIFIKAČNÍ ŘEŠENÍ – VYBRANÉ EVROPSKÉ STÁTY

V oboru certifikace kyberbezpečnostních technologií v Evropské unii vyčnívají nad ostatními čtyři státy, které za absence unifikovaného evropského řešení (a částečně i kvůli nespokojenosti se systémem Common Criteria) vytvořily vlastní úpravu, většinou pro nižší úrovně bezpečnostní záruky. Jsou jimi Velká Británie (až do Brexitu stále součástí EU), Francie, Německo a Nizozemí. V této kapitole budou stručně představeny jejich národní modely certifikace, které společně se systémem Common Criteria inspirovaly podobu nové jednotné evropské certifikace a které po jejím příchodu postupně zaniknou. Bude tak zodpovědností celého budoucího evropského certifikačního aparátu, aby nedošlo k zániku kvalitních a trhem žádaných certifikačních schémat. To by paradoxně vedlo ke stavu opačnému, než o jaký Akt o kybernetické bezpečnosti usiluje – ke snížení kybernetické bezpečnosti v některých státech. Kromě čtyř výše zmíněných států významně pracují na vlastní regulaci této materie i Itálie, Švédsko a Norsko (přestože není členem Evropské unie, je členem uskupení SOG-IS).

6.1 VELKÁ BRITÁNIE

Velká Británie spustila na začátku roku 2011 národní certifikační schéma pojmenované „*Commercial Product Assurance*“ (dále jen jako „CPA“) pro komerční kyberbezpečnostní produkty prodávané ve VB. Je určené pro produkty (nikoliv služby) pracující v méně rizikovém prostředí, které však musí vykonávat určitou zabezpečovací funkci (např. firewall nebo šifrování). Produkty jsou pak v tzv. „*CPA testovacích laboratořích*“ testovány proti požadavkům stanoveným v předem publikovaných bezpečnostních standardech (tzv. „*Security Characteristics*“, dále také jako „SC“), které

[200] Viz MERCURI, Rebecca. Uncommon criteria. *Communications of the ACM* [online]. 2002, roč. 45, č. 1, s. 172 [vid. 22. říjen 2018].

vydává Národní centrum kybernetické bezpečnosti („*National Cyber Security Centre*“).[201]

SC jsou dokumenty, které definují, jaké předpoklady musí produkt splňovat. Vzhledem k tomu, že není možné certifikovat produkt, pro který neexistuje SC, je patrné, že toto certifikační schéma je podstatně rigidnější než Common Criteria. Bezpečnostní standardy jsou rozděleny do 11 kategorií – vyskytuje se zde např. kategorie pro VPN, pro zabezpečení komunikace v reálném čase nebo pro firewall.[202]

V případě, že produkt v testech obstojí, je mu udělen certifikát „*Foundation Grade*“, který potvrzuje, že takto ohodnocený produkt je v souladu s dobrou obchodní bezpečnostní praxí. Spotřebitel je tak ujištěn, že produkt bude plnit to, co výrobce slíbil (v definovaném prostředí). Tento certifikát může být získán v určitých případech i pomocí certifikace v systému Common Criteria (pokud je produkt certifikován podle CC, může získat i „*Foundation Grade*“, systémy nejsou prostupné opačným směrem).[203] Certifikát ze schématu CPA drželo ke dni 12. 10. 2019 celkem 233 kyberbezpečnostních technologií a dalších 9 bylo posuzováno (oproti 25. 12. 2018, kdy bylo certifikováno toliko 35 kyberbezpečnostních produktů, přičemž dalších 8 bylo posuzováno).[204]

V případě, že si výrobce chce nechat svůj produkt certifikovat podle schématu CPA, musí se nejdříve ujistit, že jeho produkt je vůbec způsobilý k certifikaci (ICT produkt s aktivně zabezpečovací funkcí) a že je certifikace předpokládána, tedy, že existuje oficiální bezpečnostní standard, pod který je možné produkt podřadit. Tento standard si musí výrobce zvolit. Poté kontaktuje určitou testovací laboratoř a odešle jí specifika produktu, aby zjistil její faktické možnosti určitý výrobek otestovat. V případě, že

[201] Viz Commercial Product Assurance (CPA). *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

[202] Viz Security Characteristics collection. *NCSC Site* [online]. [vid. 28. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/document/security-characteristics-collection.

[203] Viz Commercial Product Assurance (CPA). *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

[204] Viz Certified Products. *NCSC Site* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.ncsc.gov.uk/index/certified-product?f[0] = field_assurance_scheme %3A226&f[1] = field_assurance_status%3AAssured.

laboratoř shledá svoji vlastní schopnost otestování, pošle doporučující stanovisko k Národnímu centru kybernetické bezpečnosti, které následně vyhodnotí, jestli je produkt skutečně možné otestovat podle daného standardu SC. V případě kladného výsledku může pak testovací laboratoř produkt otestovat, z čehož vzejde zpráva o průběhu testu, která je opět poslána Národnímu centru kybernetické bezpečnosti. Pokud byl test úspěšný, Národní centrum kybernetické bezpečnosti udělí certifikát „*Foundation Grade*" a zpřístupní produkt veřejnosti na webových stránkách.[205] Kromě nákladů testovacích laboratoří, které musí výrobce pokrýt, si i Národní centrum kybernetické bezpečnosti účtuje 4 690 liber (certifikát podle CC je ohodnocen stejně).[206]

Oproti CC má toto certifikační schéma jednu velikou výhodu – umožňuje bezpečnostní evoluci produktu, takže se certifikát nevztahuje pouze k jedné verzi produktu, ale k celému životnímu procesu. To, že bezpečnostní aktualizace nesnižují celkovou úroveň zabezpečení produktu, hlídá Národní centrum kybernetické bezpečnosti. Certifikát CPA je platný pouze dva roky a poté je nutné ho obnovit.[207]

Nevýhodou oproti Common Criteria je již výše zmíněná rigidita a možnost použití ve většině případů pouze na území Velké Británie. Držitel certifikátu „*Foundation Grade*" však může požádat, aby jeho produkt byl zapsán do katalogů bezpečných produktů, které vede NATO i EU.[208] NATO plně respektuje záruku poskytnutou britským Národním centrem kybernetické bezpečnosti, Evropská unie však provádí sekundární posouzení jedním ze šesti (ve skutečnosti pěti, protože Velká Británie nemůže hodnotit svůj vlastní produkt) tzv. AQUA („*Appropriately Qualified*

[205] Viz Foundation Grade explained. *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/foundation-grade-explained.

[206] Viz Products and Services Scheme fees. *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/products-and-services-scheme-fees.

[207] Viz Foundation Grade explained. *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/foundation-grade-explained.

[208] Viz Commercial Product Assurance (CPA). *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

Authorities“) – orgány situované ve Švédsku, Nizozemí, Itálii, Německu, Francii a Velké Británii.[209]

6.2 FRANCIE

Francie již po delší dobu není spokojená s kyberbezpečností certifikací prováděnou v režimu Common Criteria. Francouzi nejsou spokojeni s cenou ani s délkou testování, které jsou i u nejnižší bezpečnostní úrovně mnohdy mimo dosah malých a středních podniků (a stejně tak mimo zájem velkých).[210] Zároveň (alespoň podle neveřejných zdrojů) by se chtěli vyhnout tomu, aby museli data o svých kyberbezpečnostních produktech nadále zpřístupňovat Spojeným státům americkým, jak je tomu u systému Common Criteria. To je jedna z možných motivací, které směřovaly k vytvoření jednotného evropského certifikačního systému. Doba a cena CC certifikace pak byly motivací k vytvoření schématu „*Certification Sécuritaure de Premier Niveau*“ (dále jen jako „CSPN“), a to už v roce 2008. Tento systém je opět národním schématem a aplikuje se tak pouze na území Francie bez možnosti vzájemného uznávání. Pokud ovšem podnikatel (z jakékoliv země) chce dodávat francouzské vládě zařízení přístupná přes internet (např. webkamera), je tento certifikát stanoven jako minimální bezpečnostní požadavek.[211]

CSPN má obdobný záběr a rozsah jako Common Criteria a nabízí tak podobnou úroveň důvěryhodnosti certifikačního procesu, jenž je představován tradičním modelem (nezávislý subjekt – testovací laboratoř hodnotí, jestli produkt nebo systém splňuje bezpečnostní požadavky tak, jak je výrobce nadefinoval → obdoba Security Target u Common Criteria). CSPN se ovšem poučilo z chyb ostatních certifikačních modelů a nabízí tak značně urychlený proces testování ve lhůtě 8 týdnů. Tento systém se také

[209] Pro více informací viz https://www.ncsc.gov.uk/content/files/scheme_downloads/nato_eu_process_flow_chart.pdf.

[210] Viz Certification CSPN. *ANSSI* [online]. [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/.

[211] Viz CSPN: What U.S. companies need to know about the security certification process [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process.

vypořádal s bezpečnostní evolucí produktu (ovšem trochu robustnějším způsobem než ve Velké Británii). Na nové verze systému/produktu se certifikát sice vztahovat nutně nemusí, ale systém CSPN pak umožňuje dodatečné kontinuální certifikační procesy za sníženou cenu.[212]

CSPN je zaštítěn organizací „*Agence nationale de la sécurité des systémes d'information*" (dále jen jako „ANSSI"). Ta akredituje testovací laboratoře podle úrovně technického vybavení, tedy podle toho, co ještě mohou funkčně certifikovat, a určí jim rozsah produktů, které mohou platně certifikovat. ANSSI produkuje, stejně jako v britské verzi Národní centrum kybernetické bezpečnosti, bezpečnostní standardy a hodnotící kritéria, která opět tím pádem nemohou být tak jednoduše vytvářena, jak je tomu u Common Criterií. Proces certifikace je též totožný s britskou variantou, ovšem s tím rozdílem, že výrobce či obecně žadatel musí v dokumentaci (Security Target) k produktu nadefinovat též prostředí, ve kterém se bude produkt či systém používat.[213] V případě nejasností ohledně certifikovatelnosti produktu může žadatel kontaktovat ANSSI, které mu případně pomůže i s nalezením správné testovací laboratoře. Pokud bude překročena lhůta 8 týdnů k dokončení certifikace, může ANSSI certifikaci ukončit. Aby tomuto žadatel předešel, může navrhnout upravení časového plánu testovací laboratoři, aby bylo testování co možná nejefektivnější. Po skončení certifikačního procesu, v případě pozitivního výstupu, vyplní ANSSI certifikační zprávu, ve které ohodnotí, jak odolný je produkt vůči hrozbám. Tuto zprávu pak pošle žadateli a zveřejní ji na svých internetových stránkách, pokud k tomu žadatel dá souhlas.[214]

[212] Viz Certification CSPN. *ANSSI* [online]. [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/.

[213] Jedná se tak o konkrétnější záběr oproti britské variantě, která bez dalšího počítá s obecným, ale málo rizikovým prostředím. Tento model byl pravděpodobně zvolen kvůli časové limitaci francouzského testování a tedy snaze na limitaci rozsahu testování.

[214] Viz Certification CSPN. *ANSSI* [online]. [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/; CSPN: What U.S. companies need to know about the security certification process [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process

ANSSI na svých stránkách varuje spotřebitele, že udělený certifikát ještě neznamená, že produkt je nezranitelný (což osobně považuji za krok správným směrem). Zájem o tento typ certifikátu byl v roce 2019 přibližně srovnatelný s certifikačním systémem ve Velké Británii. Ke dni 1. června 2019 vstoupilo do hodnotícího procesu celkem 320 produktů, z nichž certifikát obdrželo 141.[215]

6.3 NIZOZEMÍ

Nizozemí se k národní regulaci kyberbezpečnostní certifikace přidalo oproti Francii a Velké Británii až relativně nedávno. Pilotní fáze projektu „*Baseline Security Product Assessment*" (dále jen jako „BSPA") byla spuštěna v roce 2015, přičemž plně funkční je až od roku 2017. Certifikační schéma BSPA je spravováno nizozemskou Národní agenturou pro bezpečnost komunikací („*Nationaal Bureau voor Verbindingsbeveiliging*", dále jen jako „NLCSA"), což je orgán kybernetické obrany spadající pod nizozemskou informační a bezpečnostní službu (obdoba naší BIS). Stejně jako francouzská úprava i BSPA nabízí možnost nezávislého posouzení souladu produktu s výrobcem proklamovanými bezpečnostními požadavky (Security Target) v omezeném čase a s omezenými náklady. Ve skutečnosti byl BSPA francouzskou úpravou notně inspirován. Poptávka po této certifikační službě rychle roste, a to zejména kvůli tomu, že společnosti podnikající v nizozemském vládním sektoru musí být v souladu se standardem definovaným v „*Baseline Informatiebeveiliging Rijksdienst*" (jednoduše BIR:2017). Certifikace podle BSPA jim tak podnikání ve vládním sektoru značně zjednodušuje, neboť byla stvořena mimo jiné pro soulad s BIR:2017.[216]

Stejně jako francouzské schéma se i BSPA soustředí na hardwarová i softwarová řešení, která mají ochránit citlivé (ale ne tajné) údaje. I zde je patrné, že se jedná o řešení nabízející nižší bezpečnostní úroveň těm, pro které jsou vyšší bezpečnostní kategorie podle CC zbytečné. Obdobně jako francouzská úprava i BSPA počítá s certifikačním procesem v maximální

[215] Viz Les produits CSPN. *ANSSI* [online]. [vid. 12. říjen 2019]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/.

[216] Viz Baseline Security Product Assessment. *SECURA* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.secura.com/pathtoimg.php?id=1326&image=bspa.pdf.

délce 25 člověkodnů, v případě systému zahrnujícího kryptografické řešení maximálně 35 člověkodnů. K tomu, aby bylo tohoto cíle dosaženo, se pracuje toliko s nainstalovaným, pracujícím prototypem a úplnou dokumentací. Samotný certifikační proces je prováděn testovacími laboratořemi, nad kterými vykonává dohled NLCSA.[217]

Security Target, který je v tomto modelu označován jako „*Security Evaluation Target*" (dále jen SET), musí opět obsahovat nejen specifikaci produktu a jeho tvrzených bezpečnostních vlastností, ale zároveň i prostředí, ve kterém bude produkt používán a kým bude používán, stejně tak jako stanovení relevantních hrozeb a následných protiopatření, jejichž spolehlivost má být testována.[218] Testovací laboratoř se tak nesoustředí na situace, které pro produkt nejsou relevantní. Explicitně jsou otestovány právě ty, které nadefinuje samotný žadatel. BSPA obsahuje 8 kategorií kyberbezpečnostních produktů (např. řešení v kategorii bezpečnost sítí = VPN, v kategorii bezpečnost souborů = šifrování složek).[219]

Testovací laboratoře netestují pouze to, jestli produkt odpovídá vlastnostem nadefinovaným v SET, ale zároveň hodnotí i efektivitu použitých bezpečnostních řešení (jestli efektivně brání proti útočníkům s nízkým a středním útočným potenciálem) a nakonec i celkový účinek produktu na cílový systém (tedy jestli není firewall tak účinný, že znemožní jakékoliv připojení k internetu). Výstupem z certifikačního procesu je tzv. „*Evaluation Technical Report*" a dokument určený spotřebitelům a zákazníkům, ve kterém je po schválení výstupní dokumentace NLCSA obsaženo oficiální Prohlášení o shodě (Statement of Conformity). Toto Prohlášení informuje o souladu produktu s tvrzenými bezpečnostními vlastnostmi a požadavky a zároveň o souladu s BIR:2017.[220]

[217] Viz Baseline Security Product Assessment [online]. B.m.: SECURA. [vid. 25. prosinec 2018]

[218] Viz Baseline Security Product Assessment. In: *BlackHat Sessions* [online]. Nieuwegein, Nizozemí. 14. červen 2018 [vid. 25. prosinec 2018].

[219] Viz Baseline Security Product Assessment. *SECURA* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.secura.com/pathtoimg.php?id=1326&image=bspa.pdf.

[220] Viz tamtéž.

6.4 NĚMECKO

Poněkud zvláštní úpravu má v tomto ohledu Německo. Spolkový úřad pro informační bezpečnost (BSI) je podle zákona o BSI oprávněn provádět certifikaci kyberbezpečnostních technologií a vydávat tak tzv. Německý certifikát. Schémata se však řídí podmínkami, postupy a kritérii, která jsou zavedena v systému Common Criteria a která jsou nezbytná pro mezinárodní uznávání, ať už v režimu CCRA nebo SOGIS-MRA. BSI totiž tento systém oficiálně na Common Criteria založilo, jedná se toliko o jeho modifikovanou verzi, kdy jsou využívány např. i profily ochrany z původního systému CC. Oproti ostatním, výše zmíněným, řešením se tedy nejedná o čistě národní certifikační systém. Ohledně uznávání Německého certifikátu BSI podepsalo dohodu o uznávání certifikátů vydaných v rámci SOGIS-MRA a přistoupilo i na celosvětovou dohodu o uznávání certifikátů vydaných v rámci Common Criterií – CCRA.[221]

Německo si tak uchovalo větší dohled nad testovacími laboratořemi (v Německu je jich devět) a ve speciálních případech i produkty (může odmítnout certifikát udělit nebo uznat z důvodu veřejného zájmu). Německá vláda může vyvíjet speciální standardy a iniciativy jak na národní, tak i na evropské úrovni. Zachovala si tak několik výhod národního řešení, aniž by obětovala mezinárodní možnost uznávání certifikátů. O Německý certifikát je veliký zájem – udává se, že je uděleno více než 100 certifikátů ročně (přičemž okolo 75 % na vysokou úroveň bezpečnostní záruky).[222]

---

[221] Viz Technical information on the IT security certification of products, protection profiles and sites - BSI 7138 [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2012 [vid. 12. říjen 2019].

[222] Viz BSI – Certification. *Bundesamt für Sicherheit in der Informationstechnik* [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html; *Technical information on the IT security certification of products, protection profiles and sites – BSI 7138* [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2012 [vid. 12. říjen 2019]; WEBER, Joachim. *The German IT Security Certification Scheme* [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2017 [vid. 28. prosinec 2018].

6.5 SPOLEČNÉ VYHODNOCENÍ NÁRODNÍCH SCHÉMAT

Právě popsaná schémata obsahují určité prvky, které mezi sebou sdílejí. Z těchto prvků je možné vyvodit, jaké aspekty státům nevyhovovaly na stávajícím systému Common Criteria až do té míry, že přistoupily k vytvoření vlastních certifikačních schémat.

V první řadě je to délka certifikačního procesu a výše nákladů. To je patrné z toho, že národní schémata obsahují limitaci obou těchto prvků. Důkladný a finančně náročný certifikační proces je jistě pochopitelný a omluvitelný v případě vysokých úrovní zabezpečení a rizikovosti prostředí, ale z úpravy schémat, které jsou naformulované zejména pro málo rizikové prostředí, vyplývá, že veliká poptávka je právě po nižších bezpečnostních úrovních, které jsou určené pro „*běžné*“ situace. A na těch je skutečně systém Common Criteria až zbytečně náročný.

Za druhé je to vnitrostátní dohled a moc nad certifikací. Tyto aspekty jsou patrné ve všech zmíněných schématech, přičemž nejvíce pravděpodobně v Německém certifikátu, který modifikoval systém CC mimo jiné právě tím, že do něj vložil možnost odmítnout certifikaci nebo certifikát pro rozpor s veřejným pořádkem nebo kvůli ohrožení bezpečnosti. K tomuto problému se přidává i politické napětí a vzájemná nedůvěra mezi členy CCRA, jak bylo napsáno v podkapitole věnující se francouzskému schématu. Státy se vcelku pochopitelně nechtějí vzdát moci nad svojí vlastní bezpečností a modifikovat chyby certifikačního systému pouze po dohodě s dalšími členy se ukázalo pro některé z nich jako příliš iritující.

Za třetí je to zvládání evoluce produktu nebo služby. Toto jsem zmiňoval i v podkapitole věnující se přímo slabinám systému CC. Většina těchto schémat přišla s vlastní variantou, jak tuto slabinu odstranit – jedná se tak o další ze silných příspěvků směrem ke konstrukci Aktu o kybernetické bezpečnosti.

Posledním přínosem, který je viditelný hlavně v případě nizozemského schématu, je hodnocení účinků bezpečnostního produktu v rámci informačního systému. I to totiž odpovídá na jednu ze slabin CC, neboť ty

jsou často zaměřené až přespříliš konkrétně a ignorují celistvý obraz bezpečnostní situace.

Na závěr si dovolím ještě podotknout jednu zajímavost, které jsem si všiml u všech schémat. Úloha akreditačního orgánu, který povoluje provoz laboratoří a CAB, je v těchto schématech přidělena vždy národní verzi úřadu pro kybernetickou bezpečnost, nikoliv národní akreditační autoritě, jako je tomu v případě Common Criterií. Tuto skutečnost si vysvětluji buď touhou států vyhnout se byrokratizaci procesu zavlečením dalšího orgánu, nebo touhou po vyšší odbornosti celého procesu. Úřad pro kybernetickou bezpečnost v postavení akreditačního orgánu je sám plně odborně způsobilý posoudit naplnění kritérií, a dokonce si troufám říct, že možná i více než akreditační orgán samostatný oddělený. To usuzuji zejména z hypotetického porovnání personálních kapacit orgánu, který se zabývá pouze kyberbezpečnostní tématikou, a orgánu, který se zabývá akreditací na daleko širším poli. Tím pádem bych se v případě druhého orgánu nedivil, kdyby bylo posuzování splněných podmínek bližší spíše formálnímu pohledu. Akt o kybernetické bezpečnosti se ovšem vydal jinou cestou, jak je popsáno v následující kapitole.

7. CERTIFIKACE PODLE AKTU O KYBERNETICKÉ BEZPEČNOSTI

V této kapitole bude kriticky rozebrána institucionální, organizační i procesní stránka certifikace podle Aktu o kybernetické bezpečnosti,[223] a kde to bude vhodné, bude provedeno i srovnání s nařízením eIDAS. Na konci kapitoly ještě stručně zrekapituluji pozitiva, která Akt do certifikace kyberbezpečnostních technologií přinese.

7.1 CÍLE CERTIFIKACE A BEZPEČNOSTNÍ CÍLE SCHÉMAT

Certifikace prováděná podle Aktu by měla směřovat ke zvýšení důvěry v kybernetickou bezpečnost ICT produktů, a to prostřednictvím osvědčení, že produkty byly důsledně prověřeny a splňují určité bezpečnostní

[223] Kdykoliv je v článku zmíněn „Akt“ bez dalšího, je tím myšlena finální verze Aktu o kybernetické bezpečnosti. Zároveň kdekoliv, kde v této kapitole budu pojednávat o produktech, jsou tím myšleny i služby a procesy, jejichž certifikaci Akt upravuje také.

požadavky. Ty jsou obsaženy v certifikačních schématech a směřují k ochraně důvěrnosti, dostupnosti, autenticity a integrity dat. Certifikace ovšem neznamená, že je otestovaný produkt naprosto bezpečný, a Akt na to sám upozorňuje v bodě 77 odůvodnění Aktu. Je pravděpodobné, že toto varování by se v budoucnu mohlo vyskytovat i v textech certifikátů samotných. V tomto bodě je zřejmý vliv francouzského národního schématu, které na nemožnost absolutní garance bezpečnosti upozorňuje (viz kapitola č. 6). Cílem celé certifikace je, aby výrobci a vývojáři pozvolna akceptovali standardy „*security by design*" (kdy se zabezpečení řeší v celém životním cyklu produktu už od projektové dokumentace) a „*security by default*" (produkty by v momentě, kdy je koncoví uživatelé převezmou, měly být již v nejbezpečnějším možném nastavení, a to bez vyžadování dalších úkonů ze strany uživatele) jako normální, běžné a přirozené.[224]

Základem důvěry v bezpečnost bude kvalitní schéma, které stanovuje dostatečné pojistky proti rizikům kyberprostoru. Akt samotný stanovuje zásady, konkrétní bezpečnostní cíle a obecný rámec pro tvorbu takových schémat, jak bylo ostatně již řečeno ve čtvrté kapitole. Konkrétní postupy certifikace by měly být stanoveny v jednotlivých schématech, aby bylo možné přizpůsobit se ad hoc potřebám produktů.[225]

Bezpečnostní cíle schémat jsou uvedeny v demonstrativním výčtu v článku 51 Aktu. Každé schéma by podle něj mělo směřovat zejména k ochraně dat před zničením, ztrátou, nedostupností, pozměněním a neautorizovaným přístupem, ukládáním nebo zpracováváním. Dále by měly obsahovat pojistky, že osoby i programy se mohou dostat jen k těm částem produktu, ke kterým mají mít přístup, a že o celkovém chování produktu jsou činěné záznamy (tzv. logy aktivit). Schémata by se zároveň měla zaměřovat na kontinuální vyhledávání a dokumentaci zranitelností a s ohledem na to také obsahovat opatření zajišťující, že produkt tyto známé zranitelnosti neobsahuje.

[224] Viz body 7 až 12 a 75 až 77 odůvodnění Aktu o kybernetické bezpečnosti.

[225] Viz bod 69 odůvodnění Aktu o kybernetické bezpečnosti.

Naplnění bezpečnostních cílů bude důležité zejména pro informovanější uživatele a profesionální odběratele produktů (příp. pro státní sektor), ale pro průměrného uživatele bude mít certifikace hodnotu spíše ve větší informovanosti o bezpečnosti produktů, jejich porovnatelnosti a možnosti učinit tak lepší volbu na trhu. Akt tak v bodě 93 odůvodnění stanovuje požadavek, aby certifikáty byly psány co možná nejvíce s ohledem na znalostní úroveň průměrných uživatelů a vystavovány online. K tomu, aby uživatelé mohli certifikáty snadno najít, dokonce Akt ukládá v článku 50 povinnost ENISA, aby za tímto účelem zřídila webovou stránku, na které budou všechny potřebné informace o certifikaci, certifikátech i platných a připravovaných schématech.

7.2 ÚROVNĚ ZÁRUKY CERTIFIKÁTŮ

Stejně jako systém Common Criteria poskytuje uživatelům možnost různé úrovně záruky za bezpečnost certifikovaného produktu (EAL), který vyjadřuje, jak náročnými testy produkt prošel a jakým hrozbám by měl být schopen čelit, zavádí úrovně záruky bezpečnosti i Akt. Oproti Common Criteria (celkem sedm) zavádí úrovně jenom tři, a to základní, významnou a vysokou.[226] V rámci každého schématu bude upraveno, na jakou úroveň záruky je umožněno produkty podle tohoto schématu certifikovat. Minimálně by tedy každé schéma mělo obsahovat jednu libovolnou úroveň, mohou však být obsaženy i všechny tři.[227] Při zahrnování úrovní do schématu by se mělo postupovat dle hodnocení rizik pro daný produkt. Stejně by mělo být postupováno i při samotném certifikování, vývojáři

[226] Takto byly úrovně přeloženy již v červencové (2018) verzi Aktu. Může se zdát trochu zbytečné, aby bezpečnostní úrovně záruk v nařízení eIDAS byly „nízká, značná a vysoká" a v Aktu „základní, významná a vysoká", když faktická bezpečnostní záruka je obdobná.

[227] V článku 54 anglické verze Aktu je formulován požadavek, aby schéma obsahovalo alespoň jednu bezpečnostní úroveň, (cituji) „*pokud je to možné*". V české verzi je tento požadavek stanoven takto: „ v *příslušných případech*". Toto považuji za velice nešťastně zvolenou formulaci, neboť v každém případě by ve schématu měla být uvedena alespoň jedna úroveň. Není znám případ, kdy by schéma nemělo obsahovat bezpečnostní úroveň, ani taková situace nedává smysl. Nad tímto se pozastavili i právní lingvisté v rámci překladu Aktu do dalších jazyků. Podle informací, které jsem měl tou dobou k dispozici po konzultacích s odborníky z prostředí Komise a Rady EU, mělo dojít k odstranění tohoto problému při překladu, leč „v příslušných případech" neshledávám jako vyřešení této nejasnosti.

a výrobci by tak před zahájením certifikačního procesu měli zhodnotit rizika, která mohou hrozit konkrétně jejich produktu, a podle výsledků se rozhodnout pro určitou úroveň záruky certifikátu. Jenom certifikát může být udělen na jakoukoliv úroveň záruky, vlastní posouzení je možné provést jen a pouze k základní úrovni záruky.[228]

Základní úroveň záruky jako taková proklamuje schopnost produktu odolat naprosto základním kybernetickým incidentům a útokům. Opatření, která takový produkt zavádí, by měla být snadno a dostatečně kontrolovatelná pouhou revizí technické dokumentace (případně obdobného testu, pokud ze své podstaty není revize dokumentace možná), tedy bez faktického testování produktu samotného. Tato úroveň je tedy určena do prostředí, kde se vyskytují buď jen základní rizika s minimálním dopadem, nebo je výskyt závažných rizik s nebezpečným dopadem vysoce nepravděpodobný. Významná úroveň záruky uživatele informuje o tom, že produkt neobsahuje známé zranitelnosti, riziko výskytu známého kybernetického incidentu je minimální a produkt je schopen odolat kybernetickým útokům ze strany aktérů s limitovanými zdroji anebo schopnostmi. Posuzování na tuto úroveň sestává z testů známých zranitelností (a zda jim produkt nepodlehne) a faktického testování dostatečné implementace nezbytných bezpečnostních opatření. Nejzajímavější v Aktu je úroveň vysoká. Ta osvědčuje, že produkt obsahuje dostatečná bezpečnostní řešení a prošel natolik důkladným testováním, že *„minimalizuje riziko výskytu kybernetických útoků využívajících nejmodernějších technologií („state-of-the-art cyber attacks“) provedených aktéry, kteří vládnou značnými zdroji a znalostmi.“*[229] Ve starší verzi návrhu byl v odůvodnění[230] uveden jako příklad takového útočníka financovaný multidisciplinární tým. Testování by mělo být prováděno alespoň formou penetračního testování a je nutné ověřit implementaci nejmodernějších

[228] Viz body 78 a 79 odůvodnění a článek 52 Aktu o kybernetické bezpečnosti.

[229] Viz článek 52 Aktu o kybernetické bezpečnosti.

[230] Viz bod 56b odůvodnění návrhu Aktu o kybernetické bezpečnosti, verze z července 2018.

bezpečnostních opatření, která mají proti takovým útokům produkt chránit.[231]

Jednotlivá schémata pak mohou nadefinovat několik různých úrovní testování produktů, která se budou lišit v přísnosti, důkladnosti a užité metodologii. Každá z testovacích úrovní by však měla odpovídat jedné z úrovní záruky. Schéma může zároveň ve speciálních případech specifikovat, že k vydání certifikátů je příslušná jenom národní autorita pro certifikaci kybernetické bezpečnosti nebo veřejnoprávní orgány akreditované na pozici subjektů posuzování shody (certifikačních těles).[232] V případě, kdy schéma vyžaduje certifikaci na vysoké úrovni záruky, je takový postup dokonce přikázaný a i zmíněné veřejnoprávní akreditované subjekty mohou certifikaci provést jen tehdy, pokud jim to povolí národní autorita pro certifikaci kybernetické bezpečnosti (případně takový orgán a priori deleguje svou pravomoc).[233]

7.3 ORGANIZAČNÍ STRUKTURA

Správa celého evropského certifikačního rámce byla primárně svěřena ENISA (dále také jako „Agentura“) ve spolupráci s Komisí. Akt je v tomto ohledu dle mého názoru trochu nerealistický, neboť faktický rozsah povinností, které uložil Agentuře, je nezměrný.

7.3.1 ENISA

Agentura je pověřená permanentním monitoringem kyberbezpečnostní situace v Evropě, stavu na trhu s kyberbezpečnostními technologiemi a vývoje v ohledu standardizace a dalších technických norem. Výstupy z tohoto monitoringu mají být zohledněny při tvorbě nových schémat, což je další velká povinnost, kterou Agentura obdržela. Na žádost (proces přípravy schémat bude rozebrán níže) musí totiž připravit návrh schématu, který je pak schválen Komisí. Dále musí Agentura vyhodnocovat fungování a účinky již schválených schémat, aby bylo v případě nutnosti možné

[231] Viz body 87 až 90 odůvodnění a článek 52 Aktu o kybernetické bezpečnosti.

[232] Viz články 52, 54 a 58 Aktu o kybernetické bezpečnosti.

[233] Viz bod 87 odůvodnění Aktu o kybernetické bezpečnosti.

nefunkční schémata upravit. Tyto revize je ENISA povinna u každého schématu udělat alespoň jednou za pět let. Rovněž je povinna zprovoznit a udržovat internetovou stránku věnovanou certifikaci, evropským certifikačním schématům platným, připravovaným, navrhnutým i zamítnutým, informacím o dotčených národních schématech i samotných certifikátech.[234]

K tomu, aby usnadnila provádění certifikací a přípravu vývojářů na ni, je povinna vytvářet a publikovat návody, výkladové materiály k bezpečnostním požadavkům a metodické manuály k zavedení osvědčené praxe ohledně certifikovaných skutečností. Agentura musí poskytovat i poradní a konzultační služby, primárně ostatním subjektům podílejícím se na vytváření schémat, ale zároveň i certifikačním tělesům, koncovým uživatelům či členským státům v ohledu certifikace.[235]

Akt sice obsahuje zvýšení ekonomických i personálních kapacit Agentury, ale dle mého názoru je zvýšení neproporcionální s množstvím povinností, které jí byly přiděleny.[236] Osobně bych očekával, že až bude certifikační rámec spuštěn, bude buď alespoň zpočátku docházet k velkým prostojům a dlouhým čekacím dobám, nebo bude většina práce „outsourcována" na ad hoc pracovní skupiny, případně bude docházet pouze k přejímání již hotové práce. Ale až praxe ukáže, jestli jsou tyto obavy oprávněné.

Minulé verze Aktu, včetně debat v rámci trialogu, obsahovaly možnost rozdělit povinnosti Agentury mezi další subjekty (např. nechat i Skupině zúčastněných stran pro certifikaci možnost připravovat návrhy schémat). V případě, že by vydání schématu stále předcházel víceúrovňový

[234] Viz články 7, 8, 39 a 48 až 50 Aktu o kybernetické bezpečnosti.

[235] Viz body 26 až 42 odůvodnění a články 48 až 50 Aktu o kybernetické bezpečnosti.

[236] Ke konci roku 2018 bylo v ENISA zaměstnáno 70 zaměstnanců (viz Annual Activity Report 2018 [online]. Řecko: European Union Agency for Cybersecurity, 2018, s. 57 [vid. 12. říjen 2019]). Do pěti let mají personální kapacity narůst o 50 % a finanční kapacity se zdvojnásobit (na 23 mil EUR, viz Questions and Answers - EU Cybersecurity. *European Commission* [online]. [vid. 12. říjen 2019]. Získáno z: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369). Toto navýšení Agentuře tedy jistě pomůže, ale jenom náročnost udržování a vytváření certifikačního rámce dle mého názoru dalece přesahuje toto navýšení.

konzultační proces, jak je nyní nastaveno, mohlo by se možná jednat o stejně bezpečné řešení, jenom efektivnější, ale byl zvolen princip ad hoc pracovních skupin.

7.3.2 EVROPSKÁ KOMISE

Komise je nejvyšším orgánem, který zaštiťuje celý certifikační aparát. Komisi vznikne v souvislosti se spuštěním certifikačního rámce povinnost zpracovat, přijmout a zveřejnit do 28. června 2020 Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (dále jen jako „Program"), ve kterém budou vymezeny strategie a cíle evropské kyberbezpečnostní certifikace. Primárně bude Program obsahovat seznam produktů, pro které je nutné/potřebné/vhodné vytvořit schéma. Na seznam se produkt může dostat z několika důvodů – existuje-li pro kategorii produktů národní schéma a hrozí kvůli tomu fragmentace trhu; pokud tak stanoví právní předpis Unie nebo je to z důvodu jejího směřování a politik vhodné; existuje po takovém schématu dostatečná poptávka na trhu; vyžaduje si to vývoj v oblasti kybernetické bezpečnosti, anebo pokud si přípravu schématu vyžádá Evropská skupina pro certifikaci kybernetické bezpečnosti (dále jen jako „Skupina").[237]

V souladu s Programem může Komise podávat žádosti Agentuře, aby připravila návrh schématu nebo provedla revizi již stávajícího. Ve výjimečných situacích může Komise (a v tomto případě i Skupina) požádat Agenturu, aby návrh připravila, dokonce i když takové schéma/postup není uveden v Programu, přičemž v takové situaci je pak nutné Program aktualizovat. Komise je nadána pravomocí přijímat schémata připravená Agenturou, a to ve formě implementačních aktů.[238]

Přestože je certifikace obecně dobrovolná a ponechána tedy v rozhodovací kompetenci členských států, jestli neučiní některé schéma obligatorním pro povinné subjekty, Komise je pověřena průběžným vyhodnocováním funkčnosti a užívání schémat, jejich celkového účinku na bezpečnost v Unii a zjištěním, zdali by neměla být určitá schémata přijata

[237] Viz článek 47 Aktu o kybernetické bezpečnosti.

[238] Viz článek 48 a 49 Aktu o kybernetické bezpečnosti.

jako povinná pro celou Unii. Při tomto hodnocení však musí dbát zejména na to, jaký by takový krok měl vliv na jednotný trh a dostupnost produktů.[239]

Evropská komise je zároveň, ve spolupráci s Agenturou a Skupinou, nadána pravomocí vstoupit do jednání s dalšími mezinárodními subjekty o uzavření dohod o vzájemném uznávání evropských certifikátů (MRA).[240]

7.3.3 PORADNÍ SKUPINA ENISA A SKUPINA ZÚČASTNĚNÝCH STRAN PRO CERTIFIKACI

Aby ENISA zůstala při svých aktivitách v kontaktu s okolním světem, vytvoří čl. 21 Aktu tzv. Poradní skupinu ENISA, která má být složena ze zástupců průmyslu (ICT odvětví), poskytovatelů služeb internetové společnosti, malých a středních podniků, správců informačních infrastruktur, spotřebitelů i akademické půdy. Součástí poradní skupiny by měly být i policejní složky a orgány dohledu nad ochranou osobních údajů. Poradní skupina radí a pomáhá tak Agentuře při naplňování jejích povinností v odborných otázkách. Její působnost se však nevztahuje na otázky ohledně certifikace. V této oblasti zastává poradní funkci Skupina zúčastněných stran pro certifikaci, která bude vytvořena podle čl. 22 Aktu. Jejími členy budou přední experti relevantních zúčastněných stran. Kromě poradní funkce ohledně certifikačního rámce má ještě za úkol na žádost poskytnout rady při formování nových schémat a standardizace, asistovat při tvorbě Programu (a zároveň má právo se k němu vyjádřit, přičemž názor této skupiny musí být vzat v potaz) a v naléhavých případech zpravit Komisi a Skupinu o potřebě vytvořit jiné schéma, než jaké je zahrnuté v Programu. Tento orgán má čistě poradní funkci, je nutné neplést ho se Skupinou (Evropská skupina pro certifikaci kybernetické bezpečnosti).[241]

V minulých verzích Aktu měly mít zúčastněné strany daleko vyšší pravomoci, ovšem v prvotním návrhu Komise se s nimi, kromě čistě

[239] Viz článek 56 Aktu o kybernetické bezpečnosti.

[240] Viz bod 105 odůvodnění Aktu o kybernetické bezpečnosti.

[241] Viz články 21 a 22 Aktu o kybernetické bezpečnosti.

konzultační role, vůbec nepočítalo. Je tak patrný vliv velice nesouhlasné reakce zúčastněných stran, která přišla po zveřejnění první verze Aktu.

7.3.4 EVROPSKÁ SKUPINA PRO CERTIFIKACI KYBERNETICKÉ BEZPEČNOSTI

Skupina je orgán ustavený v čl. 62 Aktu. Jeho název se v průběhu legislativního procesu vcelku dost měnil.[242] Jedná se o uskupení složené ze zástupců vnitrostátní orgány certifikace kybernetické bezpečnosti (dále jen jako „NCCA" z angl. „*National cybersecurity certification authorities*"), případně dalších relevantních vnitrostátních autorit. Jedná se o pomocný orgán, který má pomáhat Agentuře v naplňování a implementaci certifikačních aktivit po celé Unii, udržení konzistence implementace, koordinaci vnitrostátních politik a pomoc při přípravě schémat, přičemž Skupina je oprávněna přijmout názor k chystanému schématu, který sice není závazný, ale Agentura se s ním musí vypořádat. Skupina má právo ve zvláště odůvodněných případech požádat Agenturu o vytvoření schématu i mimo Program. Agentura je, oproti žádosti od Komise, které musí vyhovět, oprávněna tuto žádost zamítnout, ale musí takový svůj postup řádně odůvodnit.[243]

Skupina má dále usnadňovat kooperaci mezi jednotlivými NCCA, zajišťovat výměnu informací a osvědčených praktik, prozkoumávat vývoj, který se odehrává na poli kybernetické bezpečnosti a zajišťovat soulad mezi schématy a mezinárodními certifikáty. V případě úkolu posledně zmíněného je dokonce oprávněna navrhnout Agentuře zahájení jednání s příslušnou mezinárodní organizací o vyplnění úpravy a odstranění nedokonalostí. Skupina by též měla hrát významnou roli při sjednávání a zprostředkování vzájemného hodnocení, kterému budou podrobeny NCCA.[244]

Co se týká vzájemného hodnocení a křížového posuzování NCCA, jedná se o problematiku, která by mohla být Aktem upravena podstatně lépe.

[242] Např. ve verzi z července roku 2018 byla Skupina nazvána jako Skupina členských států pro certifikaci kybernetické bezpečnosti.

[243] Viz článek 48 a 62 Aktu o kybernetické bezpečnosti.

[244] Viz článek 59 a 62 Aktu o kybernetické bezpečnosti.

Obsahuje totiž několik mezer, které jsou vcelku zásadní. V rámci hodnotícího procesu např. není moc dobře upravena situace, kdy bude zjištěno, že certifikát byl vydán v rozporu s Aktem nebo schématem. Případně postup, který bude následovat poté, co se NCCA v rámci vzájemného hodnocení neshodnou. Tato část bohužel nebyla oproti prosincové finální verzi dotvořena.

7.3.5 VNITROSTÁTNÍ ORGÁNY CERTIFIKACE KYBERNETICKÉ BEZPEČNOSTI

NCCA je vnitrostátní orgán určený členským státem k výkonu dozorčí funkce nad dodržováním povinností plynoucích z tohoto nařízení pro subjekty na jeho území (subjekty posuzování shody i ostatní tržní subjekty). Členský stát může určit více než jeden NCCA nebo se domluvit s jiným členským státem na ustavení společného. Ať už členské státy rozhodnou jakkoliv, musí informovat Komisi o identitě tohoto orgánu a v případě, kdy je orgánů více, také o rozdělení jejich pravomocí. Je možné, aby byla tato role přisouzena i již existujícímu orgánu, což bude patrně situace ve většině členských států.[245]

Od NCCA je v některých případech vyžadováno též vydávání certifikátů a provádění hodnocení produktů, a proto by měly být vybavené dostatečnými kapacitami (nebo mít možnost přenést toto posuzování na veřejnoprávní CAB). Zároveň je však nutné poskytnout záruky, aby bylo posuzování produktů důsledně odděleno od výkonu dozorčí funkce. Vzhledem k tomu, že NCCA budou často orgánem členského státu, je nezbytné poskytnout záruky, aby byl nadán dostatečnou nezávislostí na ostatních složkách státní moci, jinak by dohled nad certifikací prováděnou směrem ke státnímu sektoru nebylo možné nezávisle vykonávat.[246]

Členské státy by měly zajistit, aby byly NCCA nadány dostatečnými pravomocemi a zdroji k efektivnímu a účinnému výkonu dozoru. Tento dozor se vztahuje na implementaci a vynucování případných budoucích povinných schémat; na subjekty posuzování shody (soukromoprávní

[245] Viz článek 58 Aktu o kybernetické bezpečnosti.

[246] Viz tamtéž.

i veřejnoprávní), kde NCCA aktivně spolupracují s akreditačními autoritami; a na výrobce a poskytovatele služeb, pokud provádějí vlastní posouzení shody. Mezi další úkoly patří mimo jiné i příjem a vyřizování stížností vzešlých buď z certifikačního procesu provedeného NCCA samotnou, nebo provedeného veřejnoprávním subjektem posuzování shody při certifikaci na vysokou úroveň záruky. V případě, že pokynů NCCA nebude v jakémkoliv ohledu uposlechnuto, měla by být nadána pravomocí ukládat pokuty, jejichž výši mají nadefinovat členské státy tak, aby byly přiměřené, ale účinné.[247] To by v praxi mohlo činit problémy s usazováním subjektů ve státech s nižšími pokutami, neboť pokud mají být pokuty přiměřené, tak by měly vycházet alespoň přibližně z parity kupní síly v daném státě. V tomto by mohly vzniknout rozdíly mezi státy východní Evropy a zbytkem Evropy. A pokud mají být pokuty účinné, tak se zase západ nemůže přizpůsobovat ekonomicky slabšímu východu. Ovšem záleží i na celkové výši pokut, jestli budou natolik citelné pro subjekty, že by kvůli tomu docházelo k většímu stěhování.

Všechny NCCA by měly úzce spolupracovat, koordinovat své postupy, metody a politiky a zároveň podléhat vzájemnému hodnocení („*peer review*“), aby bylo docíleno jednotného standardu při vydávání certifikátů a dohledu nad certifikačními aktivitami. Hodnocení bude probíhat na základě předem upravené a pravděpodobně jednotné metodiky[248] a bude se soustřeďovat na organizační, personální a procesuální řešení hodnotícího procesu, bezpečnostní řešení důvěrnosti informací a efektivitu vyřizování stížností. Zároveň se pak budou hodnotit i autorizované certifikáty, které by v případě nalezení neshod v certifikačním procesu mohly být staženy.[249] Otázkou zůstává, jak se bude postupovat v případě, že by se jednalo o certifikát autorizovaný spoluprací dvou a více certifikačních těles a chyba v procesu by byla nalezena pouze u jedné z nich. Já osobně zastávám názor, že by certifikát nadále zůstával potvrzením dané úrovně zabezpečení, protože by ho stále jedna z certifikačních autorit ověřila

[247] Viz článek 65 Aktu o kybernetické bezpečnosti.

[248] Jedná se o domněnku autora, Akt toto neupravuje.

[249] Viz článek 59 Aktu o kybernetické bezpečnosti. Připomínám ovšem, že tento proces není dostatečně upraven a představuje značnou slabinu Aktu.

platným způsobem. Tím pádem by nemuselo být potřeba jej z pragmatického hlediska rušit. Pádný argument ovšem nabízí i opačné řešení – porušení pravidel vydání certifikátu stanovených schématem samo o sobě vybízí ke stažení certifikátu a opačný postup posiluje možnost diskrece ohledně osudu certifikátů na velice nejistou úroveň.[250]

Provádět toto hodnocení budou alespoň dvě další NCCA z jiných členských států, přičemž každá NCCA musí být předmětem vzájemného hodnocení alespoň jednou za pět let.[251] To, jak se budou NCCA vybírat, příp. podle jakého klíče, není upravené. Dle mého názoru by mohla v tomto ohledu významně pomoci Skupina. K založení dalších pravomocí Skupiny by však bylo nutné zakomponovat takové pravomoci přímo do Aktu, což se nestalo.

Na rozdíl od CAB ovšem Akt neobsahuje konkrétnější podmínky k provozu NCCA. Původně měly být uvedeny v Příloze, ale odtud byly nakonec vyškrtnuty bez náhrady. To může představovat problém pro udržení jednotného standardu kvality mezi jednotlivými NCCA.

Zároveň je v Aktu uvedeno, že za jednání NCCA jsou odpovědné členské státy. To je sice vcelku pochopitelné, i nařízení eIDAS obsahuje podobnou úpravu, tato odpovědnost je ale v případě Aktu naformulována příliš obecně. Není patrné, jestli členské státy v případě vadného certifikátu odpovídají za skutečnou škodu, která vznikne na základě toho, že se produkt nechoval tak, jak podle certifikátu měl, nebo odpovídají i jen za pouhou skutečnost, že certifikát je vadný, aniž by vznikla reálná škoda.[252]

7.3.6 SUBJEKTY POSUZOVÁNÍ SHODY

Subjektem posuzování shody je myšlen „*subjekt, který vykonává činnosti prokazující, že byly splněny konkrétní požadavky týkající se výrobku, postupu,*

[250] Jak je vidět, bylo by třeba tuto mezeru napravit, protože obě možnosti přístupu jsou odůvodněné, jedna opírající se o formální stránku certifikátu, druhá o materiální.

[251] Co se týká procesu „*peer review*“, bylo by možné se inspirovat i v již fungujícím systému eIDAS, kde tento systém též funguje.

[252] Nařízení eIDAS obsahuje úpravu odpovědnosti za potenciální škodu, nutí tak členské státy k větší opatrnosti. Dle mého nepříliš vyhraněného názoru by však potenciální škoda např. u formálních vad certifikátů mohla být až příliš přísná a místo toho by stačila odpovědnost za skutečnou škodu.

služby, systému, osoby nebo subjektu (v případě Aktu je relevantní pouze výrobek, proces nebo služba), včetně kalibrace, zkoušení, certifikace a inspekce“.[253] K samotnému posuzování shody je nezbytná akreditace, která bude rozebrána níže. Jako subjekt posuzování shody může (a měl by) být akreditován i certifikační orgán, který je součástí NCCA, neboť je v některých případech vyžadováno, aby byla certifikace prováděna přímo NCCA. Pokud evropské certifikační schéma stanoví speciální požadavky na certifikační těleso, provádět certifikaci podle takového schématu může jen subjekt posuzování shody, který byl pro naplnění speciálních podmínek k takové certifikaci autorizován od NCCA. U každého takového schématu musí NCCA zpravit Komisi o všech autorizovaných subjektech posuzování shody.[254]

Akt se ve své úpravě soustředí na certifikační autority a odpovědnost za testovací laboratoře a úpravu vztahu mezi dvěma zmíněnými přenáší na certifikační těleso. To však stvořilo vcelku závažný problém – chybí institucionální požadavky na testovací laboratoře, včetně požadavku na umístění. Sídlo sice CAB musí mít v rámci Unie, ale o tom, kde jsou umístěné jeho laboratoře, Akt nepojednává. Je pochopitelné, že při testování produktů, které mají zabezpečovat kybernetickou bezpečnost ve členských státech, nebude žádoucí posílat tyto produkty na otestování např. do Číny nebo do Ruska. Akt ve své momentální podobě ovšem nenabízí mechanismus, jak tomuto předejít. Tato mezera nebyla vyřešena, je možné ji zhojit ještě nepřímo (např. v jednotlivých schématech).

Požadavky na provoz subjektu posuzování shody jsou upraveny v příloze k Aktu. Zprvu se musí jednat o subjekt mající právní subjektivitu a zřízený v souladu s vnitrostátním právem. Může se však jednat i o státní subjekty nebo korporace a profesní sdružení reprezentující výrobce a podnikatele v oblasti vývoje, výroby a dalšího nakládání s ICT produkty. Jediné, co musí být splněno v takových případech, je zaručení absolutní nezávislosti (a to i na úrovni vrcholného managementu), neboť subjekt

[253] Viz čl. 2 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

[254] Viz článek 60 a 61 Aktu o kybernetické bezpečnosti.

posuzování shody musí být vždy nezávislý na žadateli, jehož produkty posuzuje. Pokud by tedy takové těleso posuzovalo produkt, nesmí být v žádném ohledu spojeno s produktem – nesmí být ani dodavatelem, ani vlastníkem, ani investorem. Vždy musí být zaručena plná svoboda úsudku při posuzování produktu.

Celý model nezávislosti stojí dle mého názoru na bodu 8 přílohy k Aktu, který (mimo jiné) stanovuje, že jak subjekty posuzování shody, tak jejich personál by měly posuzování provádět prosty jakýchkoliv nátlaků a vlivů, včetně finanční závislosti, které by mohly ovlivnit výsledek posuzování. To je ustanovení, které považuji více za vroucí přání než skutečné pravidlo. Subjekty posuzování shody budou často komerčního charakteru a finance budou tedy získávat zejména z provádění certifikačních testů. Je tím pádem možné, že se CAB budou snažit provádět testování tak, aby nepřišly o zákazníky. Případně mohou žadatelé o certifikaci nechat CAB „*vyhladovět*" (buď za trest za neudělený certifikát, nebo jako motivaci pro budoucí udělení certifikátu). A možnost ekonomického „*hladovění*" certifikačních těles a jejich touhy nepřijít o zákazníky očekávám daleko silnější právě na menších trzích, které nebudou nabízet takovou soutěž mezi žadateli o certifikaci. To by pak vedlo k ohybání trhu, snížení důvěry v certifikáty a jiné nežádoucí efekty. Proto by tyto situace měly být kontrovány právě procedurami vzájemného hodnocení a revokacemi vadných certifikátů.

Co se týká úrovně technologického vybavení CAB, příloha formuluje požadavek, aby CAB byly schopné provést všechny certifikační úkony, které jim ukládá Akt. To je, dle mého názoru, další poněkud nešťastná formulace. Neznamená totiž, že všechny CAB mají vládnout kapacitami k provozování všech schémat, ale jen těch, které se samotné CAB rozhodne provozovat. Základní myšlenkou tohoto ustanovení bylo, že všechny CAB by z důvodu stejné základní bezpečnostní úrovně měly mít stejné základní vybavení, speciální požadavky by byly nadefinovány až v jednotlivých schématech. Je zde samozřejmě nebezpečí, že si trh skrz toto ustanovení rozdělí např. německé a francouzské CAB, které již potřebné vybavení mají, ale je opět otázkou budoucnosti, jestli bude tato obava naplněna. Mezi onu zmíněnou základní úroveň tedy patří nezbytný a dostatečně zkušený personál,

technologické vybavení, popisy všech hodnotících procedur (k zajištění transparentnosti), plány a politiky k přizpůsobení posuzovacího procesu velikosti žadatele (v případech právnických osob, nikoliv fyzických). Náročnost i jen základní úrovně těchto požadavků je tedy značná.

Příloha specifikuje i požadavky na personál subjektů posuzujících shodu – dostatečné odborné technické znalosti pokrývající celou materii posuzovacích aktivit, znalost bezpečnostních požadavků certifikačních schémat, přiměřenou znalost použitelných testovacích standardů a technických požadavků a schopnost odpovídajícího zaznamenávání celého certifikačního procesu, stejně tak jako schopnost vyhotovit certifikáty samotné. Jak je patrné z prvních dvou kapitol, český pracovní trh není pracovní silou, která by podobné kvalifikace splňovala, zrovna přeplněn, a tak se i tato část podmínek k vytvoření subjektu posuzování shody může ukázat pro český trh jako problematická.

Stejně jako v případě CC i Akt klade subjektům posuzování shody povinnost opatřit si certifikát podle příslušného standardu pro provoz certifikačních těles, tedy např. mezinárodní standard ISO/IEC 17065 v aktuálním znění, a zároveň jsou CAB povinny zajistit, aby odpovídající certifikát vlastnily i využívané testovací laboratoře – např. ISO/IEC 17025 v aktuálním znění. Je možné využít i jiný standard, který zajistí podobnou úroveň certifikace a testování.[255]

7.3.7 NÁRODNÍ AKREDITAČNÍ ORGÁN

Národní akreditační orgán je „*orgánem, který na základě státem delegované pravomoci v daném státě osvědčuje, že subjekt posuzování shody splňuje požadavky pro provádění konkrétních činností posuzování shody, které stanoví harmonizované normy (…).*“[256] V případě Aktu se jedná o požadavky, o kterých jsem pojednával v přechozí podkapitole. Akreditace by měla být udělována na maximální dobu 5 let a může být opakovaně udělena znovu. Akreditační orgány mohou udělenou akreditaci omezit, pozastavit její

[255] Viz body 19 a 20 Přílohy k Aktu o kybernetické bezpečnosti.

[256] Viz čl. 2 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

účinnost, nebo ji úplně odebrat, pokud subjekt posuzování shody přestane splňovat podmínky pro udělení akreditace a tento stav ani dodatečně nenapraví (případně hrubě porušuje povinnosti stanovené v Aktu). V českém prostředí je národním akreditačním orgánem Český institut pro akreditaci, o.p.s.[257]

7.3.8 KAPACITY PRO POSUZOVÁNÍ SHODY V ČR

V České republice sice s obecnou certifikací kyberbezpečnostních technologií zkušenosti zatím chybí, ovšem začaly přípravy struktur pro vytvoření vlastního CAB, k čemuž je možné využívat zkušeností z již existujících oblastí (mimo jiné eIDAS). Česká republika již také není prosta technických kapacit (soustředících se zejména na univerzitách), které jsou momentálně využívány k certifikacím pro zahraniční certifikační autority. Je proto možné, alespoň částečně, odhadnout, jak bude systém na území ČR vypadat. Podle zákona č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh, by se NCCA dalo pravděpodobně přirovnat k úloze, kterou zastává Úřad pro technickou normalizaci, meteorologii a státní zkušebnictví (dále jen „Úřad“), přičemž všechny činnosti související s tvorbou, vydáváním a distribucí technických norem (mezi které patří i standard ČSN EN ISO/IEC 27001) přešly k 1. 1. 2018 na Českou agenturu pro standardizaci.[258] Subjekty pro posuzování shody v tomto modelu posuzují shodu výrobků s technickými normami, které vydává vláda, systém tudíž není natolik rozdílný od chystaného Rámce. Podobně jako NCCA i Úřad autorizuje subjekty pro posuzování shody u vybraných produktů, u kterých je zapotřebí naplnění dalších požadavků k posuzování. Mezi autorizované subjekty patří mimo jiné TÜV SÜD Czech s. r. o. (pobočka zmíněného německého elektrotechnického standardizačního gigantu), Strojírenský zkušební ústav, s. p., či Institut pro testování a certifikaci, a.s.[259] Celkem existuje na území ČR přibližně 1200 akreditovaných subjektů pro posuzování shody a přibližně 50

[257] Viz Český institut pro akreditaci, o.p.s. *ČIA - Národní akreditační orgán* [online]. [vid. 20. leden 2019]. Získáno z: http://www.cia.cz/.

[258] Viz O Úřadu - ÚNMZ [online]. [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/o-uradu.

autorizovaných. Zákon o posuzování shody výrobků při jejich dodávání na trh uvádí ještě speciální kategorii subjektů, a to tzv. notifikované subjekty, které mají přesah do EU. Ty Úřad oznamuje Komisi a zavádí je do systému NANDO.[260]

Příkladem kvalitativně jiného subjektu pro posuzování shody je Elektrotechnický zkušební ústav, který byl prvním z momentálně tří CAB, které jsou akreditovány k provádění certifikace podle nařízení eIDAS. [261,262]

Pozici NCCA v ČR pravděpodobně zaujme Národní úřad pro kybernetickou a informační bezpečnost, akreditační orgán by se měnit neměl, neboť je jím i v případě nařízení eIDAS Český institut pro akreditaci, a v případě subjektů pro posuzování shody je možné, že vznikne sdružení ze stávajících certifikačních těles založený na bázi akademického spin-off, které dokáže vyhovět přísným požadavkům Aktu.

7.4 CERTIFIKAČNÍ PROCES

Celý certifikační proces je rozdělen na dvě fáze. První fází je tvoření certifikačních schémat, druhou certifikační proces samotný (případně provedený formou vlastního posouzení) a udělení certifikátu.

7.4.1 TVORBA SCHÉMAT

Tvoření schémat začíná na úrovni Komise, a to formulováním Programu.[263] Na vytváření programu má Komise úzce spolupracovat se Skupinou zúčastněných stran pro certifikaci a Skupinou. Program musí být průběžně aktualizován, nejdéle jednou za tři roky (zpočátku to ovšem bude pravděpodobně mnohem častěji, nebo bude docházet primárně

[259] Viz Vybrané výrobky - ÚNMZ [online]. [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/vybrane-vyrobky.

[260] Viz GUEBEL, Martine. *NANDO Information System (Europa)* [online]. [vid. 5. únor 2019]

[261] Nařízení eIDAS ovšem neobsahuje jednotlivá konkrétní certifikační schémata, požadavky na akreditované kvalifikované poskytovatele služeb jsou formulovány obecně.

[262] Viz Seznam akreditovaných subjektů pro posuzování shody podle nařízení eIDAS platný ke dni 5. 2. 2019. *European Commission - Futurium: eIDAS Observatory* [online]. [vid. 28. únor 2019]. Získáno z: https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accredited_cabs-2019-02-05.pdf.

[263] Program nebude mít právně závaznou formu.

k mimořádným žádostem o tvorbu schémat). Hlavním smyslem Programu je stanovení strategických cílů Unie v oblasti certifikace transparentním a veřejným způsobem tak, aby se všechny zúčastněné strany mohly na nástup schémat připravit. Pro tento účel by měl být součástí Programu i časový plán/odhad předkládání žádostí o vytvoření schémat.[264]

Program je obecně potřeba k tomu, aby mohla Komise požádat Agenturu k vytvoření návrhu schématu, které je uvedené v Programu.[265] Ve speciálních a zvláště odůvodněných případech[266] však může Agenturu požádat Komise i Skupina k vytvoření návrhu schématu, které není upraveno v Programu.[267] Agentura může s odůvodněním odmítnout žádost o vytvoření schématu, kterou jí předloží Skupina, není však oprávněna odmítnout žádost Komise.[268]

Komise by měla před podáním žádosti dobře zvážit účinky schématu na trh, na inovační postup, na malé a střední podniky a na konečné uživatele. Jakmile Agentura obdrží žádost, začne s přípravou schématu. V procesu přípravy schémat podle Programu by měly proběhnout konzultace se všemi podstatnými zúčastněnými stranami. Dokonce chce Agentura (jedná se o její dobrovolný krok) do konzultačního procesu zavést i veřejné konzultace, které budou přístupné komukoliv (což považuji za velice nerozumné řešení, které bude mít za následek jenom další časové prodloužení procesu tvorby schémat). Z úpravy je patrné, že při „neprogramové“ přípravě schémat se počítá s potřebou urychleného přípravného procesu, neboť do něj nejsou konzultace se zúčastněnými stranami zapojené (zůstávají ovšem dobrovolné a Agentura se možná

[264] Viz článek 47 Aktu o kybernetické bezpečnosti.

[265] Ještě v červencové verzi Aktu byl přímo v článcích zahrnut požadavek na obsah žádosti – rozsah a předmět chystaného schématu, účel a mimo jiné i doba, do kdy má být schéma hotové – max. 6 měsíců. Tento požadavek se však do finální verze nedostal kvůli tomu, že se přesně neví, jak bude příprava schémat v praxi fungovat. Byla tak Agentuře dána větší volnost.

[266] Odůvodnění Aktu uvádí jako příklad tohoto speciálního případu rapidní vzestup nové technologie. Reálně se ovšem dá očekávat, že zpočátku Program nebude příliš zaplněn a tudíž bude frekventovanější spíše „*neprogramová*“ varianta žádosti.

[267] Program je pak nutné aktualizovat, aby byla stále zachována transparentnost.

[268] Viz článek 48 Aktu o kybernetické bezpečnosti.

i v tomto ohledu přikloní k preferenci transparentnosti). Pro přípravu každého schématu zřídí Agentura ad hoc pracovní skupinu, která bude pomocným a poradním expertním orgánem. Při celé přípravě by měla ENISA kooperovat se Skupinou, která jí bude při přípravě též pomáhat, zároveň je pak Skupina nadána možností vyslovit k připravovanému schématu názor. Tento názor sice není závazný, ale ENISA by ho měla vzít v potaz vzhledem k tomu, že je Skupina složena z jednotlivých NCCA. Agentura by své tvořící aktivity měla zároveň konzultovat s evropskými standardizačními organizacemi, aby bylo dosaženo optimálního harmonizovaného vývoje.[269] Je tedy patrné, že doba přípravy složitějších schémat bude trvat skutečně dlouho.

Akt v článku 54 upravuje minimální rozsah prvků, které by schéma mělo obsahovat.[270] Schéma by mělo umožňovat technologický vývoj a být tak dostatečně flexibilní, aby nebylo třeba jej často měnit jen kvůli přílišné navázanosti na určité technologie. Některá schémata mohou z důvodu svého významu obsahovat mechanismy ke křížovému certifikačnímu procesu mezi více certifikačními tělesy. Tím by měla být kontrolována úroveň služeb poskytovaných při certifikačních procesech u zvlášť důležitých produktů. Tento systém však není dodělaný a může způsobovat problémy, neboť neobsahuje systém pro řešení konfliktu mezi CAB, ani případné následky toho, co se stane, když jeden z CAB při posuzování pochybí a druhý nikoliv.

Při formulování obsahu a vlastností schémat došlo i k teoretickému odstranění jedné z největších slabin systému CC → schémata by měla

[269] Viz článek 49 Aktu o kybernetické bezpečnosti.

[270] Jsou jimi mimo jiné předmět a rozsah schématu, účel schématu, bezpečnostní požadavky, uvedení dotčených národních schémat a také to, podle jakých standardů se případně při posuzování postupuje, úroveň záruky bezpečnosti (jedna až tři uvedené), umožnění nebo zákaz vlastního posouzení, specifické požadavky na certifikační tělesa nebo posuzovací metody, pravidla pro dohled nad zachováním compliance (tedy, že podmínky pro udělení certifikátu jsou stále splněné), úprava následků non-compliance s požadavky schématu, dobu platnosti certifikátu (v červencové verzi Aktu byla maximální doba platnosti certifikátu stanovena pro všechny budoucí schémata fixně na 5 let, ani toto ustanovení se však do závěrečné podoby textu nedostalo), pravidla pro oznamování zranitelností produktů, podmínky pro vzájemné uznávání certifikátu s třetími zeměmi nebo i formát a podoba certifikátu samotného.

obsahovat specifickou úpravu, po jakém typu aktualizace produktu je potřeba znovu provést certifikaci. Byl tedy (teoreticky) vyřešen problém bezpečnostní evoluce produktu.[271]

Hotový návrh schématu předloží Agentura Komisi. Ta může (není povinna) schéma schválit a vydat ho ve formě implementačního aktu. Schéma je přímo použitelné, není tedy nutný žádný další krok k tomu, aby ho mohly začít využívat subjekty posuzování shody. Aktivní schéma bude pak uveřejněno na webových stránkách provozovaných Agenturou. Současně budou na těchto stránkách zveřejňovány informace výrobců a vývojářů o kybernetické bezpečnosti určené pro spotřebitele a koncové uživatele.[272]

Součástí schémat by mohly (nebo i měly) být i různé správní procesy, ke kterým může při aplikace schématu dojít. Jedním z takových procesů je i revokace certifikátu. To je problematika, které se Akt úplně vyhýbá a přesunuje její úpravu na jednotlivá schémata. Kromě jádra procesu by ovšem bylo potřeba upravit i revokační proces v případě, že se na vadu certifikátu přijde při vzájemném hodnocení NCCA, tedy když bude návrh na revokaci směřovat z jiného členského státu. Otázkou zůstává i to, kdo bude mít pravomoc certifikát stáhnout, a to nejen v této situaci, ale rovněž když bude certifikát produktem křížového posuzování.

Agentura musí alespoň jednou za pět let zhodnotit fungování schémat a zjistit si zpětnou vazbu ode všech zúčastněných stran. V případě nutnosti může být Agentura pověřena Komisí nebo Skupinou k revizi schématu, případně k vytvoření revidovaného schématu.[273]

7.4.2 CERTIFIKACE

Výrobce nebo vývojář produktu, na který je připraveno schéma, by se měl se schématem seznámit (informace o něm budou zveřejňovány na internetu) a zhodnotit rizika, která hrozí jeho produktu. Na základě tohoto vyhodnocení si pak vybere požadovanou úroveň záruky bezpečnosti (pokud

[271] Viz bod 96 odůvodnění Aktu o kybernetické bezpečnosti.

[272] Viz článek 49 a 50 Aktu o kybernetické bezpečnosti.

[273] Viz tamtéž.

to schéma umožňuje), na kterou nechá svůj produkt certifikovat, a kontaktuje příslušné CAB, které testování provede v testovací laboratoři. Žadatel o certifikát by měl s hodnotitelem spolupracovat a poskytnout mu veškerou potřebnou dokumentaci společně se všemi relevantními informacemi. V případě, že produkt v testech obstojí a splní bezpečnostní požadavky, které na něj klade schéma, udělí takovému produktu CAB certifikát. Udělení certifikátu bude zaznamenáno i na internetových stránkách k tomu určených. Držitel certifikátu by měl uživatele při koupi informovat o bezpečnostních požadavcích, rizicích, spolehlivosti certifikátu, určeném prostředí ad., a to buď prostřednictvím internetu, nebo fyzicky.[274]

U držitele certifikátu se presumuje, že je v souladu s bezpečnostními požadavky daného schématu. Členské státy mohou stanovit získání certifikátu podle určitého schématu jako podmínku presumpce naplnění souladu s vnitrostátním právem (tato možnost bude pravděpodobně vcelku hojně využívána, neboť se jedná o skvělý nástroj odstranění dvojí administrativní zátěže). V případě, že po udělení certifikátu zjistí výrobce či vývojář novou zranitelnost produktu, která by mohla mít negativní vliv na bezpečnostní záruku poskytovanou certifikátem, je povinen neprodleně informovat subjekt posuzování shody, který bude řídit další postup (v případě zásadní zranitelnosti může dojít až k recertifikaci).

Certifikace by měla být implementována jednotně ve všech členských státech, aby nedocházelo k tzv. „*certification shopping*“. To označuje využívání nejednotných podmínek pro získání certifikátů, kdy je pro investory výhodnější, levnější nebo jednodušší podstoupit certifikaci v určitém členském státě.[275]

V případě, že žadatel o certifikaci nesouhlasí se subjektem posuzování shody (nebo NCCA, pokud je v roli subjektu posuzování shody) ohledně vyřízení žádosti o udělení certifikátu, je oprávněn podat proti vyřízení stížnost. K vyřízení této stížnosti je příslušný orgán, který napadané rozhodnutí vydal. Ten je povinen stěžovatele informovat o průběhu řízení, jeho vyřízení a případně i o možnosti nápravy soudní cestou. Žadatelé jsou

[274] Viz článek 55 a 56 Aktu o kybernetické bezpečnosti.

[275] Viz bod 70 odůvodnění Aktu o kybernetické bezpečnosti.

totiž podle Aktu oprávněni k efektivnímu prostředku nápravy soudní cestou, a to proti rozhodnutí o vyřízení stížnosti (stejně jako v obecném správním řízení je tedy nutné vyčerpat všechny prostředky ochrany před využitím řízení před soudem) nebo proti nečinnosti certifikačního orgánu v řízení o stížnosti. Příslušné jsou soudy toho členského státu, kde sídlí daný certifikační orgán.[276]

7.4.3 VLASTNÍ POSOUZENÍ ANEB CONFORMITY SELF-ASSESSMENT

Evropské certifikační schéma může umožnit i zvláštní režim posuzování shody a tím je vlastní posouzení. Jedná se o posouzení shody samotným výrobcem či poskytovatelem na jeho vlastní odpovědnost. Musí provést všechny kontroly toho, že produkt je skutečně ve shodě s daným schématem, a tuto kontrolu zdokumentovat. Takové posouzení je vhodné jenom pro základní bezpečnostní úroveň.

Schéma může umožňovat cestu jak vlastního posouzení, tak certifikace, ovšem v takovém případě musí stanovit jasné způsoby, jak od sebe odlišit produkty certifikované a sebehodnocené. Vlastní ohodnocení se může jevit sice jednodušší a rychlejší než hodnotící proces provedený CAB, ale v případě certifikace zůstává faktem, že za určité chování produktu se zaručila třetí osoba nezávislá na výrobci. To samo o sobě povzbuzuje důvěru (např. spotřebitele) více než vlastní posouzení. Ovšem vzhledem k tomu, že se tato metoda bude pravděpodobně masově využívat, tržní dopad této skutečnosti bude zřejmě minimální. Odpovědnost za řádné provedení vlastního posouzení spočívá plně na výrobci, což vede ke snížení limitace odpovědnosti jako účinku certifikace.[277]

Výrobce, který provede vlastní posouzení produktu a vyhodnotí, že splňuje všechny příslušné bezpečnostní požadavky, může vydat tzv. EU prohlášení o shodě, ve kterém je uvedeno, že produkt prokázal splnění bezpečnostních požadavků schématu.[278] Vydání prohlášení je dobrovolné, pokud není uvedeno v právu Unie nebo členských států jinak,

[276] Viz článek 63 a 64 Aktu o kybernetické bezpečnosti.

[277] Viz článek 53 a bod 79 až 81 odůvodnění Aktu o kybernetické bezpečnosti.

[278] V případě vydání EU prohlášení o shodě je výrobce povinen zaslat kopie tohoto prohlášení příslušné NCCA a Agentuře.

což se může jevit jako poněkud překvapivé řešení vzhledem k tomu, že je to jediný prostředek, jak informovat uživatele o provedeném vlastním posouzení.[279] Jakmile takové prohlášení vydá, přejímá plnou odpovědnost za soulad produktu se schématem. Nebezpečnou pro prohlašujícího je tak situace, kdy by došlo k revokaci certifikátu ze strany NCCA a panovaly by pochybnosti o procesu posouzení shody. V takové chvíli může totiž příslušný prodejce/dodavatel přijít o shodu u všech svých produktů.[280]

Výrobce je povinen uchovávat k dispozici NCCA jak prohlášení, tak i dokumentaci zachycující všechny skutečnosti relevantní pro posouzení shody, neboť i samoposouzený produkt se může stát předmětem kontroly nebo kontrolního posouzení provedeného NCCA.[281]

7.5 VZTAH EVROPSKÉHO CERTIFIKAČNÍHO RÁMCE K DALŠÍM CERTIFIKAČNÍM SYSTÉMŮM

Evropský certifikační rámec (dále jen „Rámec“) má být vystavěn na základech již funkčních národních a mezinárodních schémat, především tedy schématech vzešlých ze spolupráce SOG-IS. Vhodná schémata by měla být absorbována (a upravena, aby vyhovovala novým potřebám) evropským systémem tak, aby přechod mezi jednotlivými systémy byl pro členské státy co nejhladší a aby nedošlo k výraznému poklesu bezpečnostní úrovně. Rámec se tedy nesnaží o novoty za každou cenu, spíše by měl převzít, co bude možné, a učit se z chyb svých předchůdců. Tato „*zásada kontinuality*“ je explicitně uvedena mimo jiné v bodě 71 odůvodnění Aktu.

Ve vztahu k národním schématům předpokládá Rámec ukončení účinnosti takových národních schémat, která budou nahrazena evropským schématem (tedy kdy obě schémata dopadají na stejnou materii), a to od momentu účinnosti implementačního aktu Komise. Certifikátům, které byly vydány podle těchto národních schémat, doběhne doba platnosti normálně, ovšem nové již nebude možné vydat. Akt zároveň klade členským státům

[279] Je možné, že toto řešení bylo zvoleno kvůli tomu, aby subjekty, které potřebují provést vlastní posouzení jenom pro naplnění určitých interních pokynů, nemusely o takovém postupu ještě vydávat Prohlášení.

[280] Viz tamtéž.

[281] Viz bod 81 až 82 odůvodnění Aktu o kybernetické bezpečnosti.

na srdce, aby byla zrušena neúčinná, přesto nadále platná národní schémata, aby tak bylo zamezeno nepřehlednostem pro koncové uživatele.[282] Členským státům se dále zakazuje vydávat národní schémata v oblastech, nad kterými již působí některé ze schémat Rámce.[283] Tento zákaz se ovšem nevztahuje na situace, kdy jde o zachování národní bezpečnosti. Zásadně je tedy možné vydat národní schéma z důvodu národní bezpečnosti, ale členský stát o tomto svém záměru musí dopředu informovat Komisi a Skupinu. Ty zváží, jestli význam takového schématu není natolik velký, že by bylo lepší jej přijmout jako schéma Rámce, a tedy pro dobro celé Unie. Značná část těchto požadavků je zmíněna toliko v odůvodnění (bod 94) a do článků Aktu (článek 57) se dostalo pouze vyhasnutí národních schémat.

U mezinárodních iniciativ, nad nimiž nemá Unie moc, není možné nařídit vyhasnutí, dojde tak pravděpodobně ke koexistenci více certifikačních systémů, jejichž vzájemný vztah bude muset být upraven. K vedení takových jednání byla udělena pravomoc Komisi (za asistence Agentury). Výsledná dohoda může mít podobu MRA. Otázkou, která není Aktem řešena, je další osud spolupráce SOG-IS. V praxi se očekává, že by evropský rámec mohl postupně SOG-IS nahradit. Dokud ale není upraven vztah CCRA a Rámce, není rozumné SOG-IS rušit, neboť zůstává branou k úpravě certifikace podle systému Common Criteria.[284]

7.6 VZTAH AKTU KE SMĚRNICI NIS A NAŘÍZENÍ GDPR

Akt se úzce vztahuje ke dvěma důležitým unijním předpisům – směrnici NIS a nařízení GDPR. Stručně shrnuto, Akt má pomoci s implementací NIS

[282] Tato část nařízení není upravena formou příkazu, ale doporučení (z textu Aktu to téměř působí jako prosba).

[283] Viz článek 57 Aktu o kybernetické bezpečnosti.

[284] Zajímavé bylo sledovat vývoj bodu 68 odůvodnění Aktu, který se věnuje spolupráci SOG-IS, napříč různými verzemi. V textu se vystřídal přístup, který aktivity SOG-IS vychvaloval a vyzdvihoval jeho zásluhy (jedny z prvních verzí návrhu nařízení), s přístupem, který jeho aktivity odsuzoval, vyzdvihoval nedostatečnost a důvody, proč je třeba ho nahradit (např. červencové pozměňovací návrhy). Nakonec se podoba ustálila na konstatování, že spolupráce SOG-IS došla v rámci spolupráce nad CC pravděpodobně nejdál, ovšem stále se nejedná o dostatečné řešení.

a sloužit jako cesta k zabezpečení systémů, které NIS označil za podstatné. NIS se v certifikačním procesu projeví také v momentě hodnocení schémat Komisí podle článku 56, tedy zda není třeba učinit certifikaci podle některého ze schémat obligatorní. Primárně se Komise musí zaměřit na sektory, které jsou vyjmenovány v příloze II směrnice NIS, přičemž toto posouzení musí být provedeno nejpozději do dvou let od vstupu Aktu v účinnost.

Akt je stvořen jako lex generalis unijní kyberbezpečnostní certifikace, neměl by se tudíž nikterak dotknout zvláštních pravidel o certifikaci produktů, např. právě těch, která upravuje nařízení o ochraně osobních údajů. Bod 74 odůvodnění Aktu konkretizuje certifikační aktivity zavedené GDPR, na které Akt nedopadne, takto: „*(…) mechanismy pro vydávání osvědčení a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli.*“

7.7 DALŠÍ POTENCIÁLNÍ SLABINY A NEVÝHODY AKTU

Dne 16. srpna 2017, tedy ještě před zveřejněním první verze návrhu Aktu, byl zaslán Komisi otevřený dopis[285] podepsaný představiteli několika předních svazů, uskupení a komor na poli transatlantického trhu s ICT produkty a službami.[286] V tomto dopise byla Komise vyzvána, aby při přijímání Aktu a „*honu za kyberbezpečností*“ nebyl ohrožen nástup IoT v Unii. Zainteresovaná uskupení se bála zejména spojeného efektu GDPR, NIS a Aktu mimo Unii, což zůstalo obavou oprávněnou. Přestože GDPR a Akt mají mezi sebou vztah upravený, kumulativní efekt těchto tří předpisů může být pro subjekty ze třetích zemí značný, zvláště v momentě, kdy bude některé ze schémat Rámce ustanoveno jako obligatorní. V dopise byla i další varování, např. „*moc bezpečí zpomalí inovace a pokrok*“, ale jsem toho názoru, že Akt na tato varování v průběhu své legislativní evoluce uspokojivě zareagoval (důležité bude zvládnout tyto výzvy v praxi).

[285] Viz IoT Cybersecurity Coalition Letter [online]. 16. srpen 2017.

[286] Signatářem byly mimo jiné United States Chamber of Commerce, American Chamber of Commerce to the European Union, Svaz průmyslu a dopravy ČR nebo Confederation of Danish Industry.

Otázkou, která nakonec nebyla Aktem vyřešena, je délka certifikačního procesu. Ta byla jednou z hlavních slabin systému CC a bylo by rozhodně vhodné ji alespoň nějakým způsobem regulovat. Limitace délky certifikačního procesu by nyní bylo nejvhodnější upravit v rámci jednotlivých certifikačních schémat, délka procesu by se tak mohla upravit ad hoc potřebám jednotlivých produktů.

Další zajímavou otázkou je odpovědnost. V případě, že certifikovaný produkt způsobí škodu a členský stát s držením certifikátu spojil účinek „*přijetí všech rozumných opatření k zamezení újmy*“, byla odpovědnost držitele certifikátu limitována. V případě, že všechny prvky certifikačního procesu budou splněny řádně, odpovědný by pravděpodobně nebyl nikdo. Pokud by koncový uživatel užil produkt v rozporu s poučením, odpovědnost by byla jeho. Pokud by certifikační autorita provedla testování nedostatečně, odpovědnost by připadla jí (nebo členskému státu, pokud odpovědnost převezme). Nedostatečná úprava odpovědnosti států zde již byla řešena. Ale otázkou je, zdali by bylo možné se dovolat odpovědnosti Unie, resp. Komise, která schémata vydává jako implementační akty, za nedokonale připravené schéma. Podle mého názoru by takový postup byl hypoteticky možný, a to v případě zjevné nesprávnosti nebo jiném projevu hrubé nedbalosti při přípravném procesu. To ale nejen že není příliš pravděpodobné vzhledem k víceúrovňovému konzultačnímu procesu, ale též by se případné pochybení velmi obtížně prokazovalo. Proto tato otázka pravděpodobně zůstane jenom hypotetickou.

7.8 POZITIVA, KTERÁ AKT PŘINÁŠÍ

Na konec této kapitoly bych ještě rád zrekapituloval přínosy Aktu. Přes všechna negativa se totiž stále jedná o naprosto revoluční legislativní krok, který přináší certifikaci kyberbezpečnostních produktů, služeb a procesů, kdy certifikáty budou automaticky a univerzálně akceptovány napříč celou Unií. Akt má potenciál zvýšit úroveň kybernetické bezpečnosti napříč celou Unií, sjednotit evropský kyberbezpečnostní trh a zlepšit konkurenceschopnost unijních výrobců. A navíc se teoreticky dokázal

vypořádat s některými vadami certifikačních systémů, které přišly před ním (např. bezpečnostní evoluce certifikovaného produktu).

8. ZÁVĚR

Ať už za účelem zvýšit bezpečnost v kyberprostoru nebo sjednotit unijní trh s kyberbezpečnostními produkty, je zřejmé, že ekonomický i bezpečnostní význam certifikace bude v Unii významně vzrůstat. Toto téma je ovšem v České republice takřka neznámé (až na pár autorů, kteří se touto problematikou zabývají), a proto cílem tohoto článku bylo zmapovat a představit čtenáři problematiku certifikace kyberbezpečnostních technologií.

K tomu, abych tento cíl naplnil, jsem si stanovil dvě výzkumné otázky. Uspokojivá odpověď na první otázku[287] si vyžádala vcelku široký teoretický rozbor pojmů shoda (compliance), certifikace a způsobů naformulování regulatorních požadavků, stejně jako můj pokus o rámcové zasazení certifikace do systému kybernetické bezpečnosti v ČR. Při analýze stávajícího stavu v ČR a Unii vyšlo najevo, že v České republice ani Unii po dlouhou dobu neexistovala[288] žádná účinná právní úprava certifikace kyberbezpečnostních technologií. To obzvlášť v Unii vytvořilo velice neuspokojivý stav naprosto roztříštěného trhu. Vyskytuje se zde sice spolupráce SOG-IS, ale ta jednotný trh není schopná spasit. Ve zvláštní části jsem pak přešel k analýze konkrétních stávajících certifikačních systémů, zejména systému Common Criteria, který je stále ještě nejvýznamnějším z mezinárodně uznávaných certifikačních iniciativ. Při rozboru tohoto systému jsem narazil na několik podstatných slabin, které se při absenci mezinárodní politické vůle již pravděpodobně nepodaří odstranit. Národních schémat jsem pak využil k analýze toho, jak by bylo možné některé ze slabin Common Criteria „*vyléčit*“. Tím jsem tedy zjistil a zmapoval, jak fungují nejvýznamnější stávající certifikační systémy. Rozbor standardů ISO 27K v páté kapitole byl proveden naopak za účelem

[287] „Jak fungují stávající certifikační systémy?“

[288] A vzhledem k tomu, že ke dni 12. 10. 2019 stále ještě běží implementační lhůta části ustanovení Aktu týkajících se certifikace, tak taková účinná úprava ještě stále není.

odpovědi na druhou otázku, přesněji řečeno pochopení dosahu a povahy části Aktu, která dopadá na certifikaci procesů.

Odpověď na druhou otázku[289] byla analyzována primárně ve čtvrté a sedmé kapitole. Zde jsem rozebral jak legislativní vývoj Aktu, tak i jeho strukturu, kterou jsem podrobil kritické analýze. Jak je v textu patrné, Akt obsahuje mnoho slabin a vad, ale přesto se jedná o naprosto revoluční tah, který zavede do všech členských států Unie certifikaci kyberbezpečnostních produktů, služeb a procesů. Funkci stávajících certifikačních systémů tak v některých členských státech pozvedne (minimálně o certifikaci služeb), v dalších, které se doposud certifikaci nevěnovaly, pomůže certifikaci vzít na vědomí. Reaguje přitom na nejrůznější vady stávajících certifikačních systémů, jako je nevyřešení bezpečnostní evoluce produktů, nemožnost certifikovat služby, neuznávání certifikátů napříč Unií.

Jednotný evropský certifikační rámec má dostatečně velký potenciál k tomu, aby pomohl Unii se stát vůdčí certifikační silou na světě. Institucionální zabezpečení a struktura však tomuto potenciálu dle mého názoru neodpovídá a představuje slabinu Aktu. Stejně tak obsahuje Akt mnoho odvážných, přínosných, ale často nedotažených myšlenek (např. problém revokace certifikátu po vzájemném hodnocení). V rámci těchto kapitol jsem se tak pokusil odhadnout, jaký dopad může Akt na stávající podobu certifikace mít, ale je samozřejmě nutné počítat s tím, že se jedná zatím jen o teoretické úvahy a praxe může odhalit úplně jiné problémy. Zároveň byl tak naplněn i dílčí cíl článku, neboť kritické analýze a vyhodnocení slabin byl podroben jak systém Common Criteria, tak i Akt samotný.

[289] „Jak tuto funkci zlepší evropský návrh Aktu o kybernetické bezpečnosti?“

9. POUŽITÉ ZDROJE

9.1 MONOGRAFIE

[1] BASKERVILLE, Richard; STRAUB, Detmar W; GOODMAN, Seymour E. Information Security [online]. Armonk, NY, USA: Routledge, 2008, 297 s. Advances in Management Information Systems [vid. 11. listopad 2018]. ISBN 978-0-7656-1718-7. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzI3NTUxM19fQU41?sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3@pdc-v-sessmgr03&vid=9&format=EB&rid=1.

[2] CALDER, Alan. Nine steps to success an ISO27001:2013 implementation overview [online]. Ely, Cambridgeshire, U.K.: IT Governance Pub., 2013, 128 s. [vid. 11. listopad 2018]. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzEyMzI1NDFfX0FO0?sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3@pdc-v-sessmgr03&vid=7&format=EB&rid=1.

[3] HURYCHOVÁ, Klára; SÝKORA, Michal. Compliance programy (nejen) v České republice. Praha, Česká republika: Wolters Kluwer, 2018, 287 s. ISBN 978-80-7552-667-0.

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; CENTRAL SECRETARIAT. Friendship among equals: recollections from ISO's first fifty years. [online]. Geneva: ISO Central Secretariat, 1997, 87 s. [vid. 25. prosinec 2018]. ISBN 978-92-67-10260-3. Získáno z: https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/docs/en/Friendship_among_equals.pdf.

[5] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. 3., aktualiz. vyd. Praha, Česká republika: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2015.

[6] KYSELOVSKÁ, Tereza et al. Cofola 2015: Sborník z konference [online]. Edice Scientia. Brno: Masarykova univerzita, 2015, 1081 s. Acta Universitatis Brunensis Iuridica, 532 [vid. 22. listopad 2018]. ISBN 978-80-210-7976-2. Získáno z: https://www.law.muni.cz/sborniky/cofola2015/cofola2015.pdf.

[7] MEHAN, Julie E. CyberWar, CyberTerror, CyberCrime. [online]. 2nd ed. Ely, Cambridge, UK: IT Governance Publishing, 2014, 352 s. [vid. 19. srpen 2018]. ISBN 978-1-905356-48-5. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzgzODczMF9fQU41?sid=c0a75452-4a36-406f-82ad-2eb06c7ca5c0@pdc-v-sessmgr06&vid=8&format=EB&rid=2.

[8] POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. Právní problémy kybernetické bezpečnosti [online]. 1. vydání. Brno: Masarykova univerzita, 2016, 215 s. ISBN 978-80-210-8426-1. Získáno z: https://is.muni.cz/auth/repo/1375719/Polcak_kniha2.pdf?fakulta=1422;obdobi=7343;kod=MV735K;predmet=1120828.

[9] SMEDINGHOFF, Thomas J. Information Security Law [online]. Ely, Cambridge, UK: IT Governance Publishing, 2008, 182 s. [vid. 11. říjen 2018]. ISBN 978-1-905356-66-9. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzM5MTA5NV9fQU41?sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3@pdc-v-sessmgr03&vid=3&format=EB&rid=2.

[10] Technical information on the IT security certification of products, protection profiles and sites [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2012, 39 s. [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/7138_e_pdf.pdf;jsessionid=28944A61E3001F0324FDE8F91C9B173A.1_cid360?_blob=publicationFile&v=1.

9.2 ČLÁNKY Z ODBORNÝCH PUBLIKACÍ

[11] ALKALBANI, Ahmed et al. Information Security Compliance in Organizations: An Institutional Perspective. Data and Information Management [online]. 2017, roč. 1, č. 2, s. 104–114 [vid. 23. červenec 2018]. ISSN 2543-9251. Získáno z: https://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=28&sid=13ed30fd-ac9c-4f33-80e5-02ccf3fc761e%40sessionmgr4007.

[12] AXELROD, C. Warren. The creation and certification of software cybersecurity standards. In: 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT) [online]. Farmingdale, NY, USA: IEEE, 2016, s. 1–6 [vid. 22. červenec 2018]. ISBN 978-1-4673-8490-2. Získáno z: https://ieeexplore.ieee.org/document/7494112.

[13] BÂRSAN, Mihai. Aspects regarding the implementation of information security standards in organizations. Revista Română de Biblioteconomie și Știința Informării = Romanian Journal of Library and Information Science [online]. 2017, roč. 13, č. 1, s. 21–26 [vid. 29. říjen 2018]. ISSN 18411940, 25595490. Získáno z: doi:10/gfgkt8.

[14] BELLANTUONO, Giuseppe. Comparing Smart Grid Policies in the USA and EU. Law, Innovation and Technology [online]. 2014, roč. 6, č. 2, s. 221–264 [vid. 22. červenec 2018]. ISSN 1757-9961, 1757-997X. Získáno z: https://www.tandfonline.com/doi/full/10.5235/17579961.6.2.221.

[15] COGLIANESE, Cary. The Limits of Performance-Based Regulation. University of Michigan Journal of Law Reform [online]. 2016, roč. 50, č. 3, s. 525–564 [vid. 12. září 2018]. ISSN 0363-602X. Získáno z: https://scholarship.law.upenn.edu/faculty_scholarship/1858/.

[16] COGLIANESE, Cary; LAZER, David. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals. Law & Society Review [online]. 2003, roč. 37, č. 4, s. 691–730 [vid. 12. září 2018]. ISSN 0023-9216, 1540-5893. Získáno z: https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=2&sid=45e13b2c-08ac-42fd-94dd-ce0d386287f7 %40pdc-v-sessmgr02.

[17] COGLIANESE, Cary; NASH, Jennifer; OLMSTEAD, Todd. Performance-Based Regulation: Prospects and Limitations in Health, Safety and Environmental Protection. Administrative Law Review [online]. 2003, roč. 55, č. 4, s. 705–730 [vid. 20. září 2018]. ISSN 0001-8368. Získáno z: https://heinonline.org/HOL/Page?handle=hein.journals/admin55&div=29.

[18] D'AMATO, Anthony. Legal Uncertainty. California Law Review [online]. 1983, roč. 71, č. 1, s. 1 [vid. 25. únor 2019]. ISSN 00081221. Získáno z: doi:10/d48z36

[19] HEARN, J. Does the common criteria paradigm have a future? IEEE Security & Privacy Magazine [online]. 2004, roč. 2, č. 1, s. 64–65 [vid. 18. říjen 2018]. ISSN 1540-7993. Získáno z: http://ieeexplore.ieee.org/document/1264857/.

[20] ISA, Mohd Anuar Mat et al. Finest authorizing member of common criteria certification. In: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) [online]. Kuala Lumpur, Malaysia: IEEE, 2012, s. 155–160 [vid. 22. červenec 2018]. ISBN 978-1-4673-1426-8. Získáno z: http://ieeexplore.ieee.org/document/6246109/.

[21] JEŽOVÁ, Daniela. EU Digital Single Market - Are we there yet? Ad Alta: Journal of Interdisciplinary Research [online]. 2017, roč. 7, č. 2, s. 99–102. ISSN 1804-7890. Získáno z: https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=12&sid=f9683978-876b-416a-a2d0-5fa83e889a40 %40sessionmgr120.

[22] KALLBERG, Jan. The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal. IEEE Security & Privacy Magazine [online]. 2012, roč. 10, č. 4, s. 50–53 [vid. 22. říjen 2018]. ISSN 1540-7993. Získáno z: http://ieeexplore.ieee.org/document/6148206/.

[23] KALUVURI, Samuel Paul; BEZZI, Michele; ROUDIER, Yves. Bringing Common Criteria Certification to Web Services. In: 2013 IEEE Ninth World Congress on Services (SERVICES) [online]. Santa Clara, CA, USA: IEEE, 2013, s. 98–102 [vid. 22. červenec 2018]. ISBN 978-0-7695-5024-4. Získáno z: http://ieeexplore.ieee.org/document/6655681/.

[24] KANG, Sooyoung; KIM, Seungjoo. How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability. Symmetry [online]. 2017, roč. 9, č. 10, s. 12 [vid. 22. červenec 2018]. ISSN 2073-8994. Získáno z: https://www.mdpi.com/2073-8994/9/10/233/htm.

[25] KLINKE, Andreas; RENN, Ortwin. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. Risk Analysis [online]. 2002, roč. 22, č. 6, s. 1071–1094 [vid. 11. listopad 2018]. ISSN 02724332, 15396924. Získáno z: https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=16&sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3%40pdc-v-sessmgr03.

[26] KNEEPKENS, Jules. Performance Based Regulation. In: EASA Safety Conference [online]. B.m. 2012. [vid. 20. září 2018]. Získáno z: https://www.easa.europa.eu/conferences/pbo/doc/presentations/3%20-%20Kneepkens%20EU%20Performance%20Based%20Regulation.pdf.

[27] KOVÁCS, László. Cyber Security Policy and Strategy in the European Union and NATO. Revista Academiei Fortelor Terestre [online]. 2018, roč. 23, č. 1, s. 16–24 [vid. 22. červenec 2018]. ISSN 15826384. Získáno z: https://content.sciendo.com/view/journals/raft/23/1/article-p16.xml.

[28] KRISTENSEN, V.; AVEN, T.; FORD, D. A new perspective on Renn and Klinke's approach to risk evaluation and management. Reliability Engineering & System Safety [online]. 2006, roč. 91, č. 4, s. 421–432 [vid. 11. listopad 2018]. ISSN 09518320. Získáno z: doi:10/db47fv.

[29] MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. Law & Policy [online]. 2003, roč. 25, č. 4, s. 381–401 [vid. 22. září 2018]. ISSN 0265-8240, 1467-9930. Získáno z: https://heinonline.org/HOL/Page?handle=hein.journals/lawpol25&div=28.

[30] MERCURI, Rebecca. Uncommon criteria. Communications of the ACM [online]. 2002, roč. 45, č. 1, s. 172–172 [vid. 22. říjen 2018]. ISSN 00010782. Získáno z: http://portal.acm.org/citation.cfm?doid=502269.502310.

[31] MITRAKAS, Andreas. The emerging EU framework on cybersecurity certification. Datenschutz und Datensicherheit [online]. 2018, roč. 42, č. 7, s. 411–414 [vid. 11. září 2018]. ISSN 16140702. Získáno z: https://link.springer.com/content/pdf/10.1007%2Fs11623-018-0969-2.pdf.

[32] RECCHIA, Luca et al. Security Evaluation of a Linux System: Common Criteria EAL4+ Certification Experience. In: 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) [online]. Naples, Italy: IEEE, 2014, s. 77–81 [vid. 22. červenec 2018]. ISBN 978-1-4799-7377-4. Získáno z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6983806.

[33] TANTAWI, Randa. Common Criteria. Salem Press Encyclopedia [online]. 2013 [vid. 13. září 2018]. Získáno z: https://eds.a.ebscohost.com/eds/detail/detail?vid=1&sid=65cb00d8-2765-434e-802f-29a488b6180b%40sdc-v-sessmgr04&bdata=JkF1dGhUeXBlPWlwLGNvb2tpZSx1aWQmbGFuZz1jcyZzaXRlPWVkcy1saXZlJnNjb3BlPXNpdGU%3d#db=ers&AN=90558266.

9.3 PREZENTACE Z ODBORNÝCH KONFERENCÍ

[34] PRILLER, Christian. Effectively Implementing the EU Certification Framework: Market Perspectives - TÜV-SÜD-AG. In: Effectively Implementing the EU Certification Framework: Market Perspectives [online]. Brusel, Belgie. 2018. [vid. 25. září 2018]. Získáno z: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Christian-PRILLER_T%C3 %9CV-S%C3 %9CD-AG.pdf.

[35] STANTCHEV, Pentcho. Cybersecurity of Industrial Systems. In: Effectively Implementing the EU Certification Framework: Market Perspectives [online]. Brusel, Belgie. 2018. [vid. 25. září 2018]. Získáno z: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Pentcho-STANTCHEV_ORGALIME.pdf.

[36] Baseline Security Product Assessment. In: BlackHat Sessions [online]. Nieuwegein, Nizozemí. 2018. [vid. 25. prosinec 2018]. Získáno z: https://www.blackhatsessions.com/presentaties/2018/BSPA%20-%20BlackHatSessions%2003_1.pdf.

9.4 INTERNETOVÉ STRÁNKY A ZDROJE

[37] ČERMÁK, Miroslav. Regulatorní požadavky představují jen další riziko, a tak je s nimi třeba i zacházet. CleverAndSmart [online]. 2018. [vid. 8. listopad 2018]. Získáno z: https://www.cleverandsmart.cz/regulatorni-pozadavky-predstavuji-jen-dalsi-riziko-a-tak-je-s-nimi-treba-i-zachazet/.

[38] WEBER, Joachim. The German IT Security Certification Scheme [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2017, 25 s. [vid. 28. prosinec 2018]. Získáno z: http://www.isccc.gov.cn/zlzx/kyxx/images/2017/09/10/AF5C39A704EA2F5CE84A2D0419EA383C.pdf.

[39] Baseline Security Product Assessment. SECURA [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.secura.com/pathtoimg.php?id=1326&image=bspa.pdf.

[40] BSI – Certification. Bundesamt für Sicherheit in der Informationstechnik [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html.

[41] Certification CSPN. ANSSI [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/.

[42] Certification. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/certification--conformity/certification.html.

[43] Certified Products List - Statistics. New CC Portal [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/products/stats/.

[44] Certified Products. NCSC Site [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.ncsc.gov.uk/index/certified-product?f[0]=field_assurance_scheme%3A226&f[1]=field_assurance_status%3AAssured.

[45] Commercial Product Assurance (CPA). NCSC Site [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

[46] Common Criteria. New CC Portal [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/.

[47] CSPN: What U.S. companies need to know about the security certification process [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process.

[48] Český institut pro akreditaci, o.p.s. ČIA - Národní akreditační orgán [online] b.n. nedatováno [vid. 20. leden 2019]. Získáno z: http://www.cia.cz/.

[49] Členství v mezinárodních organizacích. ÚNMZ [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.unmz.cz/urad/clenstvi-v-mezinarodnich-organizacich.

[50] Developing standards. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards.html.

[51] Foundation Grade explained. NCSC Site [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/foundation-grade-explained.

[52] IAF MEMBERS: Czech Republic. International Accreditation Forum [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.iaf.nu/articles/IAF_MEM_Czech_Republic/66.

[53] IEC - About the IEC [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.iec.ch/about/?ref=menu.

[54] ISO/IEC 27001 Information security management. ISO [online] b.n. nedatováno [vid. 24. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/isoiec-27001-information-securit.html.

[55] ISO/IEC JTC 1/SC 27 - IT Security techniques. ISO [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/04/53/45306.html.

[56] Les produits CSPN. ANSSI [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/.

[57] Members. ISO [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/members.html.

[58] Members of the CCRA. New CC Portal [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.commoncriteriaportal.org/ccra/members/#CZ.

[59] O Úřadu - ÚNMZ [online] b.n. nedatováno [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/o-uradu.

[60] Products and Services Scheme fees. NCSC Site [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/products-and-services-scheme-fees.

[61] Questions and Answers - EU Cybersecurity. European Commission [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369.

[62] SCORM Compliant, SCORM Conformant, SCORM Certified. SCORM.com [online] b.n. nedatováno [vid. 26. říjen 2018]. Získáno z: https://scorm.com/scorm-explained/scorm-resources/conformance-vs-compliance/.

[63] Security Characteristics collection. NCSC Site [online] b.n. nedatováno [vid. 28. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/document/security-characteristics-collection.

[64] Seznam akreditovaných subjektů pro posuzování shody podle nařízení eIDAS platný ke dni 5. 2. 2019. European Commission - Futurium: eIDAS Observatory [online] b.n. nedatováno [vid. 28. únor 2019]. Získáno z: https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accredited_cabs-2019-02-05.pdf.

[65] SOG-IS - Home. SOG-IS [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html.

[66] SOG-IS - Status of participants. SOG-IS [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://sogis.org/uk/status_participant_en.html.

[67] The ISO Story. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/the-iso-story.html.

[68] UNMZ. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/member/00/21/2133.html.

[69] Vybrané výrobky - ÚNMZ [online] b.n. nedatováno [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/vybrane-vyrobky.

[70] What's the Difference Series: Compliance vs. Certification. Mireaux Management Solutions [online]. 2013. [vid. 26. říjen 2018]. Získáno z: http://mireauxms.com/vanguard-blog/whats-the-difference-series-compliance-vs-certification.

[71] Who develops standards. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards/who-develops-standards.html.

9.5 PRÁVNÍ PŘEDPISY

9.5.1 ZÁKONY A VYHLÁŠKY

[72] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: CODEXIS ACADEMIA [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

[73] Vyhláška 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). In: CODEXIS ACADEMIA [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

[74] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: CODEXIS ACADEMIA [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

9.5.2 PRÁVNÍ PŘEDPISY EU

[75] Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 [online]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32008R0765&from=EN.

[76] 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 a o zrušení směrnice 1999/93/ES [online]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:32014R0910

[77] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 [online]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri = CELEX:32019R0881&from = CS

[78] Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti") ze dne 20. 12. 2018 [online]. Získáno z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?
uri = CONSIL:ST_15786_2018_INIT&from = EN.

9.5.3 MEZINÁRODNÍ SMLOUVY A SMLOUVY O MEZINÁRODNÍ SPOLUPRÁCI

[79] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security [online]. 2. červenec 2014. [vid. 12. září 2018]. Získáno z: https://www.commoncriteriaportal.org/files/CCRA%20-%20July %202,%202014 %20-%20Ratified%20September%208 %202014.pdf.

[80] SOG-IS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, verze 3.0 [online]. 2010. [vid. 27. říjen 2018]. Získáno z: https://www.sogis.eu/documents/mra/20100107-sogis-v3.pdf.

9.6 KVALIFIKAČNÍ PRÁCE

[81] HARAŠTA, Jakub. Princip technologické neutrality v kybernetické bezpečnosti [online]. Brno 2017 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta. Získáno z: https://is.muni.cz/auth/th/agnuc/Princip_technologicke_neutrality_v_kyberneticke_bezpecnosti.pdf.

9.7 OSTATNÍ ZDROJE

[82] DROGKARIS, Prokopios. Considerations on ICT security certification in EU - Survey Report [online]. 2017. B.m.: European Union Agency for Network and Information Security. Získáno z: https://www.enisa.europa.eu/publications/certification_survey/at_download/fullReport.

[83] GUEBEL, Martine. NANDO Information System (Europa) [online]. [vid. 5. únor 2019]. Získáno z: http://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction = help.main.

[84] HEAD, Katie Bird. ISO workshop on Mutual Recognition Agreements. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/1998/04/Ref749.html.

[85] NEGREIRO ACHIAGA, Maria Del Mar. EU Legislation in Progress - Briefing: ENISA and a new cybersecurity act (stav ke dni 16. 1. 2018) [online]. B.m.: European Parliament Research Service. [vid. 11. říjen 2018]. Získáno z: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.

[86] VYSOKÁ PŘEDSTAVITELKA UNIE PRO ZAHRANIČNÍ VĚCI A BEZPEČNOSTNÍ POLITIKU. Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU [online]. 2017. [vid. 11. říjen 2018]. Získáno z: https://publications.europa.eu/en/publication-detail/-/publication/794f8627-985b-11e7-b92d-01aa75ed71a1/language-cs.

[87] Annual Activity Report 2018 [online]. Řecko: European Union Agency for Cybersecurity, 2018, 72 s. [vid. 12. říjen 2019]. ISBN 978-92-9204-297-4. Získáno z: https://www.enisa.europa.eu/publications/corporate-documents/enisa-annual-activity-report-2018.

[88] Commission Staff Working Document: Advancing the Internet of Things in Europe [online]. 2016. B.m.: European Commission. [vid. 12. říjen 2019]. Získáno z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN.

[89] Důvodová zpráva k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

[90] Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. 2005. B.m.: Národní bezpečnostní úřad. [vid. 4. leden 2019]. Získáno z: https://www.nbu.cz/download/bezpecnost-informacnich-systemu/container-nodeid-748/infoobit.pdf.

[91] IOCTA: Internet Organised Crime Threat Assessment 2019 [online]. 2019. B.m.: Europol – European Cybercrime Centre. [vid. 12. říjen 2019]. Získáno z: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019.

[92] Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014. [vid. 24. srpen 2018]. Získáno z: https://www.enisa.europa.eu/events/sog-is/minutes/view.

[93] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017, 106 s. [vid. 12. září 2018]. Získáno z: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5_marked_changes.pdf.

[94] IoT Cybersecurity Coalition Letter [online]. 16. srpen 2017. Získáno z: https://www.uschamber.com/iot%26cybersecurity.

[95] Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu aktu o kybernetické bezpečnosti [online]. 2017. B.m.: Evropská komise. [vid. 12. červenec 2018]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017SC0501&from=CS.

[96] Procedure File: 2017/0225(COD). Legislative Observatory | European Parliament [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2017/0225(COD)#tab-0.

[97] Report: EU coordinated risk assessment of the cybersecurity of 5G networks [online]. 2019. B.m.: NIS Cooperation Group. [vid. 12. říjen 2019]. Získáno z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

[98] Sdělení Komise Evropskému parlamentu, Radě, EHS-výboru a výboru regionů ze dne 10. 5. 2017 o přezkumu v polovině období provádění strategie pro jednotný digitální trh [online]. 10. květen 2017. B.m.: Evropská komise. [vid. 11. říjen 2018]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017DC0228&from=EN.

[99] State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks [online]. 19. září 2017. B.m.: European Comission - Press release. [vid. 11. říjen 2018]. Získáno z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiK-rnCys3gAhVtRhUIHUkMA5gQFjABegQICBAC&url=http%3A%2F%2Feuropa.eu%2Frapid%2Fpress-release_IP-17-3193_en.pdf&usg=AOvVaw261JlgSpwwQ0lkHOTKTV-A.

[100] Technical information on the IT security certification of products, protection profiles and sites [online]. 2012. B.m.: Bundesamt für Sicherheit in der Informationstechnik. [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/7138_e_pdf.pdf?_blob=publicationFile&v=1.

INSTRUCTIONS FOR AUTHORS

The Review of Law and Technology is a peer-reviewed scientific journal for technological areas of law and jurisprudence.

Since 1st January 2015 the journal is listed in the List of non-impact peer-reviewed journals published in the Czech Republic and since 24th June 2015 in ERIH PLUS database.

Contributions submitted for the Topic and Discussion sections are anonymously peer-reviewed by at least two independent reviewers and the final decision on publication is the in the sole discretion of the editorial board. Review process takes approximately one month. The submissions are not subject to language proofreading.

Contributions shall be submitted through our web-based system available at www.revue.law.muni.cz.

RECOMMENDED EXTENT OF THE CONTRIBUTIONS:

Topic section:	30 – 80 standard pages
Discussion section:	5 – 30 standard pages
Case annotation:	2 – 10 standard pages
Book review:	1 – 5 standard pages

(including spaces, footnotes and bibliography)

CITATIONS FORMAT

Citations shall be in accordance with the ISO 690:2011 citation standard.

Referencing examples are available in interpretations of the aforementioned citation standard (e. g. at www.ezdroje.muni.cz/prehled/zdroj.php?lang=en&id=441).

Individual sources are referenced in the text by upper index. The actual citation of the source is then contained in a footnote.

DEADLINES FOR CONTRIBUTIONS SUBMISSIONS

For the summer issue: 31st March

For the winter issue: 30th September

The Review of Law and Technology is a gold open access journal.

Contributions are included into respective electronic legal information systems operated by Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) and ATLAS consulting spol. s r. o. (CODEXIS).

Detailed information about the publication process, structure and format of the contributions, the review process and copyright are available in the "For the authors" section at www.revue.law.muni.cz. Further information is available upon request addressed to editorial staff (contact e-mail revue@law.muni.cz).

REVIEW OF LAW AND TECHNOLOGY

VOLUME 10 | YEAR 2019 | NUMBER 20

Review of Law and Technology
Peer-reviewed scientific journal for technological areas 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 31st December 2019.
ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. nr. MK ČR E 19707
Published by: Masaryk University, Žerotínovo nám. 9, 601 77 Brno, Czech Republic, ID-Nr. 00216224
Editor-in-chief and contact person: JUDr. Matěj Myška, Ph.D., Institute of Law and Technology, Faculty of Law, Masaryk University, Veveří 70, 611 80 Brno, Czech Republic, tel: +420 549494751, fax: +420 541210604, e-mail: revue@law.muni.cz | www.revue.law.muni.cz
Deputy editor-in-chief: Ing. Mgr. František Kasl
Editorial Staff: JUDr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek
Editorial Secretary: Anna Blechová
Editor: Anna Blechová
Editorial Board: doc. JUDr. Radim Polčák, Ph.D. (honorary chairman), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, doc. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Layout: Mgr. 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 VII“, MUNI/A/1006/2018.

MUNI LAW

Ústav práva a technologií

děkuje svým partnerům za podporu v roce 2019

vodafone

Wolters Kluwer

ROWAN LEGAL

CODEXIS®

Zákony pro lidi.cz

CATERING FOR YOU

PRÁVNÍ PROSTOR

EDPL EUROPEAN DATA PROTECTION LAW REVIEW

Diskuze

Anotace

Recenze

Téma

MUNI PRESS