23

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 12 / Rok 2021 / Číslo 23

Revue.law.muni.cz

XIII. národní konference | 9. - 10. září 2021, Právnická fakulta, MU, Brno

České právo a informační technologie 2021

pořádá Ústav práva a technologií Právnické fakulty Masarykovy univerzity
cyber.law.muni.cz

Konference bude rozdělena na plenární panelovou diskusi a jednání v šesti odborných sekcích.

Pořadatel konference vyzývá zájemce o aktivní účast, aby hlásili své příspěvky do některé z odborných sekcí. Rozšířený abstrakt v rozsahu 1-2 stran obsahující strukturu příspěvku, výzkumnou otázku a zásadní myšlenky, které budou v prezentaci představeny, posílejte do **31. 7. 2021** na adresu **cpit@law.muni.cz**.
O přijetí příspěvku k prezentaci bude rozhodnuto do 15. 8. 2021.

Písemná vyhotovení příspěvků jsou vítána k posouzení pro případnou publikaci v recenzovaném časopise **Revue pro právo a technologie**.

Další informace na webu cpit.law.muni.cz

Předběžný program konference

Čtvrtek 9. září 2021

plenární panelová diskuse

Evropská datová strategie a nařízení o správě dat (Data Governance Act)

Moderuje: Radim Polčák
Panelisté: TBC

paralelní sekce

Právní informatika

Moderuje: Jakub Harašta
právní informační systémy; experimenty s uživateli; právní informatika; strojové učení; získávání právních informací

Reforma autorského práva

Moderuje: Matěj Myška
národní transpozice Směrnice o autorském právu na jednotném digitálním trhu; upload filtry; uživatelská práva; práva nakladatelů; text a data mining; digitalizace kulturního dědictví; e-learning; umělá inteligence a autorské právo; kolektivní správa práv

Pátek 10. září 2021

paralelní sekce

Ochrana osobních údajů a soukromí

Moderuje: Jakub Míšek
osobní údaje; e-privacy; GDPR; data protection by design & by default; princip odpovědnosti správce; hodnocení dopadů zpracování; oprávněný zájem správce údajů; policejní směrnice; přímé nároky

Elektronické důkazy

Moderuje: Václav Stupka
elektronické důkazy; mezinárodní spolupráce při zajišťování elektronických důkazů; data retention

Elektronizace státní správy, online soudnictví

Moderuje: Pavel Loutocký
elektronický spis; elektronická správa dat; online komunikace v rámci státní správy (asynchronní komunikace, videopřenosy apod.); moderní přístupy k rozhodování sporů; online platformy a ochrana práv; digitální služby; elektronický dokument; digitální obsah

Kybernetická bezpečnost a obrana

Moderuje: František Kasl
kybernetické bezpečnostní incidenty; certifikace; povinnost hlášení; kritické informační infrastruktury; odpovědnost státu; nestátní aktéři; přičitatelnost; protiopatření; kybernetické zbraně; použití síly; kybernetický útok; Talinský manuál

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 12 | ROK 2021 | ČÍSLO 23

Revue pro právo a technologie
Odborný recenzovaný časopis pro technologické obory práva a právní vědy zařazený na Seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice a v databázi ERIH PLUS.
Recenzovány jsou příspěvky v sekci Diskuze a Téma.
Vychází dvakrát ročně. Toto číslo vyšlo 30. 6. 2021.
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: JUDr. Ing. František Kasl, Ph.D.
Redakce: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Tajemnice redakce: Anna Blechová
Editoři: Anna Blechová, Martin Erlebach
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 IX“, MUNI/A/1292/2020.

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

ÚVODNÍK

Vážené čtenářky, vážení čtenáři,

do dvanáctého roku své existence vstupuje časopis Revue pro právo a technologie po bezprecedentní historické události, která omezila „offline“ kontakty v odborné komunitě na nezbytné minimum. Pokusili jsme se, aby Revue pro právo a technologie i v této době byla platformou pro výměnu odborných názorů v oblasti práva i technologií. Dovolte, abych na tomto místě poděkoval svému zástupci Františkovi Kaslovi, tajemnici redakce Anně Blechové, editorovi Martinu Erlebachovi, redakci a redakční radě za jejich nasazení při vytváření tří posledních čísel v kompletně virtuálním prostředí.

I přes nepřeberné množství virtuálních konferencí a seminářů, mám za to, že pro budování odborné komunity nemůže nic nahradit setkání tváří v tvář. Proto bych si Vás rád dovolil pozvat na již třináctý ročník národní konference České právo a informační technologie, který se uskuteční ve dnech 9.–10. 9. 2021, a to doufejme již tradičně v prostorách Právnické fakulty Masarykovy univerzity. Detailní informace o konferenci naleznete v informačním letáku, který je otištěn na levé vnitřní obálce tohoto čísla.

Dovolte mi, abych Vám z pověření čestného předsedy redakční rady, pana doc. Polčáka, představil ještě jeden virtuální nástroj – mailingovou konferenci Cyberlaw Ústavu práva a technologií, která nám umožní vzájemně sdílet novinky, pozvánky na zajímavé akce, diskutovat odborné otázky či se informovat o zásadních judikátech (i prvostupňových) a pozičních dokumentech, a tím pádem rozvíjet odbornou komunitu v České republice. Informace a přihlášení naleznete zde.[1]

[1] Odkaz na mailingovou konferenci: https://mailman.muni.cz/mailman/listinfo/cyberlaw

Konečně bych Vás rád informoval o zavedení nové sekce „Essays“, která se primárně zaměřuje na publikaci kvalitních anglicky psaných studentských příspěvků řešících partikulární otázky práva a technologií. Tato sekce by měla vytvořit platformu pro zveřejňování kvalitních studentských textů v angličtině (jako např. výsledků Studentské vědecké odborné činnosti, plnění ze specializovaných předmětů atd.) a zároveň umožnit studentům se dále akademicky (publikačně) rozvíjet. Zároveň doufáme, že tato sekce umožní čtenářům získat nový náhled na specializovaná témata.

Děkuji Vám za Vaši přízeň a přeji Vám příjemné léto!

Matěj Myška
šéfredaktor

https://doi.org/10.5817/RPT2021-1-1

OCHRANA SOUKROMÍ V ČESKO-SLOVENSKÝCH CHYTRÝCH KARANTÉNÁCH

ŠIMON CHVOJKA[1]

ABSTRAKT

Technologická vyspělost obecné populace je vysoká, což vládám umožnilo využít moderních technologií v boji proti koronaviru. Článek se zaměřuje na oficiální chytré karantény v České a Slovenské republiCE, které popisuje a analyzuje z pohledu práva na soukromí a ochranu osobních údajů. Největší zjištěné problémy se týkají nedostatečnosti aplikovatelných právních rámců a také proporcionality využitého řešení. V obou případech přitom šlo o problémy, kterým se bylo možné vyhnout.

KLÍČOVÁ SLOVA

Chytrá karanténa; ochrana soukromí; eRouška, eKaranténa; COVID-19

ABSTRACT

The technological advancement of the general population is high, which has allowed governments to use modern technologies to combat the coronavirus. This paper focuses on the official smart quarantines in the Czech and Slovak Republics, which it describes and analyses from the right to privacy and personal data protection's point of view. The biggest problems identified relate to insufficient

[1] Mgr. Šimon Chvojka je absolventem Právnické fakulty Masarykovy univerzity v Brně. Kontaktní e-mail: 458884@muni.cz. Stav textu je k 31. 3. 2021. Tento článek vychází ze SVOČ zpracované v roce 2021. Autor by na tomto místě rád poděkoval za cenné připomínky a rady JUDr. MgA. Jakubovi Míškovi, Ph.D.

applicable legal frameworks and to the proportionality of the used solution. In both cases, the problems were avoidable.

KEYWORDS

Smart quarantine; privacy protection; eRouška, eKaranténa; COVID-19

1. ÚVOD

Na začátku března 2020 byly na území České republiky potvrzeny první případy nákazy koronavirem označovaného jako SARS-CoV-2, a jinak tomu nebylo na Slovensku. Rok se s rokem sešel, a to tradičně nabízí prostor pro bilancování. V tomto příspěvku bude věnován prostor tzv. chytrým karanténám.

Právě jejich nasazením se (nejen) státy Evropské unie („EU“) snaží omezit přenos viru. Ačkoliv se jejich podoba liší stát od státu, obecně lze konstatovat, že ve středu zájmu jsou mobilní telefony občanů.[2] Ty totiž jednoduše umožňují sledovat pohyb majitele, ať už skrze systém GPS, antény telefonních operátorů anebo technologii Bluetooth. Právě technologický rozvoj těchto funkcí spolu se zvyšujícím se počtem uživatelů mobilních telefonů umožnili první masové využití chytrých karantén. Plošnost nasazení na druhou stranu indikuje možnost závažného zásahu do základních práv občanů na soukromí a informační sebeurčení. Je tomu skutečně tak? A jedná se případně o proporcionální zásah?

Na tyto otázky se příspěvek snaží najít odpověď. Situaci zkoumá na příkladu oficiálních chytrých karantén v České republice a Slovenské republice. Zaměřuje se především na chaotické období první vlny na jaře 2020, kdy se státy v jisté bezradnosti, snad někdy i bezhlavě, snažily co nejefektivněji využít moderní technologie k potlačení rychle se šířícího viru.

Východiskem pro hodnocení jsou zejména veřejně dostupné údaje (právní rámec, publikované informace o projektech, informační povinnosti správců) ale také posouzení vlivu na ochranu osobních údajů („DPIA“)

[2] Pro přehled jednotlivých států a jejich chytrých karantén srov. Projects using personal data to combat SARS-CoV-2. In: *GDPRHUB.eu* [online] [cit. 12. 4. 2020]. Dostupné z: https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2

k jednotlivým řešením, které byly získány prostřednictvím zákonů o svobodném přístupu k informacím.

Cílem článku je komplexně popsat fungování chytrých karantén z pohledu práva, následně je podrobit kritickému zhodnocení (zejména jejich proporcionalitu) a případně upozornit na vybrané nedostatky v postupu odpovědných míst.

V první části je podán všeobecný přehled relevantní právní úpravy ochrany soukromí a osobních údajů v Česku a na Slovensku, který se s chytrými karanténami pojí. Druhá část popisuje fungování jednotlivých částí chytrých karantén v obou zemích v průběhu první vlny. Třetí část je částí analytickou. Popsaný stav je podroben kritickému zhodnocení z pohledu ochrany soukromí obyvatel a principů ochrany osobních údajů. Vybrané problémy jsou rozebrány podrobněji, a to i s přihlédnutím k případnému vývoji jednotlivých prezentovaných řešení.

2. OCHRANA SOUKROMÍ A OSOBNÍCH ÚDAJŮ…

Ochrana soukromí a osobních údajů v Česku a na Slovensku je téměř identická – oba státy jsou signatáři Evropské úmluvy o ochraně základních práv a lidských svobod („Úmluva“), členy EU a národní listiny práv jsou podobné. Popis právního rámce ochrany tak je rozdělen podle těchto tří okruhů.

Obecně je nutné před začátkem konstatovat, že existence krizové situace není automaticky důvodem pro benevolentnější přístup k hodnocení zásahů do základních lidských práv. Vláda práva musí fungovat i v časech krize.[3] To potvrzují i recentní rozhodnutí českých soudů, které jsou v případě přezkumu opatření z počátku pandemie benevolentnější ale s postupujícím časem požadavky (zejm. na odůvodnění) stupňují.[4]

[3] *Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis: A toolkit for member states* [online]. Council of Europe, 2020, s. 3 [cit. 14. 5. 2020]. Dostupné z: https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40

[4] Srov. rozsudek Městského soudu v Praze ze dne 13. 11. 2020, č. j. 18 A 59/2020-226, odst. 142 a tam citovanou judikaturu.

2.1 …JAKO SOUČÁST ÚMLUVY

Přímo v čl. 8 Úmluvy zabývajícím se soukromím,[5] a ani nikde jinde v Úmluvě, nenajdeme ochranu osobních údajů explicitně zmíněnu. Dosah Úmluvy i na osobní údaje vyplývá až z jejího výkladu podávaného Evropským soudem pro lidská práva („ESLP"), který má v tomto směru poměrně bohatou judikaturu.[6] Dle něj se jedná o jeden ze základních aspektů práva na soukromý a rodinný život.[7] Ochrana osobních údajů je základním předpokladem práva na soukromí.[8]

V pojetí ESLP se za osobní údaj považují informace, které se vztahují na identifikované nebo identifikovatelné jedince (tzn. obsahují informace osobního charakteru).[9] Při určení obsahu informací bere ESLP v úvahu kontext jejich získání a uložení, povahu, způsob použití a nakládání s nimi a také, co z nich může být dovozeno.[10] Příkladem, kdy informace je osobním údajem ve smyslu judikatury ESLP je tzv. zvláštní kategorie osobních údajů[11] nebo bankovní dokumenty.[12]

---

[5] Čl. 8 Úmluvy zní:

„1. Každý má právo na respektování svého rodinného a soukromého života, obydlí a korespondence.

2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných."

[6] *Guide on Article 8 of the European Convention on Human Rights* [online]. Evropský soud pro lidská práva, 2020, s. 38 an. a 44 an. [cit. 1. 9. 2020]. Dostupné z: https://www.echr.coe.int/documents/guide_art_8_eng.pdf

[7] Ibid., s. 39.

[8] Např. *S. a Marper proti Spojenému království*, rozsudek ESLP, 4. 12. 2008 č. stížnosti 30562/04 a 30566/04, odst. 103; nebo *Satakunnan Markkinapörssi Oy And Satamedia Oy proti Finsku*, rozsudek ESLP, 27. 6. 2017 č. stížnosti 931/13, odst. 137.

[9] *S. a Marper proti Spojenému království*, rozsudek ESLP, odst. 68; a *P. a S. proti Polsku*, rozsudek ESLP, 30. 10. 2012 č. stížnosti 57375/08, odst. 130.

[10] S. *a Marper proti Spojenému království*, rozsudek ESLP; odst. 67 a tam citovaná judikatura.

[11] Dříve označované jako tzv. citlivé údaje. *Guide on Article 8 of the European Convention on Human Rights*, odst. 173.

[12] Ibid.

Už jenom samotné zaznamenání těchto údajů následně zakládá zásah do soukromí,[13] není vyžadováno jejich využití.[14] V takových případech je nutné posoudit, zda je tento zásah v souladu s Úmluvou. Toto zjištění se provádí za pomoci testu stanoveným čl. 8 odst. 2 Úmluvy, který se označuje jako tzv. pětistupňový test (aplikovatelnost Úmluvy; existence zásahu; legalita; legitimní cíl; nezbytnost v demokratické společnosti).[15] V tomto článku budou klíčové zejména dva jeho kroky: legalita a nezbytnost.

Aby byl zásah legální, je nutné jej učinit na základě dostatečně kvalitního právního základu. Kvalitu práva ESLP určuje prostřednictvím jeho dostupnosti a předvídatelnosti ve spojení s existencí záruk proti svévoli veřejných orgánů při aplikaci práva.[16]

V případě nezbytnosti v demokratické společnosti se zkoumá, zda zásah odpovídal naléhavé společenské potřebě a zda byl přiměřený sledovanému legitimnímu cíli. Komentář uvádí, že tento krok funguje jako *black box* – jedná se o nejméně předvídatelný krok. Obecně je ale možné konstatovat, že v potaz bere ESLP důležitost chráněného práva, (ne)existenci evropského konsenzu, důležitost zájmu na zásahu a rozsah zásahu.[17]

Dle čl. 15 Úmluvy je státům umožněno suspendovat závazky, které jim z čl. 8 Úmluvy vyplývají. Česká ani Slovenská republika této možnosti nevyužily,[18] a tak se Úmluva uplatňuje na jejich systémy chytrých karantén v plném rozsahu.

V rámci právního rámce mezinárodní organizace Rady Evropy, pod kterou Úmluva spadá, je nutné zmínit i tzv. Úmluvu 108.[19] Tato úmluva nastavuje obecné principy zpracování osobních údajů. Dále představené ná-

---

[13] *S. a Marper proti Spojenému království*, rozsudek ESLP, odst. 67.

[14] *Leander proti Švédsku*, rozsudek ESLP, 26. 3. 1987, č. stížnosti 9248/81, odst. 48.

[15] K tomu blíže srov. KMEC, Jiří et al. *Evropská úmluva o lidských právech: komentář*. Praha: C.H. Beck, 2012, s. 99.

[16] Ibid., s. 106–109.

[17] Ibid., s. 113–117.

[18] Notifications under Article 15 of the Convention in the context of the COVID-19 pandemic. In: *Council of Europe* [online] [cit. 18.02.2021]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/62111354

[19] Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, která byla vyhlášena pod č. 115/2001 Sb. m. s.

stroje regulace ovšem představují mnohem detailnější úpravu práv a povinností,[20] a proto bude pozornost věnována především jim. Poukázat se v tomto ohledu dá pak i na další dokumenty Rady Evropy vydané v průběhu pandemie.[21]

2.2 … PODLE PRÁVA EU

V primárním právu EU najdeme právo na ochranu osobních údajů jak v čl. 16 Smlouvy o fungování EU, tak v čl. 8 Listiny základních práv EU.[22] Právo na respektování soukromého života je pak zakotveno v čl. 7 Listiny základních práv EU.[23] V souvislosti s tímto katalogem práv je nutné připomenout jednak limity jeho aplikace dané čl. 51 odst. 1 (aplikuje se pouze v případě, že stát uplatňuje právo EU) a jednak výkladové ustanovení čl. 52 odst. 3 (povinnost výkladu obdobných práv v souladu s Úmluvou).

O aplikovatelnosti práva EU není v rámci zpracování osobních údajů v chytrých karanténách pochybností. Všechny technické způsoby, kterými Česká a Slovenská republika bojují proti koronaviru spadají pod sekundární právo EU – ať už se aplikují obecná pravidla pro osobní údaje stanovená v nařízení (EU) 2016/679, obecné nařízení o ochraně osobních údajů („GDPR“), nebo sektorová úprava pro ochranu elektronické komunikace upravená směrnicí 2002/58/ES, která stanovuje možnosti zpracování údajů sbíraných mobilními operátory při poskytování služeb.

---

[20] DE TERWANGNE, Cécile. Council of Europe convention 108+: A modernised international treaty for the protection of personal data. *Computer Law & Security Review*. 2021, roč. 40, s. 3. DOI: 10.1016/j.clsr.2020.105497

[21] Např. PIERUCCI, Alessandra a Jean-Philippe WALTER. Joint Statement on the right to data protection in the context of the COVID-19 pandemic. In: *Council of Europe* [online]. 2020 [cit. 18. 5. 2020]. Dostupné z: https://rm.coe.int/covid19-joint-statement/16809e09f4 Rozcestník k dalším relevantním dokumentům lze najít na https://www.coe.int/en/web/data-protection/-/saving-lives-respecting-data-protecti-1.

[22] Čl. 8 odst. 1 a 2 Listiny základních práv EU zní:

„1. Každý má právo na ochranu osobních údajů, které se ho týkají.

2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.“

[23] Čl. 7 Listiny základních práv EU zní:

„Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.“

Pojem „osobní údaj“ je v rámci EU vykládán tzv. objektivním způsobem. To znamená, že pro posouzení údaje jako osobního postačí, pokud existuje jiná informace, která ve spojení s tou první vede k identifikaci konkrétní osoby. Tato druhá informace přitom nemusí být nutně v dispozici téže osoby, ba dokonce k ní ani nemusí mít přístup.[24]

EU je obecně v tématu ochrany osobních údajů v souvislosti s koronavirem aktivní. Na začátku krize vydala Evropská komise doporučení týkající se využití digitálních technologií[25] a následovaly i pokyny k chytrým aplikacím.[26]

2.3 … V NÁRODNÍCH PRÁVNÍCH ÚPRAVÁCH

Mimo vyjmenované předpisy mezinárodního práva a práva EU jsou soukromí a osobní údaje chráněny v České a Slovenské republice i na národní úrovni.

V České republice se jedná zejména o čl. 10 odst. 2 a 3 Listiny základních práv a svobod, které se věnují informačnímu sebeurčení.[27] Zahrnují tak i právo na ochranu před sledováním a hlídáním ze strany veřejné moci.[28] Při hodnocení zásahu do tohoto práva bere Ústavní soud ČR v potaz v zásadě stejné aspekty, jako ESLP při hodnocení zásahů do práva garantovaného čl. 8 Úmluvy.[29]

---

[24] Rozsudek Nejvyššího správního soudu ze dne 13. 8. 2020, č. j. 1 As 387/2019-56, odst. 25–28.

[25] Doporučení Komise (EU) 2020/518 ze dne 8. dubna 2020 o společné sadě nástrojů Unie pro využití technologií a dat k boji proti krizi COVID-19 a ukončování souvisejících mimořádných opatření, zejména pokud jde o mobilní aplikace a využívání anonymizovaných dat o mobilitě.

[26] Sdělení Komise Pokyny k aplikacím podporujícím boj proti pandemii COVID-19 ve vztahu k ochraně údajů 2020/C 124 I/01.

[27] Čl. 10 odst. 2 a 3 Listiny základních práv a svobod zní:

„(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“

[28] WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012, kap. Čl. 10 odst. 3.

[29] Ibid.

Z podústavních předpisů jsou pak relevantní zejména předpisy provádějící nebo implementující sekundární právo EU, jako je zákon č. 110/2019 Sb., o zpracování osobních údajů, reagující na GDPR a zákon č. 127/2005 Sb., o elektronických komunikacích („ElKomČR"), implementující směrnici 2002/28/ES. Relevantní jsou pak také některé sektorové předpisy (např. ve vztahu k bankovnictví), které budou zmíněny dále v textu. V nich jsou totiž upraveny možnosti prolomení telefonního či bankovního tajemství.

Ústava SR obsahuje zcela totožné ustanovení o ochraně osobních údajů v čl. 16 odst. 1 a čl. 19 odst. 2 a 3 jako je v české Listině základních práv a svobod. Zákonnou úpravou poté je zákon č. 18/2018 Z. z., o ochrane osobných údajov a také zákon č. 351/2011 Z. z., o elektronických komunikáciách („ElKomSR").

3. POPIS CHYTRÝCH KARANTÉN

Popsaný skutkový stav se týká zásadně prvních verzí chytrých karantén, které byly vyvinuty a nasazeny v první polovině roku 2020. Od té doby prošly oba systémy změnami, které v některých případech i zcela zásadně ovlivnily jejich fungování. Tyto změny jsou reflektovány ve třetí části, kde jsou hodnoceny zásadní nedostatky přístupu obou zemí. Časový posun ovšem může přinést problém v dostupnosti některých odkazovaných zdrojů (např. došlo k aktualizaci informací pro subjekty údajů).[30]

3.1 ČESKÁ REPUBLIKA

Chytrá karanténa se v České republice na jaře 2020 skládala ze dvou hlavních větví. První byla tvorba vzpomínkových map pro preciznější dohledání kontaktů nakaženého a druhá byla aplikace eRouška sloužící pro zaznamenávání kontaktů s osobami kolem.[31]

[30] V některých případech je možné využít služby zaznamenávající snapshoty webových stránek, např. https://web.archive.org.

[31] Chytrá karanténa – Aktuální informace o COVID-19. In: *Ministerstvo zdravotnictví ČR* [online] [cit. 5. 8. 2020]. Dostupné z: https://koronavirus.mzcr.cz/chytra-karantena/

3.1.1 VZPOMÍNKOVÉ MAPY

Vzpomínkové mapy vytvářela Krajská hygienická stanice („KHS“) během telefonátu s pozitivně testovanou osobou. Mapa se využívala k tomu, aby tato osoba mohla určit co nejvíce ostatních osob, se kterými se v inkriminované době potkala a mohla je potenciálně nakazit. Sdělení takových údajů je součástí obecné povinnosti nakaženého poskytnout součinnost při epidemiologickém šetření podle § 62a zákona č. 258/2000 Sb., o ochraně veřejného zdraví („OchrZdrČR“).

Do vzpomínkové mapy mohla být, na základě souhlasu nakaženého, přidána i data poskytnutá bankami a telefonními operátory,[32] což mělo usnadnit rozpomenutí si na všechny relevantní osoby. Pokud nakažený souhlas neudělil, vznikla vzpomínková mapa pouze z údajů, které on sám KHS sdělil.[33] Právní úprava neumožňovala předání, a ani následné zpracování v podobě vytvoření vzpomínkové mapy, na základě jiného titulu nežli souhlasu.[34] Tento článek se bude dále zabývat jenom situací, ve které souhlas byl poskytnut.

Právní rámec se skládal z podzákonných předpisů, jmenovitě usnesení vlády ČR[35] a mimořádného opatření Ministerstva zdravotnictví ČR,[36] které na základě § 69 odst. 1 písm. i) a odst. 2 OchrZdrČR uložilo mobilním operátorům a bankám povinnost předat dále uvedené údaje nakaženého. Dále mimořádné opatření stanovilo bližší podmínky zpracování takto poskytnutých osobních údajů. Povinnost bank a operátorů přitom, z důvodu povinnosti KHS získat souhlas s poskytnutím osobních údajů, přímo nekoli-

[32] *Souhrnná DPIA Jednotný informační systém KHS pro podporu call centra a vzpomínkové mapy v. 1.09*, s. 3. Po omezený čas k dispozici z: https://cutt.ly/Pk6taDW. DPIA vzpomínkových map bylo získané na základě žádosti autora podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Odpověď povinného subjektu je dostupná z: https://www.mzcr.cz/wp-content/uploads/2020/08/239_2020_A.pdf.

[33] *Chytrá karanténa – Aktuální informace o COVID-19*.

[34] NULÍČEK, Michal, Bohuslav LICHNOVSKÝ a Filip BENEŠ. *Chytrá karanténa – proč v Česku potřebujeme souhlas?* [online]. 2020 [cit. 5. 8. 2020]. Dostupné z: https://rowan.legal/chytra-karantena-proc-v-cesku-potrebujeme-souhlas/

[35] Usnesení Vlády ČR č. 250 ze dne 18. 3. 2020, k zajištění zvýšené ochrany obyvatel – trasováním.

[36] Mimořádné opatření Ministerstva zdravotnictví ČR ze dne 19. 3. 2020, č.j. MZDR 12398/2020-1/MIN/KAN.

dovala ani se zvláštní sektorovou úpravou chránící data klientů bank a mobilních operátorů.[37]

Mobilní operátoři poskytovali KHS údaje o vysílačích, na které se připojil mobilní telefon dané nakažené osoby. Podle vyjádření mobilního operátora byla přesnost určení na úrovni obcí či částí měst, ale již nikoliv na úrovni ulic či konkrétních domů.[38] Banky předávaly údaje o době a místě použití elektronického platebního prostředku nakažené osoby, a to pouze pro oblast, která byla vydefinována na základě údajů od mobilních operátorů.[39] Časový rozsah poskytnutých údajů byly až tři poslední týdny.[40]

Další osobní údaje vyskytující se v rámci tvorby vzpomínkových map byly jméno a příjmení osoby, její adresa, telefonní číslo, zdravotní stav, rodné číslo a kontakty na třetí osoby.[41]

Právním titulem pro zpracování byla zákonná povinnost poskytnutí spolupráce při epidemii podle § 62a OchrZdrČR a plnění úkolů veřejného zájmu.[42] Zpracování zvláštní kategorie poté bylo prováděno na základě veřejného zájmu.[43] Se souhlasem se počítalo pouze pro poskytnutí údajů od operátorů a bank, a nikoliv pro jejich další zpracování.[44]

Vzpomínkové mapy byly vymazány maximálně šest hodin po vytvoření.[45]

Jako správce zde vystupovalo Ministerstvo zdravotnictví ČR. V pozicích zpracovatelů se vyskytovaly další subjekty, mezi které patřila např. společnost Keboole, Amazon Web Services EMEA SARL, či Armáda ČR.[46]

---

[37] Ustanovení § 91 odst. 2 ElKomČR, jako právní úprava pro mobilní operátory, a § 38 zákona č. 21/1992 Sb., o bankách, ve vztahu k bankám.

[38] KLOUDA, Jan. Bez emocí to jde správně. In: *LinkedIn* [online]. 24. 3. 2020 [cit. 5. 8. 2020]. Dostupné z: https://www.linkedin.com/pulse/bez-emoc%C3%AD-jde-spr%C3%A1vn%C4%9B-jan-klouda.

[39] Bod I písm. b) mimořádného opatření MZDR 12398/2020-1/MIN/KAN.

[40] *Chytrá karanténa – Aktuální informace o COVID-19*.; *DPIA vzpomínkových map*, s. 4.

[41] *DPIA vzpomínkových map*, s. 10.

[42] Právní základ podle čl. 6 odst. 1 písm. c) a e) GDPR.

[43] Právní základ podle čl. 9 odst. 2 písm. g) a i) GDPR; srov. *DPIA vzpomínkových map*, s. 4.

[44] Ibid., s. 4 a 11.

[45] Ibid., s. 16.

[46] Ibid., s. 11 a 12.

Následně došlo ke kompletnímu převedení provozu na stát a soukromé společnosti jako Keboole se tedy už na zpracování osobních údajů nepodíleli.[47]

3.1.2 MOBILNÍ APLIKACE EROUŠKA

Aplikace eRouška umožňovala prostřednictvím technologie Bluetooth automatický záznam identifikátorů mobilních telefonů osob, v jejichž blízkosti se majitel telefonu nacházel. Pokud byla následně jedna z těchto osob testována pozitivně, měla možnost poskytnout tuto informaci ostatním a tím je upozornit na potenciální nakažení.

Aplikace zaznamenávala ID telefonů mající tutéž aplikaci společně se sílou signálu pro odhad vzájemné vzdálenosti.[48] Údaje, které se o „setkání" ukládaly, byly náhodný identifikační řetězec znaků identifikující protější telefon (navíc každou hodinu obměňovaný)[49], časové razítko a síla signálu Bluetooth.[50] Všechny informace byly uloženy lokálně na telefonu, a to po dobu pěti dní od vytvoření.[51] Vznikla tak decentralizovaná databáze.[52] Centrálně byl uložen náhodný identifikační řetězec spojený s telefonním číslem uživatele pro případný kontakt při hrozbě nakažení – dohromady spojit konkrétní osobu a její identifikátor tak mohla pouze KHS.[53]

---

[47] Provoz chytré karantény nyní zajišťuje Národní agentura pro komunikační a informační technologie, s. p. na základě smlouvy s Ministerstvem zdravotnictví ČR. Smlouva je dostupná z https://smlouvy.gov.cz/smlouva/13430376.

[48] *Souhrnná DPIA eRouška v. 0.2*, s. 3 a 4. Po omezený čas k dispozici z: https://cutt.ly/blhBHUh. DPIA eRoušky bylo získané na základě žádosti autora podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Odpověď povinného subjektu je dostupná z: https://www.mzcr.cz/wp-content/uploads/2020/08/239_2020_A.pdf.

[49] JANN, Ole, Pavel KOCOUREK a Jakub STEINER. *Využití technologie Bluetooth pro trasování šíření covid-19* [online]. Institut pro demokracii a ekonomickou analýzu, 2020, s. 7 [cit. 5. 8. 2020]. Dostupné z: https://idea.cerge-ei.cz/files/IDEA_Trasovani_covid19_duben2020_14.pdf

[50] Ochrana soukromí a cookies eRoušky. In: *eRouška* [online] [cit. 08.05.2020]. Dostupné z: https://erouska.cz/podminky-pouzivani; a *DPIA eRouška v. 0.2*, s. 12. Zapsaná informace vypadala např. takto: „31.3.2020 od 12:15 do 13:15 byla ve vaší blízkosti aplikace s identifikátorem ID 29091" (viz Ibid., s. 5.).

[51] *DPIA eRouška v. 0.2*, s. 4.

[52] JANN, Ole, Pavel KOCOUREK a Jakub STEINER. *Využití technologie Bluetooth pro trasování šíření covid-19*, s. 4.

Nezávislé instituce potvrdily, že aplikace odesílala seznam zaznamenaných identifikátorů pouze s výslovným souhlasem uživatele a nesbírala polohové údaje.[54]

Identifikované právní tituly pro zpracování byly veřejný zájem[55] a souhlas.[56]

Poskytnuté telefonní číslo zůstalo uloženo na serveru i po odinstalování aplikace, spolu s identifikátorem uživatele a značkou a modelem telefonu, na kterém aplikace byla.[57] Přesná retenční doba těchto údajů nebyla určena.[58]

Správcem osobních údajů bylo Ministerstvo zdravotnictví ČR, zpracovateli společnost Keboole, platforma Google Cloud a Firebase.[59] Google Cloud Platform ve zpracování vystupovalo z důvodu hostování dat na tamních serverech.[60]

3.1.3 DALŠÍ RELEVANTNÍ INFORMACE

Je také na místě upozornit, že v Česku byl v souvislosti s koronavirem aplikovatelný i obecný právní rámec o *data retention*.[61] K metadatům komunikace uživatelů se tak mohly dostat orgány činné v trestním řízení v rámci vyšetřování trestných činů spáchaných za nouzového stavu, a to i v přímé souvislosti s koronavirem.[62] Protože tuto původně možnou širokou aplikovatelnost lze nyní považovat za omezenou[63] a navíc úprava *data retention*

---

[53] *Ochrana soukromí a cookies eRoušky*.; *DPIA eRouška v. 0.2*, s. 5 a 6. Mimo uvedené údaje schraňovala aplikace i další údaje, které jsou pro zde činěné úvahy irelevantní. Konkrétně šlo o typ telefonu, typ OS, výrobce zařízení, verzi systému, jazykovou lokalizaci a různé tokeny (srov. Ibid., s. 13 a 14.).

[54] Potvrzení jsou dostupná z: https://erouska.cz/downloads/cvut3.pdf; https://erouska.cz/downloads/cvut2.pdf; a https://erouska.cz/downloads/cvut.pdf.

[55] Právní titul podle čl. 6 odst. 1 písm. e) a čl. 9 odst. 2 písm. h) a i) GDPR; *DPIA eRouška v. 0.2*, s. 15.

[56] Právní titul podle čl. 6 odst. 1 písm. a) a čl. 9 odst. 2 písm. a) GDPR; Ibid., s. 16.

[57] Ibid., s. 13.

[58] Ibid., s. 21.

[59] Ibid., s. 15.

[60] Ibid., s. 7.

[61] Ustanovení § 97 odst. 4 a 3 ElKomČR.

je v současné době shledána ústavně konformní,[64] nebude zde tomuto tématu dále věnován prostor.

4. SLOVENSKÁ REPUBLIKA

I slovenská chytrá karanténa se skládala ze dvou částí. První byla mobilní aplikace eKaranténa a druhá pak nová oprávnění Úradu verejného zdravotníctva SR („ÚVZ“) vyžadovat údaje od mobilních operátorů. Podle vyjádření vlády SR a ÚVZ v řízení před Ústavním soudem SR byla plánována i obdoba vzpomínkových map.[65] O zavedení tohoto systému ovšem nejsou dostupné jakékoliv informace.

I v případě slovenského řešení jsem žádal o poskytnutí relevantních DPIA, nicméně zatím neúspěšně.[66] Zde poskytnutý obraz je tak získaný téměř výhradně z veřejných zdrojů.

4.1 MOBILNÍ APLIKACE EKARANTÉNA

Na jaře 2020 byla povinná karanténa po překročení slovenských státních hranic v zásadě vykonávána v tzv. „státní karanténě“, tzn. v některé z k tomuto účelu vyhrazené budově, a to až do okamžiku prokázání se negativním testem.[67] Alternativou byla tzv. „smart karanténa“, která probíhala v obydlí osoby za využití mobilní aplikace eKaranténa.

Aby mohla osoba vykonat izolaci v domácí smart karanténě, musela udělit souhlas.[68] Doma pak byla prostřednictvím mobilní aplikace hlídána, přičemž její využívání bylo povinné.[69] Kontrola dodržování nařízené karantény prostřednictvím aplikace probíhala jednak skrze záznam polohy telefonu s pomocí technologie GPS a jednak skrze povinnost vyfotit na vyzvání

---

[62] Ustanovení § 88a odst. 1 zákona č. 141/1961 Sb., trestní řád. Může se jednat např. o trestný čin šíření nakažlivé lidské nemoci (§ 152 odst. 2 písm. b) zákona č. 40/2009 Sb., trestní zákoník), krádež (§ 205 odst. 4 písm. b) tamtéž), podvod (§ 209 odst. 4 písm. c) tamtéž) nebo šíření poplašné zprávy (§ 357 odst. 4 písm. a) tamtéž).

[63] Pro období nouzového stavu srov. přiměřeně rozsudek Nejvyššího soudu ze dne 16. 3. 2021, sp. zn. 15 Tdo 110/2021. Pro období tzv. „pandemické pohotovosti“ pak srov. § 14 zákona č. 94/2021 Sb., o mimořádných opatřeních při epidemii onemocnění COVID-19.

[64] Nález Ústavního soudu ČR ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.

[65] Usnesení Ústavního soudu SR ze dne 13. 3. 2020, č. j. PL. ÚS 13/2020-103, odst. 73-74.

selfie, která se automaticky porovnala s fotografií nahranou do databáze při registraci.[70] K tomu stanovil zákon související povinnosti (povolit geolokaci, umožnit aktualizace, uložit fotografii pro porovnání apod.).[71]

Porovnání polohy telefonu s oblastí, kde osoba měla vykonávat karanténu a porovnání pořizovaných selfie, se provádělo pouze na koncovém zařízení.[72] Tyto údaje poté byly vymazány do 30 dní od jejich vzniku.[73]

Aplikace eKaranténa vedle toho taktéž umožňovala, obdobně jako česká eRouška, zaznamenávání kontaktu s jinými osobami prostřednictvím tech-

[66] Žádost o poskytnutí tří relevantních DPIA podle zákona č. 211/200 Z. z., o slobode informácií („SlInf“) byla ÚVZ odmítnuta rozhodnutím ze dne 16. 7. 2020, č. RK/5554/20 (po omezený čas dostupné z https://cutt.ly/VkP4Ogz) z důvodu, že DPIA aplikace eKaranténa je obchodním tajemstvím (§ 10 odst. 1 SlInf), byla jí odevzdána třetí osobou, která se zveřejněním nesouhlasí (§ 11 odst. 1 písm. a) SlInf) a zároveň by došlo k porušení duševního vlastnictví (písm. c) tamtéž). Ministerstvo zdravotnictví SR jako odvolací orgán rozhodnutím ze dne 24. 9. 2020, č. S15047-2020-ONAPP-2 (po omezený čas dostupné z https://cutt.ly/UkP7d4z) prvostupňové rozhodnutí zrušilo jako nepřezkoumatelné a věc vrátilo k dalšímu řízení. ÚVZ následně žádost opět odmítl rozhodnutím ze dne 29. 10. 2020, č. RK/7217/2020 (po omezený čas dostupné z https://cutt.ly/GkP5q3U), tentokrát protože by poskytnutí všech DPIA bylo v rozporu s právem EU (zejména GDPR) (§ 11 odst. 1 písm. g) SlInf) a protože jde o dokumenty, které obsahují informace využitelné na plánování a vykonání narušení objektů zvláštní důležitosti (písm. i) tamtéž). Ani tomuto odůvodnění odvolací orgán nepřisvědčil a rozhodnutím ze dne 24. 11. 2020, č. S17812-2020-ONAPP-2 (po omezený čas dostupné z https://cutt.ly/CkP6fYo) věc vrátil k dalšímu řízení. Následně ÚVZ vydal dne 30. 12. 2020 další odmítavé rozhodnutí č. OK/10825/2020 (po omezený čas dostupné z https://cutt.ly/ckAqPmc), podle kterého část požadovaných DPIA nebyla zpracována a DPIA eKarantény je obchodní tajemství a duševní vlastnictví třetí osoby (bylo vypracováno advokátní kanceláří Dagital Legal, s.r.o.) (§ 10 odst. 1 SlInf a § 11 odst. 1 písm. c) SlInf), bylo vypracováno zdarma, ÚVZ nedisponuje DPIA fyzicky (má ho pouze ona advokátní kancelář) a ÚVZ by vznikla škoda (protože za jakékoliv zpřístupnění je sjednána smluvní pokuta 50.000 EUR). Toto rozhodnutí bylo rozhodnutím odvolacího orgánu ze dne 23. 2. 2021, č. S11089-2021-0ddNAPP-2 (po omezený čas dostupné z https://cutt.ly/nl2sTF9) opět zrušeno jako nepřezkoumatelné. Přípisem ze dne 23. 3. 2021 byla část žádosti (ve vztahu k DPIA aplikace eKarantény) postoupena podle § 15 odst. 1 SlInf Úřadu na ochranu osobních údajů SR, který tuto část žádosti odmítl rozhodnutím ze dne 1. 4. 2021, č. 00157/2021-Ku/2 (po omezený čas dostupné z https://cutt.ly/db0SnDV), neboť jde o dokument získaný v průběhu kontroly (§ 11 odst. 1 písm. h) SlInf). Následně ÚVZ vydal dne 22. 3. 2021 rozhodnutí č. OK/2363/2021 (po omezený čas dostupné z https://cutt.ly/4x0uRkE), kterým celou žádost opět odmítnul, neboť DPIA aplikace eKaranténa nemá v jakékoliv podobě k dispozici a DPIA předávání osobních údajů podle § 63 odst. 18 až 20 nebylo zpracováno. Odvolací rozhodnutí Ministerstva zdravotnictví SR ze dne 12. 5. 2021, č. Sl4938-2021-OddNAPP-2 (po omezený čas dostupné z https://cutt.ly/ib0P8Fy) napadené rozhodnutí znovu zrušilo a věc vrátilo k dalšímu řízení. K DPIA aplikace eKaranténa konstatovalo, že postoupí-li povinná osoba část žádosti, je nezákonným postupem, pokud ve stejné části žádost zároveň odmítne. Ve vztahu ke zbylým částem bylo rozhodnutí nepřezkoumatelné. Ve vztahu k DPIA aplikace eKaranténa

nologie Bluetooth.[74] Zaslání oznámení o možném kontaktu s nakaženou osobou mohlo být provedeno jen s jejím souhlasem.[75]

V současné době již není třeba aplikace eKarantény při vstupu na Slovensko. Původní opatření ÚVZ, kterým byla tato povinnost stanovena, bylo k 10. 6. 2020 zrušeno a povinnost využívat aplikaci eKarantény nebyla znovu stanovena.[76] Nyní již aplikace eKarantény není dostupná ani ke stažení.[77]

4.2 PŘEDÁVÁNÍ DAT MOBILNÍMI OPERÁTORY

Slovenský zákonodárce na pandemii také reagoval přijetím zákona č. 62/2020 Z. z., o niektorých mimoriadnych opatreniach v súvislosti so šírením nebezpečnej nákazlivej ľudskej choroby COVID-19 a v justícii. Tímto zákonem byly do § 63 ElKomSR, vloženy odstavce 18 až 20, které přikázaly mobilním operátorům poskytovat ÚVZ údaje o svých zákaznících. Na základě návrhu poslanců Národní rady SR pozastavil Ústavní soud SR účinnost části uvedeného ustanovení.[78] Slovenský zákonodárce

jsem tak dne 19. 5. 2021 podal novou žádost, která nebyla zatím vyřízena.

[67] Opatrenie ÚVZ pri ohrození verejného zdravia – eKarantény ze dne 22. 5. 2020, sp. zn. OLP/4311/2020.

[68] Ustanovení § 60a odst. 3 zákona č. 355/2007 Z.z., o ochrane, podpore a rozvoji verejného zdravia („OchrZdrSR“).

[69] Ustanovení § 51 odst. 1 písm. f) OchrZdrSR.

[70] Smart karanténa - najčastejšie otázky ohľadne karantény v domácej izolácii s využitím aplikácie eKarantény. In: *Korona.gov.sk* [online] [cit. 04.10.2020]. Dostupné z: https://korona.gov.sk/najcastejsie-otazky/ekarantena/

[71] Ustanovení § 60a odst. 4 OchrZdrSR.

[72] *Smart karanténa - najčastejšie otázky ohľadne karantény v domácej izolácii s využitím aplikácie eKarantény*.

[73] Ustanovení § 60d odst. 4 OchrZdrSR.

[74] Ustanovení § 60a odst. 8 písm. d) OchrZdrSR.

[75] Ustanovení § 60b odst. 3 OchrZdrSR.

[76] Opatrenie ÚVZ pri ohrození verejného zdravia – domáca izolácia, zrušenie štátnej karantény ze dne 9. 6. 2020, sp. zn. OLP/4739/2020.

[77] Aplikace byly původně dostupné na těchto adresách: https://play.google.com/store/apps/details?id=sk.nczi.ekarantena a https://apps.apple.com/sk/app/ekarantena-slovensko/id1513127897.

jednal rychle, a již o dva dny později citované ustanovení novelizoval,[79] pročež Ústavní soud SR řízení zastavil.[80] V současné době zní relevantní část tohoto ustanovení (včetně vyznačení zmíněné novelizace – ~~přeškrtnuté~~ odebráno, podtržené přidáno) takto:

> *(18) Údaje, ktoré sú predmetom telekomunikačného tajomstva podľa odseku 1 písm. b) a d) spolu s informáciou o čase vzniku lokalizačného údaju podnik v čase mimoriadnej situácie[46d] alebo núdzového stavu[46e] v zdravotníctve, a to v príčinnej súvislosti so vznikom pandémie[46g] alebo šírením nebezpečnej nákazlivej ľudskej choroby a po prijatí zodpovedajúcich technických a organizačných opatrení na ochranu súkromia a osobných údajov,[…]*
>
> *b) spracúva na účel identifikácie príjemcov správ, ktorým je potrebné oznámiť osobitné opatrenia [ÚVZ][46f] v záujme ochrany života a zdravia,*
>
> *c) spracúva výlučne v rozsahu potrebnom na identifikáciu ~~užívateľov~~ pohybu dotknutého užívateľa v záujme ochrany života a zdravia.*
>
> *(19) Údaje spracúvané podľa odseku 18 podnik poskytuje [ÚVZ] na základe odôvodnenej písomnej žiadosti a s písomným súhlasom alebo inak hodnoverne preukázateľným súhlasom dotknutého užívateľa. […]*
>
> *(20) [ÚVZ] môže po prijatí zodpovedajúcich technických a organizačných opatrení na ochranu súkromia a osobných údajov údaje spracúvané podľa odseku 18 zbierať, spracúvať a uchovávať počas trvania mimoriadnej situácie alebo*

[78] Ústavní soud SR pozastavil účinnost § 62 odst. 18 písm. c) ElKomSR a také § 63 odst. 19 a 20 ElKomSR v rozsahu, v jakém se na ně vztahuje § 63 odst. 18 písm. b) a c) téhož předpisu; srov. usnesení Ústavního soudu SR č. j. PL. ÚS 13/2020-103.

[79] Zákon č. 119/2020 Z.z., ktorým sa mení a dopĺňa zákon č. 355/2007 Z.z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa mení a dopĺňa zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov.

[80] Usnesení Ústavního soudu SR ze dne 27. 3. 2020, č. j. PL. ÚS 13/2020-18.

> *núdzového stavu v zdravotníctve, najdlhšie do 31. decembra 2020. Údaje podľa odseku 18 musí [ÚVZ] bezodkladne zničiť, akonáhle pominie dôvod na ich spracúvanie; o zničení údajov [ÚVZ] bezodkladne písomne informuje dotknutého užívateľa, pričom uvedie údaje, ktoré o ňom spracúval. [ÚVZ] podá najneskôr do 31. januára 2021 Ústavnoprávnemu výboru Národnej rady Slovenskej republiky správu o zákonnosti spracúvania údajov podľa odseku 18; pôsobnosť Úradu na ochranu osobných údajov Slovenskej republiky tým nie je dotknutá.*

Údaje, na které citované ustanovení dopadlo, byly podle § 63 odst. 1 písm. b) a d) ElKomSR telefonní číslo, označení osoby včetně adresy trvalého pobytu nebo sídla obou stran komunikace a lokalizační údaje.

Vedle této úpravy ještě zákonodárce později přijal druhou novelu ElKomSR,[81] kterým vznikl § 42 odst. 5 a § 63 odst. 21 tohoto předpisu. Ty umožnily ÚVZ získat telefonní číslo všech osob, kterým byla zaslána varovná textová zpráva týkající se ochrany osob před hrozícím nebezpečím a opatření při ochraně života a zdraví. Podle důvodové zprávy má tato možnost sloužit státu k identifikaci osob, které se vrací z tzv. „červených krajin“, v důsledku čehož musí při návratu na Slovensko nastoupit do karantény. I takové poskytování údajů představuje průlom telekomunikačního tajemství.[82]

Ke zpracování lokalizačních údajů, pro určení relevantních osob nacházejících se v zahraničí, docházelo na straně operátorů bez souhlasu či informování. ÚVZ poté mohl údaje zpracovávat maximálně 60 dní.

Prezidentka přijetí zákona vetovala, byla ovšem Národní radou SR přehlasována.[83]

[81] Zákon č. 242/2020 Z. z., ktorým sa mení a dopĺňa zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

[82] Podle § 63 odst. 1 ElKomSR se do telekomunikačního tajemství řadí mj. telefonní číslo a lokalizační údaje.

4.3 SROVNÁNÍ PROVEDENÝCH OPATŘENÍ

Už na první pohled je znát rozdílný přístup k využití technologie v rámci strategie boje proti nákaze koronavirem. Zatímco v českém případě se od začátku projektu počítalo s využitím souhlasu pro předávání osobních údajů státu, na Slovensku byla první verze legislativy nastavena bez souhlasu, který byl přidán až po rychlém zásahu Ústavního soudu SR.

Dalším znatelným rozdílem zde je, že zatímco v České republice se u chytré karantény spoléhalo na podzákonné předpisy, v případě Slovenska existovala opora přímo v zákonech.

Diametrálně odlišný přístup je i v aplikacích. Česká aplikace eRouška fungovala pouze pro zaznamenání kontaktu s jinými osobami při pohybu na veřejných prostranstvích za využití technologie Bluetooth a pro případné trasování kontaktů nakaženého, zatímco její slovenský protějšek eKaranténa byl primárně nastaven tak, že hlídal dodržování nařízené karantény skrze připojení k internetu, polohové služby a selfie uživatele.

Již nyní je zřejmé, že průběh hodnocení bude v nastíněných případech rozdílný. Přijatá opatření jsou od sebe odlišná, stejně jako okruh údajů dostupných veřejné moci.

5. ANALÝZA ČESKÉHO ŘEŠENÍ

5.1 TECHNICKÉ ŘEŠENÍ APLIKACE EROUŠKA

Jak bylo popsáno výše, aplikace eRouška zaznamenávala kontakt s ostatními osobami skrze technologii Bluetooth. V rámci jejího fungování nebyly nikdy využity geolokační údaje. Tento postup je zcela v souladu s doporu-

[83] ŠTRAHA, Štěpán a Martina RIEVAJOVÁ. *UPDATE: Slovenský Úrad verejného zdravotníctva získal prístup k vašim telefónnym číslam, aj keď mu prezidentka dala stopku* [online]. 2020 [cit. 4. 10. 2020]. Dostupné z: https://www.havelpartners.blog/blog/slovensky-urad-verejneho-zdravotnictva-nebude-mat-zatial-pristup-k-vasim-telefonnym-cislam-prezidentka-mu-dala-stopku/157

čeními Evropské komise,[84] Evropského sboru pro ochranu osobních údajů[85] i odborné veřejnosti[86] ohledně minimalizace zásahu do soukromí uživatelů.

Nemůže být pochyb ani o tom, že se jedná o technologii vhodnější z hlediska zaznamenávání kontaktu. Byla totiž zaznamenávána faktická vzdálenost mezi telefony (skrze sílu signálu Bluetooth) a nikoliv jejich poloha na mapě. Omezila se tak možnost zaznamenání kontaktu tam, kde podle geolokačních údajů byly osoby v určité blízkosti (např. osoba v přízemním bytě s osobou bydlící v podkroví stejného domu), a zachytily se pouze tam, kde skutečně došlo k přiblížení osob.

Problematickým aspektem aplikace eRouška mohla být vytvořená centrální databáze telefonních čísel. Číslo musel uživatel zadat při registraci do aplikace. V centrální databázi pak telefonní číslo bylo propojené s jednotlivými identifikačními kódy osoby, čemuž měli přístup pověření pracovníci KHS.

Telefonní číslo (a tedy celá centralizovaná databáze) přitom nebylo pro funkčnost systému zcela nezbytné. Informaci o možném nakažení je totiž možné doručovat, bez zprostředkování KHS, automaticky prostřednictvím notifikací.[87]

Přesně tímto směrem se vydala druhá verze eRoušky vydaná na konci letních prázdnin 2020 a fungující dodnes. Změna způsobu fungování aplikace umožnila odstranit všechny osobní údaje z jejího provozu – Ministerstvo zdravotnictví ČR ani KHS tak zásadně nemohou ztotožnit jednotlivé

---

[84] Sdělení Komise, Pokyny k aplikacím podporujícím boj proti pandemii COVID-19 ve vztahu k ochraně údajů, s. 6.

[85] *Dopis předsedy Evropského sboru pro ochranu osobních údajů O. Micolovi* [online]. Evropská sbor pro ochranu osobních údajů, , s. 2 [cit. 1. 9. 2020]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

[86] COUNCIL OF EUROPE DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW. *AI Breakfasts: Covid-19 - Myths and realities of tracking applications* [online], č. 0:12:00 [cit. 18. 5. 2020]. Dostupné z: https://www.youtube.com/watch?v=l9d3B6AuvdI

[87] DOČEKAL, Daniel. Jak na iPhonech funguje trasování nákazy koronavirem (COVID-19 Exposure Tracing)? In: *Lupa.cz* [online]. 21. 5. 2020 [cit. 1. 9. 2020]. Dostupné z: https://www.lupa.cz/clanky/jak-na-iphonech-funguje-trasovani-nakazy-koronavirem-covid-19-exposure-tracing/

uživatele.[88] V současné době probíhá sběr identifikátorů na stejném principu jako v předchozí verzi[89] ale změnil se způsob nakládání s nimi.

Vlastní identifikátory mohou být po prokázání nakažení odeslány na servery aplikace. Podmínkou odeslání je ověření kódem z verifikační zprávy SMS, kterou odesílá systém buď automaticky anebo na pokyn pracovníka KHS. Zabraňuje se tak nekontrolovatelnému nahrávání identifikátorů osob, které nejsou nakaženy. Ze serveru aplikace si identifikátory nakažených osob mohou ostatní uživatelé stáhnout po dobu 14 dní. Údaje jsou pak lokálně vyhodnocovány a pokud aplikace identifikuje rizikový kontakt, lokálně vygeneruje notifikaci.[90] V celém tomto procesu není nakažená osoba identifikována.[91]

5.2 ABSENTUJÍCÍ PRÁVNÍ NORMY

Pro zpracování osobních údajů v první verzi eRoušky chyběla, dle mého názoru, v právním řádu dostatečná a transparentní opora. Ministerstvo zdravotnictví ČR se v DPIA eRoušky v. 0.2 odvolávalo na zpracování na základě veřejného zájmu a pro zvláštní kategorii osobních údajů uvedlo souhlas podpořený jinými tituly. Více se k právnímu základu v DPIA eRoušky v. 0.2 již neuvádí. Ačkoliv využití titulu veřejného zájmu v tomto případě není zcela zcestné, domnívám se, že zpracování těchto údajů by mělo být založeno na jasné právní normě, a tedy titulu plnění právní povinnosti. Ke stejnému závěru se přiklání i pokyny Evropské komise.[92]

Na druhou stranu byl rozměr tohoto problému relativizován dobrovolností poskytnutí údajů. Jak instalace aplikace, tak i následné odeslání vlastních identifikátorů bylo zcela na vůli jednotlivce. Právní řád neposkytoval možnosti donucení. I při zachování současného systému

[88] *DPIA eRouška 2.0, v. 6 ze dne 4. 2. 2021*, s. 32. Po omezený čas k dispozici z: https://cutt.ly/IlhNjjK. DPIA eRouška 2.0 bylo získané na základě žádosti autora podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Odpověď povinného subjektu je dostupná z: https://www.mzcr.cz/wp-content/uploads/2021/02/56-A.pdf.

[89] Ibid., s. 15.

[90] Ibid., s. 19.

[91] Ibid., s. 16 a 17.

[92] Sdělení Komise Pokyny k aplikacím podporujícím boj proti pandemii COVID-19 ve vztahu k ochraně údajů, s. 5.

dobrovolnosti by nicméně založení zpracování na plnění právní povinnosti fungování eRoušky více zprůhlednilo. Zároveň by mohly být nastaveny zcela jasné zákonné záruky proti zneužití takových údajů, jako například doba uložení nebo zákaz zpracování pro jiné účely. Odhlédneme-li od částečně jiné povahy slovenské aplikace eKaranténa, tak její právní zakotvení by mohlo být příkladem.

I tato výtka s dalším vývojem částečně odpadla. Za prvé je to z důvodu vynechání osobních údajů z řešení eRoušky[93] a za druhé kvůli přijetí relevantní právní úpravy.[94] Té je ovšem možné vytknout nedostatečnou konkrétnost, neboť pouze zmocňuje Ministerstvo zdravotnictví ČR ke zřízení aplikace a zakotvuje dobrovolné užívání. Stále tak chybí jasné mantinely zmiňované výše, jako je např. maximální doba zpracování.

Ze dvou probíraných částí chytré karantény je nicméně potřeba jasného zákonného základu zřetelně větší u tvorby vzpomínkových map. To je odůvodněno obsahem zpracovávaných osobních údajů (bankovní a telekomunikační tajemství). DPIA vzpomínkových map se mj. odvolává na plnění zákonné povinnosti (konkrétně § 62a odst. 1 a 67 OchrZdrČR). Tyto ustanovení nicméně nejsou dle mého názoru dostatečně konkrétní a přesná. Aby mohl správce založit zpracování na titulu plnění právní povinnosti, musí mu právní řád přímo něco přikazovat.[95]

Ustanovení § 62a odst. 1 OchrZdrČR pouze opravňuje příslušné správní orgány k provádění epidemiologických šetření. Existuje tedy diskrece orgánu co do způsobu provedení a titul plnění zákonné povinnosti nelze využít. Ustanovení § 67 OchrZdrČR potom sice stanovuje povinnost rozhodnout o protiepidemických opatřeních, ale tuto povinnost dále nikterak nespecifikuje.

---

[93] Pro verzi 2.0 byly identifikovány jako právní tituly čl. 6 odst. 1 písm. e) a čl. 9 odst. 2 písm. i) GDPR (zpracování ve veřejném zájmu) a pro mezinárodní spolupráci pak slouží souhlas. Srov. *DPIA eRouška 2.0*, s. 32 a 33.

[94] Ustanovení § 62 odst. 2 až 5 OchrZdrČR, které byly vloženy zákonem č. 94/2021 Sb., o mimořádných opatřeních při epidemii onemocnění COVID-19.

[95] NULÍČEK, Michal et al. *GDPR - obecné nařízení o ochraně osobních údajů*. Wolters Kluwer, 2018, kap. čl. 6 odst. 1 písm. e).

Povinnost předat osobní údaje a podrobnosti zpracování osobních údajů u vzpomínkových map stanovuje mimořádné opatření. To se odvolává na § 69 odst. 1 písm. i) OchVeřZdČR, který umožňuje vydat „*zákaz nebo nařízení další určité činnosti k likvidaci epidemie nebo nebezpečí jejího vzniku.*" Z tohoto ale vyvstávají dva problémy. Zaprvé dochází k omezení základního práva na základě podzákonného předpisu. Oproti tomu ale platí, že meze základních práv je možné podle čl. 4 odst. 2 Listiny základních práv a svobod omezit pouze zákonem.[96] Existuje zde tak evidentní rozpor. Zadruhé lze zpochybnit pravomoc Ministerstva zdravotnictví ČR vůbec takový předpis vydat. Jakkoliv citované ustanovení představuje zbytkovou kategorii jeho pravomocí při epidemii, nejde o kategorii bezbřehou. Nejvyšší správní soud ČR zde dovodil povinnost výkladu „stejného druhu" – tzn. při jejím výkladu lze dovodit pouze takové pravomoci, které odpovídají ostatním v tomto výčtu.[97] Zkoumané mimořádné opatření tak můžeme považovat za vydané *ultra vires*. Jako pojistku proti svévolnému zasahování státu do soukromí lze nicméně považovat nutnost souhlasu pro poskytnutí údajů od bank a mobilních operátorů.

Kritickým problémem zde byla (a stále je) nepřipravenost zvláštních právních předpisů na takovou situaci. Konkrétně jde o ElKomČR a § 38 zákona č. 21/1992 Sb., o bankách. Ani jeden totiž nepamatuje na jakoukoliv možnost předávání dat státu za této situace nebo na možnost zpracování údajů chráněných bankovním či telefonním tajemstvím pro tyto účely. Nedomnívám se, že předání osobních údajů bylo zcela v rozporu se sektorovou úpravou, ale určitě se pohybuje v šedé zóně. Takové řešení je ale v případě takto širokého omezování základních práv značně nešťastné.

Závěrem bych chtěl také upozornit na fakt, že podle zjištěných informací došlo již v září 2020 k ukončení využívání dat od bank,[98] ale nikoliv již k navazující úpravě mimořádného opatření, které stanovuje rámec pro přenos či informační povinnosti správce. O konci využívání bankovních dat

[96] Obdobně pak srov. usnesení Ústavního soudu SR č. j. PL. ÚS 13/2020-103, odst. 100.

[97] Rozsudek Nejvyššího správního soudu ze dne 26. 2. 2021, č. j. 6 As 114/2020-63, zejm. odst. 142 až 144.

[98] Tato informace byla sdělena autorovi v průběhu telefonátu s pověřencem pro ochranu osobních údajů Ministerstva zdravotnictví ČR dne 15. 9. 2020.

se nadto nedají najít ani žádné oficiální publikované informace. Postup správce se tak stal matoucím a netransparentním.

Vzhledem k tomu, za jak důležitý prvek boje proti koronaviru byla celá chytrá karanténa považována,[99] jsem toho názoru, že jí měl být v rámci zákonodárství poskytnut větší prostor.[100] Zejména tedy vydefinování účelů v zákoně, spolu s poskytnutím záruk proti zneužití získaných údajů. Tato kritika ale neznamená, že by soukromí občanů anebo principy GDPR byly nějakým způsobem hrubě pošlapávány. Ono zákonné ukotvení by mělo sloužit pro zajištění právní jistoty a transparentnosti zpracování osobních údajů.

Za naplňující vytyčené nicméně nemůže být považován navrhovaný nový § 89a ElKomČR. Ten by měl umožnit hygienickým stanicím žádat po mobilních operátorech údaje o místě pobytu osoby s infekčním onemocněním v posledních třech týdnech, a to bez jejího souhlasu. Po poskytnutí má být osoba o tomto postupu notifikována. Tato nová povinnost je v důvodové zprávě pouze stroze odůvodněna potřebou efektivního trasování kontaktů.[101] Jde totiž o úpravu, která není potřebně kvalitní, podrobná, řádně odůvodněna a zajišťující dostatečnou kontrolu.[102]

---

[99] Za všechny odkazuji na Velikonoční projev Předsedy vlády ČR dostupný z: https://www.vlada.cz/cz/clenove-vlady/premier/projevy/velikonocni-projev-predsedy-vlady-180961/.

[100] Projednávané a schválené sněmovní tisky jsou důkazem toho, že projektu chytré karantény nebyl věnován jakýkoliv legislativní prostor. Jejich seznam je dostupný z https://www.psp.cz/sqw/tisky.sqw?str=13&O=8&PT=K&N=1&F=N&D=1,2,16&U=6,11&RA=20.

[101] Materiál č. j. OVA 971/20. In: *Portál Aplikace ODok* [online] [cit. 22. 3. 2021]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBSNH56J5

[102] K tomu blíže srov. RP: Návrh zákona o elektronických komunikacích je protiústavní. In: *Advokátní deník* [online]. 19. 1. 2021 [cit. 22.03.2021]. Dostupné z: https://advokatnidenik.cz/2021/01/19/rozumne-pravo-navrh-zakona-o-povinnem-predavani-dat-operatory-je-protiustavni/; nebo; RÁMIŠ, Vladan et al. Předběžné vyjádření Spolku pro ochranu osobních údajů k novele zákona č. 127/2005 Sb., navržené Ministerstvem zdravotnictví 30.11.2020. In: *epravo.cz* [online]. 17. 12. 2020 [cit. 22. 3. 2021]. Dostupné z: https://www.epravo.cz/top/clanky/predbezne-vyjadreni-spolku-pro-ochranu-osobnich-udaju-k-novele-zakona-c-1272005-sb-navrzene-ministerstvem-zdravotnictvi-30112020-112324.html

5.3 NEDŮSLEDNÉ ZPRACOVÁNÍ DPIA VZPOMÍNKOVÝCH MAP

V této části bych se rád pozastavil nad stručností DPIA vzpomínkových map. Zpracovatel DPIA totiž zcela rezignoval na detailní popis způsobu získání dat od bank a mobilních operátorů a obsah těchto dat. Tyto informace nejsou ani součástí informací o zpracování osobních údajů vydaných Ministerstvem zdravotnictví ČR. Na druhou stranu jsou ale klíčové pro kvalifikované určení rizik pro práva a svobody subjektů údajů, jak požaduje čl. 35 odst. 7 písm. c) GDPR. Jejich útržky jsou dohledatelné až z jiných veřejně přístupných zdrojů (mimořádné opatření, články autorů systému, informace od bank,[103] aktuality České bankovní asociace[104] apod.). Nelze se přitom domnívat, že by takovými informacemi správce nedisponoval. Jednak je jeho povinností, aby měl takové informace k dispozici, a jednak tyto informace jsou součástí smluv, které uzavřelo Ministerstvo vnitra ČR a společnost Keboole.[105]

Absence těchto informací při posuzování rizik ale může vést k opomenutí důležitých aspektů přenosu dat a jejich zabezpečení. V nejčernějších scénářích to pak může vést k únikům dat subjektů údajů a v důsledku ke snížení důvěry v českou chytrou karanténu. Za nepovedený příklad lze uvést neplánovaný přenos rodných čísel českých zájemců o očkování do USA.[106]

Těmto problémům mohlo být předejito. Za kritickou chybu v tomto případě lze považovat nepřizvání si Úřadu pro ochranu osobních údajů ke konzultaci či neoslovení jiných zájmových skupin hned ze samého počátku projektu. Ačkoliv se v DPIA vzpomínkových map uvádí, že Úřad pro

[103] *Informace o zpracování osobních údajů dle mimořádného opatření Ministerstva zdravotnictví ve věci předávání údajů o místě a době použití elektronického platebního prostředku* [online]. Moneta Money Bank, [cit. 1. 9. 2020]. Dostupné z: https://www.moneta.cz/documents/20143/11740692/mmb-informace-o-zpracovani-osobnich-udaju-chytra-karantena.pdf

[104] Zapojení bank do „Chytré karantény". In: *Česká bankovní asociace* [online]. 27. 4. 2020 [cit. 1. 9. 2020]. Dostupné z: https://cbaonline.cz/zapojeni-bank-do-chytre-karanteny.

[105] Smlouvy jsou dostupné z Registru smluv na adresách www.smlouvy.gov.cz/smlouva/12307632 a www.smlouvy.gov.cz/smlouva/12363956.

[106] Vyjádření Úřadu k rezervačnímu systému očkování proti COVID-19. In: *Úřad pro ochranu osobních údajů* [online]. 1. 2. 2021 [cit. 22. 2. 2021]. Dostupné z: https://www.uoou.cz/vyjadreni-uradu-k-nbsp-rezervacnimu-systemu-ockovani-proti-covid-19/d-47761

ochranu osobních údajů a další osoby byly konzultovány, podle všeho tomu tak nebylo již od začátku.[107]

5.4 PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ MIMO EU

Poslední z vytýkaných problémů vyvstal až v půlce roku 2020, kdy Soudní dvůr EU zrušil[108] právní rámec pro předávání osobních údajů do USA na základě rozhodnutí o ekvivalentní ochraně (tzv. Privacy Shield).[109] V obou zkoumaných částech české chytré karantény přitom vystupovaly společnosti se sídlem v USA v pozicích zpracovatelů, kterým přestalo být možné údaje bez dalšího předávat.

Další možností, jak v tomto případě právně zabezpečit předání osobních údajů do USA, jsou tzv. standartní smluvní doložky dle čl. 46 GDPR. Aby ovšem mohl správce předávat osobní údaje na tomto základě, musí ověřit, zda právo třetí země, do které je předáváno, má odpovídající ochranu osobních údajů a případně přijmout ještě další opatření.[110] Není-li možné přijmout takové opatření, správce nesmí osobní údaje do dané země předat. Tak tomu bude dle Soudního dvora EU např. pokud jsou příjemci údajů ve třetí zemi právem uloženy povinnosti, které jsou v rozporu se smluvními doložkami a *„mohou tedy ohrozit smluvní záruku odpovídající úrovně ochrany před přístupem orgánů veřejné moci uvedené třetí země k těmto údajům.“*[111]

Privacy Shield byl zrušen, protože USA neposkytují odpovídající úroveň ochrany, a to zejména protože využívají programy plošně sledující komu-

[107] ÚOOÚ k projektu „chytrá karanténa“. In: *Úřad pro ochranu osobních údajů* [online]. 11. 4. 2020 [cit. 1. 9. 2020]. Dostupné z: https://www.uoou.cz/uoou-k-nbsp-projektu-chytra-karantena/d-41769; *Vyjádření Spolku pro ochranu osobních údajů k projektům Chytrá karanténa a eRouška* [online]. Spolek pro ochranu osobních údajů, 2020 [cit. 01.09.2020]. Dostupné z: https://www.ochranaudaju.cz/wp-content/uploads/2020/05/Chytra_karantena_stanovisko_final.pdf

[108] Rozsudek Soudního dvora EU ze dne 16. 7. 2020, *Schrems II.*, C-311/18, EU:C:2020:559, odst. 201.

[109] Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí.

[110] Rozsudek Soudního dvora EU *Schrems II.*, odst. 133 a 134.

[111] Ibid., odst. 135.

nikaci včetně jejího obsahu.[112] Soudní dvůr EU explicitně konstatoval, že právní úprava omezující soukromí v USA není „*upravena takovým způsobem, aby odpovídala požadavkům, které jsou v zásadě rovnocenné požadavkům vyžadovaným v unijním právu*“.[113] Nabízí se tak zcela očividná otázka, zda může správce dojít vlastním hodnocení při uzavírání smluvních doložek k opačnému závěru[114] a osobní údaje tak na základě smluvních doložek opět předávat.

Domnívám se, že tomu tak v současné situaci není.[115] Ať již bude předávání osobních údajů zastřešeno smluvně jakkoliv, takový způsob nemá přednost před veřejnoprávními zákonnými ustanoveními tamního právního řádu.[116] Někteří autoři zmínili namísto přesunu dat do EU možnost zašifrování přeneseného obsahu.[117] Jak ale jedním dechem dodávali, jedná se o technicky, časově a finančně náročné řešení. Jako takové potom není v tomto případě ihned připravené zajistit práva občanů EU.

Stejně jako v předchozích kapitolách, i zde eRouška díky své nové verzi unikla negativnímu hodnocení. U vzpomínkových map je současná situace nejistá. Jejich DPIA uvádí společnost Amazon jako subzpracovatele a USA

[112] Ibid., odst. 178–184.

[113] Ibid., odst. 185.

[114] NEŠPŮREK, Robert a Vojtěch BARTOŠ. *EU-US Privacy Shield zrušen. Předávání osobních údajů do USA podle standardních smluvních doložek mohou úřady kdykoliv zakázat.* [online]. 2020 [cit. 20. 8. 2020]. Dostupné z: https://www.havelpartners.blog/blog/eu-us-privacy-shield-zrusen-predavani-osobnich-udaju-do-usa-podle-standardnich-smluvnich-dolozek-mohou-urady-kdykoliv-zakazat/147

[115] Pro stejný názor a shrnutí přístupů dohledových úřadů srov. BARNEY, Gwenn. Does Schrems II Doom Use of SCCs for EU–US Data Transfers? No Answers and Clouds are Gathering. In: *JD Supra* [online]. 4. 11. 2020 [cit. 22. 2. 2021]. Dostupné z: https://www.jdsupra.com/legalnews/does-schrems-ii-doom-use-of-sccs-for-eu-15488/; nebo MAĎAROVÁ, Helga. Schrems II: zásadná zmena v podmienkach prenosu osobných údajov mimo EÚ. In: *epravo.sk* [online]. 1. 10. 2020 [cit. 7. 3. 2021]. Dostupné z: https://www.epravo.sk/top/clanky/schrems-ii-zasadna-zmena-v-podmienkach-prenosu-osobnych-udajov-mimo-eu-4905.html

[116] Na systém zastřešený prostřednictvím standartních smluvních doložek přešel např. Amazon. Viz SCHMIDT, Stephen. *Customer update: AWS and the EU-US Privacy Shield* [online]. 2020 [cit. 1. 9. 2020]. Dostupné z: https://aws.amazon.com/blogs/security/customer-update-aws-and-the-eu-us-privacy-shield/

[117] Za všechny OLEJNIK, Lukasz. *Technology impact of Privacy Shield invalidation - is it the EU data localization?* [online]. 2020 [cit. 1. 9. 2020]. Dostupné z: http://blog.lukaszolejnik.com/technology-impact-of-privacy-shield-invalidation-is-it-the-eu-data-localization/

jako místo zpracování dat,[118] z informační povinnosti nelze zjistit více.[119] Zůstává také otázkou, jaké konkrétní osobní údaje jsou mimo EU zpracovány. Potenciálně se ovšem může jednat o vážný zásah, protože u vzpomínkových map jsou zpracovány údaje chráněné telekomunikačním tajemstvím spolu s rodným číslem a dalšími identifikačními údaji.

5.5 ČESKÉ SHRNUTÍ

V případě české chytré karantény byl problém především v nedostatečném právním základu (třetí krok testu ESLP), který byl vytvořen nedostatečným zájmem zákonodárné a výkonné moci. Dostatečně kvalitní právní rámec přitom mohl být nastaven poměrně rychle.[120] V případě eRoušky byl nakonec odpovídající právní rámec přijat na začátku roku 2021, u vzpomínkových map je situace o poznání horší. Jejich právní základ je totiž stále v legislativním procesu, a navíc nelze navrhovanou normu považovat za kvalitní.

Kromě toho vzpomínkové mapy trpí i dalšími problémy jako je nedostatečně zhodnocený způsob zpracování osobních údajů (především způsob získávání údajů) a neexistence novějšího DPIA či alespoň informační povinnosti správce reflektující právní (zrušení Privacy Shieldu) i faktický (upuštění od využívání dat od bank) vývoj.

Celkově lze ale hodnotit českou chytrou karanténu jako proporcionální zásah do práva na soukromí. Tvůrci aplikací v rámci překotného vývoje v zásadě zvolili rozumná řešení, které dbali zásad ochrany osobních údajů, a to i v prvních verzích.

Jedním dechem je třeba dodat, že technologie, jako je chytrá karanténa, plní v současné pandemii roli pouze jednoho kolečka ve velkém soukolí. Nejde o samospasné řešení na pandemii, které nás bez dalšího zachrání.

---

[118] *DPIA vzpomínkových map*, s. 13 a 14.

[119] *Chytrá karanténa – Aktuální informace o COVID-19*.

[120] Například zákon č. 94/2021 Sb., o mimořádných opatřeních při epidemii COVID-19, který obsahuje právní základ pro aplikaci eRouška, byl Poslanecké sněmovně Parlamentu ČR předložen 15. 2. 2021 a o pouhých 11 dní později, dne 26. 2. 2021 byl vyhlášen ve Sbírce zákonů ČR. Srov. Sněmovní tisk 1158. In: *Poslanecká sněmovna Parlamentu ČR* [online] [cit. 23.03.2021]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=8&t=1158

Nejlépe to lze demonstrovat na českých vzpomínkových mapách, které v současné době přestávají plnit svůj účel, neboť každý nahlásí v průměru pouze jeden rizikový kontakt.[121] Větší efektivitu zde nepřinese ani zmiňovaný návrh § 89a ElKomČR, který by umožnil polohová data předávat hygienickým stanicím bez souhlasu uživatele. Ze samostatných dat o pohybu není možné bez asistence nakaženého identifikovat další, potenciálně nakažené, osoby. Stejně na tom pak je i eRouška, kterou v současné době používá přibližně čtvrtina lidí potřebných k dostatečné funkčnosti aplikace.[122]

6. ANALÝZA SLOVENSKÉHO ŘEŠENÍ

6.1 PŘEDÁVÁNÍ ÚDAJŮ ÚVZ PŘEZKOUMANÉ ÚSTAVNÍM SOUDEM SR

Jak již bylo v popisu slovenského řešení zmíněno, Ústavní soud SR odmítnul první verzi legislativy, která umožňovala ÚVZ žádat mobilní operátory o údaje občanů. Tato kapitola se tomuto rozhodnutí věnuje, shrnuje jeho závěry a následně je aplikuje na verzi legislativy, kterou přijal slovenský zákonodárce v reakci na toto rozhodnutí.[123]

Zavedený systém povinoval mobilní operátory k uchovávání údajů a k jejich zpřístupnění veřejné moci na žádost ÚVZ.[124] Ústavní soud SR při přezkoumávání využil v souladu s judikaturou Soudního dvora EU přísných

[121] Lidé porušují karanténu. V lednu ji nedodržela třetina z pěti set kontrolovaných. In: *Aktuálně.cz* [online]. 4. 2. 2021 [cit. 12. 3. 2021]. Dostupné z: https://zpravy.aktualne.cz/domaci/karantenu-porusila-v-lednu-tretina-kontrolovanych/r~c369cbde66f711eb842f0cc47ab5f122/

[122] Pro její maximální účinnost si jí musí nainstalovat 6 mil. lidí, zatímco na konci roku 2020 mělo eRoušku nainstalováno „pouze" 1,5 mil. lidí. Srov. Aplikaci eRouška si zatím aktivoval milion lidí. Nové uživatele ‚nalákala' SMS výzva [online]. *Lidovky.cz*. 14. 10. 2020 [cit. 12. 3. 2021]. https://www.lidovky.cz/domov/aplikaci-erouska-si-zatim-aktivovalo-861-tisic-lidi-nove-uzivatele-nalakala-sms-vyzva.A201014_142758_ln_domov_sei; a Fišer, M. Aplikaci eRouška už používá 1,5 milionu lidí [online]. *Novinky.cz*. 31. 12. 2020 [cit. 12. 3. 2021]. https://www.novinky.cz/internet-a-pc/software/clanek/aplikaci-erouska-uz-pouziva-15-milionu-lidi-40346571

[123] Na ono rozhodnutí Ústavního soudu se odkazuje při svém vetu i prezidentka SR ve svém rozhodnutí ze dne 3. 8. 2020, č. 4823-2020-KPSR, s. 3.

[124] Usnesení Ústavního soudu SR č. j. PL. ÚS 13/2020-103, odst. 63, 64 a 67.

kritérií.[125] Došel při tom k závěru, že přezkoumávaná právní úprava absentuje na záruky, které jsou požadované jak jeho rozhodovací praxí, tak judikaturou Soudního dvora EU. Jedná se o:

- *subsidiaritu používání získaných údajů* – Ústavní soud SR akcentoval princip, že údaje je nutné získávat z nejméně citlivých zdrojů a pouze v nevyhnutelném rozsahu (např. pouze pro omezené časové okno na inkubační dobu nebo limitováno způsobem šíření viru). V tomto ohledu také připomněl, že by zpracování mělo být prováděno na základě souhlasu;[126]
- *jasné vymezení účelu použití těchto údajů* – zákonné ustanovení podle Ústavního soudu SR nestanovilo účel použití osobních údajů dostatečně jasně a fungovalo vlastně jako generální klauzule;[127]
- *kvalitní dohled ze strany soudu nebo nezávislého orgánu* – v rámci tohoto bodu Ústavní soud SR vyzvedl skutečnost, že není možné udělit sankce v případě porušení předmětných ustanovení ze strany ÚVZ. Úpravě chybělo i zajištění transparentnosti pro umožnění veřejné kontroly;[128]
- *zabezpečení vysoké úrovně ochrany a bezpečnosti* – čím citlivější údaje, tím lepší (technickou) ochranu je jim třeba poskytnout;[129]
- *časově podmíněné zničení údajů* – pro minimalizaci rizika zneužití údajů je nutné, po odpadnutí důvodu zpracování v daném množství a kvalitě, je znehodnotit či zničit;[130]
- *vyrozumění dotčených osob* – pokud je možné dotčené osoby vyrozumět o poskytnutí jejich údajů (tedy nebrání-li tomu nějaký zákonný důvod nebo obdobný zájem), musí tak být učiněno. To je

[125] Ibid., odst. 81.

[126] Ibid., odst. 89 a 90. Vyžadování souhlasu pro poskytnutí údajů sice vláda SR uvádí ve vyjádření adresovaném Ústavním soudu SR (srov. Ibid., odst. 57). Absence takové podmínky v zákonném znění je však deficitem, který se nedá překonat výkladem.

[127] Ibid., odst. 85 a 91.

[128] Ibid., odst. 92.

[129] Ibid., odst. 93.

[130] Ibid., odst. 94.

vyjádřením požadavku na přístup k soudu a k efektivní soudní kontrole.[131]

Nejznatelnější změnou v novelizaci provedené na základě pozastavení účinnosti bylo zakotvení povinnosti získat souhlas s poskytnutím údajů. Zákon vyžadoval souhlas pouze k poskytnutí údajů, jejich zpracování se pak zřejmě provádělo na základě titulu plnění právní povinnosti. Takto nastavený systém nelze považovat *apriori* za problematický – subjektu údajů byla stále na začátku dána možnost volby, zda osobní údaje pro tento účel poskytne.

Ačkoliv byl výmaz osobních údajů povinen provést správce, nejsou-li již potřeba pro příslušné účely, v rámci zvýšení transparentnosti a posílení právní jistoty je opětovná deklarace tohoto pravidla vítaná. S transparentností souvisí i povinnost ÚVZ předložit zprávu Národní radě SR o zákonnosti zpracování.

Zůstává ovšem otázkou, jestli byl vyřešen i problém s nedostatečně určenými účely zpracování. Novelizace totiž stanovila možnost zpracovat údaje „*výlučne v rozsahu potrebnom na identifikáciu pohybu dotknutého užívateľa v záujme ochrany života a zdravia*.“[132] Podle mého názoru nedošlo, oproti původnímu znění, ke znatelnému zúžení účelu dle požadavku Ústavního soudu SR. V jeho rozhodnutí se jako příklad dostatečně konkrétních účelů uvádělo informování obyvatelstva, vynucování karantény nebo případné vedení přestupkových a trestních řízení.[133] Zákonodárce ovšem ponechal účel definovaný obecně jenom jako „ochranu života a zdraví“. Jednalo se tak o stejnou generální klauzuli, jakou původně Ústavní soud SR kritizoval.

Při hodnocení je nutné dodat, že ze zmíněné zprávy, kterou ÚVZ předložil Národní radě SR, vyplývá, že za celou dobu využitelnosti tohoto právního rámce (do 31. 12. 2020)[134] ÚVZ ani jednou nepožádal mobilní operátory

[131] Ibid., odst. 95.

[132] Ustanovení § 63 odst. 18 odst. c) ElKomSR.

[133] Usnesení Ústavního soudu SR č. j. PL. ÚS 13/2020-103, odst. 85 a 91.

[134] To je totiž podle § 63 odst. 20 ElKomSR nejzazší den, kdy může ÚVZ zpracovávat a uchovávat údaje takto získané.

o zpřístupnění údajů.[135] Nebyly tedy zpracovány jakékoliv osobní údaje. Optikou Úmluvy a ESLP, jak byly prezentovány na začátku, nedošlo k zásahu do práv občanů. Nicméně tento závěr neznamená automatickou konformitu úpravy s Ústavou SR či slovenskými mezinárodními závazky. Identifikované problémy právní úpravy by napříště měly být slovenským zákonodárcem reflektovány.

6.2 PŘEDÁVÁNÍ TELEFONNÍHO ČÍSLA ÚVZ

Ačkoliv si zřejmě zákonodárce vzal nějaká ponaučení pro zásahy do soukromí a ochranu osobních údajů pro schvalování další úpravy (přijetí § 42 odst. 5 a § 63 odst. 21 ElKomSR), nebyl minimálně ve třech ohledech zcela důsledný. Pro připomenutí, jedná se o zplnomocnění ÚVZ k vyžádání si telefonních čísel osob, kterým byla zaslána varovná textová zpráva. V současné době jsou příslušná ustanovení stále využitelná.

Zaprvé, tato nová úprava trpí stejně nedostatečně určeným účelem, jako úprava původní. Ustanovení jako účel uvádí ochranu osob před hrozícím nebezpečím anebo přijímání opatření při ohrožení života a zdraví.[136] Vyzněním se tak jedná taktéž o generální klauzuli, která ÚVZ umožňuje zpracování osobních údajů pro množství účelů, a nikoliv pouze pro onu kontrolu osob přicházejících z „červených zemí“, jak deklaruje důvodová zpráva.

Zadruhé není vůbec jasné, proč je doba pro zpracování zrovna 60 dní.[137] Osoby překračující hranice se musí hlásit bezprostředně po vstupu na území, přičemž v opačném případě jim hrozí správní sankce.[138] Z jakého důvodu zákonodárce umožňuje údaje zpracovávat šedesát dní od poskytnutí se ze znění ustanovení nebo důvodové zprávy nedovíme.

---

[135] Správa o zákonnosti spracúvania údajov v súlade s § 63 ods. 20 ElKomSR, s. 5. Po omezený čas k dispozici z: https://cutt.ly/6kFsfgD. Tento dokument byl získán na základě žádosti autora podle SlInf. Odpověď povinného subjektu nebyla publikována, po omezený čas je k dispozici z: https://cutt.ly/lkFsDIq.

[136] Ustanovení § 63 odst. 21 ElKomSR.

[137] Ibid.

[138] Opatrenie ÚVZ pri ohrození verejného zdravia ze dne 17. 9. 2020, sp. zn. OLP/7310/2020.

Zatřetí, zákon zcela rezignuje na informování osob, jejichž číslo bylo ÚVZ poskytnuto. Dle mého názoru zde přitom nelze identifikovat důvod, pro který by dotčené osoby nemohly být o tomto předání údajů notifikovány (alespoň *ex post*). Jde tak reálně o méně lidskoprávně přívětivou úpravu, než je úprava odposlechů ve slovenských trestněprávních předpisech.[139]

Stejně jako v případě oprávnění podle § 63 odst. 18 až 20 ElKomSR, ani zde ÚVZ nepožádal o ani jednou o zpřístupnění údajů.[140] Nebyly tedy zpracovány jakékoliv osobní údaje a aplikují se výše uvedené závěry.

Je nutné poznamenat, že skrze tuto úpravu má ÚVZ přístup pouze k telefonnímu číslu. Vyhodnocení, která telefonní čísla budou předána, je na mobilních operátorech. Nebude se tak jednat o zásah stejné intenzity jako v předcházející kapitole. Na druhou stranu, i u takové úpravy je nutné trvat alespoň na předchozím patřičném odůvodnění. To ovšem v tomto případě zpracováno nebylo, neboť důvodová zpráva k zákonu je velmi stručná a nezaobírá se důležitými aspekty. Pro srovnání: tato podkapitola je o jen o deset slov kratší než obecná část důvodové zprávy v kombinaci s odůvodněním § 61 odst. 21 ElKomSR.

6.3 KONTROLA PROSTŘEDNICTVÍM EKARANTÉNY

Aplikace eKaranténa je již na první pohled invazivnější do soukromí než česká eRouška. To ovšem, s ohledem na její způsob využití (hlídání dodržování nařízené karantény oproti trasování kontaktů) není překvapivé.

Podíváme-li se na toto řešení optikou pětistupňového testu popsaného na začátku, nemám pochyb o tom, že prvními čtyřmi kroky projde řešení bez problému. V tomto případě je čl. 8 Úmluvy aplikovatelný (krok 1), zásah zde existuje v podobě povinnosti nechat se sledovat (krok 2), celé řešení má zákonný právní rámec (§ 60a a násl. OchrZdrSR) (krok 3) a sleduje legitimní cíl ochrany veřejného zdraví uvedený v čl. 8 odst. 2 Úmluvy (krok 4).

[139] Ustanovení § 116 odst. 4 zákona č. 301/2005 Z. z., trestný poriadok.

[140] Správa o zákonnosti spracúvania údajov v súlade s § 63 ods. 21 ElKomSR, s. 3. Po omezený čas dostupné z: https://cutt.ly/7b3Q9WG. Tento dokument byl získán na základě žádosti autora podle SlInf. Odpověď povinného subjektu nebyla publikována, po omezený čas je k dispozici z: https://cutt.ly/Yb3Q7Ez.

Nicméně jsem toho názoru, že systém eKarantény již neprojde pátým krokem, testem nezbytnosti (proporcionality).

Křivka počtu nakažených měla v zemích EU v zásadě stejný vývoj. Po prvotním zvýšení počtu nakažených se trend křivky otočil a počet případů začal klesat.[141] Slovensko přitom bylo jednou z mála zemí, která zvolila tento způsob vynucování karantény.[142] Nelze tak konstatovat, že by tento způsob měl svoji přidanou hodnotu (zejm. rychlejší zvládnutí pandemie), kterým by mohl tento zásah do soukromí odůvodněn. Tento přístup tak je nutné zařadit na list *bad practice*.

Dále je možné zabývat se námitkou diskriminace. Z dostupných zdrojů totiž vyplývá, že povinnost absolvovat tento způsob karantény dopadal pouze na osoby vracející se na Slovensko ze zahraničí. Osoby pobývající na území Slovenska, které se tam i nakazily, tuto povinnost neměly a absolvovaly izolaci v domácím prostředí bez dohledu eKarantény.[143] Takto rozdílné zacházení se dvěma srovnatelnými skupinami obyvatel (osoby nakažené koronavirem či s podezřením na nákazu) není vůbec odůvodněno. Na základě čeho došla slovenská exekutiva k závěru, že repatrianty je nutné hlídat skrze eKaranténu ale osoby trvale pobývající a nakažené na území Slovenska nikoliv? Existuje u nich snad větší předpoklad porušování izolace? To se již nedovíme.

V neposlední řadě bych rád zmínil, dle mého názoru, obecně chybné nastavení eKarantény. Jejím základním předpokladem totiž je, že všichni lidé nebudou izolaci dodržovat, a proto je nutné je nepřetržitě hlídat skrze GPS a fotografie. Domnívám se, že taková plošná presumpce je nepřípustná, jelikož nutí strpět větší zásah do práv všechny osoby, a nikoliv pouze ty, které izolaci porušily (jako je tomu např. u pokut) či se lze důvodně domnívat,

[141] COVID-19 country overviews. In: *Evropské středisko pro prevenci a kontrolu nemocí* [online] [cit. 4. 10. 2020]. Dostupné z: https://covid19-country-overviews.ecdc.europa.eu/#3_eueea_and_the_uk

[142] *Projects using personal data to combat SARS-CoV-2*.

[143] Jak aplikovatelné Opatrenie ÚVZ pri ohrození verejného zdravia sp. zn. OLP/4311/2020, tak i tiskové zprávy (např. COVID-19: Inteligentná domáca karanténa by sa mala spustiť od piatku. In: *Ministerstvo zdravotníctva SR* [online]. 19. 5. 2020 [cit. 8. 3. 2021]. Dostupné z: https://www.health.gov.sk/Clanok?covid-19-19-05-2020-karantena-smart) se zmiňují výhradně o osobách vracejících se ze zahraničí v souvislosti s aplikací eKarantény.

že ji poruší.[144] Navíc byla tato povinnost vynucována u osob pouze z důvodu, že překročily hranice (v kontrastu např. s osobami, které spáchaly trestný čin, pročež je jejich pohyb monitorován v rámci výkonu trestu). Analogicky lze tento způsob sledování připodobnit k situaci, kdy stát provádí plošné odposlechy všech telefonů značky Apple, a nikoliv osob s důvodným podezřením na páchání trestné činnosti.

Potřeba získat souhlas dotčené osoby se v tomto případě nedá považovat za zmírnění zásahu. Druhá možnost karantény repatriantů probíhala v budově k tomu určené státem.[145] Podmínky v těchto zařízeních byly mnohdy hraniční[146] a zabývala se jimi i slovenská ombudsmanka.[147] Ta se nakonec ohledně karantény obrátila na jaře 2021 i na Ústavní soud SR s žádostí o přezkum postupu vlády SR.[148] To tak může vést i k úvahám o (ne)dobrovolnosti uděleného souhlasu, neboť pokud jej osoba neudělila a nenastoupila do domácí karantény hlídané eKaranténou, byla nucena izolaci strávit ve státním zařízení, kde podmínky nemusí splňovat základní požadavky.

---

[144] Zde lze odkázat i na kritiku plošného sběru provozních a lokalizačních údajů a jejich předávání bezpečnostním složkám. V těchto případech Soudní dvůr EU shledal, že takové opatření není v demokratické společnosti možné považovat za odůvodněné, neboť stát schraňuje i údaje osob, u kterých neexistuje důvod domnívat se, že jejich chování souvisí se zajištěním národní bezpečnosti. Srov. rozsudek Soudního dvora EU ze dne 6. října 2020, *Privacy International,* C-623/17, EU:C:2020:790, odst. 80 a 81 a judikaturu tam citovanou.

[145] Tento typ karantény je vlastně výchozí možností. Domácí karanténa za dohledu aplikace eKaranténa je až alternativní možností, která dostupná na žádost.

[146] NEČÁSKOVÁ, Pavlína. Společné pokoje, odtažitý personál, destinace předem neznámá. Slováci sdílejí zážitky ze státní karantény. In: *iROZHLAS* [online]. 6. 5. 2020 [cit. 8. 3. 2021]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/slovensko-statni-karantena-koronavirus-cestovani-hranice_2005061304_kro

[147] *Ombudsmanka odporúča zmeniť systém povinnej štátnej karantény - tisková zpráva* [online]. Kancelária verejného ochrancu práv, 2020 [cit. 8. 3. 2021]. Dostupné z: https://www.vop.gov.sk/files/2020_23_TS_VOP_odporuca_zmenit_system_povinnej_statnej_karanteny.pdf

[148] Ombudsmanka sa obrátila na Ústavný súd, žiada posúdenie zásahov do práv počas pandémie. In: *RTVS: Správy* [online]. 10. 2. 2021 [cit. 8. 3. 2021]. Dostupné z: https://spravy.rtvs.sk/2021/02/ombudsmanka-sa-obratila-na-ustavny-sud-ziada-posudenie-zasahov-do-prav-pocas-pandemie/; Ústavní soud SR pak celý návrh přijal k dalšímu řízení, viz Ústavný súd prijal moje podanie na ďalšie konanie. In: *Verejný ochranca práv* [online]. 30. 4. 2021 [cit. 20. 5. 2021]. Dostupné z: https://www.vop.gov.sk/stavn-s-d-prijal-moje-podanie-na-al-ie-konanie

Prezentovaným způsobem zpracování osobních údajů tak dle mého názoru dochází nejen k porušení principu minimalizace osobních údajů,[149] ale jedná se o zásah do práv zaručených lidskoprávními katalogy vyčtenými v úvodu. Právní předpisy by totiž měly mj. zajistit, aby zpracovávaná data byla relevantní a přiměřená účelu, pro který jsou zpracovávána,[150] tak, aby byl zásah co nejmenšího rozsahu. To se v tomto případě nestalo.

6.4 AUTOMATIZOVANÉ INDIVIDUÁLNÍ ROZHODOVÁNÍ V EKARANTÉNĚ?

Při hodnocení, zda osoba porušila karanténu, docházelo k jejímu profilování. Aplikace sama vyhodnocovala, zda se osoba vzdálila od místa nahlášené karantény, případně o kolik. Došlo-li ke vzdálení se, odeslala orgánům veřejné moci hlášení. Ze zákona ovšem musí být porovnání fotografií (s fotografií vloženou do aplikace při registraci) a polohy prováděno přímo na zařízení, kde také musí být tyto údaje uloženy. Jejich uložení na externích serverech nebo zpřístupnění jiným osobám je explicitně zakázáno.[151]

Z důvodové zprávy poté vyplývá, že v případě neshody fotografií bylo na server odesláno hlášení, které obsahovalo pouze informaci o neshodě fotografií. Obdobně to platí pro porovnávání lokalizačních údajů. V tomto se rozchází důvodová zpráva s publikovanou informační povinností správce, kde se u kapitoly o profilování uvádí pouze informace k hodnocení polohy.[152]

Zřejmě tomu bude tak z důvodu, že pro projednání přestupků byla správnímu orgánu zpřístupněna pouze informace o porušení karantény a závažnosti tohoto porušení, nikoliv přesné polohové údaje.[153] S výsledkem porovnání fotografií se tak z nějakého důvodu pro přestupkové řízení podle dikce zákona nebo informační povinnosti správce nepočítalo.

[149] Čl. 5 odst. 1 písm. c) GDPR.

[150] *Garder proti Francii*, rozsudek ESLP, 17. 12. 2009, č. stížnosti 16428/05, odst. 62.

[151] Ustanovení § 60d odst. 5 OchrZdrSR.

[152] Podmienky ochrany súkromia - eKaranténa. In: *Korona.gov.sk* [online] [cit. 04. 10. 2020]. Dostupné z: https://korona.gov.sk/podmienky-ochrany-sukromia-ekarantena/

[153] Ustanovení § 60c odst. 2 OchrZdrSR.

Důležitým ustanovením v tomto případě je i § 54 odst. 5 OchrZdrSR, který opravňuje vykonávat státní zdravotní dozor dodržování domácí karantény pouze prostřednictvím aplikace eKaranténa.

Prvním zjevným nedostatkem zde bylo vynechání jakýchkoliv informací o porovnání fotografií a odesílání případného hlášení upozorňující na neshodu fotografií. V tomto případě docházelo taktéž k profilování.

Vyvstává zde ale mnohem důležitější otázka – a to, jak doopravdy fungoval proces ukládání pokut za nedodržení karantény? Informační povinnost správce totiž uváděla, že na základě hlášení se přestupkové řízení pouze zahajuje a rozhodnutí, kterým se končí pak mělo vždy „lidskou povahu".[154] Jinými slovy, nedocházelo k automatizovanému rozhodování a neuplatní se čl. 22 GDPR (obsahující např. právo na ověření rozhodnutí neautomatizovaným způsobem).

Při hodnocení, zda rozhodování spadá pod čl. 22 GDPR, je jedna z důležitých skutečností role člověka v rozhodovacím procesu. Pokud je jeho účast vyfabrikovaná nebo jeho činností je pouze na základě předložených údajů vydat v mezích (např. interních) instrukcí rozhodnutí, správce se přidaným povinnostem nevyhne.[155] Jako příklad takového lidského automatizovaného rozhodování lze uvést uložení pokuty za překročení rychlosti pouze na základě důkazů z radaru.[156]

Pokud tedy ukládání pokut za porušení karantény bylo prováděno pouze na základě onoho hlášení (přičemž není jisté, jak jinak by měl správní orgán obstarat další důkazy, když není ze zákona oprávněn domácí karanténu kontrolovat jinak), může se jednat o automatizované rozhodování. V takovém případě pak zajisté vyvstává i otázka, jakým způsobem by mohlo být rozhodnutí aplikace o zaslání hlášení přezkoumáváno, když podkladové údaje nesmí opustit mobilní zařízení osoby a správní orgán tak k nim nemá přístup.

---

[154] *Podmienky ochrany súkromia - eKaranténa*.

[155] Pokyny WP29 k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679, s. 21.

[156] Pokyny WP29 k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679, s. 8.

6.5 SLOVENSKÉ SHRNUTÍ

Ani jednu z částí slovenské chytré karantény nelze hodnotit pozitivně. Nastavení aplikace eKaranténa představovalo neproporcionální zásah do práva na soukromí a zákonný rámec pro předávání údajů od mobilních operátorů je nedostatečný, a to i přes rychlý zásah Ústavního soudu SR. Zákonodárce jím předložené požadavky v dalších legislativních procesech z části prostě ignoroval. Zamyšlení by mělo být při nastavování chytrých karantén věnováno také využitelnosti přijatých instrumentů, neboť ÚVZ nové pravomoci vyžádat si informace od mobilních operátorů nakonec (ať už z jakéhokoliv důvodu) nevyužil ani jednou.

Vyzdvihnut by pak měl být přístup ÚVZ k DPIA, a to jak v případě osobních údajů získaných od operátorů, tak v případě aplikace eKaranténa. V prvním případě totiž DPIA zpracováno vůbec nebylo, v druhém případě jej pak ÚVZ nemá fyzicky k dispozici (má jej pouze advokátní kancelář, která jej vypracovala) a odmítá jej poskytnout. Absence těchto podkladů (či jejich utajování) pak ztěžuje veřejnou diskusi o proporcionálnosti použitých řešení.

Právě slovenský přístup dle mého názoru příkladně ukazuje, že při nastavování chytrých karantén je klíčová právě proporcionalita řešení (pátý stupeň testu ESLP). Jak totiž demonstrovala aplikace eKaranténa, ostatní čtyři stupně testu je možné v současné pandemii poměrně lehce splnit. Proporcionalita řešení se nicméně v čase mění, a to v závislosti na aktuální situaci. Lze si tak představit poměry, ve kterých by takovéto plošné sledování osob v karanténě mohlo být považováno za proporcionální. Odůvodnění zavedení tohoto opatření ale může být dle mého názoru založeno jen a pouze na (ne)chování lidí. To stejné platí pro jakékoliv zasahování do soukromí skrze chytré karantény a jiná technická řešení.

Na rozdíl od některých jiných základních práv, na které pandemie taktéž dopadá nebo může dopadnout (shromažďovací právo, vlastnické právo či zákaz nucené práce), nelze zásah do práva na soukromí obhájit pouhými daty o počtu nakažených, rychlostí šíření viru anebo nedostatkem volných lůžek v nemocnicích. Zatímco omezení shromažďovacího práva má logicky bez dalšího potenciál snížit rychlost šíření onemocnění v populaci, jelikož

se lidé nesetkají, nepřetržité sledování izolovaných osob samo o sobě nic takového nedokáže.

V jakých poměrech by tedy mohlo být považováno plošné sledování osob v izolaci za proporcionální? Domnívám se, že by k tomu mohlo dojít pouze v případech značného porušování nařízených izolací – tedy argumentem založeným na (ne)chování lidí. Jen tehdy je totiž možné učinit výše nastíněnou dedukci (nepřetržité sledování snižuje počet osob porušujících nařízenou karanténu, což má potenciál snížit rychlost šíření onemocnění). Získání relevantních dat přitom nepředstavuje nějaký nepředstavitelný proces.[157]

Tímto způsobem pak bude do práva na soukromí zasahováno pouze ve skutečně odůvodněných případech. Zůstane tak ochráněno před ostatními vlivy, jako je rychlost šíření onemocnění, jeho smrtnost, nedůvěra občanů vládě či odborná správnost nastavených opatření, které nemají se soukromím žádné přímé spojení.

Konkrétně se pak toto dá demonstrovat právě na aplikaci eKaranténa. Byl-li by tento způsob vynucení přijat, protože repatrianti hromadně porušují domácí karanténu a šíří nákazu, zákonitě by musela být křivka nakažených jiná než v ostatních evropských zemích, které zvolily odlišný přístup. Zpětně lze ale z vývoje počtu nakažených konstatovat, že k ničemu takovému nedošlo. Zákonodárce tedy neměl ani nemohl mít relevantní důvod (či podklady) zasahovat to práva na soukromí tímto způsobem.

7. ZÁVĚR

Příspěvek se blíže zabýval oficiálními chytrými karanténami v Česku a na Slovensku z pohledu práva na soukromí. Zkoumání byly podrobeny pře-

[157] Např. za leden 2021 bylo nařízeno 245.000 karantén (srov. *Lidé porušují karanténu. V lednu ji nedodržela třetina z pěti set kontrolovaných*.). Pokud bychom využili všech 26.000 policistů hlídajících hranice okresů, aby ve dvojicích karantény postupně kontrolovaly, vychází na každou dvojici zkontrolovat 18,8 karantén. Z veřejných zpráv poté vyplynulo, že k nějaké formě dozoru nad dodržováním karantén ze strany Policie ČR mělo dojít. Srov. Policisté budou kontrolovat dodržování karantén a izolací, seznamy dodá hygiena. In: *ČT24* [online]. 22. 3. 2021 [cit. 23. 3. 2021]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3287194-policiste-budou-kontrolovat-dodrzovani-karanten-a-izolaci-seznamy-doda-hygiena. Výsledek ovšem není dohledatelný.

devším první verze z jara 2020, nicméně následný vývoj nebyl při hodnocení opomenut. Při jejich zkoumání byly zjištěny i vážnější nedostatky a neproporcionální zásahy do základních práv občanů.

Česká chytrá karanténa se skládala ze vzpomínkových map pracujících s daty od mobilních operátorů a bank, a aplikace eRouška. Obě řešení strádaly především kvůli téměř neexistujícímu zákonnému základu, přičemž tento problém není do dnešního dne uspokojivě vyřešen. Obě části je nicméně možné považovat za proporcionální zásahy. Ačkoliv následný vývoj směřoval k větší ochraně soukromí, což lze hodnotit pouze pozitivně, některé problémy stále přetrvávají (nedůsledně zpracované DPIA vzpomínkových map a absence kvalitních právních norem).

Slovenská chytrá karanténa obsahovala systém státní karantény pro repatrianty a předávání údajů ÚVZ od mobilních operátorů. Oproti českému řešení zde sice zákonný základ existoval, nicméně jej není možné v mnohých ohledech považovat za dostatečný. A to i přes instrukce, které slovenskému zákonodárci poskytl Ústavní soud SR. Největším problémem ale je neproporcionálnost sledování lidí v izolaci skrze aplikaci eKaranténa, která představovala značný zásah do soukromí. Tento způsob vynucování izolace přitom není a *priori* neproporcionální, jen potřebuje odůvodnění založené na dostatečných datech o porušování nařízených karantén, k čemuž zde nedošlo.

Široké nasazení technologií je obecně nutné zhodnotit jako rozumný prostředek mající potenciál pomoci v boji s pandemií. Z předložené analýzy lze nicméně vydestilovat několik doporučení pro příště:

- *potřeba dostatečného právního základu* – v těchto situacích by měl existovat specifický právní rámec, který bude explicitně stanovovat podmínky zpracování osobních údajů včetně dostatečných záruk;
- *užitečnost opatření* – při nastavování chytrých karantén je u jednotlivých částí nutné se pozastavit nad jejich vhodností již v okamžiku přijímání. Příkladem opaku je absolutně nevyužitá pravomoc ÚVZ;

- *proporcionalita* – je nutné se vždy zamýšlet nad proporcionalitou částí chytré karantény v konkrétní situaci, přičemž odůvodnění zásahu do práva na soukromí může být postaveno pouze na určitém (ne)chování lidí; a
- *provázanost* – s účinností chytrých karantén jsou inherentně spojeny další vlivy, jako jsou vhodně nastavená opatření, důvěra lidí a transparentnost řešení. I na to se musí státy zaměřit při koncipování a provozování chytrých karantén.

8. POUŽITÉ ZDROJE

[1] BARNEY, Gwenn. Does Schrems II Doom Use of SCCs for EU–US Data Transfers? No Answers and Clouds are Gathering. In: *JD Supra* [online]. 4. 11. 2020 [cit. 22. 2. 2021]. Dostupné z: https://www.jdsupra.com/legalnews/does-schrems-ii-doom-use-of-sccs-for-eu-15488/

[2] COUNCIL OF EUROPE DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW. *AI Breakfasts: Covid-19 - Myths and realities of tracking applications* [online] [cit. 18. 5. 2020]. Dostupné z: https://www.youtube.com/watch?v=l9d3B6AuvdI

[3] DOČEKAL, Daniel. Jak na iPhonech funguje trasování nákazy koronavirem (COVID-19 Exposure Tracing)? In: *Lupa.cz* [online]. 21. 5. 2020 [cit. 1. 9. 2020]. Dostupné z: https://www.lupa.cz/clanky/jak-na-iphonech-funguje-trasovani-nakazy-koronavirem-covid-19-exposure-tracing/

[4] FIŠER, Miloslav. Aplikaci eRouška už používá 1,5 milionu lidí. In: *Novinky.cz* [online]. 31. 12. 2020 [cit. 12. 3. 2021]. Dostupné z: https://www.novinky.cz/internet-a-pc/software/clanek/aplikaci-erouska-uz-pouziva-15-milionu-lidi-40346571

[5] JANN, Ole, Pavel KOCOUREK a Jakub STEINER. *Využití technologie Bluetooth pro trasování šíření covid-19* [online]. Institut pro demokracii a ekonomickou analýzu, 2020 [cit. 5. 8. 2020]. Dostupné z: https://idea.cerge-ei.cz/files/IDEA_Trasovani_covid19_duben2020_14.pdf

[6] KLOUDA, Jan. Bez emocí to jde správně. In: *LinkedIn* [online]. 24. 3. 2020 [cit. 5. 8. 2020]. Dostupné z: https://www.linkedin.com/pulse/bez-emoc%C3%AD-jde-spr%C3%A1vn%C4%9B-jan-klouda

[7] KMEC, Jiří et al. *Evropská úmluva o lidských právech: komentář*. Praha: C.H. Beck, 2012. ISBN 978-80-7400-365-3.

[8] MAĎAROVÁ, Helga. Schrems II: zásadná zmena v podmienkach prenosu osobných údajov mimo EÚ. In: *epravo.sk* [online]. 1. 10. 2020 [cit. 7. 3. 2021]. Dostupné z: https://www.epravo.sk/top/clanky/schrems-ii-zasadna-zmena-v-podmienkach-prenosu-osobnych-udajov-mimo-eu-4905.html

[9] NEČÁSKOVÁ, Pavlína. Společné pokoje, odtažitý personál, destinace předem neznámá. Slováci sdílejí zážitky ze státní karantény. In: *iROZHLAS* [online]. 6. 5. 2020 [cit. 8. 3. 2021]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/slovensko-statni-karantena-koronavirus-cestovani-hranice_2005061304_kro

[10] NEŠPŮREK, Robert a Vojtěch BARTOŠ. *EU-US Privacy Shield zrušen. Předávání osobních údajů do USA podle standardních smluvních doložek mohou úřady kdykoliv zakázat.* [online]. 2020 [cit. 20. 8. 2020]. Dostupné z: https://www.havelpartners.blog/blog/eu-us-privacy-shield-zrusen-predavani-osobnich-udaju-do-usa-podle-standardnich-smluvnich-dolozek-mohou-urady-kdykoliv-zakazat/147

[11] NULÍČEK, Michal et al. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vyd. Wolters Kluwer, 2018. ISBN 978-80-7598-068-7.

[12] NULÍČEK, Michal, Bohuslav LICHNOVSKÝ a Filip BENEŠ. *Chytrá karanténa – proč v Česku potřebujeme souhlas?* [online]. 2020 [cit. 5. 8. 2020]. Dostupné z: https://rowan.legal/chytra-karantena-proc-v-cesku-potrebujeme-souhlas/

[13] OLEJNIK, Lukasz. *Technology impact of Privacy Shield invalidation - is it the EU data localization?* [online]. 2020 [cit. 1. 9. 2020]. Dostupné z: http://blog.lukaszolejnik.com/technology-impact-of-privacy-shield-invalidation-is-it-the-eu-data-localization/

[14] PIERUCCI, Alessandra a Jean-Philippe WALTER. Joint Statement on the right to data protection in the context of the COVID-19 pandemic. In: *Council of Europe* [online]. 2020 [cit. 18.05.2020]. Dostupné z: https://rm.coe.int/covid19-joint-statement/16809e09f4

[15] RÁMIŠ, Vladan et al. Předběžné vyjádření Spolku pro ochranu osobních údajů k novele zákona č. 127/2005 Sb., navržené Ministerstvem zdravotnictví 30.11.2020. In: *epravo.cz* [online]. 17. 12. 2020 [cit. 22. 3. 2021]. Dostupné z: https://www.epravo.cz/top/clanky/predbezne-vyjadreni-spolku-pro-ochranu-osobnich-udaju-k-novele-zakona-c-1272005-sb-navrzene-ministerstvem-zdravotnictvi-30112020-112324.html

[16] SCHMIDT, Stephen. *Customer update: AWS and the EU-US Privacy Shield* [online]. 2020 [cit. 1. 9. 2020]. Dostupné z: https://aws.amazon.com/blogs/security/customer-update-aws-and-the-eu-us-privacy-shield/

[17] ŠTRAHA, Štěpán a Martina RIEVAJOVÁ. *UPDATE: Slovenský Úrad verejného zdravotníctva získal prístup k vašim telefónnym číslam, aj keď mu prezidentka dala stopku* [online]. 2020 [cit. 4. 10. 2020]. Dostupné z: https://www.havelpartners.blog/blog/slovensky-urad-verejneho-zdravotnictva-nebude-mat-zatial-pristup-k-vasim-telefonnym-cislam-prezidentka-mu-dala-stopku/157

[18] DE TERWANGNE, Cécile. Council of Europe convention 108+: A modernised international treaty for the protection of personal data. *Computer Law & Security Review*. 2021, roč. 40, s. 105497. ISSN 0267-3649. DOI: 10.1016/j.clsr.2020.105497

[19] WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012. ISBN 978-80-7357-750-6.

[20] Aplikaci eRouška si zatím aktivoval milion lidí. Nové uživatele ‚nalákala' SMS výzva. In: *Lidovky.cz* [online]. 14. 10. 2020 [cit. 12. 3. 2021]. Dostupné z: https://www.lidovky.cz/domov/aplikaci-erouska-si-zatim-aktivovalo-861-tisic-lidi-nove-uzivatele-nalakala-sms-vyzva.A201014_142758_ln_domov_sei

[21] COVID-19 country overviews. In: *Evropské středisko pro prevenci a kontrolu nemocí* [online] [cit. 4. 10. 2020]. Dostupné z: https://covid19-country-overviews.ecdc.europa.eu/#3_eueea_and_the_uk

[22] COVID-19: Inteligentná domáca karanténa by sa mala spustiť od piatku. In: *Ministerstvo zdravotníctva SR* [online]. 19. 5. 2020 [cit. 8. 3. 2021]. Dostupné z: https://www.health.gov.sk/Clanok?covid-19-19-05-2020-karantena-smart

[23] *Dopis předsedy Evropského sboru pro ochranu osobních údajů O. Micolovi* [online]. Evropská sbor pro ochranu osobních údajů, [cit. 1. 9. 2020]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

[24] DPIA eRouška 2.0, v. 6 ze dne 4. 2. 2021

[25] *Guide on Article 8 of the European Convention on Human Rights* [online]. Evropský soud pro lidská práva, 2020 [cit. 1. 9. 2020]. Dostupné z: https://www.echr.coe.int/documents/guide_art_8_eng.pdf

[26] Chytrá karanténa – Aktuální informace o COVID-19. In: *Ministerstvo zdravotnictví ČR* [online] [cit. 5. 8. 2020]. Dostupné z: https://koronavirus.mzcr.cz/chytra-karantena/

[27] *Informace o zpracování osobních údajů dle mimořádného opatření Ministerstva zdravotnictví ve věci předávání údajů o místě a době použití elektronického platebního prostředku* [online]. Moneta Money Bank, [cit. 1. 9. 2020]. Dostupné z: https://www.moneta.cz/documents/20143/11740692/mmb-informace-o-zpracovani-osobnich-udaju-chytra-karantena.pdf

[28] Lidé porušují karanténu. V lednu ji nedodržela třetina z pěti set kontrolovaných. In: *Aktuálně.cz* [online]. 4. 2. 2021 [cit. 12. 3. 2021]. Dostupné z: https://zpravy.aktualne.cz/domaci/karantenu-porusila-v-lednu-tretina-kontrolovanych/r~c369cb-de66f711eb842f0cc47ab5f122/

[29] Materiál č. j. OVA 971/20. In: *Portál Aplikace ODok* [online] [cit. 22. 3. 2021]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBSNH56J5

[30] Notifications under Article 15 of the Convention in the context of the COVID-19 pandemic. In: *Council of Europe* [online] [cit. 18. 2. 2021]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/62111354

[31] Ochrana soukromí a cookies eRoušky. In: *eRouška* [online] [cit. 8. 5. 2020]. Dostupné z: https://erouska.cz/podminky-pouzivani

[32] *Ombudsmanka odporúča zmeniť systém povinnej štátnej karantény - tisková zpráva* [online]. Kancelária verejného ochrancu práv, 2020 [cit. 8. 3. 2021]. Dostupné z: https://www.vop.gov.sk/files/2020_23_TS_VOP_odporuca_zmenit_system_povinnej_statnej_karanteny.pdf

[33] Ombudsmanka sa obrátila na Ústavný súd, žiada posúdenie zásahov do práv počas pandémie. In: *RTVS: Správy* [online]. 10. 2. 2021 [cit. 8. 3. 2021]. Dostupné z: https://spravy.rtvs.sk/2021/02/ombudsmanka-sa-obratila-na-ustavny-sud-ziada-posudenie-zasahov-do-prav-pocas-pandemie/

[34] Podmienky ochrany súkromia - eKaranténa. In: *Korona.gov.sk* [online] [cit. 4. 10. 2020]. Dostupné z: https://korona.gov.sk/podmienky-ochrany-sukromia-ekarantena/

[35] Policisté budou kontrolovat dodržování karantén a izolací, seznamy dodá hygiena. In: *ČT24* [online]. 22. 3. 2021 [cit. 23. 3. 2021]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3287194-policiste-budou-kontrolovat-dodrzovani-karanten-a-izolaci-seznamy-doda-hygiena

[36] Projects using personal data to combat SARS-CoV-2. In: *GDPRHUB.eu* [online] [cit. 12. 4. 2020]. Dostupné z: https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2

[37] *Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis: A toolkit for member states* [online]. Council of Europe, 2020 [cit. 14. 5. 2020]. Dostupné z: https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40

[38] RP: Návrh zákona o elektronických komunikacích je protiústavní. In: *Advokátní deník* [online]. 19. 1. 2021 [cit. 22. 3. 2021]. Dostupné z: https://advokatnidenik.cz/2021/01/19/rozumne-pravo-navrh-zakona-o-povinnem-predavani-dat-operatory-je-protiustavni/

[39] Smart karanténa - najčastejšie otázky ohľadne karantény v domácej izolácii s využitím aplikácie eKaranténa. In: *Korona.gov.sk* [online] [cit. 4. 10. 2020]. Dostupné z: https://korona.gov.sk/najcastejsie-otazky/ekarantena/

[40] Sněmovní tisk 1158. In: *Poslanecká sněmovna Parlamentu ČR* [online] [cit. 23. 3. 2021]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=8&t=1158

[41] Souhrnná DPIA eRouška v. 0.2

[42] Souhrnná DPIA Jednotný informační systém KHS pro podporu call centra a vzpomínkové mapy v. 1.09

[43] ÚOOÚ k projektu „chytrá karanténa“. In: *Úřad pro ochranu osobních údajů* [online]. 11. 4. 2020 [cit. 1. 9. 2020]. Dostupné z: https://www.uoou.cz/uoou-k-nbsp-projektu-chytra-karantena/d-41769

[44] Ústavný súd prijal moje podanie na ďalšie konanie. In: *Verejný ochranca práv* [online]. 30. 4. 2021 [cit. 20. 5. 2021]. Dostupné z: https://www.vop.gov.sk/stavn-s-d-prijal-moje-podanie-na-al-ie-konanie

[45] *Vyjádření Spolku pro ochranu osobních údajů k projektům Chytrá karanténa a eRouška* [online]. Spolek pro ochranu osobních údajů, 2020 [cit. 1. 9. 2020]. Dostupné z: https://www.ochranaudaju.cz/wp-content/uploads/2020/05/Chytra_karantena_stanovisko_final.pdf

[46] Vyjádření Úřadu k rezervačnímu systému očkování proti COVID-19. In: *Úřad pro ochranu osobních údajů* [online]. 1. 2. 2021 [cit. 22. 2. 2021]. Dostupné z: https://www.uoou.cz/vyjadreni-uradu-k-nbsp-rezervacnimu-systemu-ockovani-proti-covid-19/d-47761

[47] Zapojení bank do „Chytré karantény“. In: *Česká bankovní asociace* [online]. 27. 4. 2020 [cit. 1. 9. 2020]. Dostupné z: https://cbaonline.cz/zapojeni-bank-do-chytre-karanteny

https://doi.org/10.5817/RPT2021-1-2

VAROVÁNÍ NÚKIB V SYSTEMATICE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A MOŽNOSTI JEHO ZOHLEDNĚNÍ V ZADÁVACÍM ŘÍZENÍ[1]

JAKUB KLODWIG[2]

ABSTRAKT

Článek se nejprve zabývá pojmovou nejednotností a používáním slova „opatření“ v systematice zákona o kybernetické bezpečnosti, tak aby nedocházelo k záměně těchto jazykově velice podobných institutů. Po jasném vymezení názvosloví a charakteru jednotlivých opatření je detailně pojednáno o institutu varování, který je v mezinárodním srovnání poměrně specifický. Klade totiž vysoké nároky na samostatnou činnost povinných osob, díky čemuž však umožňuje vhodně stupňovat bezpečnostní opatření povinných osob, a tak efektivně reagovat na kyberbezpečnostní hrozby různé intenzity. Dále je prakticky pojednáno o problematickém promítnutí performativních pravidel práva kybernetické bezpečnosti a vysoce formalizovaných administrativních pravidel zadávání veřejných zakázek. Po vysvětlení správného zohlednění varování veřejnými zadavateli jsou v souladu s podpůrnými materiály NÚKIB a aktuální rozhodovací praxí předestřeny také způsoby, jakými lze v různých fázích zadávacího řízení obsah varování promítnout do předmětu veřejné zakázky.

[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.

[2] Mgr. Jakub Klodwig je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v Brně. Kontaktní e-mail: Jakub.Klodwig@law.muni.cz

KLÍČOVÁ SLOVA:

Opatření, protiopatření, varování, kybernetická bezpečnost, veřejné zakázky, právo veřejných zakázek, právo kybernetické bezpečnosti, právo ICT, NÚKIB, ÚOHS, zadávací dokumentace, hospodářská soutěž, diskriminace.

ABSTRACT

At first, the article deals with the conceptual inconsistency and the use of the word "measures" in the system of the Cyber Security Act, to not to confuse these linguistically very similar legal institutes. After a clear definition of the nomenclature and nature of measures, the institute of warning is discussed in detail. It is a specific institute in international comparison, which places high demands on individual activity of its recipients. However, it enables the recipient's security measures to be appropriately stepped up, and thus to respond effectively to cybersecurity threats of different intensity. Furthermore, the problematic projection of performative rules of cyber security law and highly formalized administrative rules of public procurement law are practically discussed. After explaining the correct implementation of warning by public authorities, the ways in which the content of warning could be reflected as a subject of a public contract are also presented at various stages of the procurement procedure, in accordance with the supporting materials of NÚKIB and current decision-making practice.

KEYWORDS

Measure, countermeasure, warning, cyber security, public procurement, public procurement law, cyber security law, ICT law, NÚKIB, ÚOHS, procurement documentation, competition, discrimination.

1. ÚVOD

Česká republika byla v celosvětovém srovnání jedním z prvních států, které přijaly vlastní komplexní právní úpravu kybernetické bezpečnosti.[3] V roce 2015, kdy byl v českém právním řádu již účinný systém skládající se ze zá-

[3] POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie*. 2015, roč. 6, č. 11, s. 95.

kona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „***ZKB***“), a prováděcích podzákonných právních předpisů, evropský normotvůrce unijní regulaci ve formě 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 (dále jen „***směrnice NIS***“) teprve formoval. Není proto divu, že některé právní instituty práva kybernetické bezpečnosti jsou v českém právním řádu odlišné od právní úpravy jiných členských států Evropské unie, které při přijímání vlastní regulace kybernetické bezpečnosti vycházely primárně z harmonizačních vodítek směrnice NIS. Právní úprava kybernetické bezpečnosti těchto států byla tudíž logicky určována primárně rámcem směrnice NIS a nikoliv již tolik vlastní legislativní invencí, jako tomu bylo v případě České republiky. Ačkoliv tedy byla směrnice NIS promítnuta s účinností od 1. srpna 2017 i do českého ZKB prostřednictvím zákona č. 205/2017 Sb.,[4] kterým byl založen také samostatný Národní úřad pro kybernetickou a informační bezpečnost (dále jen „***NÚKIB***“),[5] tak specifické prvky a originální instituty, které byly tou dobou již etablované, v českém právním řádu zůstaly. Jedním z nich je institut varování dle § 12 ZKB (dále jen „***varování***“),[6] o jehož specifikách a vlivech na právo zadávání veřejných zakázek tento článek pojednává.

[4] Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.

[5] Vznik samostatného ústředního orgánu státní správy pro kybernetickou bezpečnost byl přitom také důležitým krokem vpřed, který dosud ještě neučinila ani řada vyspělých západních států, včetně např. U.S.A. Tato poměrně brzká emancipace NÚKIB svědčí o významu a snaze o rozvoj kybernetické bezpečnosti v České republice.

[6] Výjimkou je např. právní řád Slovenska, které však vzhledem k historické, kulturní i jazykové blízkosti čerpalo právě z konceptu českého ZKB, viz např. § 27 zákona č. 69/2018 Z.z., o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, když přijalo vlastní „varovanie“, „reaktívne opatrenie“ a „ochranné opatrenie“, nebo právní řád Německa, který stejně nazvaný institut s jinými parametry zakotvuje ve svém § 7 zákona (BSIG) o Spolkovém úřadu pro bezpečnost v informační technice.

2. TERMINOLOGIE OPATŘENÍ DLE ZKB

Varování před kybernetickou hrozbou je jedním ze zákonných nástrojů, kterými může NÚKIB upozornit na existenci hrozby v oblasti kybernetické bezpečnosti a ovlivnit tak bezpečnost v klíčových českých institucích. Kromě varování má NÚKIB k dispozici také další opatření dle § 11 ZKB, kterými jsou reaktivní opatření a ochranná opatření. ZKB definuje v § 11 odst. 1 tato opatření 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.*“ Vzhledem k tomu, že označení „opatření“ je dle této definice samostatným pojmem, je z hlediska terminologie ZKB problematické, že slovo „opatření“ je součástí šesti dalších sousloví, které ZKB používá jako další pojmy. Kromě reaktivního opatření a ochranného opatření, která jsou opatřeními definovanými výše, vymezuje ZKB ještě bezpečnostní opatření, organizační opatření, technická opatření a nápravná opatření, která však nejsou opatřeními ve smyslu § 11 ZKB. Otázka, která opatření jsou opatřeními může proto mezi studenty práva nebo právníky neznalými kybernetické bezpečnosti působit oprávněné zmatení.

Bezpečnostní opatření jsou základním pojmem v terminologii kybernetické bezpečnosti, který je definovaný v § 4 odst. 1 ZKB. Pojem bezpečnostní opatření označuje množinu různých úkonů, které mají za cíl zvýšit kybernetickou bezpečnost určitého subjektu, a to ať již z důvodu prevence či v reakci na reálnou hrozbu. Vzhledem k tomu, že základním účelem ZKB a obecně práva kybernetické bezpečnosti je zvýšení kybernetické bezpečnosti informačních a komunikačních systémů (dále jen „***informačních***

systémů“),[7] jsou bezpečnostní opatření všemi těmi úkony, kterými lze tohoto cíle dosáhnout. Základní členění bezpečnostních opatření je vymezené v § 5 odst. 2 a 3 ZKB, a sice na organizační, soustředící se primárně na personální a dokumentační činnosti, a technická opatření. Vzhledem k šíři celého spektra úkonů, které bezpečnostní opatření pokrývají, se tak logicky jedná spíše o výčet kategorií, které vzhledem k performativnímu charakteru regulace musí povinné osoby zohlednit při nalézání a indukci povinností na jejich konkrétní situaci. Jakkoliv tedy byla rozdílná míra konkretizace v taxativně uvedených bezpečnostních opatřeních v minulosti kritizována,[8] lze jejich bližší vymezení najít v části II. vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „***VKB***“). Tato specifikace, zřetelně inspirovaná normami ISO/IES 27000, by tak měla posloužit subjektům povinným dle ZKB nalézt konkrétní řešení obecných požadavků ZKB.

Před dalším již detailnějším výkladem konkrétních druhů opatření, je vhodné zmínit ještě nápravná opatření, která stejně jako bezpečnostní opatření nejsou opatřeními ve smyslu § 11 ZKB. Nápravná opatření jsou specifickým institutem situovaným do § 24, který dává NÚKIB pravomoc jejich prostřednictvím nařídit kontrolovanému subjektu konkrétní povinnost a případně i způsob jakým ji musí splnit. Pokud jsou zjištění kontroly NÚKIB v určitých případech tak vážná, že hrozí významné poškození nebo

---

[7] Autor se domnívá, že „*komunikační systém*“ je významově vyprázdněný pojem, od jehož používání bude s vývojem terminologie ZKB upuštěno, jelikož definice informačního systému v sobě zahrnuje také jeho komunikační složku. Z tohoto důvodu bude v této práci nadále pod pojem „*informační systém*“ podřazován také „*komunikační systém*“. Obdobně viz VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz. *Beck-online* [online]. [vid. 25. 3. 2021]. Získáno z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge2f6mjygfpwi6q&groupIndex=0&rowIndex=0 nebo také ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti*. Brno. 18. 4. 2021.

[8] POLČÁK, Radim. Kybernetická bezpečnost. In: POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, s. 603.

zničení informačního systému, může NÚKIB nápravným opatřením používání informačního systému na stanovenou dobu dokonce i zakázat.[9] Jakkoliv se jedná o poměrně velký zásah do autonomie vůle daného subjektu, je NÚKIB oprávněn nápravné opatření použít pouze pro nápravu nedostatků, které identifikoval při kontrole dle zákona č. 255/2012 Sb., o kontrole (kontrolního řádu), ve znění pozdějších předpisů.

Při jednání o bezpečnostních opatřeních, nápravných opatřeních či ochranných opatřeních, může často dojít ke zkrácení těchto výrazů na pouhá „opatření", a to nejen při komunikaci verbální. Záliba zákonodárce ve slově „opatření" proto budí rozpaky, zvláště pokud slovo „opatření" zavede do šesti různých pojmů v ZKB, a k tomu přidá význam i samostatnému slovu „opaření". V takovém případě lze proto uvítat iniciativu akademické obce, která opatřením dle § 11 ZKB začala přezdívat „protiopatření".[10] Tato přezdívka konvenuje významu tohoto právního institutu, který směřuje proti hrozbě či již proti probíhajícímu kybernetickému bezpečnostnímu incidentu a zároveň alespoň částečně řeší předestřený terminologický překryv. Z tohoto důvodu lze iniciativu ocenit a v zájmu vyšší přehlednosti zavedený pojem „protiopatření" dále používat za účelem zpřehlednění celé problematiky.[11]

3. SPECIFIKA PRÁVNÍHO INSTITUTU VAROVÁNÍ

Varování je jedním z trojice protiopatření, které má NÚKIB dle § 11 ZKB k dispozici, pokud zjistí, že míra hrozby překročila určitou hranici, a tudíž o hrozbě nestačí jen neformálně informovat (např. na vlastních webových stránkách nebo na sociálních sítích), ale je nezbytné přistoupit k některému z těchto tří formálních nástrojů. Kritériem pro volbu vhodného protiopat-

[9] Dle § 24 odst. 2 se jedná pouze o případy, kdy toto hrozí pro systém kritické informační infrastruktury, informační systém základní služby nebo významný informační systém.

[10] POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. Brno: Masarykova univerzita, 2016, s. 30.

[11] V souladu s touto výzvou, bude opatření dle § 11 ZKB nadále v článku označováno již jen jako „protiopatření". Ostatní instituty, které se však do protiopatření řadí (tedy varování, reaktivní opatření a ochranné opatření) není nezbytné přezdívat, jelikož mají díky odlišnému přídavnému jménu v názvu dostatečnou rozlišovací způsobilost bez dalšího. V tomto duchu lze doporučit také úpravu terminologie samotného zákona.

ření přitom není míra rizika, jak by se mohlo na první pohled zdát, ale fáze, ve které se kybernetický bezpečnostní incident v daný okamžik nachází. Těmito fázemi rozumíme:

1. Fázi identifikace hrozby v oblasti kybernetické bezpečnosti;
2. Fázi bezprostředně hrozícího nebo již probíhajícího kybernetického bezpečnostního incidentu;
3. Fázi po ukončení kybernetického bezpečnostního incidentu.

Podle charakteru situace a funkce, kterou v ní hrají jednotlivá protiopatření, se liší také jejich právní forma. Zatímco varování je vydáváno ve formě úkonu podle části čtvrté zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „***správní řád***“), reaktivní i ochranné opatření ZKB umožňuje vydávat formou opatření obecné povahy.[12] Na rozdíl od varování tak reaktivním i ochranným opatřením může NÚKIB povinným osobám přímo uložit konkrétní povinnost. Vrchnostenský příkaz provést konkrétní úkon pod hrozbou pokuty je společný rys, který má jak reaktivní opatření, tak také ochranné opatření. Tato možnost koresponduje se situací, kdy kybernetický bezpečnostní incident bezprostředně ohrožuje nebo již zasáhl větší množství ohrožených subjektů, a je nezbytné, aby všechny tyto subjekty povinně přijaly určitá bezpečnostní opatření. V takovém případě lze reaktivním opatřením vrchnostensky nařídit provedení bezpečnostních opatření k odvrácení kybernetického bezpečnostního incidentu neurčitému množství povinných subjektů vymezených pomocí generických znaků, jako je například používání zranitelného softwaru.[13] K tomu, aby bylo opatření obecné povahy efektivní, využívá zákonodárce výjimky v § 173 odst. 1 správního řádu[14] a v § 15 ZKB stanoví, že protiopatření, která jsou opatřeními obecné povahy, nabývají účinnosti okamžikem jejich vyvěšení na úřední

[12] ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti*. Brno. 18. 4. 2021.

[13] O tento typ se jednalo například při vydání reaktivního opatření k zabezpečení informačních systémů používajících Microsoft Exchange dne 11. 3. 2021.

[14] § 173 odst. 1 správního řádu: *„[…] Opatření obecné povahy nabývá účinnosti patnáctým dnem po dni vyvěšení veřejné vyhlášky. Hrozí-li vážná újma veřejnému zájmu, může opatření obecné povahy nabýt účinnosti již dnem vyvěšení; stanoví-li tak zvláštní zákon, může se tak stát před postupem podle § 172. Do opatření obecné povahy a jeho odůvodnění může každý nahlédnout u správního orgánu, který opatření obecné povahy vydal.“*

desce NÚKIB. Díky této výjimce zaručující okamžitou účinnost opatření obecné povahy spolu s nemožností podat proti němu opravný prostředek, se jedná o vhodný a efektivní nástroj pro ochranu většího množství subjektů před kybernetickými bezpečnostními incidenty.

Avšak v případě, že kybernetický bezpečnostní incident ohrožuje pouze jeden subjekt nebo více konkrétních subjektů,[15] nelze pak využít opatření obecné povahy.[16] Právě pro tuto druhou variantu kybernetického bezpečnostního incidentu ZKB umožňuje vydat reaktivní opatření formou rozhodnutí, proti němuž nemá případný rozklad odkladný účinek. Zákonodárce tak reaguje i na tuto druhou variantu kybernetického bezpečnostního incidentu, kdy je nezbytné rychle zavést příslušná bezpečnostní opatření u konkrétního napadeného subjektu v zájmu ochrany jeho informačních systémů.

Obdobně také ochranné opatření může formou opatření obecné povahy vrchnostensky uložit povinnost neurčitému množství genericky vymezených subjektů přijmout bezpečnostní opatření po skončení bezpečnostního incidentu. Účelem ochranného opatření je zamezit opakování nebo adekvátně zvýšit ochranu informačních systémů v návaznosti na zkušenosti získané při odrážení již odeznělého kybernetického bezpečnostního incidentu.[17]

Varování je vedle toho právním institutem, který je značně odlišný od ostatních protiopatření. Varování nelze vydat ani formou opatření obecné povahy, ani formou rozhodnutí, ale formou sdělení podle hlavy čtvrté správního řádu. To znamená, že varováním nelze vrchnostensky uložit povinnost, nebo za jeho nedodržení uložit sankci, jako je to možné u ostatních

---

[15] Jedná se tedy o konkrétní předmět regulace.

[16] Okruh adresátů je u opatření obecné povahy z definice vymezen obecně, a tudíž nemůže dopadat adresně na konkrétní subjekt. Více viz HEJČ, David. Reaktivní a ochranná opatření (obecné povahy) před kybernetickým bezpečnostním incidentem. In: *Cofola 2015 : The Conference Proceedings*. 2015. vyd. Brno: Masarykova univerzita, 1975, s. 22–23.

[17] VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz. *Beck-online* [online]. [vid. 25. 3. 2021]. Získáno z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge2f6mjygfpwi6q&groupIndex=0&rowIndex=0.

protiopatření. Varování také dopadá na jiný okruh povinných subjektů, kterými jsou kromě správců a provozovatelů informačního systému kritické informační infrastruktury (dále jen „***KII***“), správců a provozovatelů významných informačních systémů (dále jen „***VIS***“), a správců a provozovatelů informačních systémů základní služby (dále jen „***ISZS***“), také všechny další subjekty dle § 3 ZKB včetně poskytovatelů služeb elektronických komunikací a subjektů zajišťujících síť elektronických komunikací, orgánů nebo osob zajišťujících významnou síť, provozovatelů základní služby, a také poskytovatelů digitální služby (souhrnně dále jen „***regulované subjekty***“).[18]

K vydání varování je NÚKIB, jakožto ústřední orgán státní správy pro kybernetickou bezpečnost, oprávněn a zároveň povinen[19] v případě, že se dozví z vlastní činnosti, z podnětu provozovatele vládního CERT,[20] anebo od orgánů vykonávajících působnost v oblasti kybernetické bezpečnosti v zahraničí o hrozbě v oblasti kybernetické bezpečnosti. Pokud tedy nestačí na kybernetickou hrozbu upozornit neformálně, například na vlastních webových stránkách,[21] ale výše hrozby překročí určitou míru,[22] zveřejní NÚKIB varování dle § 12 odst. 2 ZKB na svých internetových stránkách, a oznámí jej také regulovaným subjektům.[23] Ty nadále ze samotného titulu varování nemají žádné konkrétní povinnosti, co musí s takto získanou informací dělat. Související povinnosti však vyplývají z jiných titulů, jako např. varování zohlednit v hodnocení rizik, přičemž pravidelně provádět hodnocení rizik je všední odpovědností některých regulovaných subjektů, jak bude uvedeno níže. Role samotného institutu varování by se tedy dala

[18] Výčet je stanoven v § 3 ZKB.

[19] Viz § 22 písm. b) ZKB.

[20] Jedná se o vládní koordinační místo pro okamžitou reakci na počítačové incidenty (vládní CERT - Computer Emergency Response Team).

[21] Tyto lze sledovat v rubrice „Vybrané aktuality, hrozby a doporučení“ na úvodní stránce NÚKIB, viz: https://www.nukib.cz/.

[22] Tato míra rizika přitom zhruba odpovídá kritickému stupni dle přílohy č. 2 VKB, popisovaném jako riziko nepřípustné, při němž musí být neprodleně zahájeny kroky k jeho odstranění.

[23] Oznámeno bude na příslušné kontaktní údaje regulovaných subjektů, vedené v evidenci podle § 16 odst. 4 ZKB. Současně by varování mělo být zpřístupněno na webových stránkách NÚKIB po celou dobu své platnosti a účinnosti.

označit za oficiální předání aktuální a věrohodné informace o zhoršení kyberbezpečnostní situace od úřední autority. Význam takového prokazatelného sdělení přitom vytváří očekávání společnosti, že regulovaný subjekt bude adekvátně reagovat. Informace totiž není pouhým dohadem, nebo spekulací v tisku, ale vážně míněnou adresnou zprávou, která může pocházet od tuzemských zpravodajských služeb, zahraničních spojenců či v různé míře vycházet z tajných informací. Pokud tedy autorita jako je ústřední orgán státní správy varování vydá, nelze pochybovat o tom, že se jedná o pečlivě vyhodnocené informace, které byly z množství utajovaných informací zformovány do jasného sdělení. Ačkoliv je tedy podstatou varování pouze oficiální předání informací o určité bezpečnostní hrozbě pro informační systémy regulovaných subjektů, má konstrukce varování závažné nepřímé dopady, které v systému práv a povinností regulovaných subjektů dosahují svého účelu i bez hrozeb přímých sankcí či autoritativních zásahů do autonomie vůle regulovaných subjektů.[24]

Obecně totiž mají všichni správci a provozovatelé informačních systémů obecnou odpovědnost za své systémy, a případně také za služby, které prostředním nich poskytují. Slovy § 2903 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***OZ***“): „*Nezakročí-li ten, komu újma hrozí, k jejímu odvrácení způsobem přiměřeným okolnostem, nese ze svého, čemu mohl zabránit.“* Z tohoto důvodu má již neformální informování NÚKIB na svých webových stránkách určitý význam, jelikož průběžně informuje o nejrůznějších hrozbách a zranitelnostech, kterým by osoby odpovědné za bezpečnost informačních systémů měly ve svém zájmu věnovat pozornost. Zejména regulované subjekty, které spravují ty nejvýznamnější informační systémy či kritickou informační infrastrukturu a jsou si vědomi, jaké důsledky by jejich omezení nebo zničení mohlo způsobit, by měly o to více preventivně dbát o jejich bezpečnost. V tomto

[24] O nezanedbatelném efektu ostatně svědčí také mediální popularita a reakce v nejrůznějších světových médiích, které vyvolala v minulosti již vydaná varování NÚKIB. Viz např. KAHN, Jan Lopatka, Michael. Czech cyber watchdog says its Huawei warning took U.S. by surprise. *Reuters* [online]. 2019 [vid. 24. 3. 2021]. ; SANTORA, Marc; GOEIJ, Hana de. Huawei Was a Czech Favorite. Now? It's a National Security Threat. *The New York Times* [online]. 2019 [vid. 24. 3. 2021].

kontextu je proto varování velice vhodným právním institutem, který umožňuje stupňovat povinnosti, a tím adekvátně reagovat na takové hrozby, které by již vyžadovaly vyšší míru pozornosti než při běžné prevenci, ale přímý vrchnostenský zásah do správy regulovaných subjektů je stále nástroj příliš invazivní.[25]

Oficiálním předáním informací od NÚKIB o potenciálně hrozícím bezpečnostním incidentu je tedy do jisté míry povinnost se s hrozbou vypořádat, předána na regulované subjekty, jelikož se varování promítne do dalších povinností regulovaných subjektů, které budou detailněji popsány v následující kapitole. V případě, že by regulovaný subjekt nedbal varování, vystavuje se odpovědnosti nejen za škodu na vlastní infrastruktuře, ale také povinnosti hradit škodu svých zákazníků či obchodních partnerů způsobenou rizikem, o kterém regulovaný subjekt věděl, a neučinil dostatečné kroky k jeho odvrácení. V tomto kontextu přitom hrozí, že regulovaný subjekt může být odpovědný také za škodu nebo jinou újmu způsobenou třetím osobám, pokud se dle § 2901 OZ prokáže, že regulovaný subjekt: „*může podle svých možností a schopností snadno odvrátit újmu, o níž ví nebo musí vědět, že hrozící závažností zjevně převyšuje, co je třeba k zákroku vynaložit.*“[26]

4. DŮSLEDKY VAROVÁNÍ PRO REGULOVANÉ SUBJEKTY V PRAXI

Za dobu své existence vydal NÚKIB již čtyři protiopatření, z čehož se jednalo postupně o dvě varování a následně o dvě reaktivní opatření.[27] Historicky první varování bylo vydáno dne 17. 12. 2018, v následujícím znění: „*Použití technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation a jejich dceřiných společností představuje hrozbu v oblasti kybernetické bezpečnosti.*“.[28] Druhé varování ze dne 16. 4.

[25] Nutno také zmínit, že je velice problematické pro jakýkoliv externí subjekt včetně NÚKIB diagnostikovat a vyhodnotit vhodná bezpečnostní opatření pro konkrétní informační systém, bez znalosti jeho prostředí a reálného fungování.

[26] POLČÁK, Radim. Kybernetická bezpečnost. In: POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, s. 610.

[27] Počítáno bez reaktivních opatření, která podléhají utajení ke dni 25. 5. 2021.

[28] Všechna protiopatření jsou dostupná na: https://nukib.cz/cs/uredni-deska/.

2020 pak reagovalo na akutní ohrožení zejména českého zdravotnictví, zatíženého koronavirovou krizí před rozsáhlou kampaní závažných kybernetických útoků. Účinnost druhého varování NÚKIB zrušil 20. 5. 2020, jelikož došlo ke snížení pravděpodobnosti dané hrozby. Dne 16. 12. 2020 vydal NÚKIB reaktivní opatření formou opatření obecné povahy, které ukládalo povinným osobám podle § 3písm. c) až f) ZKB povinnosti v souvislosti s platformou Orion od společnosti SolarWinds, a naposledy 12. 3. 2021 vydal NÚKIB další reaktivní opatření formou opatření obecné povahy k zabezpečení informačních systémů regulovaných subjektů, používajících Microsoft Exchange Server. Vzhledem k povaze reaktivních opatření, které nemají dlouhotrvající efekt a k ukončení druhého z varování, zůstává pro regulované subjekty stále nejvýznamnější první varování ze 17. 12. 2018. V současnosti nic nenasvědčuje tomu, že jeho platnost bude v blízké době ukončena, a v kontextu výrazného rozšiřování regulovaných subjektů, jejichž počet by se měl mezi lety 2020 až 2025 téměř ztrojnásobit, význam tohoto varování opět roste.[29]

V souladu s výše uvedeným lze potvrdit, že varování nestanovuje regulovaným subjektům žádné konkrétní pokyny ani povinnosti, nicméně významově na varování navazují povinnosti stanovené v jednotlivých odstavcích § 4 ZKB, které s ním dále pracují. Nejprve § 4 odst. 2 a 3 stanovuje správcům a provozovatelům informačních systémů KII, VIS, ISZS (dále jen „***povinné osoby***“) a poskytovatelům digitálních služeb[30] obecnou povinnost zavést a provádět vhodná bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti. Odst. 4 ZKB pak následně tuto generální povinnost dále rozvádí, když povinným osobám ukládá, aby zohlednily požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro

[29] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost* [online]. 2020, s. 10 [vid. 23. 3. 2021].

[30] Poskytovatelům digitální služby na rozdíl od ostatních povinných osob nestanovuje konkrétní povinnosti VKB, ale prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný.

jejich informační systémy. To znamená, že bezpečnostní opatření, která povinné osoby zavedly na základě vlastních hodnocení rizik, jsou povinny přenést také na své dodavatele skrze smluvní ujednání, která s nimi uzavřou.

Obdobně pak také § 4 odst. 5 ZKB ukládá povinným osobám a provozovatelům základní služby, pokud jsou orgánem veřejné moci,[31] ve smlouvě s poskytovatelem cloud computingu upravit celý výčet nezbytných náležitostí. Všechna tato ustanovení tudíž ukládají povinnosti, do jejichž plnění se obsah varování pravděpodobně promítne. Povinné osoby totiž musí veškerá protiopatření včetně Varování zohlednit ve svých pravidelně prováděných hodnoceních rizik v souladu s § 5 odst. 1 písm. h) č. 3 VKB, a to podle požadavků § 5 VKB zabývajícího se řízením rizik. Povinné osoby musí hodnocení rizik provést také před výběrem významného dodavatele, v souladu s § 8 VKB a pravidelně je přezkoumávat. To obnáší nejprve analyzovat prostředí a prošetřit, jakým způsobem budou rizikové prostředky v informačních systémech využívány, a na základě této znalosti formulovat konkrétní či typové hrozby.[32] Je nutné v dedukci důsledků varování postupovat na základě konkrétních zkušeností zadavatele tak, aby pokud možno nebyly opomenuty žádné aspekty potenciální hrozby.[33] Následně je nezbytné aktualizovat hodnocení rizik a zhodnotit tato rizika ve světle varování. K hodnocení rizik může povinná osoba využít přílohu č. 2 VKB (nebo jakoukoliv jinou metodiku, jenž zabezpečí stejnou nebo vyšší úroveň procesu řízení rizik), pomocí které pro sebe vypočítá na základě hodnoty aktiv dle přílohy č. 1 k VKB, hodnoty hrozby a také zranitelnosti

[31] Toto ustanovení se v případě přijetí právě projednávaného legislativního návrhu, bude pravděpodobně rozšiřovat na všechny orgány veřejné moci.

[32] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení.* [online] 4. 1. 2020, s. 10 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

[33] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení.* [online] 4. 1. 2020, s. 10 [vid. 23. 1. 2021]. Dostupné z: https://www.mvcr.cz/soubor/priloha-c-2-podpurny-material-nukib-pdf.aspx.

dle přílohy č. 2 k VKB hodnotu rizika.[34] V případě postupu podle VKB se hodnota rizika vypočte na základě hodnoty aktiv dle přílohy č. 1 k VKB, hodnoty hrozby a také zranitelnosti dle přílohy č. 2 k VKB. Výsledná hodnota rizika pak je součinem hodnot hrozby, zranitelnosti a dopadu na aktivum, což je v souladu s § 5 odst. 1 písm. d) VKB.[35] Na základě hodnocení rizik identifikovaných v provedené analýze jsou tedy povinné osoby povinny na riziko adekvátně reagovat. Touto reakcí bude velice pravděpodobně přijetí bezpečnostních opatření, která si v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotu daného rizika povinné osoby samy navrhnou. To znamená, že bezpečnostní opatření snižují pravděpodobnost realizace identifikovaných nežádoucích jevů na přijatelnou úroveň. Díky znalosti vlastních informačních systémů jsou regulované subjekty logicky těmi nejpovolanějšími k posouzení a vyhodnocení vhodných bezpečnostních opatření, které je v dané situaci vhodné přijmout. Bylo by totiž zjevně neefektivní plošně aplikovat na všechny ohrožené informační systémy stejná bezpečnostní opatření bez ohledu na druh, způsob nastavení, či jiná specifika předmětných informačních systémů. Povinnost provést hodnocení rizik platí jak pro stávající, tak i pro nově poptávané informační systémy, přičemž řádně provést hodnocení rizik je alfou omegou pro případné ověření či přezkoumání přiměřenosti přijatých bezpečnostních opatření.

Kromě regulovaných subjektů má varování vliv také na dodavatele, kteří dodávají technické nebo programové prostředky regulovaným subjektům. Ty mohou být buď v pozici provozovatele určeného informačního systému podle § 2 písm. g) ZKB, pokud pro regulovaný subjekt zajišťují funkčnost technických a programových prostředků tvořících informační systém, anebo v pozici běžného dodavatele. Provozovatelům určených informačních

[34] SASKOVÁ, Vladěna. *Varování před kybernetickou hrozbou podle § 12 ZKB*. Národní úřad pro kybernetickou a informační bezpečnost [online] 17. 5. 2019 [vid. 1. 4. 2020]. Dostupné z: https://www.mvcr.cz/soubor/5-saskova-vladena-varovani-pred-kybernetickou-hrozbou-podle-12-zkb.aspx.

[35] Hodnota hrozby po zveřejnění varování bude v nejvyšším stupni, tedy ve výši 4 ze 4, pokud bude použita stupnice podle VKB. Pokud bude použita jiná metoda výpočtu, pak bude obdobně hodnota hrozby zvýšena na nejvyšší hodnotu, a to ačkoliv mohou být vzorce výpočtu různé.

systémů vyplývají povinnosti přímo ze ZKB, zatímco běžným dodavatelům ZKB žádné povinnosti neukládá. Běžní dodavatelé jsou tak dotčeni povinnostmi vyplývajícími ze ZKB pouze nepřímo skrze pokyny zadavatelů, pokud tito mají povinnost běžné dodavatele řídit dle § 8 VKB.

Ačkoliv je varování adresované pouze regulovaným subjektům, mohou ostatní subjekty varování zohlednit dobrovolně (dále jen „***nepovinní***"). Z hlediska kybernetické bezpečnosti není přitom rozhodné, zda má subjekt povinnost varování zohlednit z jiného důvodu (např. požadavek zřizovatele, snaha o získání certifikace ISO 27000, apod.), ale pouze zda tuto povinnost ukládá zákon.[36] V souladu s prevenční povinností dle OZ,[37] je ostatně zavedení přiměřených bezpečnostních opatření dle varování nepovinnými naprosto nezávadné a bezpochyby také v souladu s péčí řádného hospodáře. Je však nezbytné dát si pozor na to, jak budou nepovinní s varováním pracovat. Zásadní totiž je, že kvůli absenci povinnosti varování reflektovat v rámci zavádění a provádění bezpečnostních opatření podle § 4 odst. 2 ZKB se na tyto subjekty neuplatní § 4 odst. 4 ZKB ani odst. § 4 odst. 7 ZKB, zakotvující presumpci souladnosti bezpečnostních opatření s podmínkami hospodářské soutěže, a tudíž bude záviset pouze na provedeném hodnocení rizik nepovinného, a na kvalitě jeho argumentace. Hodnocení rizik a na základě něj přijatá bezpečnostní opatření, tedy musí být o to lépe vyargumentovaná, zdokumentovaná a nesmí být zmatečná a nepřezkoumatelná. Velice snadno se totiž může stát, že nepovinný v dobré víře slepě přejme předmět varování jako dogma, a nikoliv jako vstup pro vlastní zhodnocení rizika. Takové chování by však znamenalo nepochopení právní úpravy a svévolné vytváření podmínek, které mohou být v kontextu zadávání veřejných zakázek posouzeny jako bezdůvodné překážky hospodářské soutěže. V takovém případě se však nepovinný vystavuje souvisejícím sankcím, které pro veřejného zadavatele mohou mimo jiné znamenat i zrušení veřejné zakázky.

---

[36] Rozhodnutí Úřadu pro ochranu hospodářské soutěže ze dne 13. 1. 2020 sp. zn. S0358/2019/VZ, bod 59. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

[37] Detailnější popis prevenční povinnosti viz kapitola III.

5. VZTAH ZZVZ A ZKB

Zadávání veřejných zakázek je právem detailně regulovaný a vysoce formalizovaný proces výběru smluvního partnera pro uzavření smlouvy zadavatelem, upravený zejména v zákoně č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***“) a příslušných prováděcích předpisech. Zadávání veřejných zakázek se tak odlišuje od jinak málo regulovaného, a principem smluvní svobody a dispozitivnosti se řídícího kontraktačního procesu dle OZ.[38] Kromě zásad transparentnosti, přiměřenosti a rovného zacházení je proces zadávání veřejných zakázek založen zejména na zásadě zákazu diskriminace dodavatelů,[39] což má zajišťovat rovnou a nediskriminační soutěž všech dodavatelů v zájmu hospodárného, efektivního a účelného vynakládání veřejných prostředků.

Vedle toho ZKB sleduje jiné cíle, jakými je zajištění ochrany kybernetického prostoru České republiky, zajištění základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací, a obrana nedistributivních práv státu, včetně veřejného zájmu na KII, VIS a poskytování základních služeb.[40] Tyto kyberbezpečnostní cíle, které jsou dle důvodové zprávy jedním z určujících aspektů bezpečnostního prostředí v České republice,[41] ale nemusí bez dalšího odpovídat výše uvedenému rovnému přístupu ZZVZ k výběru dodavatele. ZKB totiž do zadávacího řízení vnáší jiné hodnoty, než je pouze čistě ekonomický zájem, a sice zájem bezpečnostní. ZKB tak při akcentu na zachování kybernetické bezpečnosti není překážkou hospodářské soutěži, ale vnáší do hospodářské soutěže nové mantinely, ve kterých se hospodářská soutěž odehrává.

---

[38] DVOŘÁK, David, MACHUREK, Tomáš, NOVOTNÝ, Petr, a kol. § 1 [Předmět úpravy]. In: DVOŘÁK, David, MACHUREK, Tomáš, NOVOTNÝ, Petr, a kol. Zákon o zadávání veřejných zakázek. 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, s. 1.

[39] § 6 ZZVZ.

[40] Vláda: Důvodová zpráva k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz.

[41] Ibidem.

ZZVZ a ZKB jsou oba zákonnými předpisy stejné právní síly. Nejsou tedy vůči sobě ve vztahu nadřízenosti a podřízenosti ani obecnosti a speciality.[42] Z toho vyplývá, že subjekty, které současně spadají do působnosti obou zákonů, jsou povinny postupovat tak, aby dostály povinnostem, které na ně kladou současně oba právní předpisy. Není přitom výjimkou, že regulované subjekty jsou současně zadavatelé dle ZZVZ.[43] Propojení těchto dvou předpisů však v praxi způsobuje potíže.[44] Pro mnoho regulovaných subjektů totiž může být velice náročné správně projít vysoce formalizovaným procesem zadání veřejné zakázky, a stejně tak pro mnoho veřejných zadavatelů může být provedení analýzy a hodnocení rizik v oblasti kybernetické bezpečnosti, včetně následného řízení poddodavatelů v souvislosti se ZKB a VKB, velice obtížné. Ve veřejné správě, která dlouhodobě trpí nedostatkem odborného personálu z oblasti ICT,[45] a nedostatečnou úrovní specializace a motivace svých ICT pracovníků,[46] se tyto dva problémy nesčítají, jako spíše násobí. Není proto překvapující, že regulovaný subjekt v pozici veřejného zadavatele (dále jen „***zadavatel***“) s varováním, které klade vysoké nároky na samostatné a odborné plnění povinností dle ZKB a VKB, může mít potíže. Bolestivý je v tomto kontextu fakt, že při zadávání veřejné zakázky může být i drobné procesní zaváhání pro osud veřejné zakázky fatální.

---

[42] SASKOVÁ, Vladěna, *Novela vyhlášky o VIS, varování NÚKIB a zadávání veřejných zakázek*. Národní úřad pro kybernetickou a informační bezpečnost [online] 3. 12. 2019 [vid. 1. 4. 2020]. Dostupné z: https://www.cimib.cz/novinka/125-pozvanka-na-konferenci-kbs-2019

[43] KOTZIAN, Robert, Veřejné zakázky a kybernetická bezpečnost. *epravo.*cz [online] 28. 1. 2020 [vid. 18. 1. 2021]. Dostupné z: https://www.epravo.cz/top/clanky/verejne-zakazky-a-kyberneticka-bezpecnost-110558.html.

[44] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost*. [online] 30. 7. 2020, s. 5 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

[45] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Návrh opatření zvyšujících efektivnost služeb veřejné správy a podpůrných ICT služeb* [online]. 17. červen 2014.

[46] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Digitální Česko: Metody řízení ICT veřejné správy ČR* [online]. 19. červen 2020.

6. ZOHLEDNĚNÍ VAROVÁNÍ PŘI ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK

Jak již bylo obecně nastíněno výše, každý zadavatel veřejné zakázky musí v zadávacím řízení postupovat v souladu se zásadami zadávání veřejných zakázek dle § 6 ZZVZ, tedy transparentně, přiměřeně a nediskriminačně a podle § 36 odst. 1 ZZVZ nesmí nastavit zadávací podmínky tak, aby vytvářely bezdůvodné překážky hospodářské soutěže.[47] Současně ale § 4 odst. 4 ZKB uvádí, že „O*rgány a osoby uvedené v § 3 písm. c) až f)*[48] *jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.*“ Ačkoliv by požadavky stanovené na základě povinnosti vyplývající z jiného právního předpisu měly být důvodné již ze své podstaty,[49] tak věta druhá výše uvedené citace znatelně usnadňuje unesení důkazního břemene zadavatele při přijímání soutěž omezujících bezpečnostních opatření. Zavádí totiž povinnou presumpci[50] souladu bezpečnostních opatření, které zadavatel jako povinná osoba přijme na základě požadavků ZKB, s požadavky § 36 odst. 1 ZZVZ.[51] Jinými slovy je tedy vyjádřeno, že přijetí přiměřených bezpečnostních opatření není nezákonným omezením hospodářské soutěže. Podmínkou pro uplatnění presumpce v § 4 odst. 4 ZKB je však přiměřenost

[47] Jedná se pouze o demonstrativní, a nikoliv úplný výčet zásad zadávání veřejných zakázek.

[48] Jedná se o správce a provozovatele informačních systémů KII, správce a provozovatele VIS a správce a provozovatele informačních systémů základní služby.

[49] Srov. “*Nemůže-li tak zadavatel dodržet svou zákonnou povinnost při zadávání veřejné zakázky v oblasti kybernetické bezpečnosti jinak, než přijetím sporného opatření, nejedná se o nedovolenou diskriminaci“* Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Bod 63. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

[50] Presumpce v následujícím znění: „*Zohlednění požadavků vyplývajících z bezpečnostních opatření … v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže“* je spíše zákonným příkazem či povinností, která se pohybuje na pomezí právní fikce a nevyvratitelné právní domněnky, přičemž plně nenaplňuje parametry ani jedné z nich.

těchto bezpečnostních opatření, které zadavatel posuzuje a dokládá zpracovaným hodnocením rizik.

Zadavatel tedy může na základě provedeného hodnocení rizik požadovat splnění určitých kritérií omezujících některé dodavatele nebo jimi nabízené zboží, pokud budou tato kritéria odůvodněná bezpečnostní potřebou přiměřeně dané situaci. Zadavatel tudíž musí bezpečnostní opatření volit racionálně a přezkoumatelně, aby byl schopný unést důkazní břemeno důvodnosti omezení hospodářské soutěže. Nelze totiž svévolně omezovat hospodářskou soutěž pod záštitou bezpečnostních zájmů. Omezení, ke kterým povinná osoba v konkrétním případě přistoupí, nesmí být excesivní a nepřiměřená vzhledem k hrozícímu riziku, nýbrž přiměřená a vždy obhajitelná. To potvrzuje i Úřad pro ochranu hospodářské soutěže (dále jen „***ÚOHS***“), který je dle § 248 ZZVZ dozorovým orgánem v oblasti zadávání veřejných zakázek, a je tedy oprávněn k rozhodnutí, zda byl postup zadavatele souladný s pravidly obsaženými v ZZVZ. ÚOHS potvrdil, že lze hospodářskou soutěž oprávněně omezit bezpečnostními opatřeními, které reagují na varování a vycházejí ze zpracovaného hodnocení rizik ve svém rozhodnutí S0262/2019/VZ ze dne 6. 11. 2019, když zamítl návrh společnosti Huawei Technologies (Czech) s.r.o. na zrušení veřejné zakázky, ve které zadavatel stanovil podmínku dodat další (zdvojující) kusy hardware navíc v případě dodání programových prostředků výrobců uvedených ve varování NÚKIB ze 17. 12. 2018, čímž de facto použití hardware společnosti Huawei Technologies s.r.o. vyloučil. ÚOHS však postup zadavatele označil za správný, když ve svém zamítavém rozhodnutí uvedl, že: „*Ke spornému opatření tak zadavatel nepřistoupil svévolně, nýbrž reagoval na varování NÚKIB, a to po řádně provedeném procesu hodnocení rizik.*“

Hodnocení rizik je tedy zásadní pro určení, zda se jedná o nezákonné omezení hospodářské soutěže či nikoliv. Presumpce souladnosti bezpečnostních opatření omezujících hospodářskou soutěž totiž závisí na posouzení, zda byla bezpečnostní opatření nezbytná pro splnění povinností ZKB. Na-

[51] Obdobně pak § 4 odst. 7 ZKB stanoví presumpci souladnosti bezpečnostních opatření sjednaných ve smlouvě s poskytovatelem cloud computingu s podmínkami hospodářské soutěže, pod podmínkou jejich „nezbytnosti pro splnění povinností“ dle ZZVZ.

plnění podmínek ZKB je oprávněn posoudit NÚKIB. Obdobně má ÚOHS pravomoc přezkoumat podmínky ZZVZ, ale není jeho specializací posuzovat, zda byla bezpečnostní opatření přijata v míře nezbytné pro splnění povinností ZKB.[52]

ÚOHS tedy může buď aplikovat presumpci souladnosti zavedených bezpečnostních opatření (a tudíž konstatovat souladnost), nebo požádat o posouzení nezbytnosti uvedených bezpečnostních opatření NÚKIB. V případě, že však NÚKIB rozhodne, že zavedená bezpečnostní opatření nebyla nezbytná, neznamená to nutně, že povinná osoba porušila pravidla hospodářské soutěže. Pakliže tedy povinná osoba přijme bezpečnostní opatření nad rámec požadavků ZKB (a zajistí vzhledem k situaci nadstandardní bezpečnostní opatření), musí si sám toto rozhodnutí odůvodnit a obhájit. Zavedení vyšších bezpečnostních opatření, než vyžaduje ZKB tedy nezbytně nemusí být porušením hospodářské soutěže, pokud je zadavatel schopný své rozhodnutí zdůvodnit v hodnocení rizik. Jak vyplývá z rozhodovací praxe, tak obsah hodnocení rizik je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele, které v souhrnu tvoří proces řízení rizik.[53]

Implementace varování bude vždy pro zadavatele znamenat postupnou identifikaci hrozeb, následnou identifikaci rizik, analýzu rizik a jejich vyhodnocení. Možnosti, které má zadavatel k dispozici, se ale budou lišit v závislosti na procesu zadávání veřejných zakázek, a to jak fází, ve které se zadávání veřejné zakázky nachází v okamžiku, kdy je vydáno varování, tak také druhem zadávacího řízení nebo jiného postupu zadavatele dle ZZVZ (např. zadávání veřejné zakázky malého rozsahu). Z důvodu odlišných možností zadavatele v různých fázích zadávacího řízení je nutné rozlišovat tyto čtyři časové fáze:

1.1.1 Fáze přípravy veřejné zakázky;

[52] *„Z hlediska posouzení, zda zadavatel stanovil spornou podmínku v souladu se zákonem, je rozhodné stanovisko NÚKIB, ze kterého bude vyplývat, zda zadavatel spornou podmínku stanovil v souladu s příslušnými ustanoveními ZKB a VKB či nikoliv*.“ Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Bod 102. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

[53] Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Bod 61. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

2.1.1 Fáze po zahájení zadávacího řízení a před uplynutím lhůty k podání žádosti o účast, předběžných nabídek či nabídek;

3.1.1 Fáze po zahájení zadávacího řízení a po uplynutí lhůty k podání žádosti o účast, předběžných nabídek či nabídek;

4.1.1 Fáze po zadání veřejné zakázky.[54]

Pokud se zadávání veřejné zakázky nachází na svém samotném začátku, a tudíž se teprve připravuje zadávací dokumentace či výběrové podmínky včetně smluvních podmínek (dále jen „***zadávací dokumentace***“), pak má zadavatel možnost do obsahové stránky dokumentace zasahovat a přizpůsobovat ji relativně volně. Je-li tedy vydáno varování ve fázi přípravy veřejné zakázky, musí zadavatel v souladu s § 8 odst. 1 písm. E) VKB zejména řídit rizika spojená s potenciálními dodavateli. Jak bylo vysvětleno výše, tak zadavatel nemůže bez dalšího vyloučit např. určité technické prostředky, ale musí nejprve objektivně posoudit dopad varování na jeho situaci a na předmět veřejnou zakázkou poptávaného plnění, než přijme případná bezpečnostní opatření. To zahrnuje zejména provedení hodnocení rizik podle § 5 VKB, a následné zapracování jejích závěrů do zadávací dokumentace.[55] Způsob zapracování takto dovozených požadavků je pak zcela na vůli zadavatele. Lze zvolit různé varianty zohlednění od stanovení nepřekročitelných technických podmínek, použití jako hodnotícího kritéria, stanovení požadavku na dodání redundantních zařízení, výslovného zakázání rizikových produktů, zavedení technických opatření eliminujících zranitelnosti, nebo také rozdělení zakázky na části, a stanovení rozdílných pod-

[54] Srov. SASKOVÁ, Vladěna. *Varování před kybernetickou hrozbou podle § 12 ZKB*. Národní úřad pro kybernetickou a informační bezpečnost [online] 17. 5. 2019 [vid. 1. 4. 2020]. Dostupné z: https://www.mvcr.cz/soubor/5-saskova-vladena-varovani-pred-kybernetickou-hrozbou-podle-12-zkb.aspx.

[55] Hodnocení rizik nebo analýzu s hodnocením rizik spojenou, není zadavatel povinen uveřejnit jako součást zadávací dokumentace nebo ji poskytnout dodavatelům jiným způsobem v rámci zadávacího řízení nebo výběrového řízení (současně dle ZKB zadavatel není povinen dokument poskytnout ani dle zákona č. 106/1999 Sb. o svobodném přístupu k informacím ve znění pozdějších předpisů). Zadavatel by pouze měl v případě, že na základě hodnocení rizik stanoví zadávací podmínky omezující např. využití výrobků od určitých dodavatelů, tento svůj postup odůvodnit (detailnost odůvodnění bude odpovídat rozsahu informací, které je zadavatel oprávněn dodavatelům sdělit při současném zachování pravidel kybernetické bezpečnosti - tedy neposkytne hodnocení rizik, ale přiměřeně odůvodní své kroky v dané věci).

mínek pro každou z jejích částí.[56] Při výběru způsobu zohlednění je vhodné upřednostnit nasazení dostupných technických opatření, pokud je to fakticky i finančně možné, a dle hodnocení rizik dostatečné. V opačném případě lze ze zbývajících způsobů doporučit volit spíše méně omezující způsoby, jako např. volbu redundance před výslovným zákazem určitých produktů. Jako do jisté míry jistější řešení se jeví upřednostnit kvalifikaci před hodnotícími kritérii, jelikož ačkoliv vždy záleží na způsobu nastavení hodnotících kritérií, je volba kvalifikace pro zadavatele jistějším způsobem. Při řešení prostřednictvím hodnotících kritérií totiž může nastat situace, kdy rizikové produkty v hodnocení zvítězí díky např. nižší ceně či jiným posuzovaným hodnotícím kritériím, které ve výsledku hodnocení bezpečnosti převáží, což by dostalo zadavatele do svízelné situace.

V případě, že zadávací řízení nebo výběrové řízení[57] bylo již zahájeno, ale ještě neuplynula lhůta k podání žádosti o účast, předběžné nabídky či nabídky, pak lze po řádném provedení analýzy rizik včetně hodnocení rizik v souladu s § 99 ZZVZ (nebo interními předpisy zadavatele, v případě veřejných zakázek malého rozsahu), změnit či doplnit zadávací podmínky obsažené v zadávací dokumentaci.[58] V takovém případě ale zadavatel bude povinen na povinnost změnu či doplnění uveřejnit nebo oznámit dodavatelům stejným způsobem jako původní zadávací podmínky do kterých bylo zasaženo, a také přiměřeně prodloužit lhůtu pro podání žádosti o účast, předběžné nabídky či nabídky.

Po uplynutí lhůty pro podání žádostí o účast, předběžných nabídek či nabídek již nelze zadávací podmínky měnit. Nabízí se tedy možnost pokračovat v zadávacím či výběrovém řízení, a přijmout pouze dílčí bezpečnostní opatření, nebo pozměnit způsob či účel k jakému bude předmět plnění pou-

[56] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost*. [online] 30. 7. 2020, s. 6-7 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

[57] Ačkoliv se nejedná o zákonný pojem, je výběrové řízení pojmem užívaným v praxi zadávání veřejných zakázek pro veřejné zakázky malého rozsahu.

[58] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Metodika k varování ze dne 17. prosince 2018*. [online] 4. 1. 2019, s. 14 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

žíván, pokud je to v dané situaci možné. Jakoukoliv modifikací však nesmí být dotčen postup v zadávacím řízení nebo výběrovém řízení. Alternativně je možné pokusit se dodavatele vyloučit dle některého z důvodů uvedených v § 48 ZZVZ, pokud k tomu budou splněny příslušné podmínky. V případě, že dle hodnocení rizik nelze učinit žádnou z výše uvedených možností, nezbývá než zadávací řízení zrušit podle § 127 odst. 2 písm. d) ZZVZ (výběrové řízení by se rušilo dle interních pravidel zadavatele). Varování je v tomto kontextu možné považovat za důvod hodný zvláštního zřetele, pro který nelze po zadavateli požadovat, aby v řízení pokračoval, pokud by soutěžené plnění neodpovídalo novým kyberbezpečnostním požadavkům.[59] Rozhodnutí, kterou z možností zadavatel zvolí, by se však mělo vždy odvíjet od řádně provedeného hodnocení rizik.

Jestliže již došlo k zadání veřejné zakázky vybranému dodavateli, pak je v první řadě nezbytné, aby zadavatel provedl hodnocení rizik dle výše uvedeného. Na základě výsledků je pak zadavatel povinen rozhodnout, zda je identifikované riziko akceptovatelné, a postačí zavést bezpečnostní opatření ke snížení rizik, aniž by došlo k podstatné změně závazku ze smlouvy dle § 222 ZZVZ.[60] V opačném případě, pokud zadavatel usoudí, že nestačí přijmout bezpečnostní opatření ke snížení rizika nebo tento postup nebude souladný se ZZVZ, je nutné smlouvu na veřejnou zakázku vypovědět nebo od ní odstoupit.[61] Výše uvedené nebrání zadavateli rozhodnout se ukončit smlouvu podle obecné právní úpravy v OZ, jiných právních předpisů či vlastních specifických ujednání ve smlouvě s dodavatelem. Pokud ale není specificky sjednána možnost smlouvu vypovědět nebo od smlouvy odstoupit a současně v jejím plnění nelze pokračovat z důvodu vydání varování, pak lze v souladu s § 223 odst. 1 ZZVZ závazek ukončit výpovědí či odstoupením na základě tohoto ustanovení.

---

[59] Ibidem, s. 14.

[60] Kritérium podstatné změny je však nezbytné posuzovat vždy ad hoc s ohledem na povahu původního závazku.

[61] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Metodika k varování ze dne 17. prosince 2018*. [online] 4. 1. 2019, s. 15 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

7. ZÁVĚR

Jednoznačnou výhodou české právní úpravy kybernetické bezpečnosti je, že disponuje širší paletou právních institutů, než má většina ostatních států EU, což umožňuje lépe reagovat na rizika rozličné intenzity. Používání podobných označení u různých pojmů však může mít za následek nepřehlednost a vyšší pravděpodobnost jejich záměny. Článek se proto nejprve zabývá obecně opatřeními dle čl. 11 ZKB, vysvětluje terminologii pojmů pracujících s označením „opatření“, a navrhuje přijetí označení „protiopatření“ pro opatření dle čl. 11 ZKB. Smyslem přijetí této přezdívky, která je již částečně používána v akademické sféře[62] je přitom zvýšení přehlednosti a dosažení jasné terminologie ZKB.

Jedním z právních institutů, který není převzat ze směrnice NIS, ale který byl do českého právního řádu přijat na základě vlastní legislativní iniciativy je varování dle § 12 ZKB, které přináší efektivní právní řešení pro hrozby v oblasti kybernetické bezpečnosti, pro něž nestačí obecná prevenční povinnost, ale vrchnostenský zásah do autonomie vůle regulovaných osob, stanovující práva a povinnosti, by byl již nepřiměřeně invazivní. Varování samo o sobě nestanoví regulovaným subjektům žádné přímé povinnosti, ale jeho význam spočívá v oficiálním předání informací o hrozbě. Komplex práv a povinností vyplývající ze ZKB a VKB pak povinné subjekty povinuje zohlednit hrozbu v pravidelně prováděném hodnocení rizik, a pokud zjistí takovou potřebu, pak přijmout nezbytná bezpečnostní opatření k její eliminaci. Za samotné ignorování varování a nezavedení adekvátních bezpečnostních opatřeních v reakci na hrozbu regulovaným subjektům nehrozí přímá sankce. Pokuta však hrozí povinným subjektům dle § 25 odst. 3 až 8 písm. b) ZKB, pokud nezohlední požadavky vyplývající z bezpečnostních opatření (které přijaly na základě varování) při výběru dodavatele. Další rizikem pak je potenciální povinnost hradit škody, vzniklé v důsledku vlastní nečinnosti povinného subjektu a případného omisivního jednání.

[62] POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. Brno: Masarykova univerzita, 2016, s. 30.; Shodně též ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti*. Brno. 18. 4. 2021.

V poslední části článku je pojednáno o vztahu ZKB a ZZVZ, jakožto dvou právních předpisů stejné právní síly, ale diametrálně odlišného charakteru. Zatímco ZKB usiluje o zvýšení kybernetické bezpečnosti, čehož dosahuje pomocí performativních pravidel, ZZVZ reprezentuje zájem na rovné a nediskriminační hospodářské soutěži prostřednictvím vysoce formalizovaných administrativních pravidel. Ačkoliv mají oba právní předpisy stejnou právní sílu, skloubit jejich požadavky činí často problém zejména ve veřejném sektoru, který trpí nedostatkem kvalifikovaného personálu, schopného obsáhnout obě tato specifická právní odvětví. Za tímto účelem je proto pojednáno o správném způsobu zohlednění varování v případě, že je veřejný zadavatel dle ZZVZ současně regulovaným subjektem dle ZKB. Vzhledem k tomu, že počet regulovaných subjektů má mezi lety 2020 až 2025 vzrůst téměř trojnásobně, lze předpokládat, že se bude jednat o čím dál častější jev. Nakonec jsou v souladu s podpůrnými materiály NÚKIB předestřeny také možnosti veřejných zadavatelů, jak varování zohlednit v různých fázích zadávacího řízení.

8. SEZNAM POUŽITÝCH ZDROJŮ:

[1]DVOŘÁK, David; MACHUREK, Tomáš; NOVOTNÝ, Petr; a kol. § 1 [Předmět úpravy]. In: DVOŘÁK, David, MACHUREK, Tomáš, NOVOTNÝ, Petr, a kol. *Zákon o zadávání veřejných zakázek.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, 1320 s. ISBN 978-80-7400-651-7.

[2]HEJČ, David. Reaktivní a ochranná opatření (obecné povahy) před kybernetickým bezpečnostním incidentem. In: *Cofola 2015: The Conference Proceedings*. 2015. vyd. Brno: Masarykova univerzita, s. 721–730. ISBN 978-80-210-7976-2.

[3]KAHN, Jan; LOPATKA, Michael. Czech cyber watchdog says its Huawei warning took U.S. by surprise. *Reuters* [online]. 2019 [vid. 24. 3. 2021]. Získáno z: https://www.reuters.com/article/us-huawei-europe-czech-idUSKCN1QN1DI

[4]KOTZIAN, Robert. Veřejné zakázky a kybernetická bezpečnost. *epravo.*cz [online] 28. 1. 2020 [vid. 18. 1. 2021]. Dostupné z: https://www.epravo.cz/top/clanky/verejne-zakazky-a-kyberneticka-bezpecnost-110558.html

[5]MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Návrh opatření zvyšujících efektivnost služeb veřejné správy a podpůrných ICT služeb* [online]. 17. červen 2014. [vid. 28. 3. 2021] Získáno z: https://ipodpora.odbory.info/soubory/dms/wysiwyg_uploads/a05b113e9f39c8af/uploads/Navrh-opatreni-zvysujicich-efektivnost-sluzeb-verejne-spravy-a-podpurnych-ICT-suzeb.pdf

[6]MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Digitální Česko: Metody řízení ICT veřejné správy ČR* [online]. 19. červen 2020.

[vid. 28. 3. 2021]. Získáno z: https://archi.gov.cz/_media/dokumenty:navazujici_dokument_c_1metody_rizeni_ict_vs.pdf

[7]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost* [online]. 2020. [vid. 23. 3. 2021]. Získáno z: https://nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf

[8]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Metodika k varování ze dne 17. prosince 2018*. [online] 4. 1. 2019, 17 s. [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[9]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost*. [online] 30. 7. 2020, 20 s. [vid. 23. 1. 2021].
Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[10]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení*. [online] 4. 1. 2020, 28 s. [vid. 23. 1. 2021]. Dostupné z: https://www.mvcr.cz/soubor/priloha-c-2-podpurny-material-nukib-pdf.aspx

[11]POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie*. 2015, roč. 6, č. 11, s. 95. ISSN 1805-2797.

[12]POLČÁK, Radim. Kybernetická bezpečnost. In: POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, 656 s. ISBN 978-80-7598-046-5.

[13]POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. Brno: Masarykova univerzita, 2016, 240 s. ISBN 978-80-210-8426-1.

[14]Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 6. 11. 2019, sp. zn. S0262/2019/VZ. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16400.html

[15]Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html

[16]SANTORA, Marc; GOEIJ, Hana de. Huawei Was a Czech Favorite. Now? It's a National Security Threat. *The New York Times* [online]. 2019 [vid. 24. 3. 2021]. ISSN 0362-4331. Získáno z: https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html

[17]SASKOVÁ, Vladěna. *Novela vyhlášky o VIS, varování NÚKIB a zadávání veřejných zakázek*. Národní úřad pro kybernetickou a informační bezpečnost [online] 3. 12. 2019 [vid. 1. 4. 2021]. Dostupné z: https://www.cimib.cz/novinka/125-pozvanka-na-konferenci-kbs-2019

[18]SASKOVÁ, Vladěna. *Varování před kybernetickou hrozbou podle § 12 ZKB*. Národní úřad pro kybernetickou a informační bezpečnost [online] 17. 5. 2019 [vid. 1. 4. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[19]ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti.* Národní úřad pro kybernetickou a informační bezpečnost [online přednáška]. [vid. 18. 3. 2021] Brno. 2021.

[20]VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz. *Beck-online* [online]. [vid. 25. 3. 2021]. Získáno z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge2f6mjygfpwi6q&groupIndex=0&rowIndex=0

---

https://doi.org/10.5817/RPT2021-1-3

PŘEHLED AKTUÁLNÍ JUDIKATURY I/2021

VOJTĚCH BARTOŠ, FRANTIŠEK KASL, JAKUB KLODWIG, IVANA KUDLÁČKOVÁ, PAVEL LOUTOCKÝ, JAKUB MÍŠEK, JAKUB VOSTOUPAL

1. PRÁVO DUŠEVNÍHO VLASTNICTVÍ

NÁROK NA JEDINOU SPRAVEDLIVOU ODMĚNU ZA SDĚLOVÁNÍ ZVUKOVÝCH ZÁZNAMŮ, JEŽ JSOU SOUČÁSTÍ AUDIOVIZUÁLNÍCH DĚL

Soud: Soudní dvůr Evropské unie
Věc: C-147/19 (Atresmedia)
Datum: 18. 11. 2020
Dostupnost: curia.europa.eu

Předmětem řízení o předběžné otázce byl spor mezi španělskou televizní společností Atresmedia a španělskými správci duševního vlastnictví výrobců zvukových záznamů a práva výkonných umělců ohledně platby jediné spravedlivé odměny za sdělování audiovizuálních děl, jejichž součástí jsou zvukové záznamy, na televizních kanálech společnosti Atresmedia.

Televizní společnost zakomponovala do vysílaných audiovizuálních děl zvukové záznamy, a tyto pak prostřednictvím svých kanálů sdělovala veřejnosti. Strany se přely o otázku, zda takto sdělovaný obsah lze považovat za zvukový záznam, a tedy zda za jeho užití náleží výkonným umělcům a výrobcům příslušného zvukového záznamu jediná spravedlivá odměna.

Jádrem sporu byl výklad čl. 8 odst. 2 směrnice 92/100/ES, resp. směrnice 2006/115/ES, na základě kterého mají členské státy zajistit zaplacení je-

diné spravedlivé odměny, pokud je užito zvukového záznamu vydaného k obchodním účelům nebo rozmnoženiny takového záznamu k bezdrátovému vysílání nebo jakémukoliv jinému sdělování veřejnosti. Článek 3 Úmluvy o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací (Římská úmluva) stanoví, že zvukovým záznamem je každý výlučně sluchem vnímatelný záznam zvuků uměleckého výkonu nebo jiných zvuků. Článek 2 písm. b) Smlouvy WIPO o právu autorském a Smlouvy WIPO o výkonech výkonných umělců a o zvukových záznamech (WPTT) definuje zvukový záznam jako záznam zvuků výkonu nebo jiných zvuků, anebo vyjádření zvuků, jiných než ve formě záznamu obsaženého ve filmovém nebo jiném audiovizuálním díle.

V rámci své analýzy Soudní dvůr konstatoval, že ač EU není signatářem Římské úmluvy, je při absenci definice pojmu „zvukový záznam" v unijním právu Soudní nutné přistoupit k jeho výkladu dle mezinárodního práva. To proto, že příslušné směrnice používající daný pojem mají „provést" příslušné mezinárodní právní instrumenty.[1] Tento účel posuzovaných ustanovení směrnic přitom Soudní dvůr vyčetl zejména z důvodové zprávy předcházející směrnici 92/100/ES.[2] Soudní dvůr také výslovně konstatoval, že Římská úmluva má v rámci unijního práva nepřímý účinek.[3] Soudní dvůr rovněž připomněl, že také dle WPTT nemůže být zvukový záznam začleněný do audiovizuálního záznamu považován za samostatný zvukový záznam pro účely odměny, pakliže výsledný audiovizuální záznam má status samostatného díla.[4] Na tomto závěru Soudního dvora nic nemění ani společné prohlášení přijaté diplomatickou konferencí k čl. 2 písm. b) WPTT, na základě kterého práva k zvukovému záznamu jeho začleněním do filmového nebo jiného audiovizuálního díla zůstávají nedotčena.[5] Soudní dvůr toto prohlášení chápe tak, že nedotčena zůstávají práva ke zvukovému záznamu

[1] Bod 34 anotovaného rozhodnutí.

[2] Bod 35 anotovaného rozhodnutí.

[3] Bod 36 anotovaného rozhodnutí.

[4] Bod 40 anotovaného rozhodnutí.

[5] Bod 42 anotovaného rozhodnutí.

samotnému, nikoliv však do té míry nakolik je součástí audiovizuálního díla.[6]

Z anotovaného rozhodnutí Soudního dvora tedy vyplývá zejména fakt, že audiovizuální nahrávku obsahující záznam audiovizuálního díla nelze kvalifikovat jako „zvukový záznam" nebo „rozmnoženinu takového záznamu" ve smyslu čl. 8 odst. 2 směrnice 92/100 nebo čl. 8 odst. 2 směrnice 2006/115, a tedy sdělování takové nahrávky veřejnosti nezakládá nárok na odměnu stanovenou v těchto ustanoveních.[7]

Autor: VB

NEPŘEZKOUMATELNÉ PROHLÁŠENÍ NEPLATNOSTI OCHRANNÉ ZNÁMKY CZECH POINT

Soud: Nejvyšší správní soud
Věc: 5 As 112/2018-53
Datum: 22. 1. 2021
Dostupnost: nssoud.cz

Předmětem sporu bylo rozhodnutí Úřadu průmyslového vlastnictví (dále jen „ÚPV") ze dne 7. 1. 2012, kterým byla na základě návrhu Ministerstva vnitra (dále jen „MV") prohlášena za neplatnou ochranná známka „CZECH POINT" jakožto spekulativní s ohledem na veřejnou známost projektu elektronizace státní správy a zřizování kontaktních míst s označením CZECH-POINT.[8] Ochranná známka byla zapsaná do rejstříku ochranných známek ve prospěch společnosti CZECH POINT 101 s.r.o. (dále jen „CP101") dne 16. 4. 2007 s právem přednosti ode dne 5. 4. 2006.[9]

Rozklad proti rozhodnutí byl v roce 2013 předsedou ÚPV zamítnut, následný rozsudek městského soudu z roku 2016 na základě správní žaloby CP101 byl Nejvyšším správním soudem (dále jen „NSS") roku 2017 zrušen

[6] Bod 44 anotovaného rozhodnutí.

[7] Bod 52 – 53 anotovaného rozhodnutí.

[8] Body 2-3 anotovaného rozhodnutí.

[9] Bod 1 anotovaného rozhodnutí.

pro nepřezkoumatelnost.[10] Městský soud v Praze následně v roce 2018 ve věci znovu rozhodl ve prospěch CP101 a vyhodnotil zamítavé rozhodnutí předsedy ÚPV o rozkladu jako „*nepřezkoumatelné, neboť většina jeho závěrů jsou pouhé spekulace*“.[11] Proti tomuto rozsudku podali ÚPV i MV kasační stížnosti, kterými se NSS zabýval v anotovaném rozhodnutí.

Stěžovatelé se kasačními stížnostmi domáhali zrušení rozsudku městského soudu pro jeho nesprávnost a neodůvodněnost a vrácení věci k dalšímu řízení.[12] CP101 označila rozsudek za souladný se závazným názorem předcházejícího rozhodnutí NSS a navrhla zamítnutí kasačních stížností pro nepřípustnost.[13] NSS nejprve dovodil, že na rozhodnutí NSS o nepřezkoumatelnosti nelze vztáhnout judikaturu NSS[14] omezující přípustnost opakované kasační stížnosti, následně pak obě kasační stížnosti shledal za nedůvodné a zamítl je.[15]

NSS předně zdůraznil, že pro posouzení dobré či zlé víry přihlašovatele ochranné známky nelze přikládat vliv okolnostem po okamžiku podání přihlášky.[16] To přitom ÚPV při svém hodnocení do značné míry činí.[17] Dále soud zdůraznil potřebu vycházet z presumpce dobré víry přihlašovatele, jednat při posuzování nestranně a přihlížet ke všem relevantním okolnostem případu.[18] V jednání před městským soudem přitom byla na základě výpovědi svědků zpochybněna klíčová skutečnost, a to známost spojení projektu elektronizace státní správy s pojmem CZECHPOINT širší veřejnosti v okamžiku podání přihlášky.[19] NSS nadto přímo konstatoval, že skutkový stav zjištěný ÚPV „*je v rozporu s obsahem spisu a provedenými dů-*

[10] Bod 4 anotovaného rozhodnutí.

[11] Bod 5 anotovaného rozhodnutí.

[12] Body 19 a 27 anotovaného rozhodnutí.

[13] Body 36 a 37 anotovaného rozhodnutí.

[14] Např. rozsudek NSS ze dne 10.6.2008, č.j. 2 Afs 26/2008-119.

[15] Body 38 a 39 anotovaného rozhodnutí.

[16] Bod 41 anotovaného rozhodnutí, s odkazem na rozsudky NSS ze dne 23.4.2010, č.j. 5 As 17/2009-152 a ze dne 22.5.2014, č.j. 7 As 151/2012-64.

[17] Srov. body 53-54 a 69-71 anotovaného rozhodnutí.

[18] Bod 44 anotovaného rozhodnutí.

[19] Bod 47 anotovaného rozhodnutí.

kazy“, hodnocení důkazů je do značné míry jednostranné[20] a skutková zjištění z provedených důkazů *„jsou buď „překroucená“, anebo v nich dokonce nemají žádnou oporu a následné skutkové závěry jsou tak pouhými nepodloženými spekulacemi.*“[21] Nedostatek odůvodnění správního aktu přitom nemůže být dodatečně zhojen ani v následném soudním řízení, ani analýzou v kasační stížnosti.[22]

V dalším řízení je na místě důsledně vyhodnotit, co bylo v rozhodném okamžiku skutečně známo veřejnosti a zda právo svědčilo MV, přičemž „*na nedobrou víru nelze automaticky usuzovat jen ze skutečností, které nastaly po podání přihlášky*“ a CP101 nelze klást k tíži, že vůči MV uplatňovala svá tvrzená práva.[23]

Autor: FK

JE ZPŘÍSTUPŇOVÁNÍ CHRÁNĚNÝCH DĚL PROSTŘEDNICTVÍM FRAMINGU SDĚLOVÁNÍM VEŘEJNOSTI?

Soud: Soudní dvůr Evropské unie
Věc: C-392/19 (VG Bild-Kunst)
Datum: 9. 3. 2021
Dostupnost: curia.europa.eu

Stiffung Preußischer Kulturbesitz, německá nadace kulturního dědictví je provozovatelem digitální knihovny spojující německé kulturní a vědecké instituce. Internetové stránky této knihovny obsahují odkazy ve formě náhledů (Thumbnails) na digitalizovaný obsah zúčastněných institucí, přičemž při kliknutí na náhled je uživatel ihned přesměrován na stránky relevantní organizace.[24] Organizace VG Bild-Kunst, kolektivní správce autorských práv v oblasti vizuálních umění, obecně podmiňuje uzavírání licenčních smluv implementací technologických prostředků proti framingu náhledů chráně-

[20] Blíže viz body 76-77 anotovaného rozhodnutí.

[21] Bod 51, dále pak konkrétněji body 55-68 anotovaného rozhodnutí.

[22] Body 72 a 75 anotovaného rozhodnutí.

[23] Bod 80 anotovaného rozhodnutí.

[24] Viz bod 10 anotovaného rozhodnutí.

ných děl.[25] Toto bylo ze strany nadace SPK považováno za nepřiměřenou podmínku a na VG Bild-Kunst podala žalobu.[26]

Zemský soud v Berlíně tuto žalobu zamítl, což záhy zrušil vrchní zemský soud. Kolektivní správce práv se nyní domáhá prostřednictvím opravného prostředku zamítnutí žaloby u Spolkového soudního dvora. Ten zdůraznil, že organizace kolektivní správy má dle německého práva[27] obecně povinnost poskytnout licenci každé osobě, která o to požádá, za přiměřených podmínek.[28] Výsledek řízení závisí na tom, zda framing představuje nové sdělování díla veřejnosti, neboť v takovém případě by VG Bild-Kunst mohla oprávněně podmiňovat udělení licence implementací technologických protiopatření.[29]

S ohledem na judikaturu Soudního dvora Evropské unie týkající se framingu[30] a svobody projevu v digitálním kontextu,[31] položil Spolkový soudní dvůr předběžnou otázku, zda zveřejnění chráněných děl prostřednictvím framingu lze klasifikovat jako nové sdělování díla veřejnosti.[32]

Právo kontroly autorů (ať už souhlas, omezení či zákaz) nad jakýmkoliv sdělením jejich děl veřejnosti skrze jakékoliv prostředky zakotvuje prostřednictvím povinnosti členských států takové právo autorům přiznat první odstavec článku 3 směrnice 2001/29/ES.

Soudní dvůr připomněl, že sdělování děl veřejnosti je z důvodu vyšší ochrany autorů nutné vykládat extenzivně,[33] i zveřejňování prostřednictvím náhledů tak představuje sdělení veřejnosti, které podléhá nutnému svolení

[25] Viz bod 11 anotovaného rozhodnutí.

[26] Viz bod 12 anotovaného rozhodnutí.

[27] Které provádí unijní směrnici 2014/26, o kolektivní správě autorského práva a práv s ním souvisejících a udělování licencí pro více území k právům k užití hudebních děl online na vnitřním trhu.

[28] Od tohoto se může odchýlit, pokud se tím nezneužije monopol a existuje legitimní cíl takového odchýlení (např. zájmy dotyčných osob). Viz body 12-15 anotovaného rozhodnutí.

[29] Viz body 14-17 anotovaného rozhodnutí.

[30] Usnesení ze dne 21. října 2014, BestWater International, C-348/13, nezveřejněné, EU:C:2014:2315.

[31] Viz bod 45 rozsudku ze dne 8. září 2016, GS Media, C-160/15, EU:C:2016:644. Jedná se o judikaturu, ze které vyplývá, že hypertextové odkazy přispívají k řádnému fungování internetu, výměně názorů a informací.

[32] Viz bod 18 anotovaného rozhodnutí.

nositelů práv.[34] Metoda framingu představuje v souladu s judikaturou Soudního dvora sama o sobě sdělení veřejnosti,[35] otázkou bylo, zda se v tomto případě jedná o další sdělení, tedy prostřednictvím nové technologie či vůči nové veřejnosti, neboť takové sdělení by vyžadovalo nový souhlas.[36] V porovnání s jinými případy,[37] kdy autor nevyužil opatření k omezení přístupu a zveřejnění díla tak proběhlo v podstatě vůči celé „internetové" veřejnosti, zde vyžadoval nositel práv implementaci omezujících opatření[38] a tím souhlas fakticky cílil na specifickou veřejnost, uživatele na specifických stránkách. Nikoliv na širokou internetovou veřejnost, vůči které dochází ke zveřejnění prostřednictvím framingu.[39] Pokud by tedy odkaz (např. právě framing) umožňoval obejít opatření omezující přístup ke chráněným dílům, pak by přístup, který by vyžadoval dosah prvotního souhlasu nositelů práv i na tento případ, odepíral nositelům práv faktickou kontrolu nad chráněným dílem a zaváděl by vyčerpání práva na sdělování.[40]

Soudní dvůr tedy uzavřel, že vložení chráněných děl, která jsou zpřístupněna specifické veřejnosti na internetových stránkách se souhlasem autora, prostřednictvím techniky framingu na jiné internetové stránky a obejití prostředků ochrany proti framingu požadovaných autorem, představuje sdělování díla nové veřejnosti.

Autor: JV

---

[33] Viz rozsudek ze dne 19. prosince 2019, Nederlands Uitgeversverbond a Groep Algemene Uitgevers, C-263/18, EU:C:2019:1111, bod 49 a citovaná judikatura; a bod 26 anotovaného rozhodnutí.

[34] Viz body 20–23 anotovaného rozhodnutí.

[35] Viz body 33-35 anotovaného rozhodnutí a body 20, 22 a 23 rozsudku ze dne 13. února 2014, Svensson a další, C-466/12, EU:C:2014:76.

[36] Viz body 35-37 anotovaného rozhodnutí.

[37] Viz body 37-38 anotovaného rozhodnutí.

[38] Viz body 39-40 anotovaného rozhodnutí.

[39] Viz body 42-50 anotovaného rozhodnutí.

[40] Viz body 51-55 anotovaného rozhodnutí.

2. SOUKROMÍ A OSOBNÍ ÚDAJE

DATA RETENTION OBECNĚJI

Soud: Soudní dvůr Evropské unie
Věc: C-511/18 (La Quadrature du Net a další)
Datum: 6. 10. 2020
Dostupnost: curia.europa.eu

Anotované rozhodnutí věcně navazuje na předchozí rozhodovací praxi Soudního dvora, zejména pak rozhodnutí Tele2 Sverige (spojené věci C-203/15 a C-698/15). Dále precizuje podmínky, za kterých mohou členské státy zavést takovou právní úpravu, která zakládá povinnost provozovatelům elektronických komunikací uchovávat provozní a lokalizační údaje, a která dále umožňuje příslušným orgánům veřejné moci tyto údaje využívat. Soudní dvůr nyní rozhodoval ve třech spojených věcech, které se všechny v základu týkaly otázky, jak daleko sahá výjimka čl. 15 odst. 1 směrnice 2002/58/ES, která umožňuje uchovávání a další zpracování provozních a lokalizačních údajů za účely nezbytnými pro „*zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů.*“[41]

Soudní dvůr předně připomněl, že pro výklad ustanovení unijního práva je třeba krom jeho textu zohlednit i jeho kontext a účel právní úpravy,[42] přičemž cílem směrnice 2002/58 je zajištění dodržování práv zakotvených v čl. 7 a 8 Listiny základních práv EU. Soudní dvůr dále připomíná, že z provozních a lokalizačních údajů je možné odhalit celou řadu citlivých informací o soukromém životě člověka,[43] a že při vyhodnocování možnosti aplikace výjimky je nutné vzít v potaz i další základní práva garantovaná Listinou.[44] Soudní dvůr tak opětovně uvádí, že tuto výjimku není možné aplikovat pro vytvoření obecné, plošné a preventivní povinnosti uchovávat

[41] Čl. 15 odst. 1 směrnice 2002/58/ES.

[42] Bod 105 anotovaného rozhodnutí.

[43] Bod 117 anotovaného rozhodnutí.

[44] Body 122 a následující anotovaného rozhodnutí.

provozní a lokalizační údaje. Naopak, za účelem splnění požadavku proporcionality *„musí právní úprava stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a uložit minimální požadavky, tak aby osoby, o jejichž osobní údaje jde, měly dostatečné záruky umožňující účinně chránit tyto údaje před rizikem zneužití. Tato právní úprava musí být právně závazná ve vnitrostátním právu a musí zejména vymezit okolnosti a podmínky, za nichž může být přijato opatření týkající se zpracovávání takových údajů, čímž zaručí, že se zásah omezí na to, co je nezbytně nutné.*“[45] Soudní dvůr se dále specificky věnoval variantám uložených povinností, které jsou výjimkou uvedenou v čl. 15 odst. 1 umožněny. Jde o situace, které věcně spadají do rozsahu výjimky předmětného článku a zároveň jsou dodrženy záruky bránící zneužití dat a je limitován rozsah zpracovávaných údajů pouze na nezbytné a po nezbytně dlouhou dobu.[46] Zároveň vždy platí podmínka, že legislativní opatření jsou povolena, pokud tato opatření *„pomocí jasných a přesných pravidel zajišťují při uchovávání dotčených údajů dodržení souvisejících hmotněprávních a procesních podmínek a pokud subjekty údajů mají k dispozici účinné záruky proti riziku zneužití.*“[47]

V druhé otázce věnované čl. 15 odst. 1 směrnice 2002/58/ES pak Soudní dvůr konstatoval, že toto ustanovení nebrání národní právní úpravě, která zakládá povinnost poskytovatelů služeb elektronických komunikací provádět v reálném čase automatizovanou analýzu provozních a lokalizačních údajů, pokud existují takové záruky, které zajistí proporcionalitu a minimalizaci zásahu do chráněných práv.

Soudní dvůr v anotovaném rozhodnutí potvrdil argumentační linii, kterou bylo možné pozorovat již z minulých rozhodnutí zabývajících se čl. 15 odst. 1 směrnice 2002/58/ES a jasně nastavil limity možné národní úpravy data retention. V kontextu českého práva pak toto rozhodnutí může mít zajímavé dopady, protože ukazuje, že současná úprava je v rozporu s poža-

[45] Bod 132 anotovaného rozhodnutí.

[46] Bod 168 anotovaného rozhodnutí.

[47] Závěr prvního výroku anotovaného rozhodnutí.

davky směrnice a unijního práva, a to i přes závěry nálezu ÚS ve věci Data Retention III.[48]

Autor: JM

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ A DŮKAZNÍ BŘEMENO

Soud: Soudní dvůr Evropské unie
Věc: C-61/19 (Orange Romania SA)
Datum: 11. 11. 2020
Dostupnost: curia.europa.eu

Společnost Orange România SA uzavírala během března 2018 se svými zákazníky smlouvy o poskytování telekomunikačních služeb, v nichž bylo předzaškrtnuté políčko, jímž měli zákazníci souhlasit s uchováváním kopií jejich dokladů totožnosti. Odmítnutí přitom bylo dle interních prodejních instrukcí možné pouze pokud byl zákazníkem před podpisem smlouvy vyplněn speciální formulář.

Rumunský úřad pro ochranu osobních údajů uložil za tuto praxi svým rozhodnutím ze dne 28. 3. 2018 společnosti Orange România SA pokutu,[49] proti čemuž podala společnost Orange România SA žalobu k soudu prvního stupně v Bukurešti. Soud se následně obrátil na Soudní dvůr Evropské unie se dvěma předběžnými otázkami.

Předmětem předběžných otázek bylo, jaké podmínky musí být dle čl. 2 písm. h) Směrnice č. 95/46/ES[50] splněny, aby mohl být projev vůle zákazníka považován za výslovný a vědomý, případně také svobodný?[51]

Směrnice 95/46 v čl. 2 písm. h) stanoví, že souhlasem subjektu údajů se rozumí „*jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt*

[48] Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.

[49] Bod 21 anotovaného rozhodnutí.

[50] 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.

[51] Bod 27 anotovaného rozhodnutí.

údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování."

Soudní dvůr Evropské unie konstatoval, že projev vůle dle čl. 2 písm. h) Směrnice 95/46 musí být výslovný v tom smyslu, že se musí konkrétně týkat zpracování dotčených údajů a nelze jej vyvodit z projevu vůle mající jiný účel.[52] Pokud je tedy souhlas zachycen na písemném prohlášení týkajícím se také jiných skutečností, je nezbytné, aby byl souhlas se zpracováním osobních údajů udělen takovým způsobem, který je jasně odlišitelný od souhlasu s jinými skutečnostmi.[53] Subjekt údajů by měl být také srozumitelně informován o typu údajů, totožnosti správce, době trvání, metodě a účelu zpracování,[54] přičemž důkazní břemeno o výše uvedených skutečnostech tíží správce osobních údajů.[55] Povinnost doložit souhlas zákazníků tudíž nelze splnit prostřednictvím požadavku na aktivní odmítnutí zpracování.[56]

Okolnost, že uvedení zákazníci podepsali smlouvy obsahující zaškrtnuté políčko, sama o sobě neumožňuje prokázat takový souhlas, neexistují-li informace potvrzující, že toto ujednání bylo skutečně přečteno a pochopeno.[57]

Autor: JK

NESPLNĚNÍ POVINNOSTI IMPLEMENTOVAT POLICEJNÍ SMĚRNICI

Soud:	Soudní dvůr Evropské unie
Věc:	C-658/19 (Evropská komise proti Španělsku)
Datum:	25. 2. 2021
Dostupnost:	curia.europa.eu

[52] Bod 38 anotovaného rozhodnutí a také rozsudek Soudního dvora ze dne 1. října 2019, Planet49, C-673/17, EU:C:2019:801, bod 58.

[53] Bod 39 anotovaného rozhodnutí.

[54] Bod 40 anotovaného rozhodnutí.

[55] Bod 42 anotovaného rozhodnutí.

[56] Bod 51 anotovaného rozhodnutí.

[57] Bod 46 anotovaného rozhodnutí.

Směrnice 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů (dále jen „policejní směrnice“) měla být implementována členskými státy do 6. května 2018. Evropská komise ani po uplynutí lhůty stanovené předmětnou směrnicí neobdržela od Španělska informaci o přijetí opatření nezbytných pro dosažení souladu s požadavky policejní směrnice, podala tedy žalobu o určení nesplnění povinnosti. Španělsko nezpochybnilo nesplnění povinnosti,[58] mělo ovšem za to, že měl být při určení výše penále zohledněn fakt, že komunikace s Evropskou komisí probíhala časově blízko před rozpuštěním národního parlamentu a zahájením volebního procesu.[59] V této souvislosti Španělsko odkazovalo na povinnosti ctít národní identitu členských států dle čl. 4 odst. 2 SEU.[60]

Evropská komise za žalobou domáhala určení nesplnění povinnosti a uložení penále dle čl. 260 odst. 3 SFEU.

Dle čl. 63 policejní směrnice byly členské státy povinny do 6. května 2018 přijmout a zveřejnit právní a správní předpisy nezbytné pro dosažení souladu s danou směrnicí a sdělit Evropské komisi znění takovéto národní právní úpravy.

Soudní dvůr v této souvislosti uvedl, že povinnost sdělit opatření provádějící směrnici spočívá v povinnosti uvést jedno či více vnitrostátních ustanovení, které zajišťují provedení policejní směrnice.[61] Poté je povinností Evropské komise prokázat, že některá prováděcí opatření zjevně nebyla přijata vůbec nebo se nevztahují na celé území členského státu, zkoumání správnosti provedení policejní směrnice již Soudnímu dvorů nepřísluší.[62] Soudní dvůr měl na základě komunikace mezi Španělskem a Evropskou komisí za prokázané, že Španělsko opatření provádějící policejní směrnici nesdělilo.[63] V otázce výše penále Soudní dvůr uvedl, že se jedná o vhodný

[58] Srov. bod 13 anotovaného rozhodnutí.

[59] Srov. bod 25 anotovaného rozhodnutí.

[60] Srov. bod 26 anotovaného rozhodnutí.

[61] Srov. bod 30 anotovaného rozhodnutí.

[62] Tamtéž.

[63] Srov. bod 31 anotovaného rozhodnutí.

prostředek k zajištění toho, aby Španělsko co nejrychleji ustalo v neplnění povinnosti vyplývající ze směrnice 2016/680.[64] Vnitrostátní situace nemůže odůvodnit nedodržení povinností a lhůt vyplývajících z unijních směrnice, ani jejich opožděné nebo neúplné provedení.[65] Uložením paušální částky má být dosaženo účinnému předcházení obdobnému porušování práva v budoucnu.[66]

Soudní dvůr tedy dospěl k závěru, že Španělsko nepřijetím právních a správních předpisů nezbytných pro dosažení souladu s policejní směrnicí a nesdělení předmětných opatření Evropské komisi, porušilo povinnosti vyplývající z čl. 63 policejní směrnice. Soudní dvůr uložil povinnosti uhradit paušální částku ve výši 15 mil. euro, a pro případ přetrvávajícího neplnění povinnosti ke dni vyhlášení rozsudku též denní penále ve výši 89 tis. Euro.

Autor: IK

VYUŽITÍ ÚDAJŮ O ELEKTRONICKÉ KOMUNIKACI PRO VYŠETŘOVÁNÍ BĚŽNÉ KRIMINALITY

Soud: Soudní dvůr Evropské unie
Věc: C-746/18 (Prokuratuur)
Datum: 2. 3. 2021
Dostupnost: curia.europa.eu

Paní H. K. byla odsouzena estonským soudem prvního stupně ke dvěma letům odnětí svobody za krádeže věcí a peněz, zneužití platebního prostředku a násilné jednání vůči dalším osobám, přičemž celková způsobené škoda se pohybovala v řádu tisíců euro.[67]

K odsouzení došlo mimo jiné na základě několika protokolů vycházejících z údajů o elektronické komunikaci, které vyšetřovací orgán získal od poskytovatele služeb elektronických telekomunikací během přípravného

[64] Srov. bod 61 anotovaného rozhodnutí.

[65] Srov. bod. 77 anotovaného rozhodnutí.

[66] Srov. bod 84 anotovaného rozhodnutí.

[67] Bod 16 anotovaného rozhodnutí.

řízení poté, co mu příslušné státní zastupitelství udělilo za tímto účelem několik povolení.[68]

Předmětem předběžných otázek bylo posouzení, zda dle unijního práva, zejména dle ustanovení čl. 15 odst. 1 směrnice 2002/58/ES, ve spojení s články 7, 8 a 11 a s čl. 52 odst. 1 Listiny základních práv EU, představuje přístup k provozním a lokalizačním údajům natolik závažný zásah do dotčených základních práv, že tento přístup musí být omezen na boj proti závažné trestné činnosti.[69] Soudní dvůr navíc také posuzoval, zda je v případě, kdy přístup k údajům schválilo státní zastupitelství, splněna podmínka předchozího přezkumu přístupu k údajům ze strany soudu nebo nezávislého správního orgánu.[70]

Článek 15 odst. 1 shora uvedené směrnice umožňuje členským státům zasáhnout do soukromí elektronické komunikace jednotlivců v případě, kdy je to v demokratické společnosti nezbytné, vhodné a přiměřené pro (mimo jiné) prevenci, vyšetřování, odhalování a stíhání trestných činů. Takový zásah musí být nicméně v souladu se zásadami práva EU, a tedy zejména se standardy garantovanými LZPEU jak jsou vykládány soudním dvorem.

Soudní dvůr z velké části odkazuje na minulé rozhodnutí Velkého senátu v obdobné věci, kde uznal možnost plošného sběru a uchování údajů o elektronické komunikaci stejně jako možnost přístupu k těmto údajům ze strany orgánů veřejné moci.[71] Soudní dvůr nicméně zdůraznil princip proporcionality takového zásahu, a tedy že rozsah přístupu k údajům o elektronické komunikaci musí být přiměřený závažnosti stíhané trestné činnosti. V tomto ohledu bylo tedy konstatováno, že přístup orgánů veřejné moci k souboru provozních nebo lokalizačních údajů, z nichž mohou vyplynout informace o komunikaci uživatele prostředku elektronické komunikace nebo o umístění koncových zařízení, která používá, a z nichž lze vyvodit přesné závěry o soukromém životě subjektů údajů, mohou odůvodnit pouze

[68] Bod 17 anotovaného rozhodnutí.

[69] První a druhá předběžná otázka anotovaného rozhodnutí – body 27-45.

[70] Třetí předběžná otázka anotovaného rozhodnutí – body 46-59.

[71] Rozsudek Soudního dvora ze dne 6. října 2020, La Quadrature du Net a další, C-511/18, C-512/18 a C-520/18, EU:C:2020:791.

cíle spočívající v boji proti závažné trestné činnosti nebo předcházení závažnému ohrožení veřejné bezpečnosti.[72]

Pokud jde o otázku přístupu k předmětným údajům na základě rozhodnutí státního zastupitelství, Soudní dvůr konstatoval, že právo členského státu musí stanovit dostatečné procesní a hmotněprávní záruky proti zneužití této pravomoci.[73] Unijní právo tak zejména brání takové národní právní úpravě, jako je ta estonská, která umožňuje zpřístupnění dat i jiných osob než podezřelých ze spáchání závažného trestného činu, a to navíc na základě žádosti každého státního zástupce bez předepsané formy a předchozího přezkumu soudem nebo jiným nezávislým orgánem.[74]

Velký senát Soudního dvora tímto svým rozhodnutím navázal na svou předchozí judikaturu v oblasti data retention a stanovil další limity pro přístup orgánů členských států k údajům o elektronických komunikací svých obyvatel. Anotovaný rozsudek však rozhodně nemůže být vnímán jako zákaz využívání těchto dat pro účely trestních řízení obzvláště pak v případě závažné trestné činnosti.

Autor: VB

3. OSTATNÍ

IDENTIFIKACE A DATOVÉ SCHRÁNKY

Soud:	Nejvyšší soud
Věc:	27 Cdo 143/2020
Datum:	27. 10. 2020
Dostupnost:	nsoud.cz

Společenství vlastníků jednotek reprezentované předsedou výboru se domáhalo změny či výmazu některých údajů v rejstříku společenství vlastníků. První návrh změn byl doručen rejstříku osobně předsedou výboru. Rejstříkový soud na základě tohoto návrhu společenství vlastníků vyzval k doplnění některých podkladů či opravě některých údajů. Společenství nemělo

[72] Bod 35 anotovaného rozhodnutí.

[73] Body 48 a 49 anotovaného rozhodnutí.

[74] Body 49-54 anotovaného rozhodnutí.

zřízenou datovou schránku (pro společenství vlastníků není datová schránka zřizována ze zákona, ale případně na žádost). Společenství na základě požadavků soudu doručilo některé podklady "osobně", některé byly doručeny prostřednictvím datové schránky předsedy výboru, kterou ale zřídil jako fyzická osoba.

Právě tento způsob elektronického doručení nebyl rejstříkovým soudem akceptován, jelikož dle něj návrh nebyl podán předepsaným způsobem, tedy nebyl podepsán buď elektronickým podpisem, nebo nebyl zaslán prostřednictvím datové schránky osoby, která takový návrh činí (tedy z datové schránky společenství vlastníků jednotek),[75] kde by nastoupila fikce podpisu zmiňovaná mj. stanoviskem Nejvyššího soudu Plsn 1/2017, ze dne 5. 1. 2017. Hlavním argumentem nižších soudů, které se postupně případem zabývaly (a především Vrchního soudu v Olomouci) bylo s odkazem na předchozí rozhodovací praxi, že *„úkon učiněný jinou osobou prostřednictvím ‚cizí' datové schránky (např. podání fyzické osoby z datové schránky jejího zaměstnavatele) nemá právní účinky, které zákon jinak dokumentu doručenému prostřednictvím datové schránky přiznává.*"[76]

Proti tomuto rozhodnutí podalo společenství vlastníků dovolání k Nejvyššímu soudu, který jej shledal za přípustné.

Nejvyšší soud se tak zabýval zejména formalistickým přístupem nižších soudů a zvažoval, jestli příslušná datová schránka (zřízena pro fyzickou osobu) dostatečně identifikuje tuto osobu, která ale jedná v roli předsedy výboru. Postupně shrnul relevantní právní úpravu a zdůraznil, že fyzická osoba, oprávněná jednat jménem právnické osoby (tedy v daném případě předseda výboru) *„může jménem právnické osoby učinit elektronické podání* […] *i ze své datové schránky (z datové schránky fyzické osoby podle § 8 odst. 1 zákona o elektronických úkonech).*"[77] Je-li pak z podání zřejmé, že tato osoba jedná jménem právnické osoby, jde o podání právnické osoby. V tomto kontextu pak soud shrnul, že podání učiněné z datové schránky fyzické osoby, ze kterého je ale jasné, že tato osoba jedná za osobu

[75] Bod 7 anotovaného rozhodnutí.

[76] Bod 20 anotovaného rozhodnutí.

[77] Bod 37 anotovaného rozhodnutí.

právnickou (tedy že se jedná o předsedu jednajícího za společenství vlastníků) je nutno posuzovat za podání dostatečné a předchozí právní posouzení nižšími soudy za nesprávné.

Toto rozhodnutí je nutno považovat za další pozitivní krok směrem k opuštění od přepjatého formalismu, jelikož fakticky došlo k dostatečné identifikaci příslušné osoby a jen na tom základě, že bylo k podání využito „cizí" datové schránky, nelze takové podání formálně odmítnout.

Autor: PL

NEOPRÁVNĚNÝ PŘÍSTUP K FACEBOOK ÚČTU

Soud: Nejvyšší soud
Věc: 7 Tdo 1134/2020
Datum: 4. 11. 2020
Dostupnost: nsoud.cz

Obviněný se mezi lety 2009 a 2018 dopustil opakovaného a dlouhodobého týrání své družky. Krom hrubých slovních nadávek a fyzického násilí využil znalosti hesla k jejímu účtu na sociální síti Facebook, aby ji znemožnil přístup k tomuto účtu.[78]

Okresní soud v Českých Budějovicích dne 17. 12. 2019 shledal obviněného vinným z trestných činů týrání osoby žijící ve společném obydlí podle § 199 odst. 1, 2 písm. b), d) trestního zákoníku,[79] a neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1 TZ. Krajský soud v Českých Budějovicích následně odvolání obou stran zamítl jako nedůvodná.[80] Proti zamítavému usnesení podal obviněný dovolání k Nejvyššímu soudu.

Předmětem sporu bylo mimo jiné, zda obviněný svévolným přístupem do Účtu své družky prostřednictvím hesla, které znal již z původní registrace účtu, překonal bezpečnostní opatření k účtu dle § 230 TZ.

[78] Bod 2 anotovaného rozhodnutí.

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

[80] Bod 4 anotovaného rozhodnutí.

Předmětný trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ spáchá ten kdo *„překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části […]*“.

Nejvyšší soud konstatoval, že sociální síť Facebook nelze apriori považovat za soukromou ani veřejnou, ale vždy záleží na konkrétním nastavení míry soukromí účtu nebo konkrétního příspěvku jeho uživatelem.[81] Ačkoliv tedy obviněný kdysi družce založil Google-účet, skrze který se ke svému účtu na Facebook.com přihlašovala, nebylo dohodnuto, že by mohl obviněný k družčině účtu přistupovat.[82] Nejvyšší soud tedy seznal, že účet byl založený pouze pro družku a obviněný do něj vstoupil bez jejího vědomí. Jako překonání bezpečnostního opatření pak soud identifikoval již samotné využití znalosti hesla obviněným, přičemž za přiléhavé označil přirovnání účtu k obydlí, a bezpečnostního opatření ke klíči, který obviněný využil k neoprávněnému přístupu.[83]

Nejvyšší soud v předmětném rozhodnutí postavil na jisto, že jakýkoliv neoprávněný přístup do osobního účtu bez ohledu na způsob, jakým bylo heslo či jiné bezpečnostní opatření překonáno, je překonáním bezpečnostního opatření dle § 230 TZ. Dovolací nárok obviněného byl proto odmítnut jako zjevně neopodstatněný.

Autor: JK

SPOTŘEBITELSKÁ PRÁVA A NFC FUNKCE PLATEBNÍCH KARET

Soud:	Soudní dvůr Evropské unie
Věc:	C-287/19 (DenizBank)
Datum:	11. 11. 2020
Dostupnost:	curia.europa.eu

[81] Bod 38 anotovaného rozhodnutí.

[82] Bod 39 anotovaného rozhodnutí.

[83] Bod 40 anotovaného rozhodnutí.

Rakouská bankovní instituce DenizBank poskytuje možnost využívání bankovních karet vybavených NFC[84] pro bezkontaktní platby do 25 € bez nutnosti zadat PIN. V rámci obchodních podmínek souvisejících s užíváním takového způsobu platby bylo mj. uvedeno, že „*změny všeobecných obchodních podmínek týkajících se debetních karet jsou nabídnuty klientovi nejpozději dva měsíce před datem stanoveným pro jejich vstup v platnost a že se má za to, že klient tyto změny přijal, pokud je před tímto datem výslovně neodmítne*“, dále pak že bankovní instituce „*není povinna poskytnout doklad o tom, že platby malých částek provedené bez zadání osobního kódu […] byly autorizovány*“ a zároveň se zprošťuje „*odpovědnosti a veškerých povinností k náhradě v případě, že takovéto platební transakce nebyly autorizovány držitelem karty,*“[85]

Proti takto formulovaným obchodním podmínkám podalo žalobu u rakouského soudu sdružení, které je dle právní úpravy legitimováno k ochraně zájmů spotřebitelů. Rakouské soudy postupně shledaly daná ustanovení za problematická, rakouský Nejvyšší soud pro ověření některých nejasností souvisejících s užíváním takových platebních prostředků formuloval následující předběžné otázky v souvislosti s úpravou dle směrnice PSD2.[86]

Rakouský soud se dotázal, (i) jestli poskytovatel platebních služeb může jednostranně měnit podmínky rámcové smlouvy na základě souhlasu uděleného mlčky, (ii) jestli lze NFC posoudit jako platební nástroj, (iii) jestli se v případě použití NFC jedná o anonymní použití platebního prostředku a konečně (iv) jestli v případě NFC plateb bez zadání PIN nese poskytovatel ztrátu za provedené platby.

V rámci první (i) výše uvedené předběžné otázky Soudní dvůr zdůraznil, že je patrné, že fikce mlčky uděleného souhlasu se týká jen změn ob-

[84] Jedná se o technologii, která slouží k bezdrátové komunikaci mezi zařízeními, v konkrétním případě k bezkontaktním platbám.

[85] Nejedná se však o jediné relevantní ustanovení obchodních podmínek, více viz bod 33 anotovaného rozhodnutí.

[86] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES.

chodních podmínek, nikoli uzavření nové smlouvy.[87] Nadto rovněž zdůraznil, že dané ujednání „*musí splňovat požadavky dobré víry, vyváženosti a transparentnosti stanovené směrnicí 93/13.*“[88] V této otázce tak soud rozhodl, že směrnice PSD2 neomezuje takový charakter smluvních ujednání, která lze měnit mlčky, ale pokud je uživatelem platebních služeb spotřebitel, je nutno použít směrnici o nepřiměřených podmínkách ve spotřebitelských smlouvách.[89] V souvislosti s druhou (ii) otázkou pak soud uvedl, že NFC je vzhledem ke své specifičnosti právně oddělitelná od ostatních funkcí karty a může být posuzována jako samostatný platební prostředek.[90] To má za důsledek, že se široká míra ochrany na základě směrnice PSD2 vztahuje i na tento způsob plateb (a poskytuje tedy mj. vysoký standard ochrany spotřebitele).[91] V rámci třetí (iii) otázky anonymního použití platebního prostředku Soudní dvůr zdůraznil, že v daném případě se jedná o anonymní platbu, jelikož (např. v případě krádeže) je platební nástroj používán anonymně a poskytovatel tak není schopen prokázat, že platební transakce byla opravdu autorizována oprávněným držitelem karty (v situaci, kdy není zadáván PIN). A konečně v případě čtvrté (iv) položené otázky, která souvisí s odpovědností poskytovatele služeb za neoprávněnou platbu (a nesení související ztráty) soud zdůraznil, že se poskytovatel platebních služeb nemůže omezit jen „*na tvrzení, že dotyčný platební prostředek není možné zablokovat nebo zabránit jeho dalšímu použití, ačkoli s ohledem na objektivní stav dostupných technických poznatků nelze takovou nemožnost prokázat.*“[92]

Dané rozhodnutí tak alespoň částečně vyjasnilo, za jakých podmínek je možno měnit obchodní podmínky a dále v rámci související právní úpravy přistupovat k charakteru NFC plateb (zejména bez potřeby zadat PIN, kdy se jedná o anonymní platbu realizovanou specifickým platebním prostředkem). Soudní dvůr nicméně zdůraznil, že samotná bankovní institu-

[87] Bod 47 anotovaného rozhodnutí.

[88] Bod 65 anotovaného rozhodnutí.

[89] Směrnice Rady 93/13/EHS ze dne 5. dubna 1993 o nepřiměřených podmínkách ve spotřebitelských smlouvách.

[90] Bod 77 anotovaného rozhodnutí.

[91] Bod 78 anotovaného rozhodnutí.

[92] Bod 106 anotovaného rozhodnutí.

ce nese riziko ztráty za neoprávněnou platbu (pokud je například karta odcizena), pokud dostatečně neprokáže, že je v případě nahlášení schopna platební kartu adekvátně zablokovat (v okamžiku, kdy je tedy nahlášena ztráta karty, jsou další proběhlé platby *de facto* hrazeny samotnou bankovní institucí).

Autor: PL

PRÁVO NA INFORMACE O PLATECH A ODMĚNÁCH – HLÍDACÍ PES DEMOKRACIE

Soud: Nejvyšší správní soud
Věc: 5 As 440/2019
Datum: 5. 3. 2021
Dostupnost: nssoud.cz

Žalobce se žádostí doručenou Krajskému úřadu Ústeckého kraje dne 27. 10. 2014 domáhal s odkazem na zákon č. 106/1999 Sb., sdělení informací o platu a odměnách vedoucích jednotlivých odborů, poradců hejtmana, náměstků a radních Ústeckého kraje a ředitele uvedeného krajského úřadu, přičemž požadoval mimo jiné zdůvodnění případných mimořádných odměn.[93]

Této žádosti žalovaný krajský úřad opakovaně odmítl vyhovět, přičemž jeho rozhodnutí byla opakovaně rušena nadřízeným správním orgánem (celkem 12x).[94] Žalovaný i potřinácté odmítl informace vydat, přičemž vyjádřil nesouhlas s výkladem § 8b InfZ Nejvyššího správního soudu[95].[96] Toto rozhodnutí žalobce napadl u krajského soudu, což bylo soudem shledáno jako přípustný postup z důvodu procesní minulosti, žaloba však nebyla

[93] Viz bod 1 anotovaného rozhodnutí.

[94] Viz bod 2 anotovaného rozhodnutí.

[95] Viz rozsudek ze dne 27. 5. 2011, č.j. 5 As 57/2010–79. Zároveň žalovaný vyjádřil své přesvědčení, že žalobce zneužívá své právo na informace, neboť už jednou poskytnutou informaci zveřejnil ve svém článku.

[96] Viz body 3-5 anotovaného rozhodnutí.

shledána důvodnou, neboť nebyly podle krajského soudu naplněny podmínky stanovené judikaturou Ústavního soudu[97].[98]

Proti rozsudku krajského soudu podal žalobce kasační stížnost, která se týkala výkladu § 8b zákona č. 106/1999 Sb., a aplikace rozsudku ESLP ve věci *Magyar Helsinki Bizottság* a nálezu ÚS ze dne 17.10. 2017, sp. Zn. IV. ÚS 1378/16.

Ustanovení § 8b zákona č. 106/1999 Sb. zavazuje povinné subjekty poskytnout informace o příjemcích veřejných prostředků, přičemž podmínky v případě informací o platu a odměnách zaměstnance specifikoval ÚS ve zmíněném nálezu.[99]

NSS upozornil, že jak ESLP, tak ÚS potvrdily, že právo na informace není právem absolutním, je tedy nutné vždy posoudit zvláště to, zda je uplatňováno ve veřejném zájmu či jako součást svobody projevu[100] a jak moc zasahuje do dalších práv.[101] NSS ovšem konstatoval, že krajský soud provedl tento test proporcionality chybně a v rozporu se závěry ÚS.[102] Test pak provedl sám, přičemž upozornil na klíčová pochybení krajského soudu. Za prvé kontrola, zda se státní orgány řídí judikaturou správních soudů, je bez pochyb věcí veřejného zájmu.[103] Dále pak není možné v celém procesu vycházet toliko z informací v samotné žádosti, ale i z informací, které žadatel uvede v rámci navazujících řízení, žalovanému tak muselo být mi-

[97] Viz nálezy Ústavního soudu ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16, a ze dne 3. 4. 2018, sp. zn. IV. ÚS 1200/16. Žalobce deklaroval zájem zjistit ochotu státních orgánů respektovat judikaturu NSS, nikoliv přispění k veřejné debatě či dozoru veřejnosti, což mu bylo krajským soudem vytknuto. Zmíněná kritéria však ÚS formuloval až tři roky po podání žalobcovy žádosti.

[98] Viz body 6-8 anotovaného rozhodnutí.

[99] Jedná se o a) účelem vyžádání informace je přispět k diskusi o věcech veřejného zájmu; b) informace sama se týká veřejného zájmu; c) žadatel vystupuje v roli tzv. „společenského hlídacího psa“, a d) informace existuje a je dostupná.

[100] Mimo jiné poukázal na podobnost s rozsudkem ze dne 29. 9. 2020, č. j. 4 As 91/2020–45. Viz body 28-30 anotovaného rozhodnutí.

[101] Viz bod 29 anotovaného rozhodnutí.

[102] Viz body 31-33 anotovaného rozhodnutí. Mimo jiné podotýká, že *„žalovaný si přitom v testu proporcionality odporuje, když na jedné straně vychází z premisy, že cílem žádosti stěžovatele je kontrola poskytování finančního plnění žalovaným, na druhé straně konstatuje, že tomu tak ve skutečnosti není.“*

[103] Viz bod 37 anotovaného rozhodnutí.

nimálně při druhém řízení o poskytnutí informací již jasné, že žalobce je novinář a tudíž „hlídací pes demokracie“.[104] A nakonec – kdyby se relevantní zaměstnanci vůbec nepodíleli na výkonu veřejné moci, veřejný zájem na vydání takové informace by zde nebyl, v tomto případě se však podílejí značně.[105]

NSS tak konstatoval důvodnost kasační stížnosti a zrušil napadený rozsudek krajského soudu i původní správní rozhodnutí, přičemž žalovaného zavázal vysloveným právním názorem. Nejvyšší správní soud nad rámec podané kasační stížnosti otevřeně konstatoval pohoršení a nelibost nad jednáním žalovaného, kdy opakovaně a záměrně postupoval v rozporu s (v dané době) ustálenou a nezpochybněnou judikaturou NSS, přestože byla později korigována ze strany ÚS, i v rozporu s názory odvolacího správního orgánu. Dále vytkl zcela otevřeně obstrukční jednání a zvůli žalovaného jakožto i naprosto flagrantní případ podjatosti úřední osoby.[106]

Autor: JV

[104] Viz body 30 a 35 anotovaného rozhodnutí.

[105] Viz bod 36 anotovaného rozhodnutí.

[106] Osoby, o jejichž platech se rozhodovalo, vydávaly rozhodnutí o odmítnutí poskytnutí informací. Viz body 22-23 anotovaného rozhodnutí.

ESSAYS I/2021

OBSAH SEKCE

STATE SURVEILLANCE AS THE NEW SOCIETAL NORM[1]

TEMIRLAN BEKTURGANOV[2]

1. INTRODUCTION

Privacy is an abstract term and each individual defines it in their own way, but no one can argue that privacy is not important. Surveillance has substantially developed and there are numerous conducive factors to its development. The pursuit of national security has become an acute topic and all countries joined the war on terror, however nobody raises concerns regarding its costs. We truly rely on new technologies and the matter of whether

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Surveillance. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Surveillance.

[2] Temirlan Bekturganov je studentem Fakulty sociálních studií Masarykovy univerzity, kontakt: 491700@mail.muni.cz

we are a surveillance society or not is nonsense because the answer is obvious - we are. Though, how does it affect the very idea of western values and liberal democracy? At what costs, what benefits does this notion bring about? How advanced are our technologies and how accurate are they in regards to security? These and other questions, I am aiming to examine in this paper by analyzing empirical data and inclusion of a philosophical dimension as well.

2. SUBJECTIVE OR OBJECTIVE SURVEILLANCE?

One of the phenomenal Greek philosophers, Aristotle, once said: humans are social animals and society is something that precedes the individual. Hence, I believe, we as individuals living in a society are constantly sharing and exchanging emotions, ideas, beliefs and values, and the main source of our emotions is coming from communications and observations on which we further develop assumptions. Society is complex and throughout the time, created complexity is substantially evolving further more. To solve problems, we increase complexity exaggerating the solution even more [3]. To elaborate on the complex society, firstly, I would like to use Gary Marx's analysis of the development of the 'new surveillance', as the solid ground of my argument, where he presents the development of surveillance in its context. Conceptualization is rooted in the religious surveillance that produced activities such as the policing of religious consciousness and created the basis for the division of 'us' and 'them', what is 'normal' and what is not. Later on, in the sixteenth and seventeenth centuries, the development was seen in terms of politics which introduced the notion - 'policed' society through observation and detection, increase in bureaucracy where data collection had become the new norm.[4] It is not my intention to dwell on the matter of the development of surveillance, but I would rather use an ex-

[3] Temis G. Taylor and Joseph A. Tainter are using an example of societal complexity by analyzing scarcity and the energy of fossil fuels, however, their explanation of the modern society, I believe, is applicable and universal to any examined topic which is related to the human activity TAYLOR, Temis G. a Joseph A. TAINTER, 2016. The Nexus of Population, Energy, Innovation, and Complexity. *American Journal of Economics and Sociology*. 75(4), pp. 1005–1043.

ample of the modern police which can be legitimately considered as an outcome of surveillance. Many scholars confidently state that humans are rational beings, though taking the example of police brutality in the U.S., I would argue that there is no such a thing as absolute rationality in human nature. The recent cases with Breona Taylor and George Floyd have only proved the fact that humans are irrational and our actions are driven by subjectivity presented in a form of assumptions. In an example noted above, the police officers' actions had led to such sorrowful outcomes just because they perceived their intentions in their own way, one may say that their actions were based on a justified belief, but all beliefs are precisely subjective. Yet, we still rely on the idea of rationalism and give up our protection and security to authorities who are responsible for the national and individual security by accepting the fact of state surveillance and justifying it with the idea of public interest.

3. NATIONAL SECURITY AND TERRORISM

To justify surveillance, mass media and high authorities choose to manipulate our perception of security by presenting a big impactful risk for the public, therefore they present surveillance as a tool to fight the beast for the sake of national security. What impresses me is that only a few raise questions concerning the security of an individual, yet I noticed a thought-provoking pattern of the way many perceive security by taking it as relational and drawing a correlation between national and individual security and claiming that one determines the other, though, I would argue that it is not always the case.

Indeed, surveillance is presented as a tool to solve national security issues and as we may notice, no one speaks about individual security in the framework of surveillance. The idea of national security seems tempting for the society, however, the question of costs remains neglected. To add clarity in this matter, let us look at the example of China, in particular, Xinji-

[4] MARX, Gary T., 2004. What's new about the "new surveillance"?: Classifying for change and continuity. *Knowledge, Technology & Policy* [online]. 17(1), pp. 18–37. ISSN 1874-6314. Available at: doi:10.1007/BF02687074.

ang region. One cannot deny that there is a big wave of suppression against Uighur minorities in the region and this topic is always being ignored by the international society because it concerns Chinese national security. Women's mass sterilization[5] is justifiable in a sense of national security, because it is easier to control low population insofar small number population does not entail risks for the Chinese integrity and core values (i.e. rise of nationalism and separatism). Doubtless, it is a breach of bodily privacy, violation of human rights, and is morally and ethically wrong. Hence, the argument that national security determines an individual's well-being is inappropriate and misleading.

One may argue that what if there are no violations in the privacy context exercised by the government on both individual and national levels and what if there is an actual threat of terrorist attack, how shall we expect the government not intervene into one's privacy? To answer this question, I will use Yuval Noah Harari's article on Terrorism from his book "21 lessons for the 21st century" where he claims that terrorism is no longer a major threat, but rather is a tool of mind control. Indeed, the public remembers 9/11 events as the attack on the World Trade Center, but neglects to mention the Pentagon attack because visually it is not as memorable as the former example which again proves the fact that we are of irrational nature and tend to remember events and things related to emotions caused by visually catchy images.[6] To elaborate on it and develop further analysis, I want to draw on the concept of perceived risks. Once again, as discussed in the previous section, human nature is unpredictable and we tend to make assumptions and judgements subjectively, therefore, perception of risks is not an exception. In business marketing, this concept represents uncertainty that customers encounter when purchasing goods, however, I am convinced that it is a universal pattern that also influences human's understanding and decision-making, where applying it to the perception of ter-

[5]China: Uighur women reportedly sterilized in attempt to suppress population, In: *Deutsche Welle* [online] *01.07.2020* [cit. 2021-05-26].Available at: https://www.dw.com/en/china-uighur-women-reportedly-sterilized-in-attempt-to-suppress-population/a-54018051.

[6] HARARI, Yuval Noah, 2018. *21 Lessons for the 21st Century*. 1st Edition. New York: Random House. ISBN 978-0-525-51217-2.

rorism, terrorists manipulate uncertainty that authoritive decision-makers and individuals face in a way that the issue appears to be more dangerous and serious. In point of fact, when China experienced the first wave of coronavirus back in 2019, the world remained silent because the actual risk of pandemics was never a topic and therefore no authority had come up with deliberate policies to prevent the spread of the virus, unlike, the obsessed by western powers, War on Terror which had an impact on the development of thorough representation of security, but took too much attention that in the end we ended up with weak policies towards other global threats and led to the disregard of the very idea of liberal individualism with the core values of individual rights and freedoms.

4. STATE SURVEILLANCE WITH NO PLACE FOR DEMOCRACY

The notion of censorship is something inappropriate and unacceptable in the 21st century in most parts of the world and is not especially admissible in the western liberal idea of democracy. It is my contention that in the world of human rights where the right for self-determination, freedom of speech and expression, mass surveillance and extra-policing in a form of a state surveillance are acute and not conducive driving forces of the democratic society, and it rather brings about the threat of the very idea of western liberalism because its core values are being disregarded. Collecting data and information beforehand of a crime carries out the so-called chilling effect which later on invokes self-censorship and chills behaviour of individuals and functioning of the whole society. I recall my mother's stories from the times she lived in the Soviet Union, where everyone was terrified and cautious of the outcomes of one's actions, in particular, it violated Article 19 of the Universal Declaration of Human Rights - freedom of speech and expression.[7] People were truly afraid of sharing their opinions with one another which led to distrust of your neighbours, friends and local communities because people knew they were being watched and it entailed social di-

[7] Universal Declaration of Human Rights. *United Nations* [online]. United Nations [cit. 2021-05-26]. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

vision and eventually social polarization. The character of the state surveillance with advanced technologies embodies a greater scale of chilling effect, though one may argue that this effect is mainly invoked when we are certain on the fact of being surveilled, but the central problem is the uncertainty we as individuals encounter. Since we live in a Post-Snowden world, we are no longer fooled about the fact of hidden surveillance and this raises questions of transparency that democratic institutions must uphold and maintain, although, unfortunately, the reality has proven the contrary. One must admit that nowadays developments in surveillance have shifted the roles of a suspect and the government where now a subject has to prove one's innocence and not the government which is supposed to protect its citizens fairly and equally proving one's guilt. Thus, another problem concerning western values arises from here. Surveillance, specifically mass surveillance, serves as an instrument to monitor a group of individuals within which there might be a suspected subject, however, that is absolutely unconstitutional because it does not cover a certain suspect, but a group of innocent people and this regards privacy matters, as we discussed the chilling effect and self-censorship matters previously. Ideally, in a truly democratic country with the high value of rule of law, which is the U.S. in fact is, in order to find a suspect or even a guilty person, the authorities must have an issued warrant for an investigation and surveillance which is a part of an investigation, but as Edward Snowden revealed,[8] the National Security Agency warrantlessly had allowed the search for individual's personal information, data, track of communication and the usage of other surveillance tools. That was an unprecedentedly unlawful incident and an act of disrespect towards American citizens who were not aware of an ongoing surveillance program and deriving from the past experience our questioning of government's transparency has become an acute topic and the whole idea of government which used to have an obligation to uphold an order has shifted and now we encounter the reality where individuals have no

[8] BALL, James, ACKERMAN, Spencer., NSA loophole allows warrantless search for US citizens' emails and phone calls. In: *the Guardian* [online] 09.08.2013 [cit. 2021-05-26]. Available at: http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls

longer got anything to hide, though the government's activity is vice versa hidden by all 'democratic' institutions and their representatives. Hence, I believe, people have all rights to demand transparency because this is a point where democratic-backsliding might occur if all the public has yet to awake for the sake of their own privacy.

5. DEVELOPING OR DEVELOPED TECHNOLOGIES?

As I already touched upon the topics of the society, complexity created and subjectivity, I must mention they all are obviously related to humans. Though, equally relevant to the issue are the questions of surveillance technology development. It is no secret that humans are now being replaced by algorithms, patterns and artificial intelligence mechanisms because this is the complexity we have created in order to ease our lives, however, I believe that nowadays technologies are not sufficiently advanced to feel reliance on. Roger Clarke draws the line between data and information where data is a component of which information consists and I would like to illustrate this point in a form of variables to elaborate further on it.[9] Data is an independent variable where information is dependent, hence data can be manipulated and interpreted in numerous ways and Clarke introduces at this point the notion of digital persona and its negative impact on the outcome where in an investigation all decisions and actions are being made on an inaccurate representation of a subject. This is not only the case of policing wrong suspects, but it also covers other social dimensions, to be precise, the matter of racism which only escalates already existing systemic discrimination. Facial recognition has proved to be imprecise when it comes to identifying people of colour which may lead to policing wrong suspects and as a result to detention while the actual criminal is free and is capable of committing a more serious crime.[10] In a sense of systemic racism, if these technologies are allowed for police use, it is by no doubt a systemic discrimination of minorities and again challenges the whole idea

[9] CLARKE, Roger. Introduction to Dataveillance and Information Privacy. In: *Roger Clarke's Web-Site* [online] [cit. 26.05.2021]. Available at: http://www.rogerclarke.com/DV/Intro.html

of western liberalism. In addition to that, reliance on algorithms and artificial intelligence is fraught with consequences that are not reasonable. As discussed in the first section, we all have a tendency to make only subjective assumptions and subjectivity also means that we question the other side of the coin whenever we have more information on a certain case, that is to say, if an investigation being led by a human, the more information an investigator has, the more questions appear consequently whereas if an investigation relied on technology and it allowed one systemic error, it will entail a negative result and may change or mislead the whole character of an investigation.

6. CONCLUSION

Having examined the idea of state surveillance, privacy concerns, advantages and disadvantages of the so-called advanced technologies and its relation to the usage of such aspects by irrational human beings, I arrived at the conclusion that the state surveillance has its up and down sides, at the beginning it had facilitated the war on terror and strengthened national security, though such pursuit has led to undermining the individual dimension of security. But human nature is unpredictable and as we have seen the shift of state surveillance becoming a new norm violating the very idea of liberalism which has its feature to chill societies and their ability to function properly. Mass surveillance has proved its efficiency and yet again, we have created complexity in which the solution of a problem emerges only after making it even more complex. The central issue is that there are no alternatives to surveillance with its all external obstacles and disadvantages, hence in order to come up with the alternative solution to it, we must not only change and develop new institutions controlling surveillance, but promote a new approach and novelties such as the creation of a whole new governing system, but so far, unfortunately, all we can do is only protect

[10] HARVELL, Drew. Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. In: *Washington Post* [online]. [cit. 2021-05-26]. ISSN 0190-8286. Available at: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

our privacy and speak up to stimulate massive awareness of the current issue and only when the entire society is awakened, we must seek for a deliberate solution in this regard.

7. BIBLIOGRAPHY

[1] TAYLOR, Temis G. a Joseph A. TAINTER, 2016. The Nexus of Population, Energy, Innovation, and Complexity. *American Journal of Economics and Sociology*. 75(4), 1005–1043. Available at: https://ideas.repec.org/a/bla/ajecsc/v75y2016i4p1005-1043.html

[2] MARX, Gary T., 2004. What's new about the "new surveillance"?: Classifying for change and continuity. *Knowledge, Technology & Policy* [online]. 17(1), 18–37. ISSN 1874-6314. Available at: doi:10.1007/BF02687074

[3] China: Uighur women reportedly sterilized in attempt to suppress population, In: *Deutsche Welle* [online] *01.07.2020* [cit. 2021-05-26].Available at: https://www.dw.com/en/china-uighur-women-reportedly-sterilized-in-attempt-to-suppress-population/a-54018051.

[4] HARARI, Yuval Noah, 2018. *21 Lessons for the 21st Century*. 1st Edition. New York: Random House. ISBN 978-0-525-51217-2.

[5] UNITED NATIONS. Universal Declaration of Human Rights. *United Nations* [online]. United Nations [cit. 2021-05-26]. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[6] BALL, James, ACKERMAN, Spencer., *NSA loophole allows warrantless search for US citizens' emails and phone calls*. In: *the Guardian* [online] 09.08.2013 [cit. 2021-05-26]. Available at: http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls

[7] CLARKE, Roger. *Introduction to Dataveillance and Information Privacy*. In: *Roger Clarke's Web-Site* [online] [cit. 26.05.2021]. Available at: http://www.rogerclarke.com/DV/Intro.html

[8] HARVELL, Drew. *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use.* In: *Washington Post* [online]. [cit. 2021-05-26]. ISSN 0190-8286. Available at: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

DO YOUTUBERS HAVE A RIGHT TO PRIVACY?[1]

ONDŘEJ BOŽÍK[2]

1. INTRODUCTION

Access and also approach to a person's privacy have changed noticeably recently, and one of the most affected groups of people by this trend are unarguably YouTubers. In this work, my goal is to give my opinion on the privacy of YouTubers and provide convincing information on which I based my opinion.

We should obviously not forget that being a YouTuber is a job like any other, and no one's not forced to do it in the sense of article 26 of the Charter of Fundamental Rights and Freedoms. Of course, with this job comes a certain risk - YouTubers are a more vulnerable group of people when it comes to their privacy, like actors, writers, musicians, or politicians (even though the question of public officials is more complicated in the sense that the public has the right to know about certain acts of official that contributes to public debate).[3] Privacy, as we already know, has a lot of aspects. In this case, I'm going to use Roger Clarke's division of privacy, which has 4 dimensions: privacy of the person, the privacy of personal behaviour, the privacy of personal communications, and the privacy of personal data.[4] In my opinion, the biggest interference is in the field of informational privacy, which covers both privacy of personal communications, the privacy of personal data and privacy of personal experience. Of course, it will depend on

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Free Speech and Media law. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Free Speech and Media law.

[2] Ondřej Božík je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 480493@mail.muni.cz.

[3] See Judgement of 24.6.2004 case n. 59320/00, von Hannover v. Germany, ECHR.

[4] CLARKE, Roger. Introduction to Dataveillance and Information Privacy. In: *Roger Clarke's Web-Site* [online] [cit. 30.10.2020]. Available at: http://www.rogerclarke.com/DV/Intro.html

which content the YouTuber is providing, but in general, YouTubers are more likely to share personal things with their viewers, than their address, to which restaurant they are going on a dinner with their spouse etc. As Karoliina Talvitie-Lamberg says in her dissertation work, key factors in the interaction between YouTubers (or vloggers in general) and their viewers are confessions (when the more intimate things you share, the more success you get (not always though)), self-disclosure, and honest self-representation.[5] This trend is based on the fact, that lately, they protect more bodily privacy (privacy of the person in Roger Clarke's division), than informational privacy. The goal for YouTubers is then to achieve an ideal border of (in)accessibility, as Slavík stated in his work.[6] That means, to control the amount and nature of the information that they share. People share tons of information with the outer world daily, and in a YouTubers' case, this phenomenon is even more perceptible. This is caused by the ubiquity of their content. Their job is based on a simple equation, in which the more views you get, the more money you make. Let's imagine a situation, in which you are a YouTuber and streamer with 5 million subscribers on YouTube and 1 million followers on Twitch. On the bright side, you get tons of money out of this, pleasant, not hard, job. But the dark side of this coin is, that this fame you got by sharing things with your viewers, they get more and more curious, and start intervening into the dimension of privacy, to which you don't want to let them go. These are more precisely fields of the intimate and personal zone (bodily privacy, spatial privacy, intellectual privacy, and decisional privacy in the division of Bert-Jaap Koops et. al.).[7] Shortly, the more people you let in your privacy, the bigger is the risk of someone abuses it. The risk is not only in the fact that your personal data are shared daily with thousands of people but also in the fact that the

[5] TALVITIE-LAMBERG, Karoliina. *Confessions in Social Media : Performative, Constrained, Authentic and Participatory Self-Representations in Vlogs, Dissertation thesis*. The University of Helsinki, Faculty of Social Sciences, Department of Social Studies, Communication. p. 8.

[6] SLAVÍK, Lukáš. *Význam soukromí pro mladé aktivní YouTubery a YouTuberky*. 2018, Masarykova univerzita, Fakulta sociálních studií. p. 25.

[7] KOOPS, Bert-Jaap et al. A Typology of Privacy. *University of Pennsylvania Journal of International Law*. 2017, vol. 38, n. 2.p. 2.

people watching are storing your digitized personal data, in all circumstances, all the time.

2. EXAMPLES

As the first example, I would show a video of PewDiePie, who has one of the biggest channels on YouTube, in which he asks his fans not to come to his house and invade his privacy (a right to be let alone, in this sense).[8] As the first deterrent example, there is a case of Mag Turney and Gavin Free, both YouTubers living in Austin, whose house was at night invaded by one of their fans, who was armed.[9] The fan was obsessed with Gavin Free and didn't want him to have children with Mag Turney. The fan was shot that night in a collision with police. That was a clear example of when the invasion of their privacy was out of control and certainly illegal. The second example has more to do with the mental health of the person making videos for millions of people. This is the case of Reckful, a well-known streamer and YouTuber of World of Warcraft and other games, who committed suicide this year. The reason why he committed suicide was long time depression, besides caused by the pressure from his supporters.[10] When I mentioned above that YouTubers are more vulnerable than any other group when it comes to privacy, I did not mean only their fame and huge fan base. The fact that they are YouTubers, spending hours and hours in front of the computer, is also an important fact. This type of people often has a reason, why the person likes being home, in his comfort zone, in front of the computer. This reason can be often based on depression, obsession, or other mental illnesses. That's also why I gave Reckful's example. This type

[8] Reportedly, the whole school classes were going on a trip to look at PewDiePie's house. Viz PERRY, Alex. *The biggest star on YouTube wants people to stop coming to his house* In: *Insider* [online] [cit. 22. 6. 2021]. Available at: https://www.businessinsider.com/pewdiepie-wants-people-to-stop-coming-to-his-house-2016-8

[9] KIRCHER, Madison Malone. *YouTube Couple Hides in Closet After Armed Fan Breaks Into House* In: *Newyork Intelligencer* [online] [cit. 30.10.2020]. Available at: https://nymag.com/intelligencer/2018/02/armed-fan-killed-after-breaking-into-youtube-couples-house.html.

[10] ELLIOT, K. Josh. *'RIP Byron': Pro 'Warcraft' gamer Reckful dies at age 31 - National* In: *Globalnews.ca.* [cit. 18.06.2021]. Available at: https://globalnews.ca/news/7134883/byron-reckful-bernstein-death-warcraft/.

of people is certainly even more vulnerable when it comes to their privacy. There is also a fitting article in the Economist about the mental health of gamers etc: *„And games become the destructive vice of choice for some sets of players, taking the place of drugs or alcohol in a tragic but familiar narrative. But the game is a symptom of some broader weakness, sometimes of character, occasionally of mental health – and, perhaps, of society too.“*[11] Even though he is not a YouTuber because he didn't choose it as his job, I would also like to shortly talk about the Star Wars Kid, whose story also slightly touches this issue. His video, which he never intended to publish, went viral in 2003. Later on, he started getting a lot of great responses, but sadly, also a lot of very bad ones. The responses were so harsh, that he had to seek help from a psychologist, and suffered from depression and bullying at his school. As an example, he was getting letters saying he should commit suicide etc.[12] He was one of the first victims of a new type of bullying called *cyberbullying*. This type of bullying is closely connected to the invasion of YouTubers privacy when in worse scenarios, the bullies go and search the YouTuber's address and harass them personally, and sadly, this phenomenon is even more popular among young YouTubers. We have a worldwide famous young YouTuber here, in the Czech Republic, called Misha, who even made a popular song about cyberbullying that he was object to.[13]

YouTubers are often active on all possible social networks. In that order, the next big risk is, that they can be victims of hackers. Hackers then can either steal some sensitive information or, more often, ask via some social network supporters of a YouTuber for money. That happened in July 2020, when hackers attacked the accounts of Bill Gates, Jeff Bezos and Elon Musk, and asked their followers for money with a promise, that when they

[11] AVENT, Ryan. Escape to another world In: *The Economist* [cit. 30.10.2020]. Available at: https://www.economist.com/1843/2017/02/27/escape-to-another-world.

[12] HAWKES, Rebecca. Whatever happened to Star Wars Kid? The sad but inspiring story behind one of the first victims of cyberbullying. In: *The Telegraph* [cit. 30.10.2020]. Available at: https://www.telegraph.co.uk/films/2016/05/04/whatever-happened-to-star-wars-kid-the-true-story-behind-one-of/.

[13] CYBERBULLY CHANNELS ARE CANCER!!! (Leafy, Pyrocynical, RiceGum, KeemStar, etc...) In: *YouTube* [cit. 18.06.2021]. Available at: https://www.youtube.com/watch?v=rV-ijcP6vDM&ab_channel=Misha%2FMishovysilenosti.

send money, they will get twice the amount from the businessmen. In the YouTube world, in the same month this year, the account of a famous Indian YouTuber CarryMinati was hacked, asking his viewers for bitcoins.

3. CONCLUSION

According to the examples I provided, Youtubers are definitely a very sensible group of celebrities, whose risk is even higher due to their impact on the digital world. Of course, we could argue that it is their job, that they have chosen, but nonetheless, it deserves the full protection of one's privacy than any other. In my opinion, the key is to control the border of (in)accessibility, which guarantees that viewers will be able to see and collect just that type of data, that a YouTuber wants to share, in order to keep the data they don't want to share out of their sight.

4. BIBLIOGRAPHY:

[1] AVENT, Ryan. Escape to another world. In: *The Economist* [online] [cit. 30. 10.2020]. ISSN: 0013-0613. Available at: https://www.economist.com/1843/2017/02/27/escape-to-another-world

[2] CLARKE, Roger. *Introduction to Dataveillance and Information Privacy*. In: *Roger Clarke's Web-Site* [online] 1997 [cit. 30.10.2020]. Available at: http://www.rogerclarke.com/DV/Intro.html

[3] ELLIOT, K. Josh. 'RIP Byron': Pro 'Warcraft' gamer Reckful dies at age 31 - National In: *Globalnews.ca.* [online] [cit. 30.10.2020]. ISSN: 1281-3508. Available at: https://globalnews.ca/news/7134883/byron-reckful-bernstein-death-warcraft/

[4] HAWKES, Rebecca. Whatever happened to Star Wars Kid? The sad but inspiring story behind one of the first victims of cyberbullying. In: *Telegraph.co.uk.* [cit. 18.06.2021]. Available at: https://www.telegraph.co.uk/films/2016/05/04/whatever-happened-to-star-wars-kid-the-true-story-behind-one-of/

[5] KIRCHER, Madison Malone. *YouTube Couple Hides in Closet After Armed Fan Breaks Into House* In: *NewYork Intelligencer* [online] [cit. 30.10.2020]. ISSN: 0160-2896. Available at: https://nymag.com/intelligencer 2018/02/armed-fan-killed-after-breaking-into-youtube-couples-house.html

[6] PERRY, Alex. *The biggest star on YouTube wants people to stop coming to his house* In: Insider [online] [cit. 22. 6. 2021]. ISSN 2225-2592. Available at: https://www.businessinsider.com/pewdiepie-wants-people-to-stop-coming-to-his-house-2016-8

[7] SLAVÍK, Lukáš. *Význam soukromí pro mladé aktivní YouTubery a YouTuberky*, bachelor thesis, Faculty of Social Studies, Masaryk University. [online]. 2018 [30. 10. 2020]. Available at: https://is.muni.cz/th/n55m5/ .

[8] TALVITIE-LAMBERG, Karoliina. *Confessions in Social Media: Performative, Constrained, Authentic and Participatory Self-Representations in Vlogs*. Dissertation thesis. 2014. The University of Helsinki, Faculty of Social Sciences, Department of Social Studies, Communication. [cit. 30.10.2020]. Available at: https://helda.helsinki.fi/handle/10138/44901

[9] CYBERBULLY CHANNELS ARE CANCER!!! (Leafy, Pyrocynical, RiceGum, KeemStar, etc...) - YouTube. In: *YouTube.com* [cit. 30.10.2020]. Available at: https://www.youtube.com/watch?v=rV-ijcP6vDM&ab_channel=Misha%2FMishovysilenosti

[10] Judgement of 24.6.2004 case n. 59320/00, von Hannover v. Germany, ECHR, CE:ECHR:2004:0624JUD005932000, Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61853%22]}

THE LIMITS OF JOURNALIST'S SOURCE PROTECTION[1]

BARBORA BŘEŽNÁ[2]

1. INTRODUCTION

In this essay, I would like to discuss the importance of free press as a watchdog and the obligation to protect sources and its limits. As this topic includes a variety of issues worth discussing, I will narrow it down to only few of them and I will not discuss the „private" matter any further, and by „private" matter I mean disputes between journalists and ordinary people or celebrities affected by the press (such as the case of Bladet Tromso and Stensaas v. Norway)[3]. This essay will limit its focus on the role of free press as a watchdog of politicians and democracy as such and its importance in general, instead.

The privileged position of media derives from the view that political expression plays central role in democratic society. In general, it is more acceptable to use severe and harsh criticism targeted at politicians and political matter as the freedom of expression is of vital importance in this case. Much less protection is granted to the privacy and reputation of politicians, particularly in cases when obtained information, no matter how personal, has an impact on their duties and public functions.[4] Therefore, there is no

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Free speech and media law. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Free speech and media law.

[2] Mgr. Barbora Březná je studentkou Právnické fakulty Masarykovy univerzity. Kontakt: 460108@mail.muni.cz.

[3] Amicus Curiae Opinion on the Relationship between the Freedom of Expression and Defamation with Respect to Unproven Defamatory Allegations of Fact as Requested by the Constitutional Court of Georgia [online]. Council of Europe. 2004. p. 19 [cit. 18. 6. 2021] Available at: https://www.venice.coe.int/webforms/documents/CDL-AD(2004)011-e.aspx.

[4] BYCHAWSKA-SINIARSKA, Dominika. Protecting the right to freedom of expression under the European Convention of Human Rights [online]. Council of Europe. 2017.p. 64. [cit. 18. 6. 2021] Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814.

doubt that the activities of the minister of health, such as visiting a closed restaurant with another public figure, will not be protected under the right to privacy, but supposedly celebrating an anniversary with his wife should be protected.

According to the judgement of the Grand Chamber, there is a fundamental distinction between reporting facts (which includes even controversial ones), that may contribute to public debate in democratic society relating to politicians in the exercise of their functions, and reporting of details of private life of an individual who does not exercise official functions.[5] It is important to add that public interest as such should not be a mere "interested public", but should go beyond that.

2. THE COLLISION OF SOURCE PROTECTION AND PUBLIC INTEREST

When protection of privacy and protection of media are confronted, none of them takes preferences automatically. It is needed to balance the protection of each of them in particular cases.[6]

In my point of view, media and free press are very powerful tools. In democratic society, they must be allowed to investigate affairs, provide people with information about how public figures and politicians fulfil their duty that have been entrusted to them, how they manage public finances, who they meet with, and many others. This requires a great deal of funds and financial resources to support such media. This had become increasingly difficult some time ago with media publishing a lot of its content for free (such as idnes.cz and others). This development has taken a turn lately, and it is slowly becoming normal again to pay for high-quality content and news coverage (e.g. Deník N, Hospodářské noviny and many others).

---

[5] SMITH, Robin Callender. *F*rom von Hannover (1) to von Hannover (2) and Axel Springer AG: Do Competing ECHR Proportionality Factors Ever add up to Certainty. *Queen Mary Journal of Intellectual Property*. [online].2012. Vol. 2, p. 390. [cit. 18. 6. 2021] Available at: https://heinonline.org/HOL/P?h=hein.journals/qmjip2&i=389.

[6] *WESTKAMP, Guido.* Private Life and the Margin of Appreciation, Introductory Note to the European Court of Human Rights: Alex Springer AG v. Germany and Von Hannover v. Germany (No. 2). *International Legal Materials.* [online].2012 *Vol. 51, p. 633.* [cit. 18. 6. 2021] Available at: https://heinonline.org/HOL/P?h=hein.journals/intlm51&i=677.

Furthermore, politicians are now granted additional space to address issues on their own in the form of social media. Prime Minister Andrej Babiš, Minister of Interior Jan Hamáček, Minister of Health Roman Prymula (who was the Minister of Health at least at the time when this essay was written), and many other important politicians, ministers and leaders are active on social platforms, e.g. Facebook and Twitter. They can address their followers and fans directly, without the "help" of media. Therefore, they are able to debunk many allegations themselves right away, they can explain the matter from their perspective immediately when something happens or they can simply get in touch with their voters. This, in my point of view, also weakens the position in which the media and newspaper are nowadays a little bit. They are not per se needed by politicians themselves, who can share a fair amount of their content for free online instead, but media and free press, on the other hand, need finances in order to perform their duty as a watchdog of a democratic society.

Many of the affairs that are made public would not be known without a reliable source (often very close to the politicians in particular), who confides details about particular affairs in journalists or who keeps informing them about it afterwards. This may be controversial, as the source should stay anonymous and, in most cases, his identity is never revealed to public.

The sources of information are protected under Article 10 of European Convention of Human Right. The article states that exercise of freedom of expression may be subject to formalities, conditions, restrictions or penalties as are prescribed by law in the interest and for preventing the disclosure of information received in confidence.[7] This protection of journalistic sources is one of the basic conditions of freedom of the press, otherwise (and without granted protection), sources may be discouraged from assisting the press in informing the public on matters of public interest, which, as a result, may weaken and undermine the vital public watchdog

[7] Article 10 section 2. European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16 [online]. [cit. 18. 6. 2021] Available at: https://www.echr.coe.int/documents/convention_eng.pdf.

role, because the ability of the press to provide reliable information may be adversely affected.[8]

One of the cases in which the protection of source is discussed is the case of Goodwin v. the United Kingdom. Mr Goodwin, who was a journalist, received information from his source by telephone. The source informed Mr Goodwin that the company Tetra Ltd. was about to raise a large loan while it had major financial problems. When Mr Goodwin called the company to get additional information for his article, Tetra Ltd. requested he reveals the source of information. They argued that this would help them with identifying dishonest employees and later with initiating proceedings against them.

In this case, the European Court of Human Rights ruled that protection of journalistic sources is one of the basic conditions for press freedom and the lack of protection may potentially result in chilling effect, therefore affecting the freedom of expression. Such revelation would violate the freedom of expression.[9]

Additionally, in Sanoma Uitgevers B.V. v. Netherlands[10] it was ruled by the Grand Chamber that "*orders requiring journalists to disclose their sources must be subject to the guarantee of judicial review or review by another independent and impartial review body*." Also, criteria for such review were identified as follows. Such body should be independent and separated from the executive branch and other interested parties. Power to determine whether public interest overrides the protection of journalistic sources should be vested in such body prior to the handing over of such material. Also, it should prevent unnecessary access to information capable of disclosing the sources' identity. Such body should have clear criteria, that also include whether a less intrusive measure may be sufficient. The fact that the review of material takes places only after the material was handed over, and such material may reveal the source, can undermine the essence of the right to

[8] BYCHAWSKA-SINIARSKA, Dominika. opt. cit., p. 100.

[9] Ibid.

[10] Judgment of the ECHR of 14 September 2010, appliaction *no*. 38224/03, Sanoma Uitgevers B.V. v. Netherlands, para 90-92.

confidentiality, therefore, it should take place prior to this. In addition to this, potential risks and respective interest must be weighted prior to any disclosure. Also it should be possible for the judge (or any other authority) to refuse to make a disclosure order and protect sources from being revealed, and to do so whether or not they are specifically mentioned in the withheld material, if the communication of such material creates a risk of compromising and revealing the identity of journalists' sources. Last but not least, there should be a procedure to identify information potentially leading to the identification of the source in urgent cases, and isolate those information from information that do not carry such risk, so the material is not exploited by the authorities.[11]

The courts of the Czech Republic also had to deal with the protection of the source. In this case, journalist Martin Šmok was ordered to pay a fine for refusing to identify and reveal the source of published information to the police and the prosecuting authorities, who were investigating the crime reported by the source. The Constitutional Court of the Czech Republic held that Martin Šmok should not had been ordered to pay the fine and deciding otherwise was violating the freedom of expression. In this case, the police and prosecuting authorities should have found alternative ways of identifying the source or obtaining the required information. The course of action adopted by police and prosecuting authorities was unlawful, according to the Constitutional Court.[12]

This is not the only case in the Czech Republic when journalist protecting its source was being punished for doing so. Similarly, in 2000, two journalist, Sabina Slonková and Jiří Kubík, were prosecuted on the initiative of Miloš Zeman, who was the prime minister at the time, because they refused to reveal the source of the information in so called "Olovo" affair. This, at the time, concerned Miloš Zeman and Petra Buzková, his rival and member of the same party, who had become increasingly popular with his voters. The team surrounding Miloš Zeman had plans to discredit Buzková and damage her reputation. When Slonková and Kubík made the whole af-

[11] *BYCHAWSKA-SINIARSKA, Dominika.* opt. cit., p. 102.

[12] Judgement of the Consitutional Court, 27th September 2005, I. ÚS 394/04.

fair public, they refused to reveal the source of the information. In return, Miloš Zeman initiated their prosecution. Fortunately, both journalists were granted pardon from Václav Havel, so this matter was not dealt with any further (by courts).

However, the protection of source related to the freedom of expression is not absolute or endless. There may be (and should be) cases, when this particular freedom is outweighed by something else. It is needed to balance the rights, freedoms and duties in specific cases, so that everyone's freedom may be exercised to its guaranteed and fullest extent. The journalists and their sources are not stripped of certain lawful duties. For example, they are obliged to inform the police and prosecuting authorities if they come to know that criminal act is about to happen.

3. CONCLUSION

In general, it is needed that the public interest on disclosing and revealing the source is strong enough and that it outweighs the freedom of expression (which of course may happen in certain cases). Also, the Constitutional Court in the case of Martin Šmok held that it may be permissible to reveal the source of information to the prosecuting authorities if the case is connected with particularly serious criminal act and there is no alternative for the prosecuting authorities to gain required information. However, this means that the prosecuting authorities cannot just go "the easy way" (as they often do) and try to force the journalist to reveal the source and in case he does not comply, order him to pay a fine. But, as was held, and as the common rule is, the freedoms have to be balanced and the freedom of expression may be exercised to a certain extent – until it is outweighed by something of greater importance.

4. BIBLIOGRAPHY

[1] BYCHAWSKA-SINIARSKA, Dominika. Protecting the right to freedom of expression under the European Convention of Human Rights [online]. Council of Europe. 2017.p. 64. [cit. 18. 6. 2021] Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814.

[2] European Convetnions on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16 [online]. [cit. 18. 6. 2021] Retrieved from: https://www.echr.coe.int/documents/convention_eng.pdf.

[3] SMITH, Robin Callender. From von Hannover (1) to von Hannover (2) and Axel Springer AG: Do Competing ECHR Proportionality Factors Ever add up to Certainty. *Queen Mary Journal of Intellectual Property*. [online].2012. Vol. 2, pp. 389–393. [cit. 18. 6. 2021] Retrieved from: https://heinonline.org/HOL/P?h=hein.journals/qmjip2&i=389.

[4] Amicus Curiae Opinion on the Relationship between the Freedom of Expression and Defamation with Respect to Unproven Defamatory Allegations of Fact as Requested by the Constitutional Court of Georgia [online]. Council of Europe. 2004. [cit. 18. 6. 2021] Retrieved from: https://www.venice.coe.int/webforms/documents/CDL-AD(2004)011-e.aspx.

[5] *WESTKAMP, Guido.* Private Life and the Margin of Appreciation, Introductory Note to the European Court of Human Rights: Alex Springer AG v. Germany and Von Hannover v. Germany (No. 2). *International Legal Materials.* [online] *2012, Vol. 51, pp. 631–684.* [cit. 18. 6. 2021] Retrieved from: https://heinonline.org/HOL/P?h=hein.journals/intlm51&i=677.

[6] Grand Chamber Judgment of the ECHR of 14 September 2010, appliaction *no*. 38224/03, Sanoma Uitgevers B.V. v. Netherlands.

[7] Judgement of the Consitutional Court, 27 of September 2005, I. ÚS 394/04, N 184/38 SbNU 471.

THE DANGERS A SMART HOME AND HOW TO AVOID THEM[1]

MARTIN BUKOVIČ[2]

1. INTRODUCTION

In this work, I will deal with the issue of smart homes. My main task will be to deal with one of the biggest pitfalls of smart homes, which is security. My research question, which I will try to answer, is, what are the security risks of smart homes and how to avoid these security risks? Directly related to this is the question of which devices of smart homes are the biggest security threat? I should find the answer to these questions in this work.

I will first define the term "smart home". I will define the specifics of what can be considered a "smart home". Acquiring a smart home is also related to the benefits that the smart home itself brings to its users. However, on the other hand, there are many disadvantages that a smart home brings. This is also related to security risks, which I will address in connection with the smart home in the next part of this work. I'll look at some smart devices in a smart home and explain how their security can be broken. I will explain the danger of an unwanted attacker infiltrating one of the smart devices connected to the smart home. In the last part of this work, I will try to clarify how to prevent this infiltration of attackers into the smart home. The work should provide a suitable guide on how to avoid mistakes when purchasing a smart home and thus have your home under your control.

2. WHAT IS A SMART HOME?

First, I will define the term “smart home”, which is the main topic of this work. The smart home concept is being used by more and more people.

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Smart everything. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Smart everything.

[2] Martin Bukovič je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 468344@mail.muni.cz.

This is mainly due to its simple remote control from anywhere with an internet connection via a mobile phone, tablets or another similar networked device.[3] So for example, you can switch off the heating with your phone during holidays. Smart home includes automatic systems that allow residents of a house or an apartment to better control and monitor appliances, devices and the building itself. Thanks to the smart home, you can control, for example, lighting, heating, opening windows and doors, shading blinds, controlling security cameras, airflow, the refrigerator and much more. For example, how does a smart refrigerator work, if it is connected to a smart home system? It can evaluate its contents, point to an upcoming expiration date, recommends healthy alternatives, or even if some products are consumed, the refrigerator will create and send you a shopping list all by itself.[4] It can also plan meals based on the food inside your refrigerator.[5]

Smart home devices are connected and can be controlled and accessed using a central device (smartphone, central home unit etc.). A smart home thus consists of smart devices that together form one common unit, which relieves many households of worries. E.g. the smart home system handles routine matters that would otherwise be performed by the residents of the household themselves. One of the popular benefits of a smart home is that it helps create a safe home. Residents of households can secure their homes with wireless cameras, alarms, smart locks etc. Smart sensors can easily detect water or gas leaks when in case of such danger the household resident is immediately warned using a smartphone.[6]

Energy efficiency, which is very closely linked to economic savings, is one of the most important reasons why people choose to upgrade their

---

[3] CHEN, James. Smart Home. In: *Investopedia* [online] [cit. 08.01.2020]. Available at: https://www.investopedia.com/terms/s/smart-home.asp

[4] What is a Smart Home? - Smart Home Energy. In: *Smarthomeenergy.co.uk* [online]. [cit. 08. 01. 2021]. Available at: http://smarthomeenergy.co.uk/what-smart-home

[5] All Samsung Family Hub Features | Samsung US. In: *Samsung Electronics America* [online] [cit. 08. 01. 2021]. Available at: https://www.samsung.com/us/explore/family-hub-refrigerator/apps/

[6] How a smart home can improve your home security. In: *Hestiamagazine.eu* [online]. 2021 Hestia Magazine [cit. 24. 06. 2021]. Available at: https://www.hestiamagazine.eu/how-a-smart-home-can-improve-your-home-security

homes to smart homes. With smart home appliances, homeowners can control their energy consumption well enough without having to pay extra unnecessary expenses. For example, they can set the lights to turn on automatically when they enter a room.[7] There are, for example, motion sensors that can ensure that the devices will only be active if there are people in the room. Intelligent blind control can automatically maintain the room temperature without the need to turn on the air conditioner. In addition to electricity consumption, the smart home also enables controlled water consumption, where there are intelligent shower-heads or toilets that save water consumption. However, there are many more devices that can be used in a smart home. [8]

According to the Strategic Energy Technology Plan, "smart homes" were one of the agreed strategic targets in the area of smart solutions for energy customer.[9] Smart households play a very important role in the European Union's energy system. The European Commission claimed that individuals and communities have an interest in managing energy consumption, and that is why it is necessary to "*create technologies and services for smart homes that provide smart solutions to energy consumers*".[10]

2.1 WHAT ARE THE PITFALLS OF A SMART HOME?

Despite its many advantages, a "smart home" also has a number of disadvantages that can be very dangerous for its users. One of the primary disadvantages of getting a smart home is that it can be quite expensive. Of course, you don't have to invest that much in a smart home, but you have

---

[7] 7 Greatest Advantages of Smart-Home Automation. In: *Bluespeedav.com* [online].[cit. 08. 01. 2021]. Available at: https://bluespeedav.com/blog/item/7-greatest-advantages-of-smart-home-automation

[8] How a smart home can improve your home security, opt. cit.

[9] The strategic energy technology (SET) plan. In: *Op.europa.eu* [online]. Publications Office of the EU [cit. 24. 06. 2021]. p. 39. Available at: https://op.europa.eu/en/publication-detail/-/publication/064a025d-0703-11e8-b8f5-01aa75ed71a1

[10] COMMUNICATION FROM THE COMMISSION Towards an Integrated Strategic Energy Technology (SET) Plan: Accelerating the European Energy System Transformation. In: *Set-is.ec.europa.eu* [online]. Strategic Energy Technologies Information System. [cit. 08. 01. 2021]. p. 11.Available at: https://ec.europa.eu/energy/sites/ener/files/publication/Complete-A4-setplan.pdf

to reckon with the fact that a smart home won't bring you as many benefits as if you invested more in it. Thanks to energy savings, this investment pays off in the long run. [11] Another problem that a smart home can bring is, for example, when an overvoltage arises in connection with the interconnection of devices, which can cause demand, power outages or the case of mutual incompatibility between devices.[12]

However, one of the biggest pitfalls of smart homes is the fact that all smart home devices are connected to a common network. In addition to the traditional connection of computers to the network, in the household, we can also find, for example, the mentioned refrigerator, which is connected to other devices via one network. Connecting your smart home devices to a shared network can be a security threat to you. It is so important to monitor their security level when buying smart devices. Personal data that a smart device obtains from you can be misused by hackers. It is also important to keep in mind that these devices collect personal data about you, which can be used by various companies. By secretly monitoring your online activities, the company can target you with specific ads through a smart device.[13]

3. UNAUTHORIZED LEAKAGE OF PERSONAL DATA

Connecting your smart home devices to a shared network can be a security threat to you. Malicious actors could exploit device vulnerabilities or system errors to gain access to the entire home network to which the smart home is connected. [14] Poor security of smart appliances in a smart home can thus pose a real threat to household residents. The threat itself is that smart

[11] 30 Key Pros & Cons Of Smart Homes. In: *Environmental-conscience.com* [online]. 2020 [cit. 08. 01. 2021]. Available at: https://environmental-conscience.com/smart-homes-pros-cons/

[12] Ibid.

[13] SCHNEIER, Bruce. Essays: The Internet of Things That Talk About You Behind Your Back - Schneier on Security. In: *Schneier.com.* [online] *08.01.2016* [cit. 08. 01. 2021]. Available at: https://www.schneier.com/essays/archives/2016/01/the_internet_of_thin_1.html

[14] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers. In: *Safety.com* [online]. 3. 6. 2019 [cit. 08. 01. 2021]. Available at: https://www.safety.com/how-to-protect-smart-home-from-hackers/

devices in a smart home can know virtually anything about their residents. They can monitor their activities, they know when they go to work, smart devices know their voices, their passwords and much more. These devices work with our personal data, which may fall into the wrong hands.

The most vulnerable devices include outdoor devices with a lower level of security. Examples are smart bells or an automatic garage door opener that can be easily accessed from the street, which hackers can exploit. [15] The level of security of these devices is therefore important. In November 2020, for example, Amazon UK's bestseller in smart doorbells was found to send unencrypted household names and passwords to servers in China. When purchasing these devices, the buyer should take into account the security risks and not prefer convenience. Consumers are then at high risk of their data being misused.[16]

Another vulnerable group are home devices that can be controlled via an application on your phone, tablet or home computer. These include security cameras, baby monitors, smart locks, personal home assistants and more. These can be easily compromised due to weaknesses in the communication protocol or vulnerable entry points that vendors have left accessible for subsequent maintenance.[17] In October 2016[18], a botnet known as "Mirai" infiltrated many connected devices to the Internet with the Linux operating system and turned them into a network of remotely controlled bots. He attacked mostly cameras connected to smart homes and personal home assistant devices. [19]

There are many known cases when hackers attack baby monitors. Initially, it may begin with a beep, and it may culminate in sexual exclamations, echoing through a baby monitor in the parents' room, which is con-

---

[15] Ibid.

[16] Smart doorbells „easy target for hackers" study finds - BBC News. In: *bbc.com.* [online]. 23.11.2020 [cit. 08. 01. 2021]. Available at: https://www.bbc.com/news/technology-55044568

[17] FERRON, Emily, opt. cit.

[18] CHEN, James. opt. cit.

[19] What is the Mirai Botnet?. In: *Cloudflare* [online] [cit. 08. 01. 2021]. Available at: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

nected to a camera in the children's room. Anxious parents who have heard the voice of a hacker through a baby monitor feel that someone is with their child. However, when they turn on the lights in the room, the hacker can tell them through the baby monitor to turn off the lights. The hacker can connect to other devices, incl. smart light bulbs in their smart home. However, when the child's parents come to the children's room, they find that there is no stranger in the room and find out that their smart home has been attacked by hackers. This really happened to the parents of a 4-month-old son on 17th December 2018, in Houston.[20]

Even hacking a robotic vacuum cleaner can be dangerous for households, for example, US experts have found that a robotic vacuum cleaner does not only have to collect dirt but can also collect personal data. Robotic vacuum cleaners can be hacked remotely so that they can also capture sound and eavesdrop on the occupants of the house. The robotic vacuum cleaner does not have to be fitted with a microphone. Remotely, hackers can eavesdrop on a robotic vacuum cleaner by accessing its "Lidar" reading. Lidar is a remote sensing technology for measuring distances. The emitted laser beam can be used to indicate sound vibrations acting on objects struck by the laser. Thus, hackers can practically eavesdrop on household members.[21]

Home appliances, such as refrigerators, stoves, or ovens, are less likely to be attacked, but can still be attacked by hackers. Hacking your smart refrigerator means much more to hackers than just finding out the contents of your refrigerator. This gives them access to your home network and allows them to find out all the information about you through it.[22] For example, hackers can exploit security vulnerabilities (e.g. this device does not valid-

[20] WANG, Amy B. Nest cam security breach: A hacker took over a baby monitor and broadcast threats, Houston parents say. In:*Washingtonpost.com* [online] 20.12.2018 [cit. 08.01.2021]. Available at: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/

[21] CHADWICK, Jonathan. Researchers hack a robotic vacuum cleaner to record speech remotely. In: *Mail Online* [online]. 18. 11. 2020 [cit. 08.01.2021]. Available at: https://www.-dailymail.co.uk/sciencetech/article-8961729/Researchers-hack-robotic-vacuum-cleaner-record-speech-remotely.html

[22] FERRON, Emily, opt. cit.

ate security certificates) in access to the Gmail calendar used in the refrigerator and monitor activity for the user name and password.[23]

3.1 HOW TO PREVENT MY PERSONAL DATA FROM LEAKING?

So, the question remains, how can we prevent the security threats posed by a smart home? In this section, I will present some specific tips on how to minimize the risk of hacking. It should be noted that no network is 100% secure, only the potential risk of hacking can be reduced. The first step must be taken during the selection of the smart device. We have to ask ourselves, what do we really want our smart home to be able to do? Based on that, we decide which devices to buy. It is important to look mainly at the brand and quality of the smart device. A device that is too cheap and unreliable could pose a security threat. Another step is to create a suitable network for smart devices. You should have a quality Wi-Fi router with a verified brand and set a network name and password. It is also a good idea to hide the visibility of the network. Another option is to create a second network within the home with its own name and password only for smart home devices. The hacker would possibly only get into this network separate from the one where you have your sensitive information stored. [24]

It is important to have the devices updated because each update fixes some bugs that the device had. This will prevent hackers from infiltrating the device due to these bugs. Network vulnerabilities were detected, for example, in the Philips Hue smart light bulb, which consisted of a low-power wireless protocol. That's why Philips has released a new firmware update that changes it. It is thus obviously important to update your devices regularly. [25] It is also important to keep in mind that you should have a secure

---

[23] NEAGLE, Colin. Smart refrigerator hack exposes Gmail account credentials In: networkworld.com [online]. 26.08.2015 [cit. 19.06.2021]. Available at: https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[24] FERRON, Emily, opt. cit.

[25] WINDER, Davey. How to stop your smart home spying on you. In: *the Guardian* [online]. 8. 3. 2020 [cit. 08.01.2021]. Available at: http://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy.

and specific password for each device. For example, if you use one password for all your operations and a hacker can access it, it will not be a problem for him to access your home network and thus all personal information about you.[26] To maximize security, so-called two-factor authentication is suitable for access to smart devices. To access the account of these devices, a password and secondary verification will be required, which most often consists of sending an SMS code to a mobile phone. This means that even if a hacker obtains your password, he will not get into the device, because he also needs a code sent to the mobile phone. [27] It is also advisable to disconnect devices that will not be used from electricity if we are leaving home for a long time (e.g. go on holiday). On the one hand, it will save energy and at the same time prevents hackers from hacking into your home network via this device while you are away.[28]

4. CONCLUSION

Thanks to this work, I was able to find out that a smart home consists of connecting individual smart devices to a common network, where it is possible to centrally control the devices using a smartphone, tablet or other similar networked devices. This has a number of advantages, such as energy savings, comfort or the ability to control your home from virtually anywhere. On the other hand, there are a number of disadvantages, the most fundamental of which are the security risks associated with a smart home. It is the connection of devices to the common network that is a great risk, because if a hacker gets into this network by hacking one device, he/she can then control all other devices and collect the collected data from them. This is also part of the answer to my research question. There are different levels of threat that a given smart device will be hacked. E.g. the biggest security risks are smart entrance locks and the least common are smart home appliances such as a refrigerator. There are many ways to pre-

[26] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers.

[27] COHEN, Jason. How to Protect Your Smart Home From Hackers. In: *PCMAG* [online] [cit. 08.01.2021]. Available at: https://www.pcmag.com/how-to/how-to-protect-your-smart-home-from-hackers

[28] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers.

vent hackers from gaining access to a smart home network. This can be achieved by using a strong password, choosing a suitable smart device or creating a second network only for smart home devices. However, there are many more options. That was s the answer to the second part of my research question.

In this work, I present a comprehensive view of how the safety of the residents of a smart household can be endangered and how this risk can be avoided. In principle, it can be said that it depends on the security level of the smart home. The more secure a smart home is, the more we have it under control and thus there will be no unauthorized access of third parties to our sensitive information.

5. BIBLIOGRAPHY

[1] CHEN, James. Smart Home. In: *Investopedia* [online] [cit. 08.01.2020]. Available at: https://www.investopedia.com/terms/s/smart-home.asp

[2] What is a Smart Home? - Smart Home Energy. In: *Smarthomeenergy.co.uk* [online]. [cit. 08. 01. 2021]. Available at: http://smarthomeenergy.co.uk/what-smart-home

[3] All Samsung Family Hub Features | Samsung US. In: *Samsung Electronics America* [online] [cit. 08. 01. 2021]. Available at: https://www.samsung.com/us/explore/family-hub-refrigerator/apps/

[4] How a smart home can improve your home security. In: *Hestiamagazine.eu* [online]. 2021 Hestia Magazine [cit. 24. 06. 2021]. Available at: https://www.hestiamagazine.eu/how-a-smart-home-can-improve-your-home-security

[5] Greatest Advantages of Smart-Home Automation. In: *Bluespeedav.com* [online]. [cit. 08. 01. 2021]. Available at: https://bluespeedav.com/blog/item/7-greatest-advantages-of-smart-home-automation

[6] The strategic energy technology (SET) plan. In: *Op.europa.eu* [online]. Publications Office of the EU [cit. 24. 06. 2021]. p. 39. Available at: https://op.europa.eu/en/publication-detail/-/publication/064a025d-0703-11e8-b8f5-01aa75ed71a1

[7] Communications from the Commision Towards an Integrated Strategic Energy Technology (SET) Plan: Accelerating the European Energy System Transformation. In: *Setis.ec.europa.eu* [online]. Strategic Energy Technologies Information System. [cit. 08. 01. 2021]. Available at: https://ec.europa.eu/energy/sites/ener/files/publication/Complete-A4-setplan.pdf

[8] 30 Key Pros & Cons Of Smart Homes. In: *Environmental-conscience.com* [online]. 2020 [cit. 08. 01. 2021]. Available at: https://environmental-conscience.com/smart-homes-pros-cons/

[9] SCHNEIER, Bruce. Essays: The Internet of Things That Talk About You Behind Your Back - Schneier on Security. In: *Schneier.com.* [online]. 08.01.2016 [cit. 08. 01. 2021]. Available at: https://www.schneier.com/essays/archives/2016/01/the_internet_of_thin_1.html

[10] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers. In: *Safety.com* [online]. 3. 6. 2019 [cit. 08. 01. 2021]. Available at: https://www.safety.com/how-to-protect-smart-home-from-hackers/

[11] What is the Mirai Botnet? In: *Cloudflare* [online] [cit. 08. 01. 2021]. Available at: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[12] WANG, Amy B. Nest cam security breach: A hacker took over a baby monitor and broadcast threats, Houston parents say In:*Washingtonpost.com* [online]. 20.12.2018 [cit. 08.01.2021]. Available at: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/

[13] CHADWICK, Jonathan. Researchers hack a robotic vacuum cleaner to record speech remotely. In: *Mail Online* [online]. 18. 11. 2020 [cit. 08.01.2021]. Available at: https://www.-dailymail.co.uk/sciencetech/article-8961729/Researchers-hack-robotic-vacuum-cleaner-record-speech-remotely.html

[14] NEAGLE, Colin. Smart refrigerator hack exposes Gmail account credentials In: *networkworld.com* [online]. 26. 08. 2015 [cit. 19.06.2021]. Available at: https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[15] WINDER, Davey. How to stop your smart home spying on you. In: *the Guardian* [online]. 8. 3. 2020 [cit. 08.01.2021]. Available at: http://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy.

[16] COHEN, Jason. *How to Protect Your Smart Home From Hackers.* In: *PCMAG* [online]. [cit. 08.01.2021]. Available at: https://www.pcmag.com/how-to/how-to-protect-your-smart-home-from-hackers

CHILLING EFFECT: HOW LACK OF PRIVACY AFFECTS THE POLITICAL FREEDOM AND SOCIAL DISSENT[1]

JANA KRČMOVÁ[2]

1. PRIVACY

Trying to clearly define what exactly privacy is seems like an impossible task. It has been described in a wide variety of ways, which is understandable, considering that the concept we are trying to put into words is both intangible and so subjective, so personal – it makes sense that each person's opinion on what privacy means to them would differ, sometimes very greatly. There is not much more consensus in academic spaces. In fact, one might say that one of the most common threads running through different descriptions of "privacy" would be that it is hard to describe. Complicated. Each concept is tinged with a variety of philosophical, sociological, or political theories.[3] However, its' importance – to us, as autonomous individuals, our development and wellbeing, to our relationships, and to the good of our society as a whole, is much less disputed.[4]

2. CHILLING EFFECT

Chilling effect was first articulated in express terms in the USA, during the Cold War, in connection to the First Amendment, which states that "*Congress shall make no law respecting an establishment of religion, or prohibiting*

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Surveillance. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Surveillance.

[2] Jana Krčmová je studentkou Právnické fakulty Masarykovy univerzity. Kontakt: 468555@mail.muni.cz.

[3] KOOPS, Bert-Jaap; NEWELL, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom and Maša GALIČ. A Typology of Privacy. *University of Pennsylvania Journal of International Law 38(2): 483-575 (2017), Tilburg Law School Research Paper No. 09/2016*, pp. 491-492.

[4] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Vol. 1. Stanford, California: Stanford University Press, 2010, pp. 81-88.

the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[5] In reaction to the anti-communist government measures of the time, the courts came to the conclusion that certain acts of government "might deter the free exercise" of a person's rights, because of fear of prosecution. This theory functions similarly in online spaces – people might be deterred from engaging in (or might censor themselves while engaging in) certain legal activities online (such as discussions of matters of public interest and political issues, research into certain topics, which is not only legal but vital for the function of a democratic society) because of government surveillance of these online spaces, whether because they fear actual legal retribution or they fear being labelled as "someone to watch" (they fear that the general mass surveillance they are under will turn into personal surveillance, and all this would happen without their knowledge, making it impossible to gauge if and how closely is one being watched). However, research suggests that while people might express privacy concerns in connection to their online presence, this might not actually impact their behaviour in these spaces all that much.[6]

3. BEYOND NOTHING TO HIDE

In a 2017 study titled "*Beyond nothing to hide*" Stuart and Levine examined people's position on surveillance in today's online spaces. Through analysis of interviews conducted with the participants (there were 42 participants in total, aged 18-46, all students at a British university, but not all British nationals) in focus groups, the researchers were able to make several observations.

The subjects seemed to think of surveillance as quite ubiquitous but they were not particularly stirred to oppose this. In fact, the notion that they were already under surveillance in one way or other served as an argument

[5] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 31. 11. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

[6] PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal.* 2016, Vol. 31, No. 1, pp. 125-129.

that more surveillance would not be a problem for them – as long as the way it was implemented was normal ("everyone does that") and had a legitimate goal, in improving services or providing more security. It would however be inaccurate to say that they were clearly in favour of further surveillance, or even the current state of it, but that they were resigned to it.[7] Surveillance seems to come attached with a sort of normalising effect. What would have seemed an unacceptable intrusion into a person's privacy to previous generations, we accept simply as a part of navigating the world, especially online. There is a sort of a trade-off, in which we allow some intrusion into our privacy for some sort of service.[8]

The next logical question then would be – when do we mind? In which circumstances do we find that the trade-off no longer benefits us?

Surveillance, with the use of technology, has a leg up on any more traditional sort of surveillance. It is integrated into our surroundings, in ways that make it feel inobtrusive, imperceptible, even convenient.[9] (To illustrate this point, an example from personal experience: recently I've turned off targeted ads on YouTube and then gotten legitimately annoyed at how off the mark most of the ads I had started to see were – an app store for a brand of a mobile phone which I do not have being the most often recurring one. A similar amount of car commercials though, which are as relevant to me, a 22-year-old student, as they were before when they were targeted.) That does not mean that surveillance is always perfectly seamless.

Such is the case when we consider the surveillance to be excessive – when the trade-off is mismatched. Even then, the responders either considered it to be harmless (the "nothing to hide" argument) or simply accepted it because of the necessity of the service provided (Google is necessary, therefore we have to give up privacy and place our trust in the provider of said service).[10] Secondly, the threat of future surveillance technology (discussed in the study in connection to Google Glass) – concerns that surveil-

[7] STUART, Avelie; LEVINE, Mark. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*. 2017, Vol. 47, p. 698.

[8] Ibid., p. 704.

[9] Ibid., p. 705.

[10] Ibid., pp. 698-699.

lance will become even more present (capturing not just our activity on the internet, but our 'real' lives, more on this later) and harder to detect. However, the responders also note that this development does not sit well with them simply because they are not used to it – it has not yet been normalized.[11] Lastly, instances when surveillance seems to notice 'us'. When we feel we cannot keep parts of our lives to ourselves, parts of our identities separate or when there are real, unforeseen, and unwanted consequences or when we feel misrepresented.[12]

Throughout, Stuart and Levine refer to a different study, by Ellis, Harper, and Tucker, published in 2013, "The affective atmospheres of surveillance;" in which the respondents stated that they feel they are always being observed, but they found it difficult to even articulate this in any concrete terms, a situation which does not lend itself to much resistance.[13] The last point of discussion in "Beyond nothing" deals with exactly that – how respondents deal with surveillance and its' potential negative effects, which is through separation – understood as the ability to distance oneself from undesirable associations.

Separation of the physical person and the digital person, which makes the surveillance of the digital person inconsequential to them, the "real" person. Whether you are under surveillance on the internet has little to no impact on your actual life.[14]

However, what does seem to have an immediate effect, is peer-to-peer surveillance.

4. PEER-TO-PEER SURVEILLANCE AND THE EXTENDED CHILLING EFFECT

Helen Nissenbaum's theory of privacy as contextual integrity – that we are people who exist in various social contexts, which, in order for us to perform the variety of roles we inhabit in other people's lives, must remain

[11] Ibid., p. 700.

[12] Ibid., pp. 700-702.

[13] Ibid., pp. 696.

[14] Ibid., p. 702 and p. 704.

separate. We feel that our privacy is threatened when these context-relative informational norms are being disturbed.[15]

Through social networking sites we can interact with a vast variety of people, from absolute strangers through family members both close and distant to (potential or actual) employers and co-workers. We are also afforded an opportunity that is not so present in our 'real-world' lives, the opportunity of impression management. In short, we have much more control over the image we put out on the internet, but this image we choose to project is necessarily impacted by our audiences' expectations. As said above, we play a variety of roles in different social contexts (we act differently when we are with our friends than we do in front of our employers, in each situation we make different judgements of what is and what is not appropriate), but on social networking sites, our audience is mixed, and we have to present our online personas in a way that works for all of them, without appearing dishonest, and thus making our aim at the lowest common denominator, with the intention to alienate as few people as possible.[16]

The extended chilling effect then refers to the way online surveillance might affect our presentation offline – how our image online and offline match-up, how our actions in real life might be portrayed in online spaces and impact our image that way, and changing how we act in "real life" because of how it might appear if connected to us in an online space, through social networks.[17] Examples of this might range from the innocuous ("do not tag me in that photo, I look like I'm drunk in it") to the quite serious (pictures of political protests, in which individual protesters can be identified[18]).

---

[15] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Vyd. 1. Stanford, California: Stanford University Press, 2010, p. 186.

[16] MARDER, Ben; JOINSON, Adam; SHANKAR, Avi; HOUGHTON, David. The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking. *Computers in Human Behaviour*. 2016, Vol. 60, pp. 582-584.

[17] Ibid., pp. 584-589.

[18] SHEPHERD, Katie. An artist stopped posting protest photos online to shield activists from police. Then, he was arrested. *The Washington post* [online]. The Washington Post, published 3.8.2020 [cit. 1.11.2020]. Available at: https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/

5. A DIFFERENT PERSPECTIVE

So far, "Beyond nothing to hide" has been our reference point. But, as the authors themselves point out, their subject pool was quite limited (with the respondents all being students, mostly young adults and all heavily involved with social media, while not engaging in much that might be seen as sensitive, politically – people that have "nothing to hide") – responses would likely be quite different if the people questioned were part of, for example, "stigmatised minority".[19] Such being the case, we might want to explore the chilling effect in different sorts of circumstances.

There was a noticeable shift in the wake of the Snowden leaks in how we think of surveillance. It brought certain issues to the forefront of the minds of the wider public. Previously covert surveillance was no longer so. In the aftermath of this incident, Jonathan W. Penney examined the influence of chilling effect on what might seem like quite an inoffensive activity – reading articles on Wikipedia. In particular, he examined the effect the Snowden leaks (an "exogenous shock") had on Wikipedia traffic for articles on privacy-sensitive topics, with keywords such as "Car bomb", "Homeland defence" or "Liberation Front" to pick a few at random, and did, in fact, find that there was a quite significant drop in traffic, and so was able to conclude that chilling effect had an impact on this entirely legal and in fact quite necessary activity (the public educating itself on sensitive topics).[20]

There are far more blatant examples of chilling effect to be found in the world – with Mainland China being an obvious place to look. In some ways, there is not even a lot of space for self-censure to apply – instead of being monitored, the access to quite a few websites is simply blocked, even before Xi Jinping's "Great Firewall of China", which heavily solidified these restrictions, with Chinese online space truly becoming a world onto itself.[21] But if we are to provide just one example, to tie in with the previously mentioned notion that the situation would be different if the respondents

[19] STUART, Avelie; LEVINE, Mark. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*. 2017, Vol. 47, p. 704

[20] PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal.* 2016, Vol. 31, No. 1, pp. 119-125, 159-161 and pp. 177-182.

were of a "stigmatised minority", we should not look any further than the situation of Uighur Muslims: of particular note to this topic being the language used by the people targeted (for example, disappeared people described as having "gone back home").[22]

6. CONCLUSION

Most of us (if by 'us' we mean the average user of social media in a democratic country) do not walk around constantly chilled by fear of what our everyday internet activity might mean for us, because there usually are not any actual consequences attached, imagined or real. Nevertheless, that does not mean we have to agree with the surveillance. It might make us uncomfortable, or "creeped out". We might be constrained by the expectations of our peers. We might oppose the scope of surveillance levelled at us, or the way already obtained data is handled. We might oppose having our privacy be at the whims of the free market (and we might even be right to do so),[23] but none of these really makes the chill, as it was first defined, set in – that comes with consequences. Neither the government nor the private companies that have access to our data care how often we listen to Britney Spears' hit song 'Toxic' at four a.m. Now, that might change – if Britney Spears were to poison the president of the U.S.A., the public opinion on her song would, most likely, shift – and while it still would not be (hopefully) illegal to listen to 'Toxic', the connotations around it would adjust – in response to an exogenous shock.

To conclude, aside from the notion that there maybe should be widerspread awareness of one's rights on the internet – privacy is valuable. For

[21] ECONOMY, Elizabeth C. The great firewall of China: Xi Jinping's internet shutdown. *The Guardian* [online]. Guardian News & Media Limited, published 29.6.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

[22] BUNIN, Gene A. 'We're a people destroyed': why Uighur Muslims across China are living in fear. *The Guardian* [online]. Guardian News & Media Limited, published 7.8.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/aug/07/why-uighur-muslims-across-china-are-living-in-fear

[23] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Vol. 1. Stanford, California: Stanford University Press, 2010, p.87.

us, as individual people, for our mental and social wellbeing, but it is also valuable for society, both as a collection of individuals, in which case it is certainly better that this collection of individuals was not made unwell by the strain of surveillance, and as a space in which we all come together, where we can (attempt to) come to a consensus, based on our personal experiences and our opinions, which we were able to form freely, without fear of persecution.

7. BIBLIOGRAPHY

[1] BUNIN, Gene A. 'We're a people destroyed': why Uighur Muslims across China are living in fear. *The Guardian* [online]. Guardian News & Media Limited, published 7.8.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/aug/07/why-uighur-muslims-across-china-are-living-in-fear

[2] ECONOMY, Elizabeth C. The great firewall of China: Xi Jinping's internet shutdown. *The Guardian* [online]. Guardian News & Media Limited, published 29.6.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

[3] KOOPS, Bert-Jaap; NEWELL, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom and Maša GALIČ. A Typology of Privacy. *University of Pennsylvania Journal of International Law 38(2): 483-575 (2017), Tilburg Law School Research Paper No. 09/2016*.

[4] MARDER, Ben; JOINSON, Adam; SHANKAR, Avi; HOUGHTON, David. The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking. *Computers in Human Behaviour*. 2016, Vol. 60.

[5] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. No. 1. Stanford, California: Stanford University Press, 2010.

[6] PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal.* 2016, Vol. 31.

[7] SHEPHERD, Katie. An artist stopped posting protest photos online to shield activists from police. Then, he was arrested. *The Washington Post* [online]. The Washington Post, published 3.8.2020 [cit. 1.11.2020]. Available at: https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/

[8] STUART, Avelie; LEVINE, Mark. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*. 2017, Vol. 47.

[9] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 31. 11. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

FREEDOM OF SPEECH VS. RIGHT TO BE FORGOTTEN: A COMPARISON OF EUROPEAN AND US PERSPECTIVE[1]

JANA KRČMOVÁ[2]

1. INTRODUCTION

One of the things that might be safe to say is that every internet user has heard 'Once you put it out on the internet, it'll be there forever!' or some variation thereof. It is a bit of a cliché. After all, we lose track of things on the internet all the time: servers shut down, once popular sites close, or an unexpected 'update' wipes everything you put there clean. But as children gain unrestricted access to the internet at an increasingly young age, often without much education to the tune of "Never give any of your personal information to anyone" and "Literally everyone on the internet, aside from yourself, is a 50 year old man just pretending to be a 12 year old girl" that older generations received (which, it has to be said, were quite a bit exaggerated, but they did their job of making people at least a little bit more cautious then they would have been otherwise).[3] Internet's memory, technological memory, does not function the way human memory does, it does not forget at the same rate or the same way – if it forgets at all. Embarrassing or ill-considered things once would have remained only in our parents' photo albums or our friends' stories, contained in a relatively small social circle. Even the most vicious gossip would not have much reach (if you were not already widely known, of course) and would disappear over time. Our personal data, freely floating across the internet (or downloaded or

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Rights of the data subject, Duties of the data controller. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Rights of the data subject, Duties of the data controller.

[2] Jana Krčmová je studentkou Právnické fakulty Masarykovy univerzity. Kontakt: 468555@mail.muni.cz.

[3] GREEN, Alex; WILKINS, Clare; WYLD, Grace; MANNING, Cliff. Keeping childern safe online. In: *London: New Philantrophy Capital.* [online] 2019, p. 32 [cit. 5. 12. 2020]. Available at: https://www.thinknpc.org/resource-hub/keeping-children-safe-online/

screenshotted etc.) for the rest of eternity is a daunting prospect.[4] In response to this, the right to be forgotten might come to mind. But what exactly is it? How does it work? And how does the right to free speech intersect with it?

2. FREEDOM OF SPEECH

2.1 EUROPEAN PERSPECTIVE (COUNCIL OF EUROPE/EU)

Under the European Convention on Human Rights, the protection of the freedom of expression can be found in Article 10, and includes "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".[5] Variations thereof can be found in written constitutions and bills of rights all across the globe – for example, it is expressed quite similarly in Article 11 of the Charter of Fundamental Rights of the European Union.[6] As is expressly stated in the European convention, this right protects the speaker as well as the listener. It protects not only the information itself but also the channels through which it is transmitted because the interference with means of transmission would doubtless impact the freedom of speech itself. The internet is currently an important conduit for the spread of information, whether in the hands of the traditional press, governmental or other organizations, or regular users, as the European Court of Human Rights states that 'user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression.'[7]

The importance of its protection is inarguable, on its own and in its' importance for the protection of other rights. It is vital for the basic function-

[4] POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* [online]. 2018, pp. 2-4 [cit. 5. 12. 2020]. Available at: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056

[5] Article 10 of European Convention for the Protection of Human Rights and Fundamental Freedoms, amended version. In: *European Court of Human Rights* [online]. Council of Europe [cit. 5. 12. 2020]. Available at: https://echr.coe.int/Documents/Convention_ENG.pdf

[6] Article 11 Charter of Fundamental Rights of the European Union, 12.12.2007. In: EUR-Lex [online]. Úřad pro publikace Evropské unie [cit. 5. 12. 2020]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

ing of democracy, and the personal development of every human being. This however does not mean that it is absolute and can never be restricted. On the contrary, freedom of expression clashes with other rights quite often: with the right to a fair trial, to conscience and religion, but that right to free speech seems to be in the best position to challenge is the right to privacy and the rights related to it – respect for private life, data protection, right to be forgotten etc., because, in some areas, they seem to directly oppose each other. But as with any conflict of protected rights, the balance must be struck according to each situation – no one right takes precedent automatically. The second paragraph of Article 10 of ECHR itself expresses that since the right "carries with it duties and responsibilities", it may be subject to restrictions.[8] Some forms of speech are always outside the protection provided by Article 10: hate speech, incitement to violence, holocaust denial and speech promoting the Nazi ideology.[9] Aside from this, the Court uses a three stage test to judge whether state interference is permissible: it has to be prescribed by law, pursue a legitimate aim, and be necessary for a democratic society.[10] Restriction of free speech in the Charter of Fundamental Rights of the EU functions similarly, as set forth in Article 52 paragraph 1. In paragraph 3, the Charter expressly states that 'the meaning and scope of those rights shall be the same as those laid down by the said Convention,' referring to the ECHR.[11]

---

[7] KULK, Stefan; ZUIDERVEEN BORGESIUS, Frederik. Privacy, freedom of expression, and the right to be forgotten in Europe. *Cambridge Handbook of Consumer Privacy* [online]. 2018, pp. 6-7 [cit. 5. 12. 2020]. Available at: https://www.researchgate.net/publication/320456033_Privacy_freedom_of_expression_and_the_right_to_be_forgotten_in_Europe

[8] BYCHAWSKA-SINIARSKA, Dominika. Protecting the Right to Freedom of Expression under the European Convention on Human Rights. A Handbook for Legal Practitioners. Council of Europe. 2017, p. 11-12. Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814

[9] BYCHAWSKA-SINIARSKA, op. cit., pp. 23-30.

[10] BYCHAWSKA-SINIARSKA, op. cit., pp. 32-33.

[11] EU Charter, Article 52.

2.2 US PERSPECTIVE

In the United States, protection of freedom of speech is guaranteed in the Bill of Rights, as the First Amendment states that "Congress shall make no law … abridging the freedom of speech, or of the press"'.[12] Though originating in the 18th century and thus preceding the original version of the European convention by nearly 200 years, its' intentions do not much differ, even if they are expressed considerably more succinctly. As Thomas I. Emerson writes, the necessity of functions of the First Amendment, for a liberal constitutional state, can be placed under four categories: individual self-fulfilment, means of attaining the truth, method of securing participation by the members of the society, including political, decision-making and lastly maintaining the balance between stability and change in society. Although articulated in 1961, these categories still ring true, but as he also states, the right to freedom of expression is not a new concept, and has changed before and must again, in response to different conditions and current problems.[13] Even as far as the late nineteenth century, in Warren's and Brandeis' "The right to privacy", concerns regarding the scope of the First Amendment with regards to the development of technology can be found.[14]

Unlike the ECHR, there is no provision to be found in the Bill of Rights concerning the limits of free speech – for that, we must look elsewhere, particularly to judicial decisions of the Supreme Court of the United States. Regarding specifically the issue of privacy, several important cases should be mentioned. In Cox Broadcasting Corp v. Cohn, the Supreme Court has ruled that a newspaper publishing company (Cox) could not be held liable for the dissemination of publicly available information (name of a deceased rape victim), basing this decision on public interest. In Smith v. Daily Mail Publishing, the newspaper was not found liable for the publication of the name of a juvenile murder suspect (obtained this time not from records

[12] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 5. 12. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

[13] EMERSON, Thomas I. Toward general theory of the first amendment. *Yale Law Journal.* 1963, vol. 72, no. 5, p. 878.

[14] WARREN, Samuel D., and Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*. 1890, vol. IV, pp. 193–220.

kept by the state, but by interviewing witnesses), the Supreme Court stated that an infringement on the freedom of the press would only be permissible if necessary to advance a state interest of "the highest order". A similar decision to Cox was reached in The Florida Star v. B.J.F., in which another victim of a sexual offence sought redress for the damage caused by her full name being published in connection to an ongoing case, with the perpetrator still at large, which led to her being harassed. The Supreme Court, citing public interest 'in the investigation of a violent crime', ruled in favour of the defendant. The definition of 'of public interest' in Supreme Court doctrine seems rather wide, covering a broad range, including dissemination of the sort of information that hardly seems actually relevant to the public – surely the public can be informed without putting the victim at risk.[15] Emerson in his article comments on the "unsatisfactory state" of the doctrine surrounding the first amendment, calling proponents of "absolute" interpretation of the Amendment impractical and proponents of balancing tests reductionist.[16] Leslie Kendrick, in her much more recent writing, criticises what she calls First Amendment opportunism and First Amendment expansionism and the abundance of different theories of application that surround it.[17]

3. RIGHT TO BE FORGOTTEN

3.1 EUROPEAN PERSPECTIVE (EU)

The right to be forgotten can be found in EU Regulation 2016/679, General Data Protection Regulation or as it is commonly known, the GDPR, as the right to erasure, with "right to be forgotten" in brackets. It allows for a subject to request the erasure of their personal data by the data controller, with the data controller being obliged to do so without further delay if one

[15] WERRO, Franz. The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash. *Liability in the Third Millenium*. 2009, pp. 293-297.

[16] EMERSON, op. cit., p. 877.

[17] KENDRICK, Leslie, First Amendment Expansionism. *56 WM. & MARY L. REV. 1199*. 2015, vol. 56, no. 4, pp. 1199-1220.

of the outlined conditions applies.[18] This version of the right to be forgotten is a considerable step back from the originally proposed version, which was widely criticised, with one of its' loudest critics being Peter Fleischer, chief privacy counsel of Google at the time, who outlined three categories of personal data that the proposed version covered, with each category being a greater threat to free speech than the one before it. The first category covers information that a person puts online themselves – in this category, being able to delete our own content is the norm and making this enforceable would be largely symbolic. The second covers content that people also posted themselves, which was then copied and posted by other users, which is more of a challenge to freedom of speech. The third category contains information posted about a person by a third party, which could also be deleted upon request if certain conditions were met. This would, Rosen argues, produce a chilling effect, leading data controllers to delete as requested even in ambiguous cases.[19] Although these arguments were made in regard to a never passed version of the right in question, similar suspicions follow the GDPR version as well, which is admittedly still a breakthrough, if not quite revolutionary. It draws from the concept of individuals' right to data self-determination and legislation of several European countries that include some sort of right to be forgotten, which usually pertains to individuals' criminal past, such as France's Right to Oblivion or Swiss 'die Persönlichkeitsrechte' (rights of the personality, which also include the right to be forgotten). Of particular interest is the ability of an individual to request the erasure of their data from every data controller, not only the first one, which aside from questions of law brings with it many technological challenges. As mentioned above, RtbF is surrounded by quite a bit of controversy, with solid arguments both for and against. There have been arguments for it as a human right, an expression of the broader right to

[18] Article 17 Regulation of the European Parliament and of the Council 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: EUR-Lex [online]. Publications Office of the EU [cit. 6. 12. 2020]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en

[19] ROSEN, Jeffrey. The Right to be Forgotten. *Stanford Law Review Online.* 2011/2012, vol. 64, pp. 88-92.

privacy, arguments for it as a right to identity, as an expression of a person's right to change themselves, or simply as a psychological necessity. It has been proposed that the RtbF is not intended as a tool or erasure but as more human sort of forgetting, which would allow some leeway in its' implementation. Its' opponents, as might be expected, argue against it as being unprecedently dangerous to the freedom of expression, as a tool of censorship, or as Rosen, warning of a possible chilling effect, or destroying the impartiality of search engines.[20]

3.2 US PERSPECTIVE

One of the things that all three cases listed under the section 'USA perspective' on freedom of speech have in common is that they concerned a clash between state legislation and a constitutionally protected right. That is the crux of the problem – while freedom of speech is guaranteed by the Bill of Rights, on the federal level, privacy rights in the USA are provided for primarily by the Privacy act of 1974, which does not account for current issues in privacy law. There have been attempts at change, particularly in the last decade, (the Consumer Privacy Bill of Rights in 2015, for example) but none have (so far) been successful.[21] As written above, the First Amendment has exhibited a tendency to stretch. As such, it seems that the RtbF is fundamentally at odds with the First Amendment and the theory surrounding it. This idea is expressed, for example, by R. G. Larson III, who argues that it would restrict people's decisions with regards to what they say and think, undermine the normal function of communication, limit "the degree to which people may participate in the marketplace of ideas", and, lastly but perhaps most importantly, 'grant the legislature a power best left to the people.'[22] Werro, on the other hand, argues that this position stems

[20] POLITOU et al., op. cit., pp. 11-12.

[21] SHARK, Alan. Is it time for a national Digital Bill of Rights? *FCW post* [online]. 1105 Media, Inc., published 28.1.2020 [cit. 6.12.2020]. Available at: https://fcw.com/articles/2020/01/28/comment-data-privacy-bill-of-rights-shark.aspx

[22] LARSON III, Robert G. Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech. *Communication Law and Policy*. [online]. 2013, vol. 18, no. 1, pp. 119-120 [cit. 5. 12. 2020]. Available at: https://doi.org/10.1080/10811680.2013.746140

from American distrust of centralised power and faith in the private sector and the power of the free market and free press.[23]

4. CONCLUSION

The right to be forgotten (the right to privacy in general) and freedom of speech are often put into too sharp an opposition, which is not necessary. Both rights, the right to privacy and the right to expression are vital to our freedom. We cannot give up privacy in pursuit of freedom of expression because privacy is necessary for the function of freedom of speech, and on the flip side, freedom of speech allows us to express opinions that were allowed to develop in privacy. Knowing that every ill-considered, ill-informed, foolish, misguided, or simply embarrassing thing we ever let loose on the internet is going to stay around forever is clearly not conducive to the freedom of expression, is it? Would that knowledge not cause a person to monitor much more closely what they share, constantly on the lookout for any even potentially incendiary expression of their opinions? Would this not lead to (self) censorship? Be the cause of the chilling effect?[24] An example: Jon Ronson in 'So you've been publicly shamed' describes a case of a woman who became the subject of a widely spread harassment campaign after posting a certain picture in which she was making a rude gesture in front of a monument for veterans. In particular, the book describes a process that a certain company uses to make the internet 'forget' certain information, which they accomplish by putting out great amounts of information about the person, which pushes the content the person wants to be hidden to the second page of Google search results (which might as well be the Deep Web). The content they put out is purposefully deeply bland – what shows she likes, what animals, all in the pursuit of erasing the internet's memory of the picture (which was meant as nothing more than an inside joke), which led to her being extensively harassed and to her losing her job.[25] This

[23] WERRO, op. cit., p. 299.

[24] POLITOU et al., op. cit., p. 12.

[25] RONSON, Jon. *So you've been publicly shamed.* 1st edition. London: Pan MacMillan, 2015, p. 321. ISBN 1594487138.

is surely not free speech in action, as intended. Now, this is not a call for the RtbF to function unchecked. Its' use must be considered in each case's specific circumstances (nature of the information, the person's status, the time passed). But perhaps we can reconsider our perspective on the issue – with these two rights not as opposites of each other, but as each being necessary for the function of the other.

5. BIBLIOGRAPHY

[1] GREEN, Alex; WILKINS, Clare; WYLD, Grace; MANNING, Cliff. *Keeping childern safe online* [online]. London: New Philantrophy Capital. 2019, [cit. 5. 12. 2020]. Available at: https://www.thinknpc.org/resource-hub/keeping-children-safe-online/

[2] POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* [online]. 2018 [cit. 5. 12. 2020]. Available at: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056

[3] European Convention for the Protection of Human Rights and Fundamental Freedoms, amended version. In: *European Court of Human Rights* [právní informační systém]. Council of Europe [cit. 5. 12. 2020]. Available at: https://echr.coe.int/Documents/Convention_ENG.pdf

[4] Charter of Fundamental Rights of the European Union, 12.12.2007. In: EUR-Lex [online]. Publications office of the EU [cit. 5. 12. 2020]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

[5] KULK, Stefan; ZUIDERVEEN BORGESIUS, Frederik. Privacy, freedom of expression, and the right to be forgotten in Europe. *Cambridge Handbook of Consumer Privacy* [online]. 2018, [cit. 5. 12. 2020]. Available at: https://www.researchgate.net/publication/320456033_Privacy_freedom_of_expression_and_the_right_to_be_forgotten_in_Europe

[6] BYCHAWSKA-SINIARSKA, Dominika. Protecting the Right to Freedom of Expression under the European Convention on Human Rights. A Handbook for Legal Practitioners. Council of Europe. 2017, Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814

[7] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 5. 12. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

[8] EMERSON, Thomas I. Toward general theory of the first amendment. *Yale Law Journal.* 1963, vol. 72, no. 5.

[9] WARREN, Samuel D., and Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*. 1890, vol. IV, s. 193–220.

[10] WERRO, Franz. The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash. *Liability in the Third Millenium*. 2009.

[11] KENDRICK, Leslie, First Amendment Expansionism. *56 WM. & MARY L. REV. 1199*. 2015, vol. 56, no. 4.

[12] Regulation of the European Parliament and of the Council 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: EUR-Lex [online]. Úřad pro publikace Evropské unie [cit. 6. 12. 2020]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en

[13] ROSEN, Jeffrey. The Right to be Forgotten. *Stanford Law Review Online.* 2011/2012, vol. 64.

[14] RONSON, Jon. *So you've been publicly shamed.* 1st edition. London: Pan MacMillan, 2015, ISBN 1594487138.

EU-UK DATA FLOWS IN POST-BREXIT TIMES[1]

KAREL PELIKÁN[2]

1. INTRODUCTION

We live in a highly globalized and connected world. Thus, in today's world, everybody relies on cross-border data flows, even the economy is built upon the free transfer of data. Expressed in numbers in 2014 data flows were worth $2.8 trillion of global GDP.[3] *"Globalization is a fact because of technology, because of an integrated global supply chain, because of changes in transportation, and we're not going to be able to build a wall around that,"*[4] Although I highly agree with the quote from the former United States (US) president Barack Obama, there is one wall that needs to be erected. The wall that is protecting the personal data flow. In my essay I will partly cover this topic, especially I will try to describe how Brexit will affect personal data flows between the United Kingdom (UK) and Europe.

2. PRE-BREXIT TIMES

For a better overview, I will shortly describe how the personal data flow between the UK and Europe looked like before Brexit. The UK's two first applications to join the EU in 1961 and 1963 were vetoed by the French. Finally, on 1 January 1973, the UK joined European Economic Community

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Trans-border data flow. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Trans-border data flow.

[2] Karel Pelikán je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 483377@mail.muni.cz.

[3] Cross-border data flow [online]. In: *bsa.org* [cit. 8. 1. 2021]. Available at: https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf.

[4] HELLMAN, Jessie. Obama: We can't 'build a wall' around globalization [online]. In: *The Hill.* 22. 7. 2016. [cit. 8. 1. 2021]. Available at: https://thehill.com/blogs/ballot-box/presidential-races/288887-obama-slams-trump-trade-ideas-we-cant-build-a-wall-around.

(now the European Union - EU).[5] A major change in the EU-UK relationship was the UK's EU membership referendum held on 23 June 2016, where most votes were for the option of leaving the EU. That triggered Article 50 of the Treaty of Lisbon and started the two-year period of the UK formally leaving the EU also called Brexit. It was expected that the UK will leave the EU on 29 March 2019, but due to the problems on UK's side extensions were granted by European Council, hence the UK finally on 31 January 2020 left the EU.[6]

Until 31 January 2020 UK was still a member state of the EU, hence the personal data flow was regulated primarily by the EU legislation. For the purpose of this essay, I will not cover the EU legislation on personal data before the General Data Protection Regulation (GDPR). The regulation was adopted in 2016 by the EU and was put into effect on May 25, 2018.[7] One of the purposes of the GDPR was to achieve a free flow of personal data within the EU internal market: *the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.*[8] Thus GDPR allowed a free personal data flow within the European Economic Area (EEA), which includes EU member countries and non-EU member countries such as Iceland, Liechtenstein, and Norway.[9] The above mentioned meant that there was free movement of personal data between the UK and the rest of EEA.

---

[5] When did Britain decide to join the European Union? [online]. In: *ukandeu.ac.uk*. 21. 8. 2020. [cit. 8. 1. 2021]. Available at: https://ukandeu.ac.uk/the-facts/when-did-britain-decide-to-join-the-european-union/.

[6] WALKER, Nigel. Brexit timeline: events leading to the UK's exit from the European Union [online]. In: *House of Commons Library*. 6. 1. 2021. [cit. 8. 1. 2021]. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-7960/.

[7] The History of the General Data Protection Regulation [online]. In: *edps.europa.eu* [cit. 8. 1. 2021]. Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[8] Regulation of the European Parliament and of the Council (EU) 2016/679 of 18 April 2018 on on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[9] International transfers of personal data [online]. In: *European Commission* [cit. 8. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en.

3. POST-BREXIT TIMES

After January 31, 2020 - the date the UK formally left the EU started a transition period. The transition period was set up in the revised Withdrawal Agreement that was agreed by the UK and EU in October 2019. This period spanned from January 31, 2020, until December 31, 2020. During this transition period, the GDPR continued to be applied in the UK. The UK National data protection authority - Information Commissioner's Office (ICO) stated that in the transition period it will not be necessary for organizations dealing with personal data to take immediate action such as additional safeguards.[10] Although the UK was not a member of the EEA, it has been treated as an EEA member during the transition period. That resulted in the free movement of personal data between the EEA and the UK in the transition period.[11]

Negotiations between the UK and the EU on future cooperation after Brexit in the transition period were tough and they took nine months. There was even a possibility of a hard Brexit, which would mean a no cooperation and trade agreement scenario. Finally, on 24. 12. 2020 the UK and the EU reached a comprise that lead to EU-UK Trade and Cooperation Agreement. The agreement is enormously huge it has more than 1000 pages and it covers areas such as fishing, dispute resolution, financial services etc. Most importantly for this essay, it somehow also covers the topic of data protection and data flow.[12] How is the EU-UK Trade and Cooperation Agreement going to affect the personal data flows between the UK and EEA? According to the agreement for the interim period of four to six months that started from 1 January 2021 the UK would not be treated as a third country. The benefits of not treating the UK as a third country in the

[10] SLINN, Benjamin., DE FONSEKA, Joanna. *Data Protection and Brexit* [online]. In: *Baker McKenzie* [cit. 8. 1. 2021]. Available at: https://www.bakermckenzie.com/-/media/files/insight/publications/2019/12/data-protection-and-brexit.pdf.

[11] MITCHELL, Ewen., SCHENKER, Sarah. C., Brexit: The Future of Data Flow to and from the EEA and the UK [online]. In: *GT London Law Blog*. 23. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.gtlaw-londonlawblog.com/2020/12/brexit-the-future-of-data-flow-to-and-from-the-eea-and-the-uk/.

[12] MORRIS, Chris. Brexit deal: What is in it? [online]. In: *BBC News.* 28. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.bbc.com/news/55252388.

interim period is that it is not necessary to have an adequacy decision for the UK or the organisations within the UK are not obligated to take a special safeguard based on article 46 of GDPR such as adequacy decisions, standard contractual clauses (SCC), binding corporate rules (BRC), certification mechanisms, codes of conduct, or so-called derogations. Another benefit is that this period gives the European Commission (EC) at least some time to finalise the adequacy decisions for the UK. The interim period will last for four months, but it can be extended to six months unless the UK or the EU will not raise an objection against the extension. There are two main conditions with which the UK must comply with. Firstly, UK is not allowed to change its legislation regarding data protection in the interim period. Secondly, the ICO cannot approve the transfer mechanisms or codes of conduct without permission from the EU-UK Partnership Council. The EU-UK Partnership Council is a body that oversees the EU-UK Trade and Cooperation Agreement and makes a recommendation regarding the functionality of the agreement. Furthermore, after the interim period, the UK is entitled to make changes in the data protection legislation in compliance with the fundamental principles of the GDPR and wider provisions of the EU-UK Trade and Cooperation Agreement. In the agreement, we can also find some commitments concerning personal data. For example, protection of the individuals from unsolicited direct marketing communications, sharing of passenger name records and vehicle registration information in the context of international travels or cooperation in the field related to criminal record information and DNA. Also, in the agreement, we can find the commitment to not restrict cross-border data flows for example by requiring data localisation. This will be under review and it will be evaluated within three years.[13]

From the above mentioned we know that in four or the maximum of six months the interim period will end and according to the GDPR the UK will be treated as a third country, thus according to the GDPR, a mechanism to

[13] BUNDY-CLARKE, Fiona. EU-UK Trade and Cooperation Agreement: Implications for data protection law [online]. In: *Data Protection Report*. 4. 1. 2021. [cit. 9. 1. 2021]. Available at: https://www.dataprotectionreport.com/2021/01/eu-uk-trade-and-cooperation-agreement-implications-for-data-protection-law/.

transfer data to third countries will be needed. As I mentioned above the GDPR offers a variety of mechanisms to transfer data to third countries.[14] The EC and the UK have decided to choose the adequacy decision. Based on article 45 of the GDPR: "*A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.*"[15] The adequacy decision is a multi-step process that includes a proposal from the EC, then also an opinion of the European Data Protection Board (EDB). There is also a need for approval from representatives of EU countries and finally, the decision must be adopted by EC. European Parliament (EP) and the European Council can request the EC to maintain, withdraw or amend the adequacy decision on the basis that its act exceeds implementing powers granted by GDPR. The adequacy decision allows the free movement of personal data from the EEA to a third country without any further safeguards.[16]

Is the adequacy decision an appropriate mechanism to transfer personal data to the UK? There is a certain level of uncertainty that arises from the Court of Justice of the European Union (CJEU) judgment in the Schrems II case. The case concerns the adequacy decision so-called the EU-US Data Protection Shield that enabled free movement of personal data from EEA to the US for organisations that were involved in it.[17] "*In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data*

[14] The EU Court of Justice invalidates EU-US Privacy Shield [online]. In: *dataprivacymanager-.net.* 21. 7. 2020. [cit. 9. 1. 2021]. Available at: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/.

[15] Article 45 of the regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[16] Adequacy decisions [online]. European Commission. [cit. 9. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[17] The CJEU judgment of 16th July 2020, C-311/18, Schrems II.

transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary."[18] This ruling set a high standard for adequacy decisions. It means that the level of protection must be essentially equivalent to that guaranteed within the EU by the GDPR. Based on this ruling the EU-US Data Protection Shield was invalidated.[19] The above mentioned could be a problem for the future adequacy decision for the UK because the current UK's security laws on data transfers are similar to the US ones and they grant UK's secret services quite invasive intelligence gathering powers. The US's security laws on data transfers and very powerful secrets services in term of intelligence gathering of personal data transfers were the key reasons why the EU-US Data Protection Shield was invalidated. Furthermore, according to the UK's national digital strategy, the government of the UK is planning to narrow some parts of its version of the GDPR.[20] The UK government stands before a tough decision. If they want to have an adequacy decision that would be the best data transfer mechanism from a business point of view, they will need to probably change their security laws on data transfers based on the Schrems II case.

To be precise the adequacy decision is not the only transfer mechanism to third countries, but it is the only one that does not need further safeguards mentioned in article 46 of the GDPR, hence it is the most welcome mechanism from a business organisation as it was already mentioned above. In case of no adequacy decision for the UK, the two best suitable transfer mechanisms are standard contractual clauses (SCC) and binding

[18] The EU Court of Justice invalidates EU-US Privacy Shield [online]. In: *dataprivacymanager.net*. 21. 7. 2020. [cit. 9. 1. 2021]. Available at: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/.

[19] The CJEU judgment of 16th July 2020, C-311/18, Schrems II.

[20] ARMINGAUD, Claude-Étienne; MCFADDEN, Noirin; PHIPPEN Keisha. What future for UK-EU data flows? [online]. In: *K&L Gates*. 28. 10. 2020. [cit. 9. 1. 2021]. Available at: https://www.klgates.com/What-Future-For-UK-EU-Data-Flows-10-28-2020.

corporate rules. The SCC can be described as an individual agreement that includes a contractual obligation on the side of the data exporter and importer and it also includes the rights of the individual whose personal data is being transferred. This safeguards GDPR data protection standards, and it is easy and fast to implement SCC in organisations.[21] According to the judgment in the Schrems II case, the SCC are a suitable mechanism for the transfer of personal data to third countries only if they guarantee a level of protection that is essentially equivalent to that guaranteed within the EU by the GDPR and if they are able to sufficiently protect from intelligence and security services to access such data. Another option for a data transfer mechanism is the binding corporate rules (BCR). The BCR can be described as internal rules that govern an international data flow within a multinational organisation. The implementation of BCR is very costly in time and money. Furthermore, it covers the data transfer just in a single organization.[22]

The future will show us how exactly Brexit will affect personal data flows between the UK and EEA. From the above mentioned we can assume that in 2021 an adequacy decision for the UK will be adopted by the decision of the EC, but there are some challenges that I also mentioned above. In an adequacy decision scenario, the change in personal data flows between the UK and the EEA would be almost none. In a non-adequacy decision scenario, the change to personal data flows between the UK and EEA would be pretty significant. There are two mechanisms - SCC and BCR that could be used in order to safeguard GDPR data protection standards. Both of them have some pros and cons, but in the case of the USA after the invalidation of EU-US Data Protection Shield the organisations started to use the SCC[23] and I think it would be the same in the case of the UK in non-adequacy decision scenario.

---

[21] Ibid.

[22] Ibid.

[23] *The EU Court of Justice invalidates EU-US Privacy Shield* [online]. In: *Dataprivacymanager.net.* 21. 7. 2020. [cit. 9. 1. 2021]. Available at: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/

.

4. BIBLIOGRAPHY

[1] HELLMAN, Jessie. Obama: We can't 'build a wall' around globalization [online]. In: *The Hill.* 22. 7. 2016. [cit. 8. 1. 2021]. Available at: https://thehill.com/blogs/ballot-box/presidential-races/288887-obama-slams-trump-trade-ideas-we-cant-build-a-wall-around.

[2] Cross-border data flows [online]. *bsa.org.* [cit. 8. 1. 2021]. https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf

[3] When did Britain decide to join the European Union? [online]. *ukandeu.ac.uk.* 21. 8. 2020. [cit. 8. 1. 2021]. Available at: https://ukandeu.ac.uk/the-facts/when-did-britain-decide-to-join-the-european-union/

[4] The History of the General Data Protection Regulation [online]. *edps.europa.eu.* [cit. 8. 1. 2021]. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[5] WALKER, Nigel. Brexit timeline: events leading to the UK's exit from the European Union [online]. In: *House of Commons Library*. 6. 1. 2021. [cit. 8. 1. 2021]. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-7960/.

[6] International transfers of personal data [online]. *European Commission.* [cit. 8. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

[7] Regulation of the European Parliament and of the Council (EU) 2016/679 of 18 April 2018 on on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)

[8] SLINN, Benjamin; DE FONSEKA, Joanna. *Data Protection and Brexit* [online]. In: *Baker McKenzie* [cit. 8. 1. 2021]. Available at: https://www.bakermckenzie.com/-/media/files/insight/publications/2019/12/data-protection-and-brexit.pdf.

[9] MITCHELL, Ewen; SCHENKER, Sarah. C., Brexit: The Future of Data Flow to and from the EEA and the UK [online]. In: GT London Law Blog. 23. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.gtlaw-londonlawblog.com/2020/12/brexit-the-future-of-data-flow-to-and-from-the-eea-and-the-uk/.

[10] MORRIS, Chris. Brexit deal: What is in it? [online]. In: *BBC News.* 28. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.bbc.com/news/55252388.

[11] BUNDY-CLARKE, Fiona. *EU-UK Trade and Cooperation Agreement: Implications for data protection law* [online]. In: *Data Protection Report*. 4. 1. 2021. [cit. 9. 1. 2021]. Available at: https://www.dataprotectionreport.com/2021/01/eu-uk-trade-and-cooperation-agreement-implications-for-data-protection-law/.

[12] *Adequacy decisions* [online]. In: *European Commission.* [cit. 9. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[13] The CJEU judgment of 16th July 2020, C-311/18, Schrems II, ECLI:EU:C:2020:559

[14] *The EU Court of Justice invalidates EU-US Privacy Shield*. In: *dataprivacymanager.net.* [online] 21. 7. 2020. [cit. 9. 1. 2021]. Available ar: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/

[15] ARMINGAUD, Claude-Étienne; MCFADDEN, Noirin; PHIPPEN Keisha. *What future for UK-EU data flows?* [online]. In: *K&L Gates*. 28. 10. 2020. [cit. 9. 1. 2021]. Available at: https://www.klgates.com/What-Future-For-UK-EU-Data-Flows-10-28-2020.

SMART HOME'S DATA, NEW GOLD VEIN?[1]

MARTIN ZMYDLENÝ[2]

1. INTRODUCTION

I am quite a huge fan of all kinds of modern solutions such as smart devices, the Internet of Things and smart homes. Even though I do not understand all (most) of the technical aspects of these things, I still consider myself as someone who knows and follows the newest trends. Well, except TikTok, that is something I just do not understand…

Nowadays, things which we never imagined are connected through the internet among themselves. Acquiring and collecting our data, which are then used by manufacturers of these devices to "improve" their customer services. Some companies collect and use more data than others. In the end, the customer, the house owner, mostly does not even know which data is collected, because we all know, how people "read" terms and conditions on the Internet. So lets find out why we love smart solutions and why we want our houses to become smart even though the disadvantage of losing privacy is enormous.

2. WHAT IS THE INTERNET OF THINGS (IOT) AND WHY IT IS IMPORTANT TO SMART HOMES?

In a nutshell, a smart home is an interconnected network of various devices based on the Internet of Things (IoT). When a lot of people hear about the Internet of Things, they think the IoT only includes "things." So, if we use the terminology of our Civil Code in section 489: *"A thing in legal terminol-*

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Smart everything. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Smart everything.

[2] Martin Zmydlený je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 405111@mail.muni.cz.

ogy is everything that differs from a human being and serves humans."[3] Quoting more legal definitions of things will not be necessary, it is mostly the same. Well except the definition from Roman law where, as a thing, were considered human slaves. The point is, in our legal knowledge we know "things" as things, stuff, belongings – inanimate objects. But in the terminology of the Internet of Things, the part of the network can be even humans or animals! *"A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network."*[4] This means people and animals can be a part of IoT, even though they aren't exactly things.

The whole ecosystem of IoT is growing and will be enormous including billions and billions of devices connected through various sensors or communication hardware. These devices will be collecting data about their users to improve enjoyment and benefits from using smart devices on the Internet of Things. IoT devices will share their collected data with other devices connected to the web and on behalf of acquired information, other devices will behave and act without the need of human assistance.

For example, when we run out of milk, the fridge will add milk to our shopping list on our smartphones. In another scenario the information about the need for milk can be sent to a delivery service like Rohlík.cz in the Czech Republic or to Amazon in the US and Jeff Bezos will send some of his drones[5] with the needed milk.

IoT should help us live and work smarter, and also help us have more time for our family, our hobbies by solving some of the easy tasks for us, maybe even without us noticing anything.

---

[3] Section 489 of the Act No. 89/2012 Sb., Civil code.

[4] GILLIS, Alexander S., Definition– internet of things (IoT), In: *IoT Agenda* [online]. [cit. 18. 6. 2021]. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[5] Amazon Prime Air [online]. [cit. 18. 6. 2021] Available at: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

2.1 FROM SMARTPHONE TO SMART HOME. FROM SMART HOME TO DUMB FOE?

Although it sounds pretty melodic, the smarter devices are, the dumber are people. If not dumber, we rely more on our smart devices than on our knowledge and skills. I can see it on myself, even if I drive a known route to my mother's home, I rather use GPS navigation on highways, because one can never know what can be ahead. My father never used GPS navigation back some 10 or 20 years ago, and we always found our final destination in Italy, Croatia and elsewhere. But now he also tends to use the navigation on his smartphone, because it is so much easier to follow a route on a smartphone's screen, which would recalculate a better route if something happened than to be stuck in a traffic jam on a highway for hours and then start looking in the map for a possible detour. Is it because we know less than before? No, it is not, we only got used to it and these devices make our lives easier so we use them.

I like the image of a man from probably the 80s or 90s standing with like 20 devices and the description: "*Everything in this picture is now in your pocket."* [6] We very quickly got used to our smartphones solving many of our troubles. We do not need a PC to surf the internet, we do not need a camera for photographs or videos, we even do not need tape measures for measuring or a spirit level. That and all others are in our smartphone and they work very well. (My shelves are in top horizontal shape, thank you iPhone). Due to the habit of using smartphones, smart homes do not seem like something new to us. It is just that we, as people, make another huge part of our life smarter and easier to use.

Technological giants like Apple with Apple HomeKit, Google Home from Google, Amazon's Alexa are now the most trending smart home ecosystems. Companies don't invent smart home ecosystems only to make the life of their customers easier. There is another reason. The numbers of smart homes differ, but there is one thing everyone agrees with and that is the value of smart home devices growing a lot and we are just only at the

[6] The described meme [online]. [cit. 18. 6. 2021]. Available at: https://imgur.com/gallery/NQvsYvd

beginning. The most expected scenario is around 12 - 16% of growth every year from USD 80,83 billion in 2019 to USD 207,88 by 2027.[7] Or USD 66,4 billion in 2019 to USD 175,98 billion by 2025.[8] In the year 2025, there should be around 300 million smart homes in the world. [9] It isn't only that people are lazier or less clever, but it is also caused by lower expenses[10] with acquiring smart home ecosystems and devices. A positive (or negative?) thing about various smart home ecosystems from different companies is the incompatibility among them. This means the companies would need to work together to find solutions for their devices to work on other platforms or we will end up with iDevices working only with Apple's HomeKit and Android devices running only on Google.

The benefits of using smart homes are tremendous and the mostly known. For example, all home devices can be managed by one device in one place. With smart cameras linked to the homeowners' phones, you can always keep an eye on your home. Energy efficiency with a smart thermostat, which will learn our schedule and lower the temperature when we aren't home and adds heat when we watch TV. Lights can turn off when we forget to turn them off and leave the house. The fridge, which can call Bezos's drones, can set the right temperature based on its fullness and type of goods stored in.

The other side of the coin is that all devices collect data and then share them among themselves which means big uncontrollable customers data flows. But where can that data go?

---

[7] Smart Home Market Worth $ 207.88 Billion, Globally, by 2027 at 13.52% CAGR: Verified Market Research. *In: prnewswire.com* [online]. [cit. 18. 6. 2021]. Available at: https://www.prnewswire.com/news-releases/smart-home-market-worth--207-88-billion-globally-by-2027-at-13-52-cagr-verified-market-research-301165666.html

[8] Statista: Smart Home worldwide – statistic [online]. [cit. 18. 6. 2021]. Available at: https://www.statista.com/outlook/283/100/smart-home/worldwide#market-revenue

[9] Ibid.

[10] Ibid.

3. SMART HOME'S DATA, NEW GOLD VEIN?

As I mentioned in the last part, data collected from smart devices in a smart home ecosystem will be tremendous. Because I am not an IT expert, I borrowed for describing various data collected by IoT devices from an IoT development company called Digiteum.[11]

First are status data. These data are about basic information like if a device is turned off or on. This is useful for overall planning for maintenance, decision-making and others. Status data must be paired with other IoT data otherwise they are worthless.

Location data are data known to everybody from our smartphones. Location data contains locations of devices and their movement.

Automation data. Type of data that helps IoT systems to control smart home devices, vehicles on the road and other moving objects in the IoT ecosystem. These data are crucial because if data from one device does not work perfectly, the whole ecosystem is at stake.

Actionable data are extensions of status data, but they do not only collect status data, but processes them and transform them into instructions. These data are often used for lowering energy consumption, efficiency optimization and are used for long-term decision-making.

The meaning of this little technical insert is that data from the IoT ecosystem of our smart home are diverse and can be very specific. Status data that track if a device is turned off or on, can look a little worthless. But if we consider these data can be collected e.g. from alarm device, then it is pretty valuable information.

Similarly with my favourite smart fridge. Information on how much milk we drink, the food we eat, is not valuable for most subjects. But if this information is used in a targeted advertisement by our ecosystem provider or a third party, it can be pretty valuable. Another thing is that governments can be curious about these data as well. In the US, which is the lea-

[11] How Does IoT Data Collection Work?. In: digiteum.com. [online] 13.2.2020 [cit. 18. 6. 2021]. Available at: https://www.digiteum.com/iot-data-collection/

ding market of smart homes,[12] there are already known cases, when the police obtained information from Amazon Echo to solve a murder, same as from FitBit.[13] Amazon's acquisition Ring is known for its cooperation with police, the doorbell company changed from "DoorBot" to a device surveilling the suburbs and partnering with the police.[14]

Yes, these scenarios help to solve crimes and the data from smart homes are used by a "third party" for common good, but it does not have to be that way…

4. CONCLUSION

In this essay, I tried to describe how we as a people rely on our smart devices and why we tend to also rely on our smart homes. What the possible benefits of smart homes are, but also what the main disadvantage of smart home is or rather the danger of smart homes. Collected data can help us to customize our smart homes, but the costs of possible data breach and data abuse are a real threat.

Collected data can be abused by a collector, the company with the smart home ecosystem. Or rather can be stolen by hackers. The government would also want to get our data for their own use.

Another problem I see with IoT and smart homes is the possibility of corrupting one device, which can lead to corruption of the whole ecosystem like if we get corrupted by some virus on our phone, we can infect the whole smart home and stolen data can be very crucial.

In conclusion, I would say smart homes will have a great positive impact on our daily lives, but we need to try to secure our collected data because problems associated with data breaches can be terrible.

---

[12] Statista: Smart Home worldwide – statistic [online]. [cit. 18. 6. 2021]. Available at: https://www.statista.com/outlook/283/100/smart-home/worldwide#market-revenue

[13] WHITTAKER, Zack. Many smart home device makers still won't say if they give your data to the government. In: *Tech Crunch* [online]. 11.12.2019 [cit. 18. 6. 2021] Available at: https://techcrunch.com/2019/12/11/smart-home-tech-user-data-government/

[14] HASKINS, Caroline. How Ring Went From "Shark Tank" Reject to a America's Scariest Surveillance Company. In: *vice.com* [online]. [cit. 18. 6. 2021] Available at: https://www.vice.com/en/article/zmjp53/how-ring-went-from-shark-tank-reject-to-americas-scariest-surveillance-company

5. BIBLIOGRAPHY

[1] Act No. 89/2012 Sb., Civil code.

[2] GILLIS, Alexander S., Definition– internet of things (IoT). In: *IoT Agenda* [online]. [cit. 18. 6. 2021]. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[3] Amazon Prime Air [online]. [cit. 18. 6. 2021] Available at: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

[4] Smart Home Market Worth $ 207.88 Billion, Globally, by 2027 at 13.52% CAGR: Verified Market Research, *In: prnewswire.com* [online]. [cit. 18. 6. 2021]. Available at: https://www.prnewswire.com/news-releases/smart-home-market-worth--207-88-billion-globally-by-2027-at-13-52-cagr-verified-market-research-301165666.html

[5] Statista: Smart Home worldwide – statistic [online]. [cit. 18. 6. 2021]. Available at: https://www.statista.com/outlook/283/100/smart-home/worldwide#market-revenue

[6] How Does IoT Data Collection Work? In: digiteum.com. [online]13.2.2020 [cit. 18. 6. 2021]. Available at: https://www.digiteum.com/iot-data-collection/

[7] WHITTAKER, Zack. Many smart home device makers still won't say if they give your data to the government. In: *Tech Crunch* [online].11.12.2019 [cit. 18. 6. 2021] Available at: https://techcrunch.com/2019/12/11/smart-home-tech-user-data-government/

[8] HASKINS, Caroline. *H*ow Ring Went From "Shark Tank" Reject to a America's Scariest Surveillance Company. In: *vice.com* [online]. [cit. 18. 6. 2021] Available at: https://www.vice.com/en/article/zmjp53/how-ring-went-from-shark-tank-reject-to-americas-scariest-surveillance-company

---

HUSOVEC, M.; MESARČÍK, M.; ANDRAŠKO, J.: PRÁVO INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ.

MICHAL ČERŇANSKÝ[1]

HUSOVEC, M.; MESARČÍK, M.; ANDRAŠKO, J.: Právo informačných a komunikačných technológií. Zv. 1. Bratislava: TINCT, 2020, 262 s. , ISBN: 978-80-973837-0-1

Pred niekoľkými týždňami obohatilo vydavateľstvo TINCT slovenský knižný trh s odbornou právnickou literatúrou svojim v poradí druhým vydavateľským počinom v podobe vysokoškolskej učebnice s názvom „Právo informačných a komunikačných technológií 1.“ Už samotná táto skutočnosť si zaslúži pozornosť a uznanie, nakoľko v podmienkach Slovenskej republiky ide vôbec o jednu z prvých publikácií, ktorá svojim obsahovým zameraním prináša študentom pohľad na problematiku IKT z hľadiska právnej úpravy platnej a účinnej na území SR.

Navyše - zloženie autorského kolektívu, ktorý tvoria mladí, no medzičasom mnohými skúsenosťami už „ošľahaní“ odborníci po stránke praktickej i pedagogickej, predstavovalo jeden z predpokladov nasvedčujúcich tomu, že recenzovaná publikácia bude z hľadiska vecnej stránky spracovaná adekvátne. No súčasne, pamätajúc na svojich primárnych adresátov – študentky a študentov práva, napísaná dostatočne zrozumiteľným jazykom, prostredníctvom ktorého bude učebná matéria podaná čitateľom „stráviteľným“ spôsobom tak, aby študenti nielen zvládli prípravu na postupové sk-

[1] JUDr. Michal Čerňanský, PhD., je advokátsky koncipient v advokátskej kancelárii PETKOV & Co s. r. o. so sídlom v Bratislave, e-mail: cernansky.m@gmail.com

úšky, ale pokiaľ možno otvárali publikáciu s radosťou zo štúdia a získavania nových poznatkov v predmetnej oblasti. Tento svoj zámer autori *expressis verbis* prezentujú v úvode publikácie, keď uvádzajú, že publikáciu pripravovali v snahe čo najlepšie vysvetliť, no súčasne študentov i nadchnúť pre fascinujúcu matériou práva IKT, a to okrem iného (či snáď lepšie povedané predovšetkým) prostredníctvom sprostredkovania zaujímavých prípadov z rôznych oblastí života, úvah a reflexii o fungovaní a poslaní práva v oblasti IKT.

Po prečítaní recenzovanej publikácie konštatujeme, že základný cieľ, ktorí si autori pri písaní publikácie stanovili, sa im, podľa nášho názoru, podarilo naplniť.

Publikácia predstavuje výborný učebný materiál, napísaný zrozumiteľným spôsobom, ktorý študentovi poskytuje najmä základné informácie zo siedmych autormi do publikácie zaradených tematických okruhov, tvoriacich samostatné, no pritom logicky usporiadané kapitoly, vzájomne tvoriace homogénny celok. Na druhej strane je potrebné podotknúť, že autori sa neobmedzili iba na suchopárne popísanie existujúceho právneho stavu. Pridanou hodnotou učebnice je, že vo veľkej miere sú v nej skutočne (podľa prísľubu autorov, ktorý dali čitateľom v úvode publikácie) obsiahnuté argumentačne podopreté úvahy o súčasnom stave technológií, o výhliadkach rozvoja technológií do budúcna, a s tým spojené právne problémy (reálne alebo hypotetické) s dopadom na život jednotlivca (na jeho práva a povinnosti) v súčasnej technologickej a informačnej spoločnosti.

Za hlavné piliere recenzovanej učebnice môžeme označiť:

1. textom celej učebnice prežarujúci zreteľ na základné práva a slobody jednotlivca z hľadiska medzinárodného, európskeho i slovenského ústavného poriadku v kontexte neustáleho prenikania a prítomnosti technológií v živote spoločnosti, a s tým spojené pozitívne i negatívne vplyvy naň.
2. bohatý aparát reálnych alebo do úvahy prichádzajúcich problémov na pomedzí práva a technológií v súčasnom svete, ktorý autori hojne na vhodných miestach v publikácii vo forme príkladov používajú. A to či už na uvedenie do problematiky, na bližšie vysvet-

lenie matérie alebo za účelom upozornenia na aplikačné či legislatívne nedostatky.

3. poukazy na výsledky súdnej praxe slovenských či zahraničných súdov a medzinárodných súdnych autorít (SDEÚ, ESĽP). V tomto smere je potrebné vyzdvihnúť, že text učebnice je doslova popretkávaný či už citáciami (neraz aj rozsiahlymi) zo súdnych rozhodnutí alebo odkazmi na relevantné rozhodnutia súdov a ich závery. Autori ako skúsení pedagógovia tak nepochybne urobili z dôvodu, že výučba má absolventov práva pripraviť do praxe, čoho predpokladom je oboznamovať študentov s výsledkami aplikácie práva, a tým ich primäť nielen čítať text ako právnik, ale i cibriť svoje vyjadrovacie schopnosti a právne myslenie, založené na argumentačných zdatnostiach. Na druhej strane - ako lepšie priblížiť študentovi preberanú látku, než prostredníctvom „príbehov" reálnych osôb, v ktorých museli orgány aplikácie práva vysloviť *quid iuris*?
4. multimediálny obsah nadväzujúci na obsah jednotlivých kapitol. Autori zaradili do každej z kapitol QR kód, po zosnímaní ktorého bude čitateľ presmerovaný na webovú stránku, na ktorej sú zverejnené odkazy predovšetkým na nadstavbové (bonusové) študijné materiály, relevantné právne predpisy, rozhodnutia súdov či dokonca videá, vďaka ktorým sa môžete dozvedieť napr. to, ako funguje internet.

Z hľadiska štruktúry učebnica pozostáva z úvodu a siedmych častí (kapitol), ktoré sú následne vhodne rozčlenené do podkapitol zameraných na čiastkové témy spadajúce do rámca tej-ktorej „hlavnej" kapitoly. Na konci každej z nich je zároveň súhrn desiatich otázok, ktoré majú nepochybne slúžiť ako podnety do diskusie v rámci výučbového procesu počas seminárov a cvičení.

V prvej kapitole s názvom „Právo, technológie a informačná spoločnosť" autori vovádzajú čitateľa do problematiky práva IKT najskôr vysvetlením základných pojmov ako sú „informačná spoločnosť" či „znalostná ekonomika", a to na podklade stručného historického exkurzu, vďaka ktorému sa

študenti budú môcť dozvedieť, že žijeme vo veku štvrtej industriálnej revolúcie, pre ktorý je charakteristická dennodenná interakcia medzi ľudstvom (spoločnosťou) a technológiami, a teda nevyhnutne aj medzi technológiami a právom, ako jedným zo základných spoločenských poriadkov regulujúcich život jednotlivca. Na príkladoch z každodenného života autori študentom približujú, ako technológie ovplyvňujú právo a *vice versa* – ako právo ovplyvňuje technológie. Kedy sú technológie a ich rozvoj cieľom práva (zabezpečenie technologického rozvoja) a na druhej strane, kedy sú technológie predmetom práva (regulácia technológií ako potenciálneho zdroja rizika). Autori v kapitole zoznamujú čitateľa i s vývojom vedy kybernetického práva od počiatku 90-tych rokov 20. storočia, vysvetľujú špecifickosť uplatňovania pravidiel v kyberpriestore, načrtávajú obsahový rámec a význam tzv. *lex informatica,* vovádzajú nás do architektúry internetu a približujú nám jeho charakteristické črty. V závere kapitoly je pozornosť venovaná špecifikám práva informačných technológií a jeho prameňov. Záujemcov o „bonusové" študijné materiály, ktoré autori čitateľom sprostredkúvajú prostredníctvom QR kódu kapitoly, určite potešia odkazy na pramene poznania, vďaka ktorým sa možno bližšie zoznámiť s myšlienkami Lessiga, Easterbrooka či Reidenberga.

Druhá kapitola s názvom „Právo duševného vlastníctva ako podpora technológií" ponúka metodologický základ k štruktúre práva duševného vlastníctva ako vednej disciplíny a odvetvia objektívneho práva, vysvetľuje jeho základné poslanie, no približuje aj jeho „trecie plochy" (limity) vo vzťahu k iným právam a slobodám. V druhej polovici kapitoly je pozornosť zameraná na softwareové právo, právo ochrany databáz a právo výrobcov databáz. Matéria je zo strany autorov podávaná erudovaným, no pre študenta príťažlivým spôsobom. To všetko najmä vďaka citáciám relevantných právnych predpisov a judikatúry ESD. Uvedené zabezpečuje, že študenti majú bezprostredný kontakt s právom v jeho normatívnej i kauzistickej podobe.

V poradí tretia kapitola publikácie nesie názov „Ľudské práva ako všeobecný limit technológií". Ide o jednu z kľúčových a zároveň najpútavejšie spracovaných častí publikácie. Autori v nej na podklade starostlivo zozbie-

ranej relevantnej judikatúry ESĽP a ESD skúmajú hranice využiteľnosti technológií v podmienkach demokratického právneho štátu patriaceho do zoskupenia Rady Európy. Upozorňujú na riziká spojené s uplatňovaním technológií v každodennom živote s dosahom na základné ústavné práva a slobody. Svoju pozornosť autori zamerali na mantinely (limity) reprezentované právom na ochranu súkromia, právom na ochranu osobných údajov (v tejto súvislosti špecificky venujú pozornosť nástrahám plošného zberu údajov, s ktorými sa v období pandémie COVID-19 musel popasovať i Ústavný súd SR a slovenský zákonodarca), právom na prístup k informáciám a jeho hraniciam, právom na slobodu prejavu, slobodou podnikania a inými. Mimoriadne podnetnou však bola záverečná časť kapitoly, ktorá bola zameraná na britské fiasko s maturitnými známkami udelenými zo strany škôl študentom na základe algoritmického rozhodovania o týchto známkach. Uvedená časť kapitoly nastoľuje zásadné otázky, ktoré majú významný dosah na spôsob aplikácie práva či už zo strany orgánov štátnej správy alebo súdov. Je možné, že stroje jedného dňa nahradia sudcu? Budú toho schopné v adekvátnom rozsahu? Alebo je to výlučne človek a jeho ľudský cit pre nachádzanie spravodlivosti, ktorý je v spoločnosti, aj napriek riziku justičných omylov, nenahraditeľný?

Vo štvrtej kapitole zamerali autori svoju pozornosť na digitálny trh v priestore EÚ a jeho princípy (princíp krajiny pôvodu, princíp zákazu cezhraničnej diskriminácie), sieťovú neutralitu či na otázky rozsahu zodpovednosti poskytovateľov služieb informačnej spoločnosti za vlastný i cudzí obsah a jednotlivým dôvodom vylúčenia zodpovednosti. V kapitole sú opäť významne zastúpené závery aplikačnej praxe, vo vzťahu ku ktorým autori vyjadrujú neraz i kritický postoj, odhaľujú a pomenúvajú nedostatky aplikačnej praxe a prezentujú vlastný pohľad na možný ďalší vývoj v tomto smere.

Piata kapitola je venovaná problematike doménových mien a rôznym modelom ich ochrany v rámci doménových sporov (výlučná súdna ochrana, kombinované modely ochrany, alternatívne modely ochrany). Za obzvlášť prínosné časti predmetnej kapitoly považujeme časti 5.3 a 5.4, v ktorých sú čitatelia oboznámení na podklade rozhodovacej činnosti EISi so systémom

ADR v oblasti doménových mien uplatňovanom na území SR, ako aj s jednotlivými druhmi prípadov, v ktorých dochádza (môže dochádzať) k porušovaniu práv viažucich sa k doménovým menám (klamlivé registrácie, parazitné registrácie, „kúp si ma“ registrácie, blokačné registrácie atď.).

Identita osoby v právnom štáte je prostriedkom, ktorý zabraňuje tomu, aby bol konkrétny jednotlivec postavený štátnou mocou do role objektu, v ktorej by sa stal púhym prostriedkom a bol by umenšený do podoby druhovo zameniteľnej veličiny. Technologický rozvoj spoločnosti so sebou priniesol novú, elektronickú podobu výkonu verejnej moci. Vďaka tomuto javu sa do popredia záujmu právnej vedy dostáva špecifická zložka právnej identity fyzických a právnických osôb – ich elektronická identita. Práve tej je venovaná predposledná (šiesta) kapitola recenzovanej publikácie. Okrem vymedzenia pojmov ako sú elektronická identita, identifikátor, atribút, identifikácia, autentifikácia či autorizácia, sa čitateľ môže oboznámiť so základmi úpravy elektronického podpisovania, s európskymi štandardami vzájomného uznávania prostriedkov elektronickej identifikácie, s cezhraničnou autentifikáciou alebo s dôveryhodnými službami.

Ako prezrádza názov poslednej, siedmej kapitoly recenzovanej učebnice - „Ochrana súkromia a osobných údajov“ - jej obsahovým ťažiskom je problematika ochrany osobných údajov fyzických osôb. Autori v nej reflektujú predovšetkým európsky rozmer právnej úpravy zameranej na ochranu osobných údajov, za kľúčový prameň ktorej možno v súčasnosti označiť GDPR. Po úvodnej časti, v ktorej autori vychádzajúc z modelového príkladu z bežného života ozrejmujú potrebu ochrany osobných údajov ako špecificky cenného druhu informácie o osobe v súčasnej spoločnosti (údaje vo všeobecnosti označujú ako „nové zlato“ v informačnej spoločnosti), nasleduje stručný exkurz do histórie právnej úpravy ochrany osobných údajov v európskom priestore. Autori prechádzajú od obdobia roku 1970, kedy bol na európskom kontinente prijatý vôbec prvý zákon o ochrane osobných údajov (hesenský Datenschutzgesetz), následne približujú legislatívne aktivity vo Švédsku, Francúzku či Nemecku, a na záver neopomínajú ani právotvorné procesy na pôde OECD, Rady Európy a Európskej únie od ich

počiatkov až po súčasnosť (GDPR, smernica EP a Rady č. 2016/680, nariadenie EP a Rady č. 2018/1725). V ďalšej podkapitole venujú autori pozornosť vzájomnému vzťahu medzi GDPR a slovenským zákonom č. 18/2018 Z. z. o ochrane osobných údajov, ako aj pôsobnosti GDPR:

1. prizmou teritória (miestna pôsobnosť). Na podklade príkladov vysvetľujú aplikačné pravidlá intrateritoriality a extrateritoriality GDPR.
2. prizmou subjektov (osobná pôsobnosť), pričom približujú čitateľovi pojmy ako prevádzkovateľ, sprostredkovateľ, dotknutá osoba či tretia strana.
3. prizmou matérie (vecná pôsobnosť), v rámci čoho vysvetľujú rozsah pozitívnej a negatívnej vecnej pôsobnosti GDPR.

Vysvetľujú základné pojmy ako sú spracúvanie, osobný údaj, citlivý osobný údaj a profilovanie. Autori v kapitole neobišli ani stručné a výstižné vymedzenie základných zásad GDPR ako primárnych interpretačných pilierov tohto predpisu, oboznamujú čitateľa so základnými povinnosťami prevádzkovateľov a sprostredkovateľov v súvislosti so spracúvaním osobných údajov, či so základnými právami dotknutých osôb a limitmi týchto práv. Pozornosť je tiež zameraná na problematiku cezhraničných prenosov osobných údajov. Autori nezabudli pojednať o štvorkrokovom teste pre cezhraničné prenosy, a prostredníctvom záverov prijatých na pôde ESD vo veciach Schrems I. a Schrems II. vymedzujú jeho kontúry a obsahové zložky. Záver kapitoly je venovaný problematike dozoru nad ochranou osobných údajov, sankčnému mechanizmu pri neoprávnenom spracúvaní osobných údajov a formám domáhania sa ochrany voči neoprávnenému spracúvaniu osobných údajov.

Záverom zdôrazňujeme, že autorom sa ich ciele, ktoré si stanovili v úvode recenzovanej publikácie, podarilo naplniť. Publikácia je vhodným učebným materiálom. No odporúčame, aby po nej siahli aj advokáti, sudcovia alebo príslušníci iných právnických profesií, ktorí budú mať záujem rozšíriť si svoje obzory, alebo z titulu svojho povolania budú vystavení potrebe získania informácií v danej oblasti. Vďaka štýlu, akým je publikácia

napísaná, ako aj vďaka množstvu citácií, odkazov a reflexií na závery aplikačnej súdnej praxe pôjde nepochybne o cennú pomôcku.

Autorom želáme do budúcna veľa energie, síl a entuziazmu pri ich snahách o rozvoj práva informačných a komunikačných technológií ako vedeckej a pedagogickej disciplíny.

---

https://doi.org/10.5817/RPT2021-1-4

CO NÁS ČEKÁ V PRÁVNÍ ÚPRAVĚ VYUŽÍVÁNÍ OBNOVITELNÝCH ZDROJŮ ENERGIE?[1]

JAN JENDŘEJAS[2]

ABSTRAKT

Zimní balíček legislativy EU v oblasti energetiky pod názvem „Čistá energie pro všechny Evropany" přináší na pole právní úpravy podpory využívání obnovitelných zdrojů energie řadu novinek. Díky němu tak po letech stagnace český zákonodárce zřejmě připraví řadu legislativních změn s potenciálem značně zamíchat českou energetikou. V první části tohoto článku se zabývám evropskou legislativou v této oblasti z pohledu podpory využívání obnovitelných zdrojů energie a rozebírám nové instituty energetického práva, kterým dá nová úprava vzniknout. V další části se pak věnuji české transpozici předmětného sekundárního práva, a to novele zákona o podporovaných zdrojích energie a věcnému záměru nového energetického zákona. Posuzuji splnění cílů stanovených unijní legislativou a zejména potenciál k výraznému navýšení podílu obnovitelných zdrojů energie na energetickém mixu a tím snížení negativních dopadů lidské činnosti na globální klima. Závěrem podrobuji navrhované změny kritickému hodnocení.

---

[1] Článek vznikl úpravou závěrečné části diplomové práce na téma Veřejnoprávní úprava využívání obnovitelných zdrojů energie v České republice, obhájené začátkem roku 2021 na katedře správního práva Právnické fakulty Univerzity Karlovy v Praze. Žádná část práce nebyla původně určena k samostatné publikaci, k té vedla až nečekaná změna podmínek uznání diplomové práce jako práce rigorózní. Pro dosažení publikovatelného formátu byly některé části textu zkráceny a došlo k úpravě použitých zkratek, aniž by bylo nutné do textu substantivně zasahovat. Rovněž byl doplněn úvod a závěr.

[2] Mgr. Jan Jendřejas je absolventem Právnické fakulty Univerzity Karlovy, pracuje jako advokátní koncipient v advokátní kanceláři Squire Patton Boggs, kontaktní e-mail: jendrejasjan@gmail.com.

KLÍČOVÁ SLOVA

obnovitelné zdroje energie, OZE, energetické právo, energetika, ukládání energie, energetický zákon

ABSTRACT

The winter package of EU legislation in energetics called "Clean energy for all Europeans" brings a number of novelties to the field of renewable energy sources' support legislation. Thanks to the package will apparently the Czech legislator, after years of stagnation, prepare a number of legislative changes with a significant potential to reshuffle Czech energetics. In the first part of this article I concern with European legislation in this area from a viewpoint of a support of renewable energy sources usage and I analyse new institutes of energy law, which will be introduced by the new legislation. In the next part I attend to the Czech transposition of the secondary law in question, i.e. to the amendment to the supported energy sources act and a white paper of a new energy act. I assess the fulfillment of goals set up by the legislation of the union and, in particular, a potential to increase significantly the share of renewable energy sources of the energy mix and therefore mediation of negative impacts of human activities to a global climate. Lastly, I subject the proposed changes to a critical evaluation.

KEY WORDS

renewable energy sources, RES, energy law, energetics, energy storage, the energy act

1. ÚVOD

Spory o společenský přínos využívání obnovitelných zdrojů energie („**OZE**“) se již před lety přesunuly z oblasti vědecké do oblasti ideologické. V dnešní kultivované debatě je jen velmi těžké popírat nutnost využívání OZE pro snížení dopadu lidské civilizace na Zemi a její ekosystémy, ač se o to stále poměrně značná část společnosti snaží. Nárůstu využívání OZE ale stojí v cestě i celá řada dalších překážek. Zcela legitimně je možné

hovořit o nedostatku potřebných finančních zdrojů a investic v této oblasti nebo technologických překážkách, jakými jsou zejména nedostatečná přenosová infrastruktura a neexistence efektivní technologie uchovávání energie. Řada překážek rychlejšího rozvoje OZE má ale svůj původ v právu. Turbulentní vývoj úpravy podpory OZE v letech 2008-2014 způsobil pokles zájmu investorů o působení na českém trhu s OZE. Právní jistota spojená se státní podporou využívání OZE v ČR utrpěla obrovskou ránu, ze které se bude ještě dlouho vzpamatovávat. Řada právně-administrativních překážek pak může bránit vstupu menších subjektů trh s energií z obnovitelných zdrojů. Právě tyto problémy je právo schopné adresovat a zmírnit, změna právní úpravy tak může mít obrovský vliv na faktický rozvoj v této oblasti. Zprostředkovaně pak navíc může právní úprava přispět i k překonávání ostatních zmíněných překážek rozvoje, nárůst právní jistoty povede k nárůstu objemu investic, který povede k investicím do infrastruktury a výzkumu. Zdá se tedy, že zkvalitnění právní úpravy v této oblasti by mělo být vysoko na seznamu priorit. V České republice se ale s tímto přístupem příliš často nesetkáváme.

Právní úprava podpory využívání OZE v České republice neprochází v posledních letech zrovna turbulentním vývojem. Z pochopitelných důvodů jí není věnována příliš velká pozornost zákonodárce či Ministerstvo průmyslu a obchodu, které má tuto oblast v gesci. Velké změny v této oblasti už jsou ale na cestě, ať už si jich politická reprezentace chce či nechce všímat. V tomto článku rozeberu ty nejspolehlivější indikátory změn, a to unijní legislativu, navrženou novelu zcela zásadního zákona č. 165/2012 Sb., o podporovaných zdrojích energie („**Zákon o PZE**“) a Věcný záměr nového energetického zákona[3] a posoudím, do jaké míry mohou vést k rozvoji využívání OZE v ČR a které části nové legislativy budou mít na skutečný rozvoj zásadní vliv.

[3] Ministerstvo průmyslu a obchodu. Věcný záměr energetického zákona. 2020. [online]. [cit. 2020-11-11]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBQLGLK0X („**Věcný záměr nového energetického zákona**“).

2. HYBATEL ZMĚN – ZIMNÍ BALÍČEK EVROPSKÉ LEGISLATIVY

V listopadu 2016 navrhla Evropská komise řadu legislativních změn v oblasti energetiky, které měly za cíl naplnit závazky z Pařížské klimatické dohody a umožnit a podpořit přechod z fosilních paliv na OZE. Pro osm legislativních změn přijatých v období mezi květnem 2018 a květnem 2019 se zavedl název Zimní balíček – čistá energie pro všechny Evropany. Legislativní změny zahrnují změnu Směrnice o energetické účinnosti,[4] Směrnice o energetické náročnosti budov[5] a zejména kompletní přepracování dvou zásadních směrnic a dvou nařízení zasahujících do oblasti OZE. Novými dokumenty jsou tak Nová směrnice o POZE,[6] Směrnice o společných pravidlech,[7] Nařízení o vnitřním trhu s elektřinou[8] a Nařízení o správě energetické unie.[9] Všechny legislativní změny v Zimním balíčku směřují k ambiciózním cílům v oblasti moderní energetiky – vysoké energetické účinnosti, decentralizaci výroby elektřiny a značné dekarbonizaci energetiky jako celku. Nastavených met nebude pro jednotlivé státy vůbec jednoduché dosáhnout. Celkové cíle v podobě zvýšení podílu OZE na hrubé spotřebě energie v EU na 32 % a úspor energie ve výši 32,5 % oproti stavu bez zásahů se pak z dnešního pohledu mohou zdát nesplnitelné. Rychlý rozvoj a dramatické snížení nákladů na investice do OZ v posledních letech

---

[4] Směrnice Evropského parlamentu a Rady 2012/27/EU ze dne 25. října 2012 o energetické účinnosti, o změně směrnic 2009/125/ES a 2010/30/EU a o zrušení směrnic 2004/8/ES a 2006/32/ES („**Směrnice o energetické účinnosti**“).

[5] Směrnice Evropského parlamentu a Rady 2010/31/EU ze dne 19. května 2010 o energetické náročnosti budov („**Směrnice o energetické náročnosti budov**“).

[6] Směrnice Evropského parlamentu a Rady (EU) 2018/2001 ze dne 11. prosince 2018 o podpoře využívání energie z obnovitelných zdrojů („**Nová směrnice o POZE**“)

[7] Směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU („**Směrnice o společných pravidlech**“).

[8] Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou („**Nařízení o vnitřním trhu s elektřinou**“).

[9] Nařízení Evropského parlamentu a Rady (EU) 2018/1999 ze dne 11. prosince 2018 o správě energetické unie a opatření v oblasti klimatu, kterým se mění nařízení Evropského parlamentu a Rady (ES) č. 663/2009 a (ES) č. 715/2009, směrnice Evropského parlamentu a Rady 94/22/ES, 98/70/ES, 2009/31/ES, 2009/73/ES, 2010/31/EU, 2012/27/EU a 2013/30/EU, směrnice Rady 2009/119/ES a (EU) 2015/652 a zrušuje nařízení Evropského parlamentu a Rady (EU) č. 525/2013 („**Nařízení o správě energetické unie**“).

nicméně naznačují, že i nereálně vypadající cíle mohou být v kombinaci s úpravami legislativního rámce v budoucnu dosažitelné. A současný přístup některých národních vlád včetně české, zase ukazuje, že bez ambiciózních závazných cílů nedojde v oblasti legislativy k výraznému posunu k moderní, čisté energetice.

2.1 NOVÁ SMĚRNICE O POZE

Zřejmě nejdůležitějším zdrojem budoucí české právní úpravy bude Nová směrnice o POZE. Z toho důvodu je vhodné hlouběji rozebrat nejpodstatnější povinnosti, které členským státům ukládá. Pro zachování stručnosti se budu věnovat pouze těm ustanovením, která dle mého názoru budou mít velmi významný dopad na českou právní úpravu využívání OZE.

Původní směrnice o POZE[10] nastavila závazný cíl pro podíl OZE na konečné spotřebě, a to jak pro celou EU, tak pro členské státy. Na tento přístup částečně navazuje nová verze, když stanovuje ambicióznější cíl pro celou EU. Původní návrh Komise z roku 2014[11] stanovil celkový cíl EU na 27% podíl, nicméně v dalším vývoji, zejména ve spojitosti s Pařížskou dohodou, byl nakonec tento cíl zvýšen na 32 %. Jednotlivé vnitrostátní příspěvky ke splnění tohoto cíle si pak stanoví členské státy ve svých integrovaných vnitrostátních plánech v oblasti energetiky a klimatu, jejichž pořízení ukládá Nařízení o správě energetické unie. To i v příloze II stanovuje nezávazný[12] vzorec pro výpočet vnitrostátního příspěvku konkrétního členského státu, který bere v potaz jak celkový cíl, tak cíl pro rok 2020, HDP na obyvatele, potenciál členského státu k výrobě energie z OZ a úroveň propojení elektroenergetické soustavy členského státu s ostatními.

Nová směrnice o POZE členským státům umožňuje pro dosažení stanovených cílů uplatnit režimy podpory. Těmi se rozumí jakékoliv nástroje,

---

[10] Směrnice Evropského parlamentu a Rady 2009/28/ES ze dne 23. dubna 2009 o podpoře využívání energie z obnovitelných zdrojů a o změně a následném zrušení směrnic 2001/77/ES a 2003/30/ES („**Původní směrnice o POZE**“).

[11] Evropská Komise. Zelená kniha. Rámec politiky pro klima a energetiku do roku 2030. COM/2013/0169.

[12] Na rozdíl od Původní směrnice o POZE, která stanovila cíle pro členské státy závazně. Čl. 3 odst. 1 Původní směrnice o POZE.

které podporují užívání energie z OZ, demonstrativně investiční pomoci, daňové pobídky, povinnost využívat energii z OZ, zelené certifikáty a samozřejmě přímá podpora cen, včetně výkupních cen a plateb bonusů (jako jsou české zelené bonusy),[13] které splní obecné a široké požadavky stanovené Novou směrnicí o POZE.[14] Členské státy pak mohou určité technologie vyřadit (omezit výběrová řízení), pokud by jejich užití vedlo k horším výsledkům například v oblasti dlouhodobého potenciálu technologie, diverzifikace nebo stability sítě.[15] Česká republika má tedy možnost silně omezit podporu např. pro fotovoltaiku, ale současně zachovat podporu pro jiné zdroje. Takové omezení může být obhájeno potřebou diverzifikace a stability sítě. Obecně by pravidla poskytování podpor měla vést k vysoké míře realizace projektů a platí pro ně obvyklé podmínky otevřenosti, transparentnosti, konkurence, nediskriminace a nákladové efektivity.[16] Tyto režimy podpory mohou být za určitých podmínek zpřístupněny i výrobcům nacházejícím se v jiných členských státech, případně pro elektřinu vyrobenou v jiných členských státech.[17] Z českého pohledu je velmi podstatný čl. 6 předmětné směrnice, který ukládá členským státům zajistit stabilitu finanční podpory. Členské státy musí zabránit takové revizi úrovně podpory nebo s ní spojených podmínek, která by měla *„negativní dopad na práva udělená v rámci uvedené podpory a podrýval ekonomickou životaschopnost již podpořených projektů.“*[18] Tato podmínka může Českou republiku omezit v možnosti opakovat pokusy o nápravu chyb při nastavení podpory, jakými bylo například zavedení solárního odvodu, recyklačních fondů nebo přísných kontrol tzv. překompenzace.

Členské státy se v určitých případech mohou dohodnout na statistickém převodu energie z OZ z jednoho státu do druhého.[19] To může být jeden ze

[13] Čl. 2 odst. 5 Nové směrnice o POZE.

[14] Podpora musí být *„poskytována otevřeně, transparentně, konkurenčně, nediskriminačně a nákladově efektivně.“* Čl. 4 odst. 4 téhož.

[15] Čl. 4 odst. 5 téhož.

[16] Čl. 4 téhož.

[17] Čl. 5 téhož.

[18] Čl. 6 odst. 1 téhož.

[19] Čl. 8 téhož.

způsobů, jak dosáhnout potřebného podílu, i když na něj reálné výsledky členského státu nestačí. Stejně tak je možné realizovat společné projekty, a to dokonce i s třetími zeměmi, ačkoliv je k tomu třeba splnění řady dalších podmínek.[20]

2.1.1 SPRÁVNÍ POSTUPY POD TLAKEM NOVÉ ÚPRAVY

Nová směrnice o POZE dále ukládá členským státům poměrně rozsáhlé povinnosti týkající se správních postupů a právních předpisů v oblasti veřejné správy. Mluví o povinnosti členských států zajistit přiměřenost a nezbytnost pravidel pro schvalovací postupy, vydávání osvědčení a povolení v oblasti využívání OZE tak, aby byla prováděna zásada „energetická účinnost v první řadě". Správní postupy mají probíhat rychle, na příslušné správní úrovni a za stanovených předvídatelných lhůt. Pravidla pak mají být objektivní, transparentní a přiměřená, nediskriminovat a zohledňovat specifika různých technologií, správní poplatky transparentní a odpovídající nákladům. A nakonec schvalovací postupy pro decentralizovaná zařízení a pro výrobu a skladování energie mají představovat menší zátěž a být zjednodušené.[21]

Značné požadavky klade v této oblasti Nová směrnice o POZE i na oblast územního plánování a regionální správní orgány. Tyto by měly již v rané fázi plánování počítat se začleňováním a zaváděním energie z OZ, včetně samospotřeby. Členské státy jsou pak povinny doporučit místním a regionálním správním orgánům, aby při plánování městské infrastruktury počítaly s vytápěním a chlazením využívajícím OZ, a dále konzultovaly s provozovateli sítě dopady svých energetických programů na rozvoj infrastruktury provozovatelů.[22]

Zajímavý je pokyn směrnice členským státům zavést vhodná opatření ve stavebních předpisech za účelem zvýšení podílu energie z OZ ve stavebnictví. Je-li to technicky, funkčně a ekonomicky proveditelné, mají stavební předpisy stanovit pro nové a důkladně renovované budovy požadavek vyu-

[20] Čl. 9-13 téhož.

[21] Čl. 15 odst. 1 téhož.

[22] Čl. 15 odst. 3 téhož.

žívání minimálního množství energie z OZ a umožnit dosažení tohoto požadavku pomocí dálkového vytápění a chlazení.[23] Tato opatření mohou být v ČR provedena například změnou vyhlášky č. 268/2009 Sb., o technických požadavcích na stavby, nebo mohou být přímo součástí nového stavebního zákona. Konkrétní podmínky pro stavby by potom byly určeny v rámci stavebního povolení, které již v tuto chvíli může stanovit požadavky mj. na ochranu životního prostředí.[24]

Podobným směrem jako Zákon o hospodaření energií pak míří Nová směrnice o POZE u veřejných budov. Ty by podle ní měly sloužit jako příklad, jde-li o nové nebo důkladně renovované budovy. Toho může být dosaženo splněním předpisů pro budovy s téměř nulovou spotřebou energie podle Směrnice o energetické náročnosti budov, nebo například uložením povinnosti využití střech těchto budov k instalaci zařízení na výrobu energie z OZ.[25]

Členským státům bylo též uloženo odstranit neodůvodněné překážky pro dlouhodobé smlouvy o nákupu elektřiny z OZ a usnadnit jejich přijímání.[26] To by mělo vést k usnadnění dlouhodobé spolupráce mezi výrobci elektřiny z OZ a velkými, průmyslovými odběrateli, která je v současné době komplikovaná.

Značný tlak je Novou směrnicí o POZE kladen též na povolovací řízení k výstavbě, modernizaci, provozu či připojení zařízení na výrobu energie z OZ k síti. Měla by být zřízena kontaktní místa, jejichž prostřednictvím bude probíhat celé řízení a žadatel nebude muset kontaktovat pouze jedno z nich. Všechny potřebné postupy má zahrnovat jedno řízení. Kontaktní místo k tomu poskytne žadateli veškeré nezbytné informace a transparentní poradenství a, bude-li to třeba, zapojí další správní orgány. Zpřístupní také *„manuál postupů pro zhotovitele projektů v oblasti výroby energie z obnovitelných zdrojů“* s důrazem na malé projekty a samospotřebitele. Směrnice

[23] Čl. 15 odst. 4 téhož.

[24] MACHAČKOVÁ, Jana, FIALOVÁ, Eva, KÝVALOVÁ, Miroslava, VÍCHOVÁ, Jitka, HOLENDOVÁ, Lenka, SMÍŠEK, Jaroslav. *Stavební zákon*. 3. vydání. Praha: Nakladatelství C. H. Beck, 2018, s. 862–863.

[25] Čl. 15 odst. 5 Nové směrnice o POZE.

[26] Čl. 15 odst. 8 téhož.

dále stanovuje poměrně krátké lhůty pro průběh celého povolovacího řízení včetně všech dalších relevantních řízení – dva roky pro elektrárny a jeden rok pro zařízení s el. výkonem nižším než 150 kW. Pro pouhou modernizaci stávajícího zařízení mají členské státy zajistit povolovací řízení zjednodušené s roční lhůtou.[27] Pro malá zařízení samospotřebitelů elektřiny a pilotní projekty s el. výkonem maximálně 10,8 kW pak směrnice dokonce nařizuje zavedení postupu pro připojení k síti na základě prostého oznámení (ohlášení). Během jednoho měsíce po oznámení bude moci provozovatel distribuční soustavy odmítnout daný bod připojení k síti nebo navrhnout jeho alternativu, bude-li mít opodstatněné obavy o bezpečnost nebo technologickou slučitelnost systému. Postup na základě ohlášení mohou členské státy zavést i pro zařízení s el. výkonem až do 50 kW, zachovají-li stabilitu, spolehlivost a bezpečnost sítě.[28]

2.1.2 SAMOSPOTŘEBITELSTVÍ JAKO NÁSTROJ ROZVOJE OZE

Nová směrnice o POZE se poměrně rozsáhle věnuje tématu samospotřebitelství. Samospotřebitelem elektřiny z OZ je takový konečný zákazník (tedy včetně podnikatelů bez ohledu na definici pojmu spotřebitel), který vyrábí elektřinu z OZ pro svou vlastní spotřebu a může ji ukládat nebo prodávat, nepředstavuje-li to jeho hlavní obchodní nebo profesní činnost.[29] Problematika samospotřebitelství není výjimečná evropskému právnímu prostoru ani energetice, zmiňuje se o ní i odborná literatura, operující s pojmem *„prosumer“*.[30] Samospotřebitelům poskytuje směrnice poměrně rozsáhlá práva, která navíc předchází oprávnění spotřebitele vůbec se samospotřebitelem stát. Směrnice navíc umožňuje samospotřebitelství jak individuální, tak prostřednictvím tzv. agregátorů, tedy jakýchsi sdružení spotřebitelů. Práva, která musí členský stát podle směrnice poskytnout, zahrnují například právo vyrábět, skladovat a prodávat elektřinu z OZ bez diskriminačních nebo nepřiměřených postupů a poplatků, instalovat a provozovat akumula-

[27] Čl. 16 téhož.

[28] Čl. 17 téhož.

[29] Čl. 2 odst. 14 téhož.

[30] JACOBS, Sharon B. *The Energy Prosumer*. In: Ecology Law Quarterly. [online]. 2016. [cit. 2020-12-06]. Dostupné z: https://scholar.law.colorado.edu/articles/709

ci elektřiny bez dvojích poplatků, obdržet případnou odměnu za elektřinu z OZ, kterou dodávají do distribuční soustavy a při tom všem si zachovat práva a povinnosti konečných spotřebitelů.[31] Zajímavá je povinnost členských států umožnit samospotřebitelům nacházejícím se v jedné budově společné zapojení do výroby, akumulace a prodeje elektřiny z OZ, stejně jako sdílení této elektřiny, a to bez dotčení síťových a jiných poplatků, odvodů a daní každého z nich.[32] Toto ustanovení by mohlo umožnit provoz výroben elektřiny z OZ v rámci společenství vlastníků jednotek i tam, kde by pro každého vlastníka zvlášť neměla výroba či akumulace elektřiny ekonomický smysl.

Členským státům je v tomto kontextu uloženo zavést rámec umožňující podporovat a usnadňovat rozvoj samospotřeby. Takový rámec musí řešit řadu otázek, jako například přístupnost samospotřeby pro nízkopříjmové nebo zranitelné domácnosti, neodůvodněné překážky pro financování projektů, neodůvodněné regulační překážky, pobídky pro majitele budov k vytváření příležitostí k samospotřebě pro nájemce, přístup samospotřebitelů k režimům podpory a podíl samospotřebitelů na nákladech na soustavu. Rámec by měl být zahrnut do integrované vnitrostátní politiky v oblasti energetiky a klimatu, jejíž české verzi bude věnován prostor níže.[33]

Se samospotřebitelstvím úzce souvisí další téma, kterým se Nová směrnice o POZE zabývá – společenství pro OZ. Tím je samostatný právní subjekt s dobrovolnou a otevřenou účastí, kontrolovaný členy, jimiž mohou být fyzické osoby, malé a střední podniky nebo místní orgány (i obce), a „*jehož hlavním účelem není vytváření zisku, ale poskytování environmentálních, hospodářských nebo sociálních společenských přínosů svým podílníkům nebo členům anebo místním oblastem, kde provozuje svou činnost.*“[34] Koneční zákazníci mají mít právo zapojit se do takového společenství při zachování svých práv a povinností jako konečných zákazníků a bez neodůvodněných nebo diskriminačních podmínek nebo postupů. Tato společenství budou moci vyrábět,

[31] Čl. 21 odst. 1 a 2 Nové směrnice o POZE.

[32] Čl. 21 odst. 4 téhož.

[33] Čl. 21 odst. 6 téhož.

[34] Čl. 2 odst. 16 téhož.

spotřebovávat, skladovat a prodávat elektřinu z OZ, a to i pomocí smluv o nákupu elektřiny z OZ, kterými se kupující zavazuje nakoupit tuto elektřinu přímo od jejího výrobce. Dále budou společenství oprávněna sdílet ve svém rámci energii, kterou sama vyrobí a vstupovat na vhodné trhy s elektřinou. Směrnice pak ukládá členským státům podobný rámec podpory jako v případě samospotřebitelství zavést i u společenství pro OZ, mimo jiné zahrnující i zajištění spolupráce provozovatele distribuční soustavy se společenstvími.[35]

I v kontextu vytápění a chlazení nastavuje Nová směrnice o POZE cíle v podobě zvýšení podílu energie z OZ. Zvýšení je i konkretizováno na 1,3 procentního bodu ročního průměrného zvýšení, případně 1,1 procentního bodu pro státy, které nevyužívají odpadní teplo a chlad. Směrnice pak demonstrativně vyjmenovává opatření, kterými mohou členské státy tohoto zvýšení dosáhnout, a ukládá státům zaměřit se na zajištění přístupnosti pro všechny spotřebitele, zejména nízkopříjmové a zranitelné domácnosti.[36] Ke zvýšení uvedeného podílu mají podle následujícího článku směrnice přispívat i soustavy dálkového vytápění a chlazení. Ten zavádí i mnoho dalších povinností členských států v souvislosti s dálkovým vytápěním a chlazením, které jsou spíše technického charakteru.[37]

Nová směrnice o POZE přináší i úpravu velmi diskutovaného a kontroverzního tématu biopaliv. Směrnice záměrně vyčleňuje biopaliva, biokapaliny a paliva z biomasy vyrobená z potravinářských a krmných plodin a stanovuje jim přísná omezení. Státy musí jejich užívání postupně snižovat, a do roku 2030 je úplně vyřadit.[38] Tato omezení jsou zdůvodňována nežádoucím rozšiřováním zemědělské půdy do oblastí s velkou zásobou uhlíku, tedy do lesů, mokřadů a rašelinišť, čímž dochází k uvolňování skleníkových plynů.[39]

[35] Čl. 22 téhož.

[36] Čl. 23 téhož.

[37] Čl. 24 téhož.

[38] Čl. 26 téhož.

[39] Recitál téhož, bod 81.

Určitý prostor je věnován OZ v odvětví dopravy. Členským státům je stanoven minimální podíl OZ na konečné spotřebě energie v tomto odvětví na 14 %.[40] S tím nicméně velmi úzce souvisí přísná kritéria udržitelnosti biopaliv. Biopaliva, biokapaliny a paliva z biomasy musí v první řadě splňovat stále se zpřísňující kritéria úspor emisí skleníkových plynů. Tato úspora musí být o to vyšší, čím později bylo zařízení, které je vyrábí, uvedeno do provozu. Postupně se dostane až na 80 %, a to u zařízení uvedených do provozu po 1. 1. 2026.

Dalším kritérium se vztahuje na biopaliva, která mají původ v odpadech a zbytcích ze zemědělské půdy. U těch musí provozovatelé nebo vnitrostátní orgány sledovat a zkoumat dopady na kvalitu půdy a uhlík v půdě. Dále pokračuje povinnost, kterou už pokrývá Původní směrnice o POZE, a to nezískávat suroviny pro výrobu biopaliv z půdy s vysokou hodnotou biologické rozmanitosti. Směrnice vyjmenovává, na kterou půdu konkrétně se toto označení vztahuje, například mezi ně patří původní les a zalesněné plochy obecně, kde nejsou viditelné známky lidské činnosti, biologicky rozmanitý les nebo travní porosty a tak dále. V dalším odstavci zapovídá směrnice získávání surovin pro výrobu biopaliv, biokapalin a paliv z biomasy z půdy s vysokou zásobou uhlíku, tedy již zmíněných mokřadů a souvisle zalesněných oblastí. Stejně tak nesmí být tyto suroviny získávány z rašelinišť. Biopaliva pocházející z lesní biomasy potom musí splňovat další kritéria týkající se těžby této biomasy (legalita těžby, obnova lesa, zachování kvality půdy a biologické rozmanitosti atd.). Země původu lesní biomasy také musí splňovat určitá kritéria, jako například být smluvní stranou Pařížské dohody apod. Elektřina z paliv z biomasy se potom zohlední ve statistikách pouze, vyrábí-li se v zařízeních vyhovujících určitým technologickým a výkonovým omezením.[41]

Z množství a složitosti kritérií pro využívání biopaliv, biokapalin a paliv z biomasy a jeho podporu je zřejmé, že se v současné době jedná o velmi složité téma a celkový přínos těchto OZE je značně rozporován. Negativní

[40] Čl. 25 téhož.

[41] Čl. 29 téhož.

dopady biopaliv na kvalitu půdy a uvolňování uhlíku do ovzduší jsou čím dál tím více znát a evropská legislativa to reflektuje.

Nová směrnice o POZE stanovuje ambiciózní cíle ve všech oblastech a značně zpřísňuje některá, již dříve uvedená kritéria. Její správná transpozice nebude pro ČR jednoduchá, ale hlavní výzva leží zejména ve způsobu dosažení cílového podílu OZE na konečné spotřebě energie. Současný vývoj nenaznačuje nástup razantní podpory, státních investic nebo prostředků umožňujících dosažení stanoveného cíle. Česká republika dokonce v některých aspektech aktivně odmítá cíl splnit, jak je vidět z finální verze Vnitrostátního plánu České republiky v oblasti energetiky a klimatu, ve kterém ČR ani neplánuje splnění cílů stanovených na evropské úrovni.[42]

Mnoho obsáhlých novinek a ambicióznost cílů stanovených Novou směrnicí o POZE, stejně jako Směrnicí o společných pravidlech si budou žádat přijetí rozsáhlé nové české právní úpravy. V tuto chvíli probíhá připomínkové řízení k věcnému záměru nového energetického zákona, vzhledem k absenci paragrafovaného znění by ale jeho hodnocení zde bylo předčasné. Zákonodárným procesem nicméně také prochází Novela zákona o PZE,[43] která je rozebrána níže.

2.2 SMĚRNICE O SPOLEČNÝCH PRAVIDLECH – UKLÁDÁNÍ ENERGIE, AKTIVNÍ ZÁKAZNÍCI A ENERGETICKÁ SPOLEČENSTVÍ

Ačkoliv v oblasti OZE není Směrnice o společných pravidlech zdaleka tak významná jako Nová směrnice o POZE, její přijetí a nutnost transpozice (ve většině do konce roku 2020)[44] povedou ke značným změnám v českém právním řádu, které na oblast OZE dopadnou. Směrnice je součástí Zimního balíčku, jehož příprava i přijímání byly velmi silně poznamenány snahou o posílení využívání OZE a dekarbonizaci energetiky.

---

[42] Bod 2.1.2 i. Vnitrostátního plánu České republiky v oblasti energetiky a klimatu.

[43] Poslanecká sněmovna Parlamentu České republiky. Sněmovní tisk 1121, Novela z. o podporovaných zdrojích energie – EU. 2020. [online]. [cit. 2020-11-11]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=6&t=1121 („**Novela zákona o PZE**“).

[44] Čl. 71 odst. 1 Směrnice o společných pravidlech.

Zcela zásadní novinkou je zavedení regulace ukládání energie a zařízení pro ukládání energie.[45] Už definice ukládání energie je významným krokem, neboť bude možné právně odlišit ukládání energie od výroby energie.[46] Díky tomu se ukládání energie bude moci stát samostatnou činností a tato oblast se stane obecně přehlednější. Problematika ukládání energie je pro rozvoj OZE naprosto klíčová, neboť řada OZE je sužována nepředvídatelnými výkyvy ve výkonu, způsobenými zejména změnami počasí. Některé oblasti jsou navíc pro výrobu energie z OZ vzhledem ke svým přírodním podmínkám vhodnější než jiné, kde ale může být vyšší poptávka. Tento problém je charakteristický zejména pro Německo, kde je větrný sever bohatě využíván k výrobě elektřiny ve větrných elektrárnách, spotřeba je ale výrazně vyšší v lidnatém jižním Německu, zejména Bavorsku a Bádensku-Württembersku.[47] Řešením těchto problémů je právě efektivní ukládání energie, mimo jiné i pomocí technologie power-to-gas, která by navíc usnadnila transport „energie" a snížila ztráty způsobené dálkovým přenosem elektřiny. Tato technologie zřejmě spadá do definice ukládání energie[48] a v kombinaci s vodíkovými plynovody by mohla přispět k řešení zmiňovaných problémů zejména větrné a solární energie.[49]

Z hlediska OZE je dále zajímavý článek pojednávající o aktivních zákaznících. S nimi velmi úzce souvisí problematika samospotřebitelství, které se

---

[45] Čl. 2 odst. 59 Směrnice o společných pravidlech definuje ukládání energie v elektrizační soustavě jako „*odložení spotřeby elektřiny na pozdější okamžik, než byla vyrobena nebo přeměna elektřiny na takovou formu energie, kterou lze ukládat, ukládání takové energie, a následná zpětná přeměna takové energie na elektřinu nebo použití jako jiný nosič energie.*"

[46] Z fyzikálního hlediska totiž ukládat energii, resp. elektřinu v tradičním slova smyslu nelze. Je možné ji přeměnit na jinou formu energie, jak to činí například přečerpávací elektrárny, kterou je možné později přeměnit zpět na elektřinu. Technicky vzato se ale jedná o spotřebu elektřiny a její následnou výrobu.

[47] SCHOLZ, Ulrich, ANTE, Johann. *Electricity regulation in Germany: overview*. In: Practical Law. [online]. 2021. [cit. 2021-02-22]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/5-524-0808?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

[48] FLEMING, Ruven. Clean or renewable – hydrogen and power-to-gas in EU energy law. In: *Journal of Energy & Natural Resources Law*. [online]. 20. 10. 2020. [cit. 2021-02-22]. Dostupné z: https://doi.org/10.1080/02646811.2020.1795382

[49] BENRATH, Daniel. Applicable law to hydrogen pipelines for energy purposes in Germany. *Journal of Energy & Natural Resources Law*. 2020, roč. 38, č. 1 s. 65.

věnuje Nová směrnice o POZE. Aktivní zákazníci mají podle Směrnice o společných pravidlech mít poměrně rozsáhlá oprávnění zahrnující prodej elektřiny vyrobené z vlastních zdrojů, účast na programech flexibility a energetické účinnosti, pověření třetí osoby správou potřebných zařízení apod. Současně by se na ně neměly vztahovat netransparentní nebo diskriminační síťové poplatky a aktivní zákazníci mají být finančně odpovědní za jimi způsobené odchylky v rámci elektrizační soustavy.[50]

Aktivní zákazníci mohou mimo jiné vlastnit zařízení pro ukládání energie, velmi významný nástroj pro širší využívání OZE, ale také zvyšování energetické účinnosti. S ohledem na tyto aktivní zákazníky stanovuje směrnice další povinnosti členských států. Spadají tam povinnosti odpovídající právu na připojení k síti v přiměřené lhůtě, vyvarování se jakémukoliv dvojímu zpoplatnění, neúměrným požadavkům a poplatkům za udělení licence a právo poskytovat souběžně několik služeb.[51]

Další podstatnou část úpravy tvoří článek o občanských energetických společenstvích. Směrnice o společných pravidlech stanovuje základní pravidla pro regulační rámec těchto společenství, tedy například jejich otevřenost a dobrovolnost, možnost vystoupení, udržení práv a povinností zákazníků v domácnostech, kteří se stanou členy společenství apod.[52] Stejně jako aktivní zákazníci mohou občanská energetická společenství hrát při navyšování podílu OZ na konečné spotřebě energie značnou roli, neboť zřejmě povedou k rozložení vysokých pořizovacích nákladů na zařízení sloužící k výrobě elektřiny z OZ na více osob. Tím mohou vést k jejich zpřístupnění výrazně širšímu okruhu osob, a to i osob bez většího finančního zázemí. Význam občanských energetických společenství pro rozvoj využívání OZE zmiňuje i recitál Směrnice o společných pravidlech, když mluví o komunitních energetických inciativách, které mají potenciál usnadnit zavádění nových technologií a značnou environmentální hodnotu.[53]

[50] Čl. 15 odst. 1 Směrnice o společných pravidlech.

[51] Čl. 15 odst. 5 téhož.

[52] Čl. 16 téhož.

[53] Bod 43 recitálu téhož.

Jak je zřejmé, Směrnice o společných pravidlech se věnuje oblasti OZE spíše okrajově. Poskytuje ale důležitý rámec opatřením obsaženým v Nové směrnici o POZE a je možné ji tedy přirovnat k českému energetickému zákonu a jeho významu v oblasti OZE.

3. ČESKÁ TRANSPOZICE – NOVELA ZÁKONA O PZE

Zákonodárce v tuto chvíli pracuje na transpozici rozebíraných norem přijatých v rámci Zimního balíčku. 20. 5. 2020 předložila vláda Poslanecké sněmovně Novelu zákona o PZE. Má-li být transpozice provedena v souladu s požadavky evropských předpisů, musí nabýt účinnosti nejpozději 30. 6. 2021. Mimo snadno rozpoznatelných cílů souvisejících s transpozicí směrnic sleduje Novela zákona o PZE i další cíl – udržení současných výroben elektřiny nejméně do roku 2030. Velké části z nich totiž okolo roku 2028 skončí doba provozní podpory, kterou v současné době čerpají. Vzniká tak riziko odstavování těchto výroben, které může způsobit značný pokles v podílu OZE na celkové konečné spotřebě energie. Je tedy nutné zavést taková opatření, která budou provozovatele předmětných zařízení motivovat k jejich dalšímu provozu. Podle důvodové zprávy k návrhu Novely zákona o PZE se jedná zejména o výrobny využívající biomasu a bioplyn, riziko odstavování fotovoltaických elektráren důvodová zpráva nezmiňuje.[54] Podle mého názoru by nicméně bylo vhodné zaměřit pozornost i na ně, přestože na rozdíl od výroben využívajících biomasu či bioplyn jsou náklady na jejich provoz zanedbatelné a riziko odstavování je tedy nízké. Kompletní odstavení zde sice spíše nehrozí, nicméně v průběhu životnosti fotovoltaických panelů dochází k poklesu jejich výkonnosti a některé panely mohou být během provozu poškozeny.[55] Z toho důvodu by bylo vhodné počítat i s poklesem výroby ze stávajících fotovoltaických elektráren a případně motivovat jejich provozovatele k modernizaci, což Novela zákona o PZE, zdá se, neřeší.

[54] Novela zákona o PZE, s. 71.

[55] LOMBARDO, Tom. *What Is the Lifespan of a Solar Panel?* In: engineering.com. [online]. 20. 4. 2014. [cit. 2020-11-11]. Dostupné z: https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/7475/What-Is-the-Lifespan-of-a-Solar-Panel.aspx

Při postupu paragrafovaným zněním vidíme, že Novela zákona o PZE přidává do podporovaných kategorií k elektřině a teplu také biometan, který dosud nebyl podporován podle Zákona o PZE a jehož podpora má být nástrojem k plnění cílů v oblasti dopravy. Novela zákona o PZE pak ve svém znění opouští cíl přispět k podílu energie z OZ v ČR a nahrazuje jej cílem přispět k tomuto podílu v EU.

Následují poměrně nevýznamné změny v definicích, například upřesnění, že za bioplyn se považuje také kalový a skládkový plyn nebo odstranění fikce povahy zemního plynu u biometanu. Další definice byly doplněny v důsledku přidání podpory biometanu. Dále byl vložen nový odstavec 2, který stanovuje mimo jiné definice zdroje elektřiny, palivového zdroje elektřiny, nepalivového zdroje elektřiny, referenční aukční ceny nebo aukčního bonusu, kterými je vhodné zabývat se podrobněji.

První tři pojmy týkající se zdrojů elektřiny souvisí s novým dělením na zdroje palivové a nepalivové. S tímto dělením je možné se setkat už dnes, když jej MPO využívá při kontrolách tzv. překompenzace, a je zřejmé, že bude nabývat na významu. Mezi nepalivové řadí zdroje využívající větrnou, solární, geotermální a vodní energii. Palivovými zdroji jsou pak ty, jež spalují biomasu, bioplyn nebo důlní plyn nebo využívají kombinovanou výrobu elektřiny a tepla. V české právní úpravě nepřekvapí, že toto dělení nemá původ v právu evropském, konkrétně ani v jedné ze směrnic, ze kterých Novela zákona o PZE vychází. Důvodová zpráva přímo nevysvětluje nutnost dělení zdrojů elektřiny na palivové a nepalivové, Novela zákona o PZE ale využívá toto dělení velmi často a jeho význam je značný. Jako příklad lze uvést určení rozsahu podpory pouze pro nepalivové zdroje, kdy podpora zdrojů palivových bude přesunuta do podpory tepla. Tento motiv prolíná celou Novelu zákona o PZE, kdy značná část změn vyplývá právě z přesunu podpory palivových zdrojů pod podporu tepla.

Dalším zajímavým definovaným pojmem je modernizace výrobny elektřiny. Tím se rozumí „*obnovení výrobny elektřiny zahrnující úplné nebo částečné nahrazení zařízení nebo provozních systémů a vybavení za účelem náhrady instalovaného výkonu nebo zvýšení účinnosti nebo instalovaného výkonu výrobny elektřiny.*“ Na rozdíl od předchozích pojmů se zde ale jedná o defi-

nici zcela přejatou z Nové směrnice o POZE.[56] Ta mimo jiné ukládá členským státům usnadnit modernizaci zařízení tím, že zajistí zjednodušené a rychlé povolovací řízení.[57] Novela zákona o PZE *prima facie* tento požadavek nereflektuje, spíše stanovuje podmínky, za kterých je možné poskytnout investiční podporu pro modernizaci výroben elektřiny apod.

U elektřiny i tepla Novela zákona o PZE stanoví požadavek maximálního stáří technologických celků pro nové a modernizované výrobny, které činí 5 let v den uvedení do provozu. Takovou podmínku již dnes stanovují cenová rozhodnutí Energetického regulačního úřadu („**ERÚ**"), nicméně vzhledem k jejímu dlouhodobému charakteru se ji zákonodárce rozhodl přesunout přímo do zákona.

3.1 DOČKÁME SE V ČECHÁCH ÚSPĚŠNÉHO ZAVEDENÍ AUKČNÍ PODPORY?

Nové definice pokračují v souvislosti s aukční podporou. Zavedení formy podpory v podobě aukcí je jedním z požadavků Nové směrnice o POZE, ale je možné se domnívat, že by zákonodárce zvolil tuto formu podpory i kdyby nemusel plnit závazky plynoucí z evropského práva. Jak ukazuje například studie organizace IRENA[58] již mnoho zemí organizuje aukce v oblasti OZE, které pomáhají snížit konečné ceny energie o desítky procent.[59] Novela zákona o PZE zavádí povinné aukce na podporu elektřiny z OZE pro všechny výrobny s výkonem vyšším než 1 MW s výjimkou větrných elektráren, kde limit činí 6 MW nebo 6 jednotek. V souvislosti s OZE je významná soutěž o tzv. referenční aukční cenu, kterou Novela zákona o PZE definuje jako cenu elektřiny nabízenou předkladatelem nabídky v aukci. Vyhlašováním aukcí bude pověřeno MPO za využití § 146 zákona č. 500/2004

[56] Čl. 2 odst. 10 Nové směrnice o POZE.

[57] Čl. 16 odst. 6 téhož.

[58] The International Renewable Energy Agency (IRENA) je mezivládní organizací sdružující 160 států a EU, jejímž hlavním cílem je zajišťovat spolupráci a výzkum a podporovat udržitelné využívání obnovitelných zdrojů energie.

[59] IRENA. *Renewable energy auctions: Status and trends beyond price*. Abu Dhabi: International Renewable Energy Agency. [online]. 2019. [cit. 2021-02-22]. Dostupné z: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Dec/IRENA_RE-Auctions_Status-and-trends_2019.pdf

Sb., správní řád, o řízení o výběru žádosti. Novela zákona o PZE stanoví přesné podmínky vyhlašování aukcí a konkrétní obsah vyhlášení aukce. Tato nová forma podpory může být žádaným stimulem pro rozvoj využívání OZE v ČR za výhodných podmínek blížících se tržním. Veškerá moc v této oblasti ale leží v rukou MPO, které tento ověřený nástroj může a nemusí využívat v závislosti na politické vůli představitelů vlády ČR. Sice je tedy možné, že nová úprava povede v této oblasti k rozvoji, ale rozhodně se nebude jednat o rozvoj bez dalšího.

3.2 ZMĚNY V PŘÍPRAVĚ KONCEPČNÍCH NÁSTROJŮ PODPORY OZE

Novela zákona o PZE dále v reakci na změny na evropské úrovni mění nastavení hlavního koncepčního dokumentu v oblasti OZ v ČR. Původní Národní akční plán se mění na integrovaný vnitrostátní plán v oblasti energetiky a klimatu. Ten musí vyhovovat požadavkům Nařízení o správě energetické unie a jeho první a druhá verze budou předmětem samostatné části. Jeho vypracováním je i nadále pověřeno MPO a schválením vláda.

Do téhož paragrafu přidává nicméně Novela zákona o PZE velmi významnou změnu, která bude zřejmě formovat reálnou podobu podpory využívání OZE v ČR do budoucna. Od 1. 1. 2021 bude totiž prakticky jakoukoliv podporu stanovovat vláda nařízením, a to zřejmě na ad hoc principu. Zákon o PZE tedy stanoví určitá pravidla, nicméně skutečnost se bude vždy odvíjet jen od politické vůle na straně vlády. Dá se tedy předpokládat, že vláda bude při rozhodování o podpoře brát v potaz zejména rozpočtové a jiné politické faktory, a vývoj v této oblasti je tak velmi náročné předvídat.

Novela zákona o PZE poté přidává ustanovení pro regulaci a kontrolu dosahování cílů podle vnitrostátního plánu a případné zastavení podpory, dojde-li k jejich překročení. Rovněž povinuje MPO ke zveřejnění předpokládané výše provozní podpory na další 3 kalendářní roky.

Jak bylo uvedeno, jedním z cílů Novely zákona o PZE je udržet současné výrobny elektřiny z OZ, kterým končí doba podpory před rokem 2030 v provozu. Z toho důvodu zavádí Novela zákona o PZE ustanovení o udržovací podpoře elektřiny. Tu Novela zákona o PZE koncipuje jako do-

rovnání rozdílu mezi provozními náklady při využití biomasy a fosilních paliv pro výrobu energie. To je logickou nápravou negativních externalit souvisejících s využíváním fosilních paliv tak, aby zůstal alespoň současný podíl výroby elektřiny z biomasy a výrobci se nevrátili k fosilním palivům. K tomu Novela zákona o PZE upravuje i případy, kdy dojde k úpravě či modernizaci výroben a stanovuje podmínky další podpory, která má provozovatele výroben k úpravám a modernizacím motivovat.

Novela zákona o PZE připravuje právní prostředí na kompletní opuštění systému podpory formou výkupních cen. Po nabytí účinnosti již bude možné čerpat podporu pouze formou zeleného nebo aukčního bonusu. Podporu formou výkupních cen by měly nahradit aukční bonusy. Hlavním rozdílem mezi aukčním a cenovým systémem podpory je způsob určení výše bonusu/výkupní ceny. Zatímco u výkupních cen stanovoval jejich výši každoročně ERÚ, výše aukčních bonusů má více tržní charakter a odpovídá nejvýhodnější nabídce potenciálního výrobce energie. Maximální výši aukčního bonusu či referenční aukční ceny stanoví podle Novely zákona o PZE MPO, čímž fakticky nahradí roli ERÚ při stanovování výše podpory OZE.

3.3 PODPORA TEPLA Z OZE

Zásadních změn po nabytí účinnosti Novely zákona o PZE nabyde podpora tepla z OZ. Již zmiňovaná podpora biometanu dostane v hlavě páté Zákona o PZE vlastní díl, kdy díl první bude věnován podpoře tepla s výjimkou biometanu.

Podpora výroby tepla zůstane po Novele zákona o PZE rozdělená na podporu provozní a investiční, kdy provozní podporu bude možné i nadále čerpat pouze formou zeleného bonusu. Podstatné změny přináší Novela zákona o PZE u podpory provozní, kde zpřesňuje podmínky jejího čerpání, ale zejména zavádí podmínku udržitelnosti pro paliva z biomasy, kterou v tuto chvíli známe zejména z oblasti biopaliv. Tato kritéria stanoví vyhláškou MPO, a to v souladu s příslušnými ustanoveními evropského práva. Nově pak bude přímo v zákoně uvedeno, že podpora se nevztahuje na teplo vyrobené spalováním odpadů, pro které se zákonodárce rozhodl podporu ne-

zavést. Investiční podpora tepla dozná pouze malých změn, kdy nejviditelnější je zrušení požadavků na transparentnost akciových společností.

Stejně jako u výroby elektřiny zavádí Novela zákona o PZE udržovací podporu i u výroby tepla. Konkrétní ustanovení jsou analogické k udržovací podpoře elektřiny a pouze reflektují specifičnost výrobu tepla, zejména s ohledem na konkrétní zdroje. Analogicky postupuje zákonodárce i u zeleného bonusu na teplo.

Další díl se bude nově věnovat výhradně podpoře biometanu. Podpora jeho výroby je analogická k podpoře tepla formou zeleného bonusu (jinou formou nebude podpora poskytována). Novela zákona o PZE stanoví rámcově podmínky na výrobu biometanu, kdy konkrétní požadavky například na jeho kvalitu, odorizaci nebo udržitelnost stanoví jednotlivé příslušné prováděcí předpisy (vyhlášky MPO). Výši zeleného bonusu na biometan bude stanovovat ERÚ podle pravidel určených Novelou zákona o PZE a prováděcím právním předpisem. Jak již bylo zmíněno, podpora biometanu je směrována zejména do sektoru dopravy, kdy Novela zákona o PZE dokonce stanoví, že pokročilý biometan (biometan vyrobený ze surovin stanovených vyhláškou MPO) lze uplatnit pouze v sektoru dopravy.

3.4 PŘIMĚŘENOST PODPORY – DALŠÍ BIČ NA FOTOVOLTAIKU?

Změny v oblasti financování podpor reflektují již rozebírané novinky, tedy podporu formou aukcí a podporu biometanu. Další změny jsou pak technického charakteru. Souvisí s nimi ale velmi zásadní legislativní novinky uvedené v následujících paragrafech, které se týkají přiměřenosti podpory energie z obnovitelných a druhotných zdrojů. Přiměřenosti podpor je věnována zvlášť velká pozornost, když dokonce důvodová zpráva k Novele zákona o PZE rozebírá tuto oblast na 22 stranách.

Přiměřenost podpory je pro Novelu zákona o PZE opravdu zásadní téma, které bylo zahrnuto z více důvodů, primárně ale souvisí s problémy s výpočtem podpory při solárním boomu, které byly rozebírány výše. V souvislosti s těmito problémy došlo k vydání zásadních rozhodnutí Komise týkajících

se slučitelnosti podpory OZE s vnitřním trhem EU.[60] Rozhodnutí mimo jiné zavazují Českou republiku k přijetí opatření určených na zajištění přiměřenosti podpory OZE v ČR, tedy zavedení procesů směřujících k zjištění, zda nedochází k tzv. překompenzaci a jejímu případnému odstranění. Pouze z rozhodnutí Komise SA.43451 (2015/N) vyplývají povinnosti zpětné kontroly poskytnuté podpory pro výrobny elektřiny z OZE uvedené do provozu v letech 2006-2012, tedy přímo v období solárního boomu. Za přiměřený rozsah návratnosti investic bylo určeno 6,3 % až 10,6 % a v případě, že z různých důvodů došlo k překročení tohoto rozsahu (typickým důvodem je snížení výrobních nákladů v návaznosti na výrazné snížení cen technologií), je nutné, aby české orgány přijaly opatření zajišťující snížení podpory, a dokonce v nutných případech i vrácení již vyplacených podpor. Aby bylo tomuto požadavku vyhověno, zavádí Novela zákona o PZE mechanismus prověření přiměřenosti podpory elektřiny. Pro účely prověření budou zavedeny hranice vnitřního výnosového procenta, od kterých bude podpora považována za nepřiměřenou. Zcela zásadní je tato hranice u výroben elektřiny využívajících energii slunečního záření, kde činí 6,3 %. Zde je nutné upozornit na fakt, že zmíněné rozhodnutí Komise SA. 40171 (2015/NN) mluví o vnitřním výnosovém procentu 6,3 % u fotovoltaických elektráren jako o spodní hranici přípustné návratnosti investice. Za nejvyšší přípustnou pak považuje 8,4 %.[61] Český zákonodárce tak značně přesahuje ukládaná opatření, aniž by vysvětloval, proč považuje návratnost do 6,3 % za dostatečnou a cokoliv mezi 6,3 % a 8,4 % za nepřiměřenou. Tento přístup se zdá být pro českého zákonodárce v oblasti OZE typický, když takříkajíc skáče po každé příležitosti k nápravě svých chyb z let 2006–2013, aniž by jakkoliv dbal o pokrok ve využívání OZE. Hranice 6,3 % až 8,4 % byly navíc navrženy českou stranou, když ještě v původním návrhu Novely zákona o PZE před zapracováním změn a schválením vládou bylo operováno právě s hranicí 8,4 %. MPO ale hranici 8,4 % považuje slovy minist-

[60] Rozhodnutí Komise SA.40171 (2015/NN) ze dne 28. listopadu 2016, SA.35177 (2014/NN) ze dne 11. června 2014, SA.43182 (2015/N) ze dne 22. srpna 2016 a SA.43451 (2015/N) ze dne 22. srpna 2016.

[61] Rozhodnutí Komise SA.40171 (2015/NN) ze dne 28. listopadu 2016, bod 46.

ra Karla Havlíčka za příliš vysokou.[62] Otázka zní, zda takto nízký výnos nebude pro některé výrobce energie likvidační, když vnitřní výnosové procento nebere v potaz cenu financování projektů, tedy úrokové sazby úvěrů poskytnutých na výstavbu fotovoltaických elektráren. Mohlo by tedy docházet k případům, kdy podle MPO přiměřená podpora nebude výrobci stačit ani k pokrytí nákladů a vzniklé provozní potíže povedou k soudním sporům nebo i komerčním arbitrážím proti České republice.

U ostatních zdrojů nebyla většinou hranice nastavena takto přísně, ale stále se nejedná o vysoká čísla, když nejvyšší hodnota přípustného vnitřního výnosového procenta dosáhla 10,6 % u výroben využívajících bioplyn. U větru, vody a geotermální energie se jedná o 7 % a u biomasy o 9,5 %. Stejná rizika jako u solární elektřiny tak zřejmě hrozí i u elektřiny větrné, vodní a geotermální.

Kontrola přiměřenosti podpory se nebude vztahovat na ty výrobce, jejichž výše podpory nedosahuje 200 000 EUR za tři kalendářní roky podle pravidla de minimis. Důvodová zpráva k Novele zákona o PZE uvádí i konkrétní hodnoty instalovaného výkonu elektráren vyrábějících z jednotlivých zdrojů, a to i s ohledem na rok uvedení do provozu. Pro ilustraci se u elektráren vodních jedná o 105 kW, u větrných 320 kW (u obou pro roky 2008–2015) a u solárních o 110 kW v letech 2006–2007 s vzestupnou tendencí až na 315 kW pro elektrárny uvedené do provozu v roce 2011.[63] Z toho lze dovodit, že kontrola nezasáhne pouze ty opravdu nejmenší výrobce.

Novela zákona o PZE zavádí pro kontrolu přiměřenosti podpory institut sektorového šetření. Sektory budou určeny prováděcím předpisem podle zdrojů elektřiny, roku uvedení do provozu, užitého primárního zdroje energie a výkonu. Šetření bude provádět MPO a jeho výstupem bude zpráva o provedeném sektorovém šetření, která bude obsahovat informaci o tom,

[62] ČTK. *Vláda schválila snížení podpory pro solární elektrárny*. In: *OEnergetice*. [online]. 27. 4. 2020. [cit. 2020-11-11]. Dostupné z: https://oenergetice.cz/elektrarny-cr/vlada-schvalila-snizeni-podpory-pro-solarni-elektrarny

[63] Poslanecká sněmovna Parlamentu České republiky. Sněmovní tisk 1121, Novela z. o podporovaných zdrojích energie – EU. 2020. [online]. [cit. 2020-11-11]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=6&t=1121

zda existuje riziko nadměrné podpory v daném sektoru, a pokud ano, tak o kolik zjištěná výše vnitřního výnosového procenta přesahuje příslušnou limitní hodnotu. MPO bude při šetření vycházet mimo jiné z informací povinně poskytnutých výrobci (technické a ekonomické údaje o výrobně elektřiny a jejím provozu). Neposkytnutí těchto informací bude přestupkem, za který bude možné uložit pokutu až do výše ročního nároku na podporu. Sektorové šetření tak přinese výrobcům další administrativní povinnosti, které rozhodně nebude v jejich zájmu ignorovat. Podle výsledku sektorového šetření pak ERÚ stanoví výši další podpory tak, aby celkově (za celou dobu životnosti zařízení) bylo dosaženo požadované hodnoty vnitřního výnosového procenta. Výrobci pak do dvou měsíců ode dne nabytí účinnosti předmětného cenového rozhodnutí ERÚ budou moci podat žádost o stanovení individuálních podmínek podpory, o které bude rozhodovat SEI a bude moci jejím prostřednictvím zmírnit případnou přílišnou tvrdost dopadu přijatých plošných opatření na konkrétní výrobce. Právě v těchto řízeních je možné očekávat velké množství sporů, které budou zřejmě předmětem soudních řízení podle soudního řádu správního.

Další velmi spornou oblastí je nově uvedená možnost zahájení řízení o stanovení podmínek podpory z moci úřední. V tomto řízení bude SEI mimo jiné oprávněna odejmout výrobci právo na podporu a uložit povinnost vrátit prostředky ve výši, ve které došlo k nadměrné podpoře. Řízení bude možné zahájit i v případě, že sektorovým šetřením nebylo zjištěno riziko nadměrné podpory, což je další z řady přísných opatření dopadajících na současné výrobce elektřiny z OZE.

Ačkoliv Novela zákona o PZE ještě neprošla legislativním procesem, už v tuto chvíli proběhla předběžné sektorová šetření pro zdroje uvedené do provozu v letech 2006–2008. Informace MPO žádalo od výrobců na dobrovolné bázi, i tak ale byla míra součinnosti zřejmě dostatečná, neboť se

MPO podařilo prověrku dokončit s konstatováním, že riziko nepřiměřené provozní podpory elektřiny z OZ nebylo v tomto sektoru zjištěno.[64]

4. VĚCNÝ ZÁMĚR NOVÉHO ENERGETICKÉHO ZÁKONA

Významné novinky uvedené Zimním balíčkem přináší mimo jiné i potřebu změn v Energetickém zákoně.[65] Jelikož ten ale prošel již velkou řadou novelizací (v tuto chvíli se počet už blíží třiceti), jeho struktura nevyhovuje požadavkům evropské právní úpravy a oblast energetiky se od přijetí Energetického zákona značně změnila, rozhodl se zákonodárce pro vytvoření nového energetického zákona. Věcný záměr nové úpravy zpracovalo MPO a předložilo jej v červnu 2020 do připomínkového řízení. To bylo ukončeno 14. 7. 2020 a v tuto chvíli je tedy očekáváno zapracování připomínek a začátek přípravy paragrafovaného znění.

Energetický zákon je jedním z nejvýznamnějších právních norem v oblasti využívání OZE, proto bude věcnému záměru níže věnován určitý prostor. Není však možné obsáhnout všechny navrhované změny a novinky, zaměřím se tedy jen na ty části, které mají největší dopad na využívání OZE v ČR a kvalitu transpozice dokumentů obsažených v Zimním balíčku. Velká část věcného záměru nového energetického zákona vychází ze Směrnice o společných pravidlech, jejíž hlavní body byly již předmětem stručného rozboru. Bude tak možné posoudit, jak se český zákonodárce vypořádává se svými závazky plynoucími z evropského práva.

Nová právní úprava má podle věcného záměru sledovat cíle, z nichž hned několik je možné považovat za úzce související s oblastí OZE. Cílem je mimo jiné příprava právního a regulatorního rámce pro nový model energetického trhu s důrazem na cíle v oblasti dekarbonizace, vypořádání se s prolínáním právních úprav uvedených v Zákoně o podporovaných zdrojích energie nebo transpozice Nové směrnice o POZE. Bohužel věcný záměr

[64] Odbor elektroenergetiky a teplárenství. *Prověření přiměřenosti podpory obnovitelných zdrojů energie uvedených do provozu v letech 2006 až 2008*. In: Ministerstvo průmyslu a obchodu. 30. 9. 2019. [online]. [cit. 2020-11-11]. Dostupné z https://www.mpo.cz/cz/energetika/elektroenergetika/obnovitelne-zdroje/provereni-primerenosti-podpory-obnovitelnych-zdroju-energie-uvedenych-do-provozu-v-letech-2006-az-2008--249308/

[65] Zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon)(„**Energetický zákon**“)

nezmiňuje dekarbonizaci, ochranu klimatu nebo přímo využívání obnovitelných zdrojů v rámci základních východisek navrhované právní úpravy, což připomíná například i ministr životního prostředí.[66]

4.1 VYKONAVATELÉ ČINNOSTÍ V ENERGETICE PODLE NOVÉ ÚPRAVY – SAMOSPOTŘEBITELÉ A ENERGETICKÁ SPOLEČENSTVÍ NA OBZORU

Zásadní změny by měl nový energetický zákon přinést v oblasti výkonu činností v energetice. Tím není míněno jen samotné podnikání, ale i různé neziskové činnosti nebo spotřebitelství. S novou koncepcí energetiky je totiž očekáváno, že se hranice mezi podnikateli v energetice a spotřebiteli budou do jisté míry rozostřovat a zejména na straně odběratelů dojde k významnému nárůstu aktivity. Získání licence jako oprávnění k podnikání v energetice by mělo být do budoucna zjednodušeno, a to v závislosti na druhu licence. Se změnami u spotřebitelů souvisí zavádění nových subjektů na trh s elektřinou – aktivního zákazníka a energetických společenství. Oba tyto typy subjektů jsou upraveny ve Směrnici o společných pravidlech a jejich průmět do českého práva si zaslouží bližší rozbor.

Pojem aktivního zákazníka navrhuje věcný záměr definovat jako zákazníka s možností aktivního působení na trhu s elektřinou. K tomu by měl nový energetický zákon poskytnout aktivním zákazníkům práva podle požadavků Směrnice o společných pravidlech pro vnitřní trh s elektřinou – prodávat elektřinu vyrobenou z vlastních zdrojů, provozovat zařízení pro ukládání energie, nepodléhat diskriminačním poplatkům a podobně. Ač je problematika ve věcném záměru popsána poměrně vágně, lze konstatovat, že hrubé obrysy vyhovují evropským požadavkům. Je pravděpodobné, že aktivní zákazníci budou tvořit důležitý segment trhu pro zvyšování podílu OZE na celkové konečné spotřebě elektřiny, a to zejména díky provozování malých „domácích“ výroben a zařízení pro ukládání energie. S pojmem aktivního zákazníka ale souvisí i pojem samospotřebitele, který byl rozebírán výše. Ačkoliv o něm jasně hovoří Nová směrnice o POZE,[67] věcný záměr ani

[66] Ministerstvo průmyslu a obchodu. Věcný záměr energetického zákona. 2020. [online]. [cit. 2020-11-11]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBQLGLK0X

[67] Čl. 21 Nové směrnice o POZE.

Novela zákona o PZE tento institut nijak nereflektují. To může být podstatné z hlediska budoucího nastavení podpor pro OZE, když se očekává, že právě samospotřebitelé budou častými žadateli o podporu v budoucích programech navazujících na program Nová zelená úsporám.

Věcný záměr nového energetického zákona také operuje s pojmem zranitelný zákazník. Tento pojem je zaváděn v návaznosti na Směrnici o společných pravidlech.[68] Ačkoliv zmíněná směrnice nechává definici zranitelného zákazníka do jisté míry na členských státech, je s podivem, jak úzce věcný záměr zranitelného zákazníka definuje. Směrnice hovoří o kritériích, kterými mohou být například výše příjmů, podíl výdajů na energii v rámci disponibilního příjmu, energetická účinnost domácností, kritická závislost na elektrických zařízeních ze zdravotních důvodů nebo věk. Věcný záměr si z těchto kritérií vybírá pouze jediné – kritickou závislost na zdrojích energie ze zdravotních důvodů. Konkrétně hovoří o těch zákaznících, jejichž životní funkce jsou závislé na odběru elektřiny, nebo který byl orgánem sociálního zabezpečení uznán invalidním ve třetím stupni a elektřinu nebo plyn využívá k vytápění.[69] Tato definice tak vůbec nezahrnuje například zákazníky s velmi nízkým příjmem nebo vysokým věkem. Český zákonodárce se tak do jisté míry snaží vyhnout problémům v některých oblastech, kde směrnice ukládají členským státům zajistit přístup i zranitelným domácnostem (například k samospotřebitelství či energetickým společenstvím).

Zákazníkům obecně potom věcný záměr nového energetického zákona přiznává určitá práva, která by mohla mít pozitivní vliv na rozvoj využívání OZE v ČR. Jsou jimi zejména právo na informaci o původu elektřiny, právo poskytovat podpůrné služby, provozovat vlastní náhradní zdroj, prodávat elektřinu vyrobenou z vlastních zdrojů nebo provozovat zařízení pro ukládání energie.[70]

Druhým zmíněným novým subjektem jsou energetická společenství, jejichž konkrétní atributy věcný záměr nového energetického zákona zmi-

[68] Čl. 28 Směrnice o společných pravidlech.

[69] Věcný záměr energetického zákona s. 81.

[70] Věcný záměr nového energetického zákona, s. 76.

ňuje. V první řadě by se mělo jednat o právnické osoby, které podle předmětných směrnic umožňují dobrovolnou a otevřenou účast, tedy možnost dobrovolně a bez omezení do společenství vstoupit i vystoupit. Konkrétní právní formu nechávají směrnice na členských státech, věcný návrh nového energetického zákona pak navrhuje téměř úplnou volnost výběru právní formy, pouze s několika výjimkami (právnické osoby nečlenského typu, tedy nadace a nadační fondy už z podstaty, dále společenství vlastníků jednotek, neboť účast v něm je vázána na vlastnictví jednotky, zřejmě opomenuto bylo bytové družstvo, které je nevhodné ze stejného důvodu). Pokud by taková úprava prošla legislativním procesem, umožnila by zakládání energetických společenství i například ve formě společností s ručením omezeným nebo komanditních společností. Zejména u těchto dvou forem je ale nutné s věcným návrhem polemizovat, neboť *prima facie* nesplňují požadavek otevřenosti členství, když podíly v těchto společnostech nejsou neomezeně převoditelné a není možné bez dalšího ze společností vystoupit.[71] Ze stejného důvodu se zdá naprosto jako naprosto nevhodná forma veřejné obchodní společnosti, která se navíc výpovědí společníka zrušuje.[72] Výhrady by bylo možné mít i k některým typům akciových společností a již zmíněnému bytovému družstvu. K tomu, aby česká právní úprava splnila požadavky, bude nutné zmíněné problémy adresovat a upravit další podmínky, například na specifická ustanovení zakladatelských právních listin energetických společenství. Jako vhodná se jeví forma spolku či družstva, které navíc vyhovují dalšímu z definičních znaků, kterým je zásadní neziskovost energetických společenství.

V souvislosti se ziskovostí zmiňuje zahraniční literatura i potenciální problém přílišné orientace energetických společenství nebo některých jejich členů na zisk či snižování nákladů na provoz a tím zvýšení vlastního zisku na úkor primárních cílů energetických společenství.[73] Těmi by měly být zejména poskytování environmentálních, ekonomických nebo sociálních vý-

[71] § 207 a násl., § 123 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech.

[72] § 113 odst. 1 písm. a) zákona č. 90/2012 Sb., o obchodních společnostech a družstvech.

[73] SOKOŁOWSKI, Maciej M. Renewable and citizen energy communities in the European Union: how (not) to regulate community energy in national laws and policies. *Journal of Energy & Natural Resources Law*. 2020, roč. 38, č. 3 s. 6.

hod členům. Je tak doporučováno v právní úpravě jednoznačně odlišit vytváření či prohlubování zisku od poskytování výhod, a dále vyloučení entit orientovaných na zisk z oblasti energetických společenství. Toho lze dosáhnout například již zmíněnými požadavky na obsah zakladatelských právních listin.

Věcný záměr nového energetického zákona pak upravuje energetická společenství pouze v oblasti elektroenergetiky, což zřejmě odpovídá požadavkům evropského práva. Nicméně Ministerstvo životního prostředí navrhuje jít dál a umožnit vznik těchto subjektů i pro plynárenství a teplárenství.[74] S touto připomínkou je možné souhlasit, neboť zahrnutí výroby tepla nebo využití plynu (zejm. bioplynu) do činnosti energetických společenství by mohlo mít pozitivní vliv na využívání OZE, například kombinovanou výrobou elektřiny a tepla z biomasy nebo bioplynu.

Správné zavedení institutu energetických společenství může mít obecně velký pozitivní dopad na energetický sektor ČR. Je ale nutné překonat některé problémy, které mohou bránit vzniku těchto společenství. Hlavní jsou překážky jak v samotném vzniku společenství, tak ale zejména v zahájení provozu společenství, spojené často s připojením do sítě. Před tím varuje zahraniční literatura a klade důraz na možnost připojení do sítě na základě pouhého jednoduchého ohlášení, jak implikuje i Nová směrnice o POZE.[75] Zatím zůstává otázkou, jak konkrétně se k tomuto problému český zákonodárce postaví. Ve věcném záměru se totiž zatím omezuje jen na fráze o zajištění nediskriminačního přístupu na trh a zacházení při výkonu jejich činnosti, práv a povinností. Na konkrétní podmínky vstupu na trh a činnosti energetických společenství si tak zřejmě budeme muset počkat na paragrafované znění nového energetického zákona.

[74] Body 7, 16 a 18 připomínek Ministerstva životního prostředí k Věcnému záměru energetického zákona.

[75] SOKOŁOWSKI, Maciej M. Renewable and citizen energy communities in the European Union: how (not) to regulate community energy in national laws and policies. *Journal of Energy & Natural Resources Law*. 2020, roč. 38, č. 3 s. 1.

4.2 JAK SE NOVÝ ENERGETICKÝ ZÁKON POPASUJE S UKLÁDÁNÍM ENERGIE?

Věcný záměr dále zcela správně upozorňuje na problém chybějící právní úpravy v oblasti ukládání energie, který se po vzoru Nové směrnice o POZE pokouší řešit. Nově by mělo být ukládání energie definováno jako samostatná činnost, což by mohlo a mělo vést ke zvýšení atraktivity ukládání energie a jeho zpřístupnění širším vrstvám adresátů právní úpravy. Český zákonodárce jde ve věcném záměru cestou poněkud užší definice ukládání energie, než jaká se objevuje ve Směrnici o společných pravidlech.[76] Věcný záměr argumentuje tím, že širší pojetí definice uvedené ve zmíněné směrnici by mohlo zahrnovat i taková zařízení, která nemá český zákonodárce v plánu regulovat. Jako příklad uvádí bojlery. Jazykovým výkladem ustanovení čl. 2 odst. 59 Směrnice o společných pravidlech bychom opravdu mohli dojít k tomuto poněkud absurdnímu závěru, i když představa ukládání elektrické energie pomocí teplé vody je přinejmenším úsměvná.

V návrzích jednotlivých opatření, které by se měly promítnout do paragrafovaného znění, byly z definice zařízení pro ukládání elektřiny výslovně vyňaty přečerpávací vodní elektrárny. Na jednu stranu je tento krok pochopitelný, neboť i do užší definice by přečerpávací vodní elektrárny zřejmě spadaly. Na druhou stranu se ale z téhož důvodu jedná o značné omezení budoucího podnikání v oblasti ukládání energie. Přečerpávací vodní elektrárny totiž spíš svým charakterem často připomínají spíše baterie a jiná zařízení k akumulaci energie než běžné elektrárny. Bylo by tedy možné si představit situaci, kdy vlastník přečerpávací vodní elektrárny je pouhým provozovatelem zařízení k ukládání energie a sám „novou“ elektrickou energii nevyrábí. Vynětí přečerpávacích vodních elektráren z definice zařízení pro ukládání elektřiny ovšem tuto variantu znemožňuje. Je možné se domnívat, že tak MPO, potažmo český zákonodárce, činí záměrně, neboť množství elektrické energie, které jsou přečerpávací vodní elektrárny schopny akumulovat, v tuto chvíli násobně převyšuje jakákoliv jiná zařízení pro ukládání energie. Vynětí přečerpávacích vodních elektrá-

[76] Čl. 2 odst. 59 Směrnice o společných pravidlech.

ren do samostatné úpravy, případně pouhé zařazení mezi výrobny elektřiny by pak mohlo poskytovat určitou vyšší míru ochrany, neboť na ně může být aplikován vyšší standard nároků, který směřuje „běžné“ výrobny elektřiny. V případě samostatné právní úpravy by pak bylo možné k přečerpávacím vodním elektrárnám přistupovat specificky. Do budoucna ovšem považuji takové úvahy za nevhodné, neboť žádný zákonodárce nedokáže odhadnout možnost růstu kapacit zařízení pro ukládání energie a také požadavků na ně. Přečerpávací vodní elektrárny by se navíc za předpokladu poklesu pořizovacích nákladů technologií mohly stát žádaným a efektivním způsobem ukládání elektrické energie. Takový pokles jsme už v historii mohli pozorovat například v oblasti solární energie, což nám umožnilo i ověřit schopnost českého zákonodárce na něj včas reagovat. Zde by vyloučení přečerpávacích vodních elektráren z definice zařízení pro ukládání energie mohlo mít za následek nežádoucí omezení trhu a snížení konkurenceschopnosti České republiky v oblasti akumulace energie, v hypotetických extrémních případech i ohrožení stability sítě.

Věcný záměr nového energetického zákona nám poskytuje jistý náhled do priorit českého zákonodárce a způsobu reakce na unijní legislativu. Výraznější než obsah je ale samotná existence věcného záměru a průběh legislativního procesu. Mnoho problémů adresovaných věcným záměrem sužuje českou energetiku už řadu let, legislativa navíc značně zaostává za rozvojem technologií. Skutečnost, že jsou nutné legislativní změny stále pouze ve fázi věcného záměru zákona ukazuje, že modernizace energetiky není pro českého zákonodárce v tuto chvíli prioritou. Vzhledem k blížícímu se konci lhůty k implementaci Nové směrnice o POZE,[77] stejně jako již uplynulé lhůtě k implementaci Směrnice o společných pravidlech[78] je ale takové nastavení priorit přinejmenším nešťastné.

[77] Ve většině rozsahu musí být dosaženo souladu s Novou směrnicí o POZE do 30. 6. 2021. Čl. 36 odst. 1 Nové směrnice o POZE.

[78] Hlavní část Směrnice o společných pravidlech měla být zapracována do 31. 12. 2020. Čl. 71 odst. 1 Směrnice o společných pravidlech.

5. ZÁVĚR

Výše provedený rozbor je možné uzavřít konstatováním, že velmi rozsáhlá novelizace Zákona o PZE sama o sobě zřejmě nepovede ke zvýšení objemu podpory využívání OZE. Za světlé body lze rozhodně označit zavedení systému aukcí, který se v zahraničí prokázal jako velice efektivní způsob poskytování podpory, a dále uzákonění udržovací podpory, která pomůže udržet současné výrobny v provozu i po skončení doby jejich očekávané podpory. Jak již ale bylo uvedeno, Novela zákona o PZE dává značnou moc nad podporou OZE vládě a MPO, čímž tento sektor podřizuje politickým výkyvům spojeným zejména s okamžitou popularitou jednotlivých opatření, místo toho, aby přinášela jistotu pro investory. Velmi přísné nastavení prověřování přiměřenosti podpory pak zřejmě povede k dalšímu znejistění podnikatelského sektoru, pro který budou opatření v návaznosti na prověřování představovat zásah do právní jistoty a rozhodně nepovedou k nárůstu zájmu o podnikání v této oblasti se státní podporou. Podle mého názoru tak Novela zákona o PZE nepovede k naplňování cílů určených Novou směrnicí o POZE a dalšími dokumenty.

Věcný záměr nového energetického zákona přináší jistou naději, zejména v oblasti energetických společenství, samospotřebitelství a ukládání energie. Stále jsme ale na začátku celého procesu, k paragrafovému znění je ještě daleko a průchod legislativním procesem v tomto funkční období Poslanecké sněmovny se rozhodně nedá očekávat.

Unijní legislativa tak zcela jistě tlačí českého zákonodárce k posunu vpřed, aktuální značné společenské a ekonomické potíže ale jeho snahy odsouvají na vedlejší kolej. S obměnou v energetice je ale často spojována i ekonomická obroda po krizi způsobené současnou pandemií, množí se plány na tzv. Green New Deal, ať už v kterékoliv z mnoha variant.[79] Dále je jisté, že předpisy ze Zimního balíčku evropské legislativy nebudou poslední úpravou v probíhajícím procesu dekarbonizace evropské energetiky. Bylo

[79] Zcela zásadní je v této oblasti plán Evropské Komise na tzv. European Green Deal, který zahrnuje řadu legislativních návrhů, včetně jeho centrálního návrhu nařízení EP a Rady, kterým se stanoví rámec pro dosažení klimatické neutrality (evropský právní rámec pro klima).

by tak obrovskou újmou české společnosti, kdyby rozvoji OZE měl bránit nedostatečný právní stav.

6. POUŽITÉ ZDROJE

6.1 LITERATURA

[1] BENRATH, Daniel. Applicable law to hydrogen pipelines for energy purposes in Germany. *Journal of Energy & Natural Resources Law*. 2020, roč. 38, č. 1 s. 65-89. DOI: 10.1080/02646811.2019.1696519

[2] ČTK. *Vláda schválila snížení podpory pro solární elektrárny*. In: *OEnergetice*. [online]. 27. 4. 2020. [cit. 2020-11-11]. Dostupné z: https://oenergetice.cz/elektrarny-cr/vlada-schvalila-snizeni-podpory-pro-solarni-elektrarny

[3] FLEMING, Ruven. Clean or renewable – hydrogen and power-to-gas in EU energy law. In: *Journal of Energy & Natural Resources Law*. [online]. 20. 10. 2020. [cit. 2021-02-22]. Dostupné z: https://doi.org/10.1080/02646811.2020.1795382

[4] IRENA. *Renewable energy auctions: Status and trends beyond price*. Abu Dhabi: International Renewable Energy Agency. [online]. 2019. [cit. 2021-02-22]. Dostupné z: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Dec/IRENA_RE-Auctions_Status-and-trends_2019.pdf

[5] JACOBS, Sharon B. *The Energy Prosumer*. In: Ecology Law Quarterly. [online]. 2016. [cit. 2020-12-06]. Dostupné z https://scholar.law.colorado.edu/articles/709

[6] LOMBARDO, Tom. *What Is the Lifespan of a Solar Panel?* In: engineering.com. [online]. 20. 4. 2014. [cit. 2020-11-11]. Dostupné z: https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/7475/What-Is-the-Lifespan-of-a-Solar-Panel.aspx

[7] MACHAČKOVÁ, Jana, FIALOVÁ, Eva, KÝVALOVÁ, Miroslava, VÍCHOVÁ, Jitka, HOLENDOVÁ, Lenka, SMÍŠEK, Jaroslav. *Stavební zákon*. 3. vydání. Praha: Nakladatelství C. H. Beck, 2018, 1216 s. ISBN: 978-80-7400-558-9.

[8] Odbor elektroenergetiky a teplárenství. *Prověření přiměřenosti podpory obnovitelných zdrojů energie uvedených do provozu v letech 2006 až 2008*. In: Ministerstvo průmyslu a obchodu. 30. 9. 2019. [online]. [cit. 2020-11-11]. Dostupné z: https://www.mpo.cz/cz/energetika/elektroenergetika/obnovitelne-zdroje/proverenи-primerenosti-podpory-obnovitelnych-zdroju-energie-uvedenych-do-provozu-v-letech-2006-az-2008--249308/

[9] SCHOLZ, Ulrich, ANTE, Johann. *Electricity regulation in Germany: overview*. In: Practical Law. [online]. 2021. [cit. 2021-02-22]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/5-524-0808?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

[10] SOKOŁOWSKI, Maciej M. Renewable and citizen energy communities in the European

Union: how (not) to regulate community energy in national laws and policies. *Journal of Energy & Natural Resources Law*. 2020, roč. 38, č. 3 s. 289-304. DOI: 10.1080/02646811.2020.1759247

6.2 PRÁVNÍ PŘEDPISY ČR

[11] Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech
[12] Zákon č. 165/2012 Sb., o podporovaných zdrojích energie
[13] Zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon)

6.3 PRÁVNÍ PŘEDPISY EU

[14] Směrnice Evropského parlamentu a Rady 2012/27/EU ze dne 25. října 2012 o energetické účinnosti, o změně směrnic 2009/125/ES a 2010/30/EU a o zrušení směrnic 2004/8/ES a 2006/32/ES
[15] Směrnice Evropského parlamentu a Rady 2010/31/EU ze dne 19. května 2010 o energetické náročnosti budov
[16] Směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU
[17] Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou
[18] Nařízení Evropského parlamentu a Rady (EU) 2018/1999 ze dne 11. prosince 2018 o správě energetické unie a opatření v oblasti klimatu, kterým se mění nařízení Evropského parlamentu a Rady (ES) č. 663/2009 a (ES) č. 715/2009, směrnice Evropského parlamentu a Rady 94/22/ES, 98/70/ES, 2009/31/ES, 2009/73/ES, 2010/31/EU, 2012/27/EU a 2013/30/EU, směrnice Rady 2009/119/ES a (EU) 2015/652 a zrušuje nařízení Evropského parlamentu a Rady (EU) č. 525/2013
[19] Směrnice Evropského parlamentu a Rady 2009/28/ES ze dne 23. dubna 2009 o podpoře využívání energie z obnovitelných zdrojů a o změně a následném zrušení směrnic 2001/77/ES a 2003/30/ES

6.4 OSTATNÍ

[20] Rozhodnutí Evropské Komise SA.40171 (2015/NN) ze dne 28. listopadu 2016
[21] Rozhodnutí Evropské Komise SA.35177 (2014/NN) ze dne 11. června 2014
[22] Rozhodnutí Evropské Komise SA.43182 (2015/N) ze dne 22. srpna 2016
[23] Rozhodnutí Evropské Komise SA.43451 (2015/N) ze dne 22. srpna 2016
[24] Rozhodnutí Evropské Komise SA.40171 (2015/NN) ze dne 28. listopadu 2016
[25] Zelená kniha Evropské Komise. Rámec politiky pro klima a energetiku do roku 2030. COM/2013/0169

[26] Poslanecká sněmovna Parlamentu České republiky. Sněmovní tisk 1121, Novela z. o podporovaných zdrojích energie – EU. 2020. [online]. [cit. 2020-11-11]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=6&t=1121
[27] Ministerstvo průmyslu a obchodu. Věcný záměr energetického zákona. 2020. [online]. [cit. 2020-11-11]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBQLGLK0X
[28] Ministerstvo průmyslu a obchodu. Vnitrostátní plán České republiky v oblasti energetiky a klimatu [online]. [cit. 2020-11-11]. Dostupné z: https://www.mpo.cz/cz/energetika/strategicke-a-koncepcni-dokumenty/vnitrostatni-plan-ceske-republiky-v-oblasti-energetiky-a-klimatu--252016/

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:

Discussion:	5 – 30 standard pages
Annotation:	2 – 10 standard pages
Essays:	5 – 10 standard pages
Book review:	1 – 5 standard pages
Topic section:	30 – 80 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 12 | YEAR 2021 | NUMBER 23

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 30th June 2021.
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: JUDr. Ing. František Kasl, Ph.D.
Editorial Staff: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editorial Secretary: Anna Blechová
Editors: Anna Blechová, Martin Erlebach
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 IX“, MUNI/A/1292/2020.

THE ALGORITHMIC SURVEILLANCE STUDY GROUP

Everyone with interest in legal, ethical and technological issues around algorithmic surveillance is welcome to join this group. It is expected that research students from the UK, EU and US will be the most represented cohort in this group, but taught students and postdoctoral researchers are also welcome to join.

From Autumn 2021 (exact starting date TBC), this group will meet bi-weekly to discuss seminal writings in this field.
The meetings will be online. It is expected that participants will spend on average at least 2 hours of reading in preparation for each meeting.

Participation is free. There is no formal reward, but you could meet new like-minded colleagues, sharpen your critical reading and analytical skills, engage in a good argument, experience tutorial-styled learning, and gain new insights from outside your area of expertise.

The group is led by Václav Janeček.

If you have any questions, please write to vaclav.janecek@law.ox.ac.uk or vaclav.janecek@law.muni.cz.

SIGN UP HERE.

(Background: National Archives, INF 3/232 – Be Careful what you say poster)

You never know who's on the wires!

BE CAREFUL WHAT YOU SAY

Diskuze

Anotace

Essays

Recenze

Téma

MUNI PRESS