Západočeská univerzita v Plzni

Fakulta právnická

Diplomová práce

Právní aspekty digitalizace v Evropské unii se zaměřením na eGovernment

Martin Černý Plzeň 2019

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: **2018/2019**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin ČERNÝ**
Osobní číslo:	**R14M0027P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Název tématu:	**Právní aspekty digitalizace v Evropské unii se zaměřením na eGovernment**
Zadávající katedra:	**Katedra ústavního a evropského práva**

Zásady pro vypracování:

1. Úvod do problematiky
2. Evropská unie v současnosti
3. Popis a zhodnocení stávající právní úpravy
4. Srovnání právní úpravy v České republice s právní úpravou v Německu
5. Budoucnost, chystané změny a další vývoj
6. Závěr

Rozsah grafických prací:

Rozsah kvalifikační práce: **103**

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

- **MATES, Pavel a Vladimír SMEJKAL. E-government v České republice: právní a technologické aspekty. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.**
- **JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. Internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.**
- **BROWN, Alan W., Mark THOMPSON a Jerry FISHENDEN. Digitizing government: understanding and implementing new digital business models. New York, NY: Palgrave Macmillan, [2014]. ISBN 9781137443625**
- **Internetrecht Gebundene Ausgabe von Niko Härting, 2017. ISBN 3504560967**
- **Digitalisierte Verwaltung - Vernetztes E-Government, von PD Dr. Margrit Seckelmann (Herausgeber, Autor), Prof. Dr. Marion Albers (Autor), 2018**

Vedoucí diplomové práce: **JUDr. Tomáš Pezl**
Katedra ústavního a evropského práva

Datum zadání diplomové práce: **21. března 2018**

Termín odevzdání diplomové práce: **31. března 2019**

Doc. JUDr. Jan Bauly, CSc.
děkan

Západočeská univerzita v Plzni * Fakulta právnická *
L.S.

Doc. JUDr. Monika Večeřová, Ph.D.
vedoucí katedry

V Plzni dne 27. června 2018

Prohlášení autora

„Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem ve vědecké práci obvyklým.“

Plzeň, březen 2019 Martin Černý ……...

Poděkování

Rád bych tímto poděkoval panu JUDr. Tomáši Pezlovi za odborné vedení mé diplomové práce, za vstřícnost a cenné rady, které mi pomohly k jejímu vypracování.

Obsah

1 ÚVOD

Ve své diplomové práci se zabývám právními aspekty digitalizace v Evropské unii, přičemž se zaměřuji především na digitalizaci veřejné správy. Používání digitálních technologií v soukromém i veřejném sektoru dnes již neodmyslitelně patří k fungování moderní společnosti. Potenciál je zde stále obrovský a i při neustálém rozvoji lze denně sledovat nové pokroky a vylepšení v IT. Tento technologický vývoj s sebou kromě sociologických, ekonomických a dalších společenských změn a dopadů samozřejmě přináší i nové výzvy právní.

Jedná se o téma s velice širokým záběrem, které lze pojmout mnoha způsoby. Odborných publikací na dané téma jako takové je stále poskrovnu, zpravidla jsou dostupné pouze monografie zabývající se pouze dílčími otázkami dané problematiky. V obecné části práce, kde popisuji politiku, záměry a kompetence EU v dané oblasti, tedy vycházím především z oficiálních zdrojů orgánů Evropské unie, velice aktuální literatury zahraniční a odborných článků. Celé téma je převážně popisováno obecně, v evropské rovině, kdy jsou řešeny základní otázky a vybrané instituty. Daná problematika je doplňována srovnáním určitých aspektů se Spolkovou republikou Německo, přičemž však tato komparace není stěžejním prvkem práce, nýbrž skutečně jen doplněním pro lepší celkový vhled do tématu a získání přehledu o současném stavu.

EGovernment ve své podstatě označuje veřejnou správu, která při realizaci svých činností užívá digitálních (informačních a komunikačních) technologií. Jedná se o velmi komplexní pojem, jehož obsah je mnohem širší, než by se na první pohled mohlo zdát. Nezahrnuje jen elektronický podpis nebo datové schránky, jak je často prezentováno, nýbrž se může jednat v podstatě o veškerou interakci občan-stát, nebo přesněji občan – veřejná správa. Obsahem tohoto vztahu je pak výkon práv a povinností prostřednictvím digitálních technologií. Činností realizovanou v rámci eGovernmentu může být elektronické vyřízení živnostenského oprávnění, přes elektronickou účast na veřejné zakázce až po elektronické hlasování ve volbách do Evropského parlamentu. Právě v celé rovině Evropské unie se jedná o velice progresivní záležitost, kdy je zde ze strany institucí EU, především Evropské komise, značná snaha o rozvoj eGovernmentu ve všech členských státech a jeho propojení v rámci celé EU. Dle prognóz přinese digitalizace spojená se zavedením eGovernmentu nejen větší rychlost, efektivitu a transparentnost, ale také úsporu

finančních prostředků. Roční úspora při zavedení eGovernmentu na předpokládané úrovni dosáhne dle odhadů až 50 miliard Euro.[1]

V současné době lze však konstatovat, že se jedná až na výjimky o opomíjenou oblast a digitální rozvoj v členských zemích nedosahuje předpokládané úrovně. Pro úspěšnou realizaci je klíčovým prvkem efektivní spojení práva a technologií. Bez odpovídající právní regulace není možné zavádět nové technologie, a už vůbec ne na státní úrovni. Právo je velice konzervativním systémem, zatímco v sektoru IT platí, že co je dnes nové, je zítra vhodné „na výstavu do muzea". Z principu není možné sladit tato dvě odvětví a právo nikdy nebude zcela pružně reagovat na nové technologie, objevy v ICT a podobně. Domnívám se však, že současná snaha by měla být značná, a že je třeba o dosažení jakési alespoň částečné koherence usilovat.

Nejprve popisuji Evropskou unii jako celek, záměry a cíle v oblasti eGovernmentu a digitalizace obecně, její fungování a přijímaní legislativy. Následuje popis legislativních (ať už úspěšných nebo neúspěšných) snah o digitalizaci státní správy na celoevropské úrovni, přičemž je zde podrobný popis zásadních zákonů a srovnání současné situace v České republice se Spolkovou republikou Německo jakožto blízkými evropskými partnery. Mým cílem není podrobný a vyčerpávající popis všech instrumentů eGovernmentu, nýbrž podat přehled základních předpokladů, principů a otázek spojených s pokračující digitalizací veřejné správy v rámci Evropské unie, poukázat na některé související problémy, popsat vybranou normotvorbu ve stěžejních oblastech a výhledy do budoucna. V průběhu celého textu práce pak také prezentuji vlastní myšlenky a názory na danou problematiku, které jsou komplexně shrnuty v samém závěru práce.

[1] eGovernment & Digital Public Services | Digital Single Market [online]. European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/digital-single-market/en/policies/egovernment

2 ÚVOD DO PROBLEMATIKY

2.1 DIGITÁLNÍ REVOLUCE

Kryptoměna, Big Data, umělá inteligence, krádež dat, cloud, virtuální, rozšířená nebo smíšená realita, kyberválka, telemedicína, sociální média, autonomní řízení, průmysl 4.0, trestní právo 4.0. Digitalizace nepřináší jen tyto nové pojmy, ale mění životy nás všech. Digitální technologie formují naši duchovní a materiální skutečnost, mění naše sebepojetí, modifikují, jak vystupujeme ve vzájemných vztazích a přinášejí nový pohled na chápání světa jako takového. Filozofové a sociologové mají jasno: žijeme v době digitální kultury, v době tzv. čtvrté průmyslové revoluce, v době revoluce digitální.[2]

Slovo revoluce evokuje spíše rozvášněný dav, chystající se provést státní převrat než objev převratné digitální technologie. Tato zakořeněná představa je logická vzhledem k historii lidstva, která překypuje takovými obrazy revolucí. Nicméně má toto slovo ještě své místo v průmyslu, totiž při označování zásadních milníků lidstva, charakterizujících technologický pokrok. Za symbol první průmyslové revoluce, jejíž začátek spadá zhruba do šedesátých let 18. století, je považován vynález parního stroje a charakteristickým rysem je postupný přesun manufakturní výroby do továren. Charakteristikou druhé průmyslové revoluce je vynález montážní linky a rozšířeným užíváním elektrického proudu. Třetí průmyslová revoluce se vyznačuje automatizací, tedy přechodem od manuálního provádění činností k automatizovaným procesům. [3]

Doba čtvrté, digitální revoluce, která v současnosti stále probíhá, je snad nejprogresivnější a nejglobalizovanější celospolečenskou změnou v dějinách. Technologické inovace, které lidem pomáhají v každodenním životě a nabízí stále lepší, efektivnější a rychlejší řešení všech problémů lidského života, jsou dnes již nedílnou součástí lidstva jako takového. Život bez e-mailové schránky nebo mobilního telefonu je dnes již těžko představitelný. Jistá míra počítačové gramotnosti je dnes již základním předpokladem pro úspěch v pracovním životě člověka a vůbec pro jeho základní společenské fungování. Počítač a připojení k

[2] FLORIDI, Luciano. The 4th revolution: how the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014. ISBN 9780199606726.
[3] SIRŮČEK, Pavel. Hospodářské dějiny a ekonomické teorie: (vývoj, současnost, výhledy). Slaný: Melandrium, 2007. ISBN 9788086175539.

internetu mělo v roce 2017 jen v Evropské unii 87 % domácností, téměř dvojnásobek oproti roku 2007.[4]

Méně srozumitelné počítačové terminologii se v tomto úvodu nelze vyhnout, tedy pár pár pojmů techničtější rázu pro začátek. Co je to vlastně digitalizace?

„Digitalizace je proces konverze informací do digitálního (tj. počítačem čitelného) formátu, ve kterém jsou informace uspořádány do bitů. Výsledkem je reprezentace objektu, obrazu, zvuku, dokumentu nebo signálu vytvořením řady čísel, které popisují diskrétní množinu bodů. V moderní praxi jsou digitalizovaná data v podobě binárních čísel, která usnadňují počítačové zpracování a další operace. Avšak digitalizace v nejjednodušší podobě znamená konverzi analogového materiálu na číselný formát.“[5]

Příkladem digitalizace analogového zdroje může být naskenování ručně psané smlouvy do počítačové databáze. Projevem digitalizace je podepsání takové smlouvy unikátní kombinací datových znaků, reprezentující elektronický podpis podepisujícího. Digitalizovaná lednička sama vyhodnotí, jaké potraviny jsou již snězené, a vytvoří objednávku, kterou odešle do nejbližší prodejny potravin.

V souvislosti s digitalizací je také používán termín elektronizace, kdy v mnoha případech mají tyto pojmy stejný význam a jsou v podstatě zaměnitelné. Elektronizace - obecně vzato se jedná o modernizaci procesů pomocí informačních a komunikačních technologií (například elektronizace veřejné správy při zavádění eGovernmentu). Termín je také používán k popsání procesu převodu informací z papírové formy na formu elektronickou (digitalizace).[6]

V souvislosti s digitalizací je stále více o současné společnosti hovořeno jako o „společnosti informační“ “. Samotná Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, nese název o určitých aspektech služeb informační společnosti, transpoziční zákon v České republice reflektující tuto směrnici pak Zákon č. 480/2004 Sb., o některých službách informační společnosti.

[4] Digital economy and society statistics - households and individuals - Statistics Explained [online]. European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals
[5] IT Slovník [online]. [cit. 25.3.2019]. Dostupné z: https://it-slovnik.cz/pojem/digitalizace
[6] IT Slovník [online]. [cit. 25.3.2019]. Dostupné z: https://it-slovnik.cz/pojem/elektronizace

„Informační společnost je charakterizována podstatným využíváním digitálního zpracovávání, uchovávání a přenosu informací. Ze zpracování informací se stává významná ekonomická aktivita, která jednak prostupuje tradičními ekonomickými či společenskými aktivitami a jednak vytváří zcela nové příležitosti a činnosti, které podstatně ovlivňují charakter společnosti.“[7]

Pravděpodobně největší výzvou v následujících letech bude využití potenciálu, které nové technologie přináší, a zároveň zachování odpovědného přístupu a zdravého rozumu.

2.2 PRÁVO A TECHNOLOGIE

Digitalizace má nepochybně své filozofické, sociologické, psychologické, ekonomické a další společenskovědní aspekty, které jsou předmětem každodenního zkoumání celosvětové odborné vědecké komunity. Má také své aspekty právní. Právo, jakožto základní regulátor lidských vztahů i zde funguje jako esenciální prvek. Vzniká zde poměrně unikátní vztah, kdy je nutné v právní úpravě reflektovat technologické aspekty, kdy by v ideálním případě obě složky měly koordinovaně a efektivně fungovat.

Propojení práva a technologií je jednou z klíčových výzev moderního digitálního světa. Adaptace práva na digitální svět ale ze své podstaty není jednoduchou záležitostí, neboť ze své podstaty jde o velmi odlišné systémy. Úspěch těchto snah bude pravděpodobně závislý na hledání a aplikaci vhodných kompromisů.

V souvislosti s technologickým vývojem vznikl v podstatě již samostatný právní obor „právo informačních technologií“, také IT právo, ICT (Information and Communication Technology) právo a podobně. Také se lze setkat s označeními a výrazy jako počítačové právo, EDV právo, internetové právo, softwarové právo a podobně. Za zastřešující pojem je však považováno právo informačních

[7] ZLATUŠKA, Jiří. Informační společnost [online]. Zpravodaj ÚVT MU. 1998, roč. 8., č. 4, s. 1–6. ISSN 1212-0901[cit. 25.3.2019]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/122.html.

technologií. Jeho podoblastmi je zmíněné právo internetové, softwarové a podobně.[8]

Problematika digitalizace a eGovernmentu je součástí IT práva jako celku, zasahuje do podoblasti internetového práva (internetové stránky úřadů, správa vládních domén, elektronická komunikace s úřady apod.) i softwarového práva (software jako takový, ochrana dat, outsourcing, cloud computing a další).[9]

2.3 POJEM EGOVERNMENT

Definice pojmu eGovernment[10] není zcela jednoznačná. Výraz je zkratkou z anglického slovního spojení „electronic government“, neboli v překladu „elektronická vláda“[11], kdy je však výraz „vláda“ logicky interpretován ve smyslu spravování, veřejné správy.

S technologickým rozvojem přirozeně roste také očekávání občanů. V rámci veřejných služeb očekávají rychlost, efektivitu a transparentnost. Díky rozvoji informačních a komunikačních technologií a související automatizaci, koordinaci a harmonizaci daných procesů je možné tyto nároky průběžně plnit.[12]

Jak jsem již zmiňoval v úvodu, pojem eGovernment je chápán velmi široce. Nelze vymezit ani negativně, ani pozitivně, protože pozitivní taxativní výčet veškerých činností je téměř nemožné provést, neboť agenda veřejné správy je velice rozsáhlá. Negativní výčet je z podobných důvodů také téměř vyloučen. V odborných publikacích a článcích lze nalézt obecné definice, kdy pro jejich pochopení je nejprve nutné ujasnění pojmu veřejná správa. Pojem veřejná správa lze odborně definovat pomocí určujících kritérií, tedy jako správu veřejných

[8] JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. Internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4. S. 21.
[9] JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. Internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4. S. 22.
[10] Poznámka autora: Psaní samotného výrazu není jednotné. Užívá se tvar eGovernment, E-Government a další.
[11] government - překlad do češtiny | slovník slovniky.lingea.cz [online]. Slovníky Lingea | On-line slovníky, překlady, gramatiky a konverzace [cit. 25.3.2019]. Dostupné z: https://slovniky.lingea.cz/anglicko-cesky/government
[12] Buhl, H.U., Hirsch, T. & Loeffler, M. Wirtsch[online]. Inform Manag (2012) 4: 28. [cit. 25.3.2019]. Dostupné z: https://doi.org/10.1365/s35764-012-0122-1

záležitostí, ve veřejném zájmu, za veřejné prostředky[13]. Pojem eGovernment je pak v odborné literatuře popisován jako „*série procesů, vedoucích k výkonu státní správy a samosprávy a uplatňování občanských práv a povinností fyzických a právnických osob, realizovaných elektronickými prostředky*[14]*“*

Nejjednodušší a možná nejvýstižnější definici nabízí tzv. Speyerova definice: *„EGovernment je označením pro realizaci společenských procesů vládnutí a správy s pomocí informačních a komunikačních technologií.“*[15] Na základě výše uvedeného lze pojem eGovernment chápat jako užívání informačních a komunikačních technologií při procesech realizace práv a povinností občana (evropského občana) ve vztahu k veřejné správě, ke státu, resp. k Evropské unii, stejně tak užívání digitálních technologií při výkonu procesů mezi úřady státní správy a správními institucemi navzájem. Díky digitálnímu rozvoji zde existuje předpoklad, že veškeré tyto procesy bude možné provádět elektronicky.[16]

Pokud hovoříme o zavádění regulace v oblasti eGovernmentu, hovoříme v podstatě o vytvoření právního rámce pro digitální fungování veřejné správy. Východiskem je kromě jiného právě výše zmíněné propojení práva a technologií.

Vzhledem k tomu, co vše pojem eGovernment zahrnuje, není možné popsat veškeré činnosti, které pod něj svým obsahem lze zařadit. Uvádím tedy několik příkladů: eIdentita – elektronická totožnost občana, vedení základních registrů občanů v elektronických databázích, elektronický podpis, datové schránky, autorizovaná konverze dokumentů, elektronické zadávání veřejných zakázek, cloudové služby ve veřejné správě, eHealth – databáze veškerých záznamů ve zdravotnictví a další.

Související pojmy jako Smart Government, Open Government a E-Voting jsou vysvětleny níže.

[13] MALAST, Jan. Správní právo přehledně [online]. JUDr. PhDr. Jan Malast, Ph.D., 2018 [cit. 25.3.2019]. Dostupné z: https://www.spravko.cz/produkty/ebook-spravni-pravo-prehledne/
[14] VANÍČEK, Zdeněk a Stanislav A. MARCHAL. *Právní aspekty eGovernmentu v ČR*. Praha: Linde, 2011. ISBN 9788072018550.
[15] Jörn von Lucke/Heinrich Reinermann[online]. Speyerer Definition von E-Government, 2000, S. 1[cit. 25.3.2019]. Dostupné z: http://www.joernvonlucke.de/ruvii/Sp-EGov.pdf
[16] Huesmann, J. & Galbis, A. Wirtsch [online]. Inform Manag (2015) 7: 18. [cit 25.3.2019]. https://doi.org/10.1007/s35764-015-0535-8

2.4 SMART GOVERNMENT

Důležité pro celou problematiku je taktéž vymezení tohoto pojmu. Stále nepanuje v odborných kruzích shoda, zda je nadřazen či podřazen pojmu eGovernment, nebo snad jsou si tyto pojmy rovnocenné. Pojem Smart Government je na mezinárodní úrovni chápán ve smyslu používání inteligentních věcí a kybersystémů ve veřejném sektoru.[17] Inteligentně propojené vládní a správní jednání užívá v rámci procesů inteligentně propojených věcí a kybersystémů pro účely efektivního plnění veřejných úkolů.

V podstatě tento pojem reflektuje rozvíjející se novou oblast, tzv. Internet věcí (Internet of Things). Internet věcí je specifickým označením pro síť elektronických zařízení, která jsou vybavena určitým hardwarem, softwarem a především možností připojení k internetu, v rámci kterého si mohou vyměňovat data. Tyto zařízení jsou součástí vozidel, domácích spotřebičů, dopravní infrastruktury, zemědělských zařízení, zdravotnických pomůcek a mnoha dalších.[18] Jedná se o fyzické předměty každodenního užívání, které jsou digitalizovány. Netřeba dále popisovat, jaké obrovské možnosti a potenciál internet věcí přináší nejen ve veřejné správě.

2.5 OPEN GOVERNMENT A E-VOTING

Další pojem, se kterým je možné se v rámci dané problematiky setkat, je open government. Opět se obsah tohoto pojmu do značné míry prolíná s obsahem pojmů eGovernment a Smart Government. Ve své podstatě jsou tyto tři pojmy odlišovány pouze lehkými niancemi, kdy většinou označují částečně odlišnou agendu fungování státu. Spojuje je však nejen právě výkon veřejných a správních procesů, ale i jejich digitalizace.

„Koncept Open governmentu přináší možnost využití technických možností k efektivnímu zajištění legitimity a transparentnosti činnosti veřejné správy právě

[17] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 204.
[18] Internet of Things Global Standards Initiative [online]. Copyright © ITU [cit. 25.03.2019]. Dostupné z: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

novými formami, které umožňují občanům podílet na správě veřejných záležitostí a řízení státu.“[19]

Open government s sebou přináší pojem Open Data. Jedná se o čím dál více prosazovaný princip, kdy má být veškerým subjektům zajištěn přístup k datům, která spravují veřejnosprávní orgány ve svých databázích (pokud se samozřejmě nejedná o utajované informace dle příslušných zákonů). Tato data jsou poskytovány ve strojově čitelném formátu a posléze mohou být využity ke komerčním účelům, například pro soukromé služby, pro obchodní činnosti, podnikání a podobně. Přístup k těmto datům a jejich získávání musí mít jasná pravidla. Zvláštní důraz je zde kladen na zachování práva na ochranu osobních údajů a soukromí, poskytování těchto dat tedy musí respektovat práva jiných a nesmí nikomu způsobovat újmu.

Elektronická participace občanů na veřejné správě a elektronické volby jsou další nové možnosti, které přináší pokračující digitalizace a které jsou předmětem častých odborných i laických diskuzí. Elektronická participace může představovat online realizaci petičního práva nebo online připomínkové řízení k normotvorným návrhům členů samosprávných orgánů. Elektronické volby jsou velice specifickou oblastí digitalizace a v některých státech jsou již realitou. Je zřejmé, že podobné postupy obsahují již zmiňované výhody internetu – rychlost, jednoduchost, dostupnost. Nevýhodou jsou pak především vysoké technické nároky na zajištění precizního fungování těchto systémů a rizika spojená se zneužitím těchto systémů.

Elektronické volby jsou zajímavým fenoménem, na který je však v různých státech bez ohledu na kontinent či příslušnost k Evropské unii nahlíženo zcela odlišně a názory na jeho zavedení či fungování jsou velmi rozporuplné.

Estonsko je v elektronických volbách pravděpodobně nejdále. Bylo první zemí, která umožnila elektronicky volit i v parlamentních (národních) volbách. I-voting (volby jsou označovány jako internetové) umožňuje rychle a jednoduše oprávněným voličům odvolit přes internetového rozhraní za použití identifikační karty, která je ve své podstatě elektronickým občanským průkazem. Dle statistik této možnosti využívá zhruba každý třetí oprávněný volič.[20]

[19] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 74.
[20] Internet voting in Estonia[online]. Elections in Estonia. [cit 25.3.2019]. Dostupné z: https://www.valimised.ee/en/internet-voting/internet-voting-estonia

V roce 2014 upozornil tým nezávislých mezinárodních expertů ve své studii na kritické bezpečnostní chyby a další závažné nedostatky v celém estonském internetovém volebním systému.[21] Celkovou úroveň zabezpečení online volebního systému označil za velmi zastaralou a názorně demonstroval nejrůznější způsoby prolomení a obejití ochranných opatření, jejichž výsledkem bylo narušení nezávislosti voleb, porušení jejich principů a jejich naprosté znevěrohodnění. Prakticky šlo o shození systémů, prolomení volebního tajemství zjištěním totožností voličů a jejich konkrétní volby až po samotnou manipulaci s hlasy a výsledky. Na základě těchto zjištění doporučil expertní tým okamžité zrušení estonských internetových voleb.[22]

K výše uvedenému je třeba podotknout, že se jedná o 5 let starou studii, nicméně jsou tyto hrozby a rizika stále aktuální.[23] V současnosti internetový volební systém v Estonsku stále funguje, poslední volba do národního parlamentu, kdy bylo možné plně hlasovat online, proběhla 3. 3. 2019.

Ve Spolkové republice Německo bylo možné elektronicky odevzdat svůj hlas při volbách do Spolkového sněmu v roce 2005, kdy tak učinilo zhruba dva miliony oprávněných voličů. V návaznosti na tyto volby bylo v roce 2009 rozhodnuto o následných volebních stížnostech na elektronickou možnost hlasování. Spolkový ústavní soud označil odevzdání hlasu ve volbách prostřednictvím počítače za protiústavní, přičemž vycházel zejména z článku 38 ústavy Spolkové republiky Německo (Grundgesetz), který v kombinaci se základními principy právního státu obsažených v článku 20, odstavec 1 a odstavec 2 stanoví takzvanou „veřejnost voleb“. Spolkový ústavní soud tedy argumentoval tím, že až na ojedinělé případy podléhají veškeré kroky při volbách kontrole veřejnosti, samozřejmě kromě samotné konkrétní volby strany nebo kandidáta, které je tajné. Obecně je tím myšlena samotná realizace voleb, kontrola od volební komise, cesta za plentu a vhození lístku do urny. Dva miliony hlasů, odevzdaných elektronicky zůstalo platnými a zvolení zástupci setrvali, nicméně má toho rozhodnutí Spolkového ústavního soudu precedenční charakter a ve své podstatě v

[21] J. Alex Halderman [online]. Copyright © [cit. 25.03.2019]. Dostupné z: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf
[22] J. Alex Halderman [online]. Copyright © [cit. 25.03.2019]. Dostupné z: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf
[23] Viz kapitola Kyberbezpečnost

současnosti vylučuje konání elektronických voleb ve Spolkové republice Německo.[24]

V České republice jsou zatím elektronické online volby zmiňovány jen v rámci velice obecných úvah bez jakýchkoliv konkrétních návrhů nebo časového horizontu.

[24] BVerfG, Urteil des Zweiten Senats vom 03. März 2009 - 2 BvC 3/07 - Rn. (1-163)

3 EVROPSKÁ UNIE V SOUČASNOSTI

3.1 EVROPSKÁ UNIE A PRÁVO EVROPSKÉ UNIE

Evropská unie je „*nadnárodním uskupením států"*, kdy „*vztahy mezi Unií a členskými státy mají tzv. subordinační povahu.*"[25] V rámci této subordinační povahy daného vztahu přeneslo všech 28 členských států výkon svých určitých svrchovaných pravomocí na orgány EU. Na základě společného konsensu dobrovolně omezily část své suverenity ve prospěch celku, přičemž dochází ke vzniku samostatného právního systému – práva Evropské unie (taktéž právo EU, unijní právo). Právo EU tedy reprezentuje obecně závazný právní řád nadřazený všem členským státům Evropské unie. Je to právní řád sui generis, členské státy se zavázali jej respektovat a aplikovat. Definice práva EU zahrnuje výše zmíněné, právo EU (taktéž unijní právo) je definováno jako „*soubor přímo či nepřímo aplikovatelných právních pravidel, přijatých mezi členskými státy nebo na úrovni Unie za účelem resp. v důsledku svěření některých pravomocí členských států ve prospěch Unie*."[26]

3.1.1 ORGÁNY EVROPSKÉ UNIE

Evropská unie je tvořena orgány, kterým náleží výkon svěřených pravomocí. Orgány Evropské Unie vytvářejí komplexní systém, který zajišťuje činnost Unie jako celku. Výčet orgánů Evropské unie je obsahem článku 13 Smlouvy o Evropské unii (SEU). Dle tohoto článku orgány Unie jsou: Evropský parlament, Evropská rada, Rada (EU), Evropská komise, Soudní dvůr Evropské Unie (SDEU), Evropská centrální banka a Účetní dvůr.

Evropský parlament je volený orgán Evropské unie, který má legislativní, rozpočtovou a dozorčí pravomoc. Je tvořen 751 přímo volenými poslanci. Každá země disponuje určitým počtem mandátů dle své velikosti.

[25] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 55.
[26] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 56.

Evropská rada je tvořena představiteli členských států a Evropské unie. Členské státy v Evropské radě zastupují předsedové vlád nebo prezidenti, případně jiná hlava státu, za Evropskou komisi je členem předseda Evropské komise, vysoký představitel pro zahraniční věci a bezpečnostní politiku. Evropská rada určuje základní cíle politiky EU.

Rada Evropské unie je tvořena ministry vlád členských zemí dle jejich rezortů. Kromě jiného koordinuje politiky EU a schvaluje právní předpisy.

Evropská komise je kolegiálním orgánem, který především navrhuje právní předpisy a kontroluje jejich dodržování. Každý členský stát má jednoho komisaře.

Soudní dvůr Evropské unie je soudním orgánem Evropské unie. *„Soudní dvůr Evropské unie provádí výklad práva EU, aby bylo uplatňováno stejných způsobem ve všech státech EU, dále urovnává právní spory mezi jednotlivými státy a orgány EU. V určitých případech se na něj jednotlivci, podniky nebo organizace mohou obrátit s žádostí, aby zasáhl, pokud se domnívají, že některý z orgánů EU porušil jejich práva.“*[27]

Soudní dvůr Evropské unie ve svých rozhodnutích právo vykládá, vymáhá, zrušuje právní předpisy EU, zajišťuje činnost ze strany orgánů EU a postihuje orgány EU. Výklad práva je realizován například při rozhodování o předběžné otázce, vznesené vnitrostátním soudem členského státu. Vymáhání práva je činností charakterizující žalobu pro nesplnění povinnosti, kdy je žalován členský stát pro neplnění povinností, vyplývající z práva Evropské unie. Zrušení právního předpisu může být následkem při řízení o žalobě na neplatnost právního předpisu EU. Žaloba na nečinnost může být podána v případech domnělého nekonání Evropského parlamentu, Rady a Evropské komise, kdy je možné takto orgánům EU uložit, aby konaly. Dále SDEU rozhoduje o žalobách na náhradu škody, pokud byla tato škoda způsobena při činnosti orgánů EU.[28]

Obecně se na tvorbě a schvalování právních předpisů v legislativním procesu podílí především Evropský parlament, Rada Evropské unie a Evropská

[27] Soudní dvůr Evropské unie | Evropská unie[online]. EUROPA - European Union website, the official EU website [cit. 25.3.2019]. Dostupné z: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_cs

[28] Soudní dvůr Evropské unie | Evropská unie[online]. EUROPA - European Union website, the official EU website [cit. 25.3.2019]. Dostupné z: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_cs

komise. Zpravidla navrhuje právní předpisy Evropská komise a Evropský parlament a Rada EU je schvalují.

3.1.2 PRAVOMOCI EVROPSKÉ UNIE – ZÁSADA SVĚŘENÝCH PRAVOMOCÍ, PRINCIP PROPORCIONALITY A SUBSIDIARITY

Dělba pravomocí mezi členskými státy a Evropskou unií je založena ve Smlouvách primárního práva. Tyto pravomoci se dělí do několika kategorií, přičemž každá z těchto kategorií obsahuje vymezení konkrétních oblastí společenských vztahů a fungování. Každá kategorie těchto pravomocí je ve své podstatě konkrétním stanovením rozsahu oprávnění a specifikuje, kdo a jakým způsobem může ve vymezených oblastech přijímat právně závazné akty.[29] Z této konkretizace se odvíjí jakákoliv další činnost Evropské unie, neboť určuje, které svrchované pravomoci členské státy na Unii přenesli a které náležejí zároveň členským státům i Evropské Unii. Platí zde tzv. zásada svěřených pravomocí, stanovená v článku 5 Smlouvy o Evropské unii: *„Vymezení pravomocí Unie se řídí zásadou svěření pravomocí. Výkon těchto pravomocí se řídí zásadami subsidiarity a proporcionality"*[30] Další úvodní články Smlouvy o Evropské Unii pak rozdělují pravomoci na konkrétní druhy a definují jejich obsah. Tyto druhy jsou označovány jako výlučná pravomoc, sdílená pravomoc, koordinační pravomoc a podpůrná pravomoc. Výkon těchto pravomocí je pak obecně omezen zásadou subsidiarity a proporcionality, jak je taktéž stanoveno v článku 5 Smlouvy o Evropské unii.

Výlučné pravomoci jsou upraveny v článku 3 Smlouvy o fungování Evropské unie. *„Výlučná pravomoc znamená, že pouze Unie může v dané oblasti vytvářet a přijímat právně závazné akty."*[31] Do výlučné pravomoci Evropské unie spadá například celní unie nebo společná obchodní politika.

Sdílená pravomoc, jak již označení napomíná, umožňuje přijímání právně závazných aktů v určité oblasti jak Evropské unii, tak členským státům, přičemž *„členské státy vykonávají svou pravomoc v rozsahu, v jakém ji Unie dosud*

[29] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 153.
[30] Smlouva o Evropské unii, Článek 5
[31] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 154.

nevykonala.“[32] Sdílená pravomoc je definována v článku 4 Smlouvy o fungování EU a obsahuje demonstrativní výčet oblastí, které pod ni spadají, například vnitřní trh, doprava, transevropské sítě, energetika, prostor svobody, bezpečnosti a práva a další.[33]

Koordinační pravomoc je definována v článku 5 SFEU. Ustanovení umožňují přijímat opatření, koordinující hospodářské politiky v rámci EU, politiky zaměstnanosti a podněty ke koordinaci sociálních politik členských států.[34]

Podpůrná pravomoc dle článku 2, odstavce 5 SFEU umožňuje Unii podnikat v určitých oblastech podpůrnou činnost, *„aniž by přitom v těchto oblastech nahrazovala jejich pravomoc.“*[35] Oblasti této činnosti jsou například průmysl, kultura, cestovní ruch nebo správní spolupráce.

Zásada proporcionality a zásada subsidiarity patří k základním zásadám, na kterých je založeno fungování činnosti Unie jako celku a které zaručují legitimní dělbu moci mezi Evropskou unií a členskými státy. Zásada subsidiarity ve své podstatě stanoví hranice pro činnost Unie v oblastech, které nenáležejí do její výlučné pravomoci. *„Podle zásady subsidiarity jedná Unie v oblastech, které nespadají do její výlučné pravomoci, pouze tehdy a do té míry, pokud cílů zamýšlené činnosti nemůže být dosaženo uspokojivě členskými státy na úrovni ústřední, regionální či místní, ale spíše jich, z důvodu jejího rozsahu či účinků, může být lépe dosaženo na úrovni Unie“*[36]

V rámci zásady proporcionality pak „nepřekročí obsah ani forma činnosti Unie rámec toho, co je nezbytné pro dosažení cílů Smluv.“ Cíle zakotvené ve Smlouvách primární práva jsou tedy určitým objektivním kritériem činnosti Evropské unie, které musí Unie vždy respektovat a zohlednit.

Mechanismy pro kontrolu dodržení zásady subsidiarity a proporcionality se uplatňují před samotným přijetím návrhu legislativního aktu. Postup této kontroly blíže konkretizuje Protokol o používání zásad subsidiarity a proporcionality. Dle

[32] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 155.
[33] Smlouva o fungování Evropské unie, Článek 4
[34] Smlouva o fungování Evropské unie, Článek 5
[35] Smlouva o fungování Evropské unie, Článek 2, Odstavec 5
[36] Smlouva o Evropské unii, Článek 5, Odstavec 3

Protokolu vede komise před předložením návrhu legislativního aktu konzultace, v rámci kterých má být hodnoceny především regionální a místní dopady zamýšlené činnosti. Každý legislativní návrh Komise musí být řádně odůvodněn, a to kromě jiného i z hlediska zásady subsidiarity a proporcionality.[37]

Na základě Protokolu jsou všechny legislativní návrhy postupovány vnitrostátním parlamentům. Ty disponují kontrolními mechanismy, které ve výsledku mohou vést k nepřijetí předkládaného legislativního návrhu. V závislosti na okolnostech uplatnění těchto mechanismů jsou popořadě označovány jako mechanismus žluté, oranžové a červené karty. Pokud je i přes výhrady vnitrostátních parlamentů a uplatnění kontrolních mechanismů legislativní návrh přijat, jsou členské státy aktivně legitimovány k podání žaloby na neplatnost k Soudnímu dvoru Evropské unie.

Mechanismus žluté karty je aktivován, pokud třetina vnitrostátních parlamentů předloží stanovisko, ve kterém dospěje k závěru, že legislativním návrhem došlo k porušení zásady subsidiarity. Komise posléze návrh znovu přezkoumává a může jej odložit.

Mechanismus oranžové karty umožňuje zastavit legislativní proces, pokud Komise nadále trvá na projednání legislativního návrhu, i když je nadpoloviční většinou vnitrostátních parlamentů konstatován jeho rozpor se zásadou subsidiarity. O zastavení legislativního procesu pak rozhoduje Rada nebo Evropský parlament.

Červená karta je specifickým mechanismem, který umožňuje zablokování využití zvláštní přechodové klauzule v oblastech rodinného práva s mezinárodním prvkem.[38]

3.1.3 PRAMENY PRÁVA EU

Hlavní prameny práva Evropské unie jsou označovány jako primární právo a sekundární právo. Primární právo představují samotné zakládací smlouvy EU – Smlouva o Evropské unii (SEU), Smlouva o fungování EU (SFEU), Smlouvu o založení Evropského společenství pro atomovou energii, dále například smlouvy o přistoupení jednotlivých členských států a další. Sekundární právo představují

[37] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 157.
[38] Tamtéž S. 158.

především jednostranné akty EU, které jsou vydávány na základě „zmocnění“, obsaženého ve smlouvách primárního práva. Jednostrannými, právně závaznými akty, které jsou přijímány unijním legislativním postupem, jsou nařízení, směrnice a rámcová rozhodnutí.

3.1.4 ZÁSADY A HODNOTY EVROPSKÉ UNIE

Evropská Unie je demokratickým uskupením států, které je založeno na respektování a ochraně přirozených hodnot lidství a na dodržování základních lidských práv a svobod. Článek 2 Smlouvy o Evropské Unii konkretizuje: *„Unie je založena na hodnotách úcty k lidské důstojnosti, svobody, demokracie, rovnosti, právního státu a dodržování lidských práv, včetně práv příslušníků menšin. Tyto hodnoty jsou společné členským státům ve společnosti vyznačující se pluralismem, nepřípustností diskriminace, tolerancí, spravedlností, solidaritou a rovností žen a mužů.“*[39] Tyto jsou základní předpokladem jakékoliv další činnosti a fungování Evropské Unie, včetně legislativní činnosti. Účelem legislativní činnosti je vždy naplňování cílů Unie, tedy podpory obecného blahobytu, ekonomického rozvoje, ochrana přírody a krajiny a v neposlední řadě zachování míru[40]

3.2 DIGITALIZACE V EU – EGOVERNMENT VE SPOLEČNÉ EVROPĚ

Úspěšná digitální transformace veřejné správy je jedním z klíčových elementů současnosti v rámci celé Evropské unie. Snaha o koordinaci a společný postup v této oblasti je jednou z priorit. *„Elektronická veřejná správa (eGovernment) podporuje správní procesy, zvyšuje kvalitu služeb a také vnitřní účinnost veřejného sektoru.“*[41] Využívání digitálních technologií ve veřejné správě má nejen ekonomický, ale i sociální přínos pro společnost. Digitalizace veřejné správy zjednodušuje veškerou interakci občanů a podniků s příslušnými státními orgány, snižuje administrativní zátěž, snižuje finanční náklady, zajišťuje mnohem větší transparentnost a v neposlední řadě přispívá ke konkurenceschopnosti Evropské unie.[42] Logickými důsledky efektivní veřejné správy je pak samozřejmě

[39] Smlouva o Evropské unii, Článek 2
[40] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 195.
[41] Akční plán EU pro „eGovernment“ na období 2016–2020 Urychlování digitální transformace veřejné správy, COM/2016/0179 final S. 1.
[42] Tamtéž, S. 1.

větší atraktivita Evropské unie pro investory, lepší podmínky pro podnikání, živnostenskou činnost a každodenní život občanů.

Evropská vize je taková, že do roku 2020 *„budou orgány veřejné správy a veřejné instituce v Evropské unii otevřené a měly by podporovat začlenění a všem občanům a podnikům v EU budou bez ohledu na hranice poskytovat uživatelsky vstřícné, účinné, komplexní digitální veřejné služby.“*[43]

Koordinace a soulad právních předpisů na celoevropské úrovni je zásadním předpokladem pro realizaci vytyčených cílů. Vlastní úsilí jednotlivých států je samozřejmě vždy vítané, nicméně v určitých případech nevhodné, neboť může mít za následek roztříštěnost právní úpravy, a to jak z hlediska materiálního, tedy obsahu, tak z hlediska časového, tedy příliš pozdnímu přijetí odpovídající regulace a zaostávání některých členských států za jinými. Dle Evropské komise je nutné odstranění digitálních překážek a vytvoření otevřeného, důvěryhodného a efektivního digitálního prostředí a v neposlední řadě také zabránění dalšímu rozdělování právní úpravy.[44]

3.3 PRAVOMOC EU V OBLASTI REGULACE EGOVERNMENTU

V podkapitole 3.1.1 byly stručně popsány pravomoci Evropské unie, jejich druhy a základní zásady činnosti. V rámci eGovernmentu je nejprve nutné zkoumat, zda a v jakém rozsahu disponuje Evropská unie odpovídající pravomocí pro vydávání právně závazných aktů pro tuto oblast. Na základě zásad demokratického právního státu, ke kterým se hlásí i celá Evropská unie je vždy nutné, aby byly akty sekundárního práva EU vytvářeny a přijímány oprávněným orgánem v mezích jeho působnosti a pravomoci (kompetencí).

Při vytváření právní regulace určité oblasti se dále v rámci legislativního procesu samozřejmě řeší nejrůznější otázky. Ptáme se po samotném smyslu normy, proč dané společenské vztahy potřebují regulovat, do jaké míry a jakým způsobem. Jsou analyzovány dopady takové regulace, přínos pro stát, přeneseně Unii a další aspekty. V zemích OECD se jedná již o standardizovaný proces, označovaný jako

[43] Akční plán EU pro „eGovernment“ na období 2016–2020 Urychlování digitální transformace veřejné správy, COM/2016/0179 final S. 1
[44] Tamtéž, S. 2.

Regulatory Impact Analysis (RIA) neboli hodnocení dopadů regulace.[45] Naprosto zásadní je zmiňovaná otázka legality a legitimity daného předpisu.

Sekundární právo Evropské unie vzniká na základě zmocnění z primárních smluv. Obecně je normotvorba Evropské unie realizována pomocí nařízení, směrnic a rozhodnutí. *„Nařízení je obecně závazné, přímo použitelné a má zpravidla přímý účinek. Má v zásadě charakter zákona s celounijní působností"*[46] Tedy nařízení je striktním způsobem regulací, která zamýšlené následky způsobuje ve všech členských státech bezprostředně. Je přímo účinné a má jednotnou formu pro celou Unii. Přímý účinek nařízení garantuje přímou aplikaci obsažených právních norem ve všech členských státech vnitrostátními orgány a možnost jednotlivce dovolávat se takové aplikace.[47] V případě eGovernmentu je velmi významným například Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, o kterém bude podrobněji pojednáno níže.

Naproti tomu směrnice *„stanoví pro všechny členské státy určitý rámec, tedy společné zásady, resp. základní pravidla nebo minimální standard. Vlastní úprava v takto daném rámci zůstává v dispozici členských států "*[48]. Jinými slovy, členským státům je stanoveno, čeho má být dosaženo, avšak jakým způsobem daného cíle dosáhnou, je na jejich vlastním uvážení a provedení.

Rozhodnutí je označením pro další normativní i individuální akty, které mají účinky jako nařízení. Je definováno velmi obecně v článku 288 SFEU: *"Rozhodnutí je závazné v celém rozsahu. Pokud jsou v něm uvedeni ti, jimž je určeno, je závazné pouze pro ně. "*[49]

Vždy je tedy nutné posoudit konkrétní záměr, čeho má být v rámci unijní úpravy dosaženo, jaké prostředky mají či nemají být užity a jaký má být výsledek. Celkový kontext a okolnosti dané regulace jsou zásadní, nejinak je tomu v oblasti eGovernmentu a digitalizace. Právních aktů zabývajících se touto oblastí je v EU

[45] Více k hodnocení dopadů regulace například na http://www.oecd.org/regreform/regulatory-policy/ria.htm (v anglickém jazyce), nebo https://www.vlada.cz/cz/ppov/lrv/ria/hodnoceni-dopadu-regulace-160402/ (v českém jazyce)
[46] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 108.
[47] Tamtéž, S. 109
[48] Tamtéž, S. 109.
[49] Smlouva o fungování Evropské unie, Článek 288

skutečně mnoho a konstantně jich přibývá, což mimo jiné nepochybně svědčí o značném úsilí dosáhnout v této oblasti pokroku. Kvalita a reálná použitelnost daných předpisů je samozřejmě věc druhá.

V každém takovém aktu sekundárního práva EU (např.: nařízení) je uvedeno, na základě kterého článku smlouvy primárního práva je daný akt vydán, a tím je i zaručena celková legitimita. *„Legislativní činnost může být vykonávána jen v případech, kdy byla Unii členskými státy svěřena legislativní pravomoc. Tato pravomoc je pak v legislativním aktu konkretizována odkazem na příslušné ustanovení primárního práva, které je legislativním zmocněním a právním základem pro vydání legislativního aktu a které také v zásadě určuje postup pro jeho přijetí.“* [50] V oblasti eGovernmentu však již zde vzniká částečný problém.

Absolutním základem pro vytváření a přijímání právně závazných aktů Evropské unie je zásada svěřených pravomocí dle článku 5 Smlouvy o Evropské unii a následné vymezení oblastí, které spadají do odpovídajících kategorií daných pravomocí. Evropská unie však nedisponuje na základě primárního práva odpovídající pravomocí regulovat oblast veřejné správy jednotlivých členských států, a tedy „*ve výsledku chybí také kompetenční základ pro prosazování jednotné strategie v oblasti eGovernmentu*“[51].

Dochází k situacím, kdy je velmi složité odůvodnit právní akty sekundárního práva EU, které svým obsahem do jisté míry (spíše nepřímo) ovlivňují veřejnosprávní regulaci členských států, odpovídajícím právním základem. Například v případě Směrnice Evropského parlamentu a Rady 2014/55/EU ze dne 16. dubna 2014, o elektronické fakturaci při zadávání veřejných zakázek je odkazováno na ustanovení článku 114 SFEU, o sbližování právních předpisů. Jedná se ale o poměrně obecné ustanovení, kdy zkráceně orgány EU „*přijímají opatření ke sbližování ustanovení právních a správních předpisů členských států, jejichž účelem je vytvoření a fungování vnitřního trhu.*“[52] Vhodnou interpretací lze dané ustanovení v podstatě použít jako velmi obecný právní základ a odůvodnění pro téměř každý sekundární právní akt EU. Právě v oblasti

[50] TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533, S. 195.
[51] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 204.
[52] Smlouva o fungování Evropské unie, Článek 114

eGovernmentu je často užívána „nutnost rozvoje vnitřního trhu“ jako nejen právní základ a argument pro přijetí dané úpravy.[53]

Z dosavadní praxe je zřejmé, že onen chybějící jasný primární právní základ či obecnější odůvodnění přijetí určitého sekundárního aktu práva EU nemusí nutně za určitých okolností zakládat pochybnosti o legalitě takového aktu. V tomto případě je zde jasná a zřejmá snaha všech členských států postupovat určitým způsobem, kterou nejen deklarují společnými prohlášeními, ale aktivně podnikají kroky k přijetí vhodné právní úpravy. Právní normy sekundárního práva EU tedy regulují určité oblasti, týkající se veřejné správy, neboť je toto pro dosažení cílů eGovernmentu a jednotného vnitřního trhu Evropské unie nezbytné. Jako určitá garance legitimity daných předpisů zde působí zmiňovaná zásada subsidiarity dle článku 2 SEU a oprávnění z ní pro členské státy plynoucí. Níže popisované deklarace, akční plány i strategie využívají orgány EU právě k prosazování jednotné strategie a k co nejvyšší možné míře zachování legitimity vytyčených postupů. „*Orgány EU podnikají rozmanité snahy, aby zajistili zamýšlený efekt opatření v oblasti eGovernmentu na základě společné shody ve všech členských státech, i když chybí primární kompetence a právní základ pro společnou realizaci cílů v této oblasti.“*[54] Jedná se například o záměry zveřejňované Komisí označované termínem „soft law“, které však, jak už jejich označení napovídá, nejsou pro členské státy právně závazné a tedy ani vynutitelné. Protože jsou však vydávané orgánem EU, nepochybně vyvolávají legitimní očekávání a důvěru v jejich realizaci a snad také určitou závaznost neformální.

3.3.1 TALLINNSKÁ DEKLARACE

V říjnu roku 2017 na vrcholné schůzce ministrů členských států příslušných pro eGovernment bylo vydáno toto společné prohlášení. Není náhodou, že se tak stalo zrovna v Tallinnu, protože Estonsko je v současné době na evropské špičce v indexu digitalizace a eGovernmentu. Deklarace obsahuje priority a cíle, kterých má být dosaženo a stanoví další kroky pro konstantní a efektivní rozvoj. Tallinnská

[53] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 204.
[54] Tamtéž, S. 205.

deklarace je vnímána jako důležitý akt mezi členskými státy, kdy neformálně zavazuje k plnění stanovených cílů.[55]

Ministři 32 členských států Evropské unie a Evropského sdružení volného obchodu v tallinské deklaraci konstatují, že Evropa čelí závažným společenským, ekonomickým a politickým změnám. Uvědomují si, že digitální pokrok mění základ naši společnosti, ekonomický základ fungování celé Unie a že na tyto změny a výzvy musí být vhodně reagováno.

„Vývoj eGovernmentu je základním předpokladem úspěšné odpovědi na tyto výzvy a rozvoj digitálních technologií. Digitální transformace může posílit důvěru ve vlády kromě jiného zvýšením transparentnosti, přístupnosti, spolehlivosti a integrity veřejné správy.“[56]

Dále je v tallinnské deklaraci konstatováno, že digitální transformace veřejné správy je kolektivním snažením na národních, regionálních i lokálních úrovních v rámci členských států a Evropských institucí, při respektování dělby kompetencí. Společné snahy mohou být velmi usnadněny intenzivní spoluprací, efektivním řešením interoperability a sdílením poznatků z již úspěšně realizovaných pokroků.[57]

3.3.2 AKČNÍ PLÁNY

Komise prezentuje záměry pro rozvoj eGovernmentu v Akčních plánech, které jsou vydávány ve formě sdělení. Jedná se vždy o pětiletou perspektivu, kdy je v současné době realizován plán pro léta 2016 – 2020, který nese podtitul „*Urychlování digitální transformace veřejné správy*.“[58] Ve své podstatě jsou tyto akční plány politickými nástroji, jež mají za cíl sjednotit a koordinovat společný postup všech členských států. Obsahují komplexní vize a nejzásadnější cíle, kterých má být v určitém období dosaženo. Do jaké míry se tak daří, je otázka zčásti subjektivního hodnocení každého občana, avšak předchozí akční plán z let 2011-2015 dle oficiálních zdrojů *„přispěl k soudržnosti vnitrostátních strategií v oblasti*

[55] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017, Úvod
[56] Tamtéž, Úvod
[57] Tamtéž, Úvod
[58] Akční plán EU pro „eGovernment“ na období 2016–2020 Urychlování digitální transformace veřejné správy, COM/2016/0179 final

elektronické veřejné správy, jakož i k výměně osvědčených postupů a k interoperabilitě řešení mezi členskými státy a vedl k rozvoji technologických prvků, které zásadním způsobem usnadňují přístup k veřejným službám a jejich využívání"[59].

Komise předložila v roce 2017 ve formě sdělení taktéž Akční plán interoperability. Obsahuje 22 opatření, cílů, časový plán realizace a příslušnost. Má sloužit jako příručka pro prosazování evropského rámce interoperability.[60] Charakterizované mechanismy nejsou zdaleka k dispozici, jedná se teprve o avizovaný postup a cíle.

Formulace v akčních plánech působí velice slibně a jejich potencionální naplnění zcela jistě posune digitalizaci veřejné správy na další úroveň. Je zcela jistě pozitivní, že se členské státy dokážou dohodnout na konkrétních řešeních na evropské úrovni, avšak vzhledem k zmiňované chybějící primární kompetenci pro zasahování do úpravy veřejné správy jednotlivých států bude včasná a kvalitní realizace přinejmenším obtížná.

3.3.3 STRATEGIE

Evropská komise ve formě sdělení zveřejnila taktéž „Strategii pro jednotný digitální trh v Evropě". Komise si uvědomuje obrovský potenciál informačních a komunikačních technologií, dokonce je považuje za základ *„všech moderních inovativních ekonomických systémů."*[61] Představované nástroje sice do sféry veřejné správy bezprostředně zasahují poměrně nevýrazně, neboť se primárně jedná o strategii dopadající na jednotlivé tržní aktéry, nicméně nepřímý vliv zde je již markantnější. Jde o velmi důležité sdělení, které opět nepřímo potvrzuje nezbytnost prioritní diskuze o digitalizaci a nutnost evropské spolupráce na nejvyšší úrovni. *„Jednotný digitální trh zajišťuje volný pohyb zboží, osob, služeb a kapitálu a pro občany a podniky znamená bezproblémový přístup k činnostem on-line a k jejich provádění za podmínek spravedlivé hospodářské soutěže, s vysokou ochranou*

[59] Akční plán EU pro „eGovernment" na období 2016–2020 Urychlování digitální transformace veřejné správy, COM/2016/0179 final
[60] Evropský rámec interoperability – Strategie provádění – Akční plán interoperability, COM(2017) 134 final, Annex 1
[61] Strategie pro jednotný digitální trh v Evropě, COM(2015) 192 final, Úvod

spotřebitelů a osobních údajů bez ohledu na státní příslušnost nebo místo bydliště"[62]

Další strategií, která byla Evropskou komisí prezentována ve formě sdělení, je Evropský rámec interoperability – Strategie provádění. Tato strategie uvádí již konkrétnější záměry v oblasti digitalizace veřejné správy. Daná ustanovení ve strategii opět nemají přímou právní závaznost, působí tedy spíše jako doporučení, ostatně jsou tak v samotném sdělení i označována. Uvedená doporučení mají orgánům veřejné správy obecně pomoci zlepšit řízení svých činností, přispět k zefektivnění procesů podporující digitální služby a zajistit nezbytný soulad právních předpisů. Výsledkem má být lepší řízení činností v členských státech, využívání společných modelů při zavádění digitálních služeb veřejné správy a reflektování zájmů občanů ostatních členských států EU. V neposlední řadě také komplexní správa všech údajů a jejich snadnější organizace.[63]

3.4 ZÁKLADNÍ ZÁSADY A VÝCHOZÍ BODY EGOVERNMENTU

Je zde několik základních zásad a výchozích bodů, které ve své podstatě podmiňují realizaci cílů v oblasti eGovernmentu. Jsou sice deklarovány v Akčním plánu Evropské komise pro eGovernment pro roky 2016-2020, ale vzhledem k tomu, že agenda eGovernmentu je typickým průřezovým tématem, je potřeba jejich základ hledat ve značném množství nejrůznějších sekundárních právních aktů a dalších dokumentů Evropské Unie.[64]

3.4.1 DIGITAL BY DEFAULT (STANDARDNĚ DIGITALIZOVANÉ)

Jak již označení této zásady napovídá, týká se požadavku digitalizace jako výchozího základu pro činnosti v rámci eGovernmentu. *„Orgány veřejné správy by měly jakožto upřednostňovanou možnost poskytovat služby digitálně; zároveň by však měly udržovat otevřené i další kanály pro ty, kteří nejsou buď z vlastního rozhodnutí, nebo z nutnosti připojeni."*[65] Doporučuje tedy standardně

[62] Strategie pro jednotný digitální trh v Evropě, COM(2015) 192 final, Úvod
[63] Evropský rámec interoperability – Strategie provádění – Akční plán interoperability, COM(2017) 134 final
[64] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 203.
[65] Akční plán EU pro „eGovernment" na období 2016–2020 Urychlování digitální transformace veřejné správy, COM(2016) 179 final, strana 4

upřednostňovat digitální formu činnosti, avšak s ohledem na to, že by nucená elektronická (digitální) forma jednání mohla působit diskriminačně[66] a pro mnohé může být stále variantou volby „klasická“ komunikace a způsoby vyřizování svých záležitostí. Dále je obsahem zásady také jisté doporučení zřízení jednotného kontaktního místa, kde by mohly být veřejné služby vyřizovány. Smyslem této zásady je tedy stanovení určitého směřování, avšak stále se souběžným sekundárním zachováním současného „analogového“ stavu.

3.4.2 INTEROPERABILITA

„Tradičním problémem v případě elektronického propojení různých systémů eGovernmentu je skutečnost, že tyto dva systémy spolu nejsou kompatibilní.“[67] Právě dlouho chybějící jednotná či nejasná strategie má za následek tento stav, neboť se dané systémy vyvíjejí odlišným způsobem. Orgány EU se tomuto stavu pochopitelně snaží právně předcházet a sjednocovat společný postup všech členských států. Zásadním je v tomto směru rozhodnutí Evropského parlamentu a Rady EU 2015/2240, kterým se zavádí program pro řešení interoperability a společné rámce pro evropské orgány veřejné správy, podniky a občany (program ISA2) jako prostředek modernizace veřejného sektoru. Toto rozhodnutí je odůvodňováno především odkazem na článek 172 SFEU, který umožňuje Evropskému parlamentu a Radě přijímat opatření, týkající se hlavních směrů, zahrnující cíle, priority a hlavní rysy opatření předpokládaných v oblasti transevropských sítí a jejich interoperability[68]. Interoperabilita je v tomto Rozhodnutí legálně definována jako: „*schopnost interakce různých nesourodých organizací, která přispívá k dosažení vzájemně prospěšných a dohodnutých společných cílů a zahrnuje sdílení informací a znalostí mezi organizacemi pomocí podnikových procesů, které tyto organizace podporují, na základě výměny údajů mezi jejich systémy informačních a komunikačních technologií (IKT);*“[69].

Reflektována je interoperabilita samozřejmě v Akčním plánu Evropské komise pro eGovernment pro léta 2016-2020. *„Orgány veřejné správy, veřejné*

[66] Viz. například Článek 3, odstavec 3 Smlouvy o Evropské Unii: „Unie bojuje proti sociálnímu vyloučení a diskriminaci, podporuje sociální spravedlnost a ochranu, rovnost žen a mužů, mezigenerační solidaritu a ochranu práv dítěte.“
[67] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 210.
[68] Smlouva o fungování Evropské unie, Článek 172
[69] ROZHODNUTÍ (EU) 2015/2240 ze dne 25. listopadu 2015, Článek 2, odstavec 1

subjekty, podniky a uživatelé sami nejlépe vědí, co potřebují. Volba systémů a technologií pro distribuované či centralizované koncepce by měla vplné míře odpovídat jejich volbě a potřebám, je však nutné, aby zcela respektovala dohodnuté požadavky na interoperabilitu"[70] Je zde určitým způsobem naznačena možnost volby, avšak na druhé straně stanoven požadavek (i když právně nezávazný), aby vždy byla primárně zohledněna interoperabilita daných prostředků.

Částečně je interoperabilita také zmiňována v Nařízení evropského parlamentu a rady EU 2015/848, o insolvenčním řízení. V článku 26, kde se hovoří o nákladech v souvislosti s vytvořením a propojením insolvenčních rejstříků všech členských států, obsahuje odstavec 2 následující ustanovení: *„Každý členský stát nese náklady spojené s vytvořením a přizpůsobením svých vnitrostátních insolvenčních rejstříků tak, aby byly interoperabilní s portálem evropské e-justice, i náklady spojené se správou, provozem a údržbou těchto rejstříků"*[71]

Dále je zajištění interoperability právně předpokládáno v již zmiňovaném Rozhodnutí 2015/2240: „V oblasti práva obchodních společností směrnice Evropského parlamentu a Rady 2012/17/EU (2) požaduje dosažení interoperability v oblasti ústředních, obchodních a podnikových rejstříků členských států pomocí centrální platformy – jinými slovy, propojení všech obchodních rejstříků a jednotný přístup ve všech členských státech, *„čímž se v Unii zlepší právní jistota v podnikatelském prostředí."*

V neposlední řadě zmiňuje interoperabilitu také Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu: „*Pro přeshraniční uznávání kvalifikovaných elektronických podpisů jsou předpokladem přeshraniční interoperabilita a uznávání kvalifikovaných certifikátů.*"[72]

Počet právních aktů obsahujících ustanovení týkající se interoperability je tedy více než značný. Dosažení optimálního stavu na celoevropské úrovni bude pochopitelně velmi složité, neboť vyžaduje nejen společné právní, ale i technické

[70] Akční plán EU pro „eGovernment" na období 2016–2020 Urychlování digitální transformace veřejné správy, COM(2016) 179 final, Strana 4
[71] NAŘÍZENÍ (EU) 2015/848, o insolvenčním řízení, Článek 26, odstavec 2
[72] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, Důvod 54

postupy. *„Dosavadní zkušenosti z některých členských států hovoří o tom, že jen sjednocení rejstříků na vnitrostátní úrovni je velmi obtížné.“* [73]

Současné rumunské předsednictví Rady EU a zástupci Evropského parlamentu dospěli 5. 2. 2019 k předběžné dohodě o návrzích dvou zásadních nařízení, které zavádějí nové složky v rámci interoperability v oblasti zjišťování totožnosti osob a její ochrany. Je plánováno zřízení Evropského vyhledávacího portálu, který by umožnil příslušným orgánům prohledávat několik informačních systémů EU zároveň s využitím biografických i biometrických údajů občanů EU a také občanů třetích zemí, a jejich následné srovnávání. [74]

3.4.3 JEDNOTNÝ PŘÍSTUP

Jednotným přístupem k veřejným službám se zabývá aktuální nařízení Evropského parlamentu a Rady (EU) 2018/1724 ze dne 2. října 2018, kterým se zřizuje jednotná digitální brána pro poskytování přístupu k informacím, postupům a k asistenčním službám a službám pro řešení problémů a kterým se mění nařízení (EU) č. 1024/2012. Účelem je umožnit všem občanům co nejjednodušší získávání potřebných informací a digitální používání veřejných služeb. Nařízení k tomuto účelu předpokládá zřízení jednotného přístupového portálu k co možná nejširšímu spektru veřejných služeb a jejich vzájemné propojení.[75] To v praxi znamená, že dosavadní roztříštěnost správní agendy by postupně měla směřovat k tomu, aby co největší množství veřejnosprávních záležitostí bylo možné vyřídit pouze v rámci jednoho kontaktního bodu. Tímto bodem by měl být internetový portál veřejné správy, kdy po zaručené identifikaci občana/podnikatele apod. bude možné právně jednat jako na běžném úřadě.

V nařízení je odkazováno na články 21(2), 48 a 114(1) SFEU ve vztahu k článku 26(2) SFEU. Článek 26(2) SFEU obsahuje ustanovení o vnitřním trhu, předpokládá *„přijímání opatření k vytvoření nebo zajištění fungování vnitřního*

[73] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 213.
[74] Interoperabilita mezi informačními systémy EU: Předsednictví Rady a Evropský parlament dosáhly předběžné dohody - Consilium[online]. Home - Consilium [cit. 25.3.2019]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2019/02/05/interoperability-between-eu-information-systems-council-presidency-and-european-parliament-reach-provisional-agreement/
[75] Nařízení Evropského parlamentu a Rady (EU) 2018/1724 ze dne 2. října 2018, kterým se zřizuje jednotná digitální brána pro poskytování přístupu k informacím, postupům a k asistenčním službám a službám pro řešení problémů a kterým se mění nařízení (EU) č. 1024/2012

trhu.“[76] Opět zde v kombinaci s článkem 114 SFEU, O souladu právních předpisů, působí jako legální základ pro přijetí tohoto sekundární aktu EU. Zásadním argumentem je opět zajištění fungování vnitřního trhu, přičemž má přijetí tohoto návrhu značný dopad do oblasti digitalizace veřejné správy. Důležitý je i odkaz na článek 21 SFEU, o svobodě pohybu, který je svým způsobem doplnění celkového záměru sjednocování vnitřního trhu bez jakýchkoliv hranic a omezení v rámci členských států EU.

3.4.4 ZÁSADA „POUZE JEDNOU“

Zásada pouze jednou, v anglickém znění „Once only principle“, směřuje k dosažení vysoké míry efektivity, transparentnosti a úspory času při činnostech v oblasti veřejné správy, především z hlediska jejich adresátů.

„Orgány veřejné správy by měly zaručit, že občané a podniky budou muset tytéž informace poskytnout orgánům veřejné správy pouze jednou. Je-li to povolené, orgány veřejné správy přijímají opatření s cílem tato data opětovně interně používat, přičemž náležitě dodržují pravidla ochrany údajů, aby občané ani podniky nebyli dodatečně zatěžováni.“[77]

Právní základ pro tuto zásadu je obsažen ve Směrnici Evropského parlamentu a Rady 2013/37/EU ze dne 26. června 2013, kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru.

Zásada a směrnice mají zajistit, že tytéž informace budou od občanů a podniků vyžadovány pouze jednou, při prvotním vstupu či jednání. Posléze již veřejná správa bude mít dané informace uložené v databázích a nebude nutné je znovu od občanů vyžadovat. V rámci interoperability a přeshraničního přístupu by tyto informace měly být dostupné příslušným orgánům v celé EU bez nutnosti je znovu poskytovat, například při pobytu občana v jiném členském státě.

Dle studie, která byla provedena Evropskou komisí, se však tuto zásadu daří naplňovat jen omezeně. Překážky v podobě nedostatečného technického zázemí, nevyhovující organizace a komunikace mezi jednotlivými složkami úřadů a v neposlední řadě také nedostatečná právní úprava značně omezují aplikaci této

[76] Smlouva o fungování Evropské unie, Článek 26, odstavec 2
[77] Akční plán EU pro „eGovernment“ na období 2016–2020 Urychlování digitální transformace veřejné správy, COM(2016) 179 final, strana 3

zásady, a s ní spojené usnadnění komunikace mezi veřejnou správou a občany. Toto se dle studie stále týká většiny členských států.[78]

Problematické je zejména zajištění ochrany dat, nedostatečná interoperabilita rejstříků a celková absence zásadnější politické vůle k efektivnějšímu prosazování tohoto principu.

3.4.5 KYBERBEZPEČNOST

Rozvoj informačních technologií ve veřejném, ale i soukromém sektoru s sebou samozřejmě přináší závažná rizika v mnoha formách. Kyberterorismus, hacking, phishing, špionáž, krádeže dat, identity a software a další kybernetické zločiny se stávají čím dál tím víc sofistikovanějšími a jsou vysoce reálným bezpečnostním rizikem s potencionálně velice nebezpečnými následky.[79] Je potřeba efektivně bránit evropskou počítačovou infrastrukturu a počítačovou infrastrukturu jednotlivých členských států (kyberprostor). Kyberbezpečnost nyní patří k prioritám v rámci celé Evropské unie.[80]

Základem je samozřejmě kvalitní právní regulace v kombinaci s fungováním specializovaných evropských a státních institucí. Je třeba zatraktivnit službu v těchto institucích pro IT experty, neboť je známým faktem, že v soukromém sektoru je IT odvětví mnohem lépe platově ohodnocené. Následkem je pak podstav IT specialistů ve sféře veřejné. Dále je nutné zajistit odpovědné chování státních zaměstnanců a v neposlední řadě také každého občana.

V rámci kybernetické bezpečnosti hovoříme mnoha odvětvích. Dle útoku a cíle se rozlišuje kybernetická kriminalita, kybernetický terorismus, kybernetická špionáž a kybernetická válka. Kybernetická kriminalita je v podstatě kybernetickou trestnou činností, tedy trestnou činností, která má spojitost s určitým způsobem nakládání s daty. Kybernetický terorismus je digitální obdobou terorismu, kdy má za cíl vyvolat strach, paniku a další ochromení společnosti za použití agresivních technik. Zpravidla je takováto činnost prováděna za dosažením cílů s ideologickým,

[78] EU-wide digital Once-Only Principle for citizens and businesses:
Policy options and their impacts [online]. European Commission [cit. 25.3.2019]. Dostupné na http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42301
[79] Savin, A. (2017). EU internet law. Northampton, MA: Edward Elgar Pub. ISBN: 9781784717957. S. 328
[80] Závěry Evropské rady, 18. října 2018 (EUCO 13/18)

náboženským a dalším podtextem. Kybernetická špionáž je obdobou špionáže, kdy se určité subjekty snaží pomocí zisku citlivých dat dosáhnout převahy. Kybernetická válka je ve své podstatě válečným konfliktem, kdy je cíleno na digitální infrastrukturu státu.

Pokud se týče přímo trestněprávní politiky v oblasti kyberbezpečnosti, má Evropská unie jako celek jen omezené možnosti, neboť kompetence v záležitostech trestního práva náleží převážně členským státům.[81] Důraz je tedy kladen spíše na preventivní ochranu a spolupráci.

Více o kybernetické bezpečnosti jakožto klíčovém základu pro rozvoj eGovernmentu ve 4. kapitole této práce.

3.4.6 OCHRANA OSOBNÍCH ÚDAJŮ

Získávání, shromažďování, ukládání, zveřejňování a třídění osobních údajů získalo v digitálním věku zcela nový rozměr. Celosvětový dosah internetu zcela přepsal zažité standardy, kdy například šíření osobních údajů je možné v obrovském rozsahu a v rámci vteřin. Osobní údaje jsou poté v podstatě neodstranitelné. Ochrana osobních údajů je klíčovým prvkem moderní digitální doby, kdy je jasná a přísná regulace jistě žádoucí. Při činnosti orgánů veřejné správy, tedy i při elektronickém výkonu těchto činností dochází samozřejmě k enormnímu nakládání s osobními údaji a jejich zpracovávání.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, známé jako GDPR (General Data Protection Regulation) přineslo zásadní změny a opatření pro ochranu osobních údajů. Pro rozvoj eGovernmentu má zásadní význam.

Více o ochraně osobních údajů jakožto klíčovém základu pro rozvoj eGovernmentu ve 4. kapitole této práce.

[81] Savin, A. (2017). EU internet law. Northampton, MA: Edward Elgar Pub. ISBN: 9781784717957. S. 329

3.4.7 OTEVŘENOST A TRANSPARENTNOST

Další zásadou, která je velice podstatnou pro eGovernment, je transparentnost evidovaných dat a přístup k výsledkům těchto databází. Občanům musí být umožněn přístup k informacím, které vedou jednotlivé úřady a další orgány veřejné správy při zachování práva na ochranu osobních údajů.[82] Tyto informace mohou být relevantní například pro účely podnikání nebo obchodování na vnitřním trhu. Komise jde zde příkladem, kdy provozuje svůj vlastní otevřený portál, kde lze dohledat všechny veřejně dostupné informace, které byly publikovány orgány EU. Lze je užít také pro komerční účely.[83] Tato zásada úzce souvisí se zásadou „pouze jednou“ (once only principle). Částečná úprava je taktéž obsažena ve směrnici měrnici Evropského parlamentu a Rady 2013/37/EU ze dne 26. června 2013, kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru.

3.4.8 ELEKTRONICKÁ PRÁVNÍ KOMUNIKACE

S rozmachem digitálních technologií se čím dál tím více pro komunikaci užívá elektronických forem namísto analogových, „papírových“. Nejinak je tomu i v „komunikaci právní“, totiž elektronických právních transakcích prováděných „na dálku“ pomocí informačních a komunikačních technologií, a to jak v soukromém, tak veřejném sektoru. Nepochybně jde o velice pohodlný a rychlý způsob, kdy v ideálním případě zcela odpadá nutnost osobního kontaktu. Na druhou stranu s sebou provádění takových transakcí samozřejmě přináší určité zvýšené požadavky na svou formu a proces.

Klíčovým předpokladem v rámci užívání elektronických komunikačních kanálů při elektronických právních transakcích je právní jistota.[84] Zásada právní jistoty je jednou ze základních zásad právního státu[85], k dodržování této a dalších se všechny členské státy zavázaly ve Smlouvách primárního práva EU[86]. Je tedy nutné pomocí digitálních technologií zjistit totožnost jednajícího, celý proces

[82] Akční plán EU pro „eGovernment“ na období 2016–2020 Urychlování digitální transformace veřejné správy, COM(2016) 179 final, strana 3
[83] http://open-data.europa.eu
[84] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 285.
[85] HENDRYCH, Dušan, a kol. Právnický slovník. Praha: C. H. Beck, 2009. ISBN 978-80-7400-059-1. Heslo Právní jistota.
[86] Smlouva o Evropské unii, Preambule

autentizovat a tím zajistit legitimitu celé transakce. V souvislosti s digitálními technologiemi je ona právní jistota kromě jiného přímo závislá na zabezpečení konkrétní informační a komunikační technologie. Má-li být užíváno digitálních technologií pro uskutečňování relevantních právních transakcí, musí být tento postup podpořen technikou s odpovídající úrovní zabezpečení, která garantuje autenticitu takové transakce.[87] Je nutné zajistit, že určitý úkon činí skutečně ta osoba, za kterou se vydává, tedy zajistit, že je tato osoba důvěryhodně identifikována. V rámci vnitřního trhu Evropské Unie je pak více než důležité, aby tyto transakce bylo možné provádět i mezi členskými státy při zachování stejné míry autenticity, jako při provádění transakcí v rámci jednoho členského státu. Není tedy překvapující, že jsou předpisy upřesňující prostředky a postupy, na základě kterých posléze může být legitimita konkrétní transakce zajištěna, přijímány na celoevropské úrovni, a to zejména s odkazem na neustálou snahu o rozvoj vnitřního trhu EU.

Evropská Unie se zabývá elektronickou právní komunikací především v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, e elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Velice aktuální je Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace. Jak již název napovídá, směrnice vytvořila jednotná pravidla pro komunikaci vedenou v elektronické podobě.

3.4.9 ZÁKLAD PRO ELEKTRONICKOU ČINNOST VEŘEJNÉ SPRÁVY

Právní základ pro elektronickou činnost veřejné správy na celoevropské úrovni lze nalézt především v Chartě základních práv EU. Z hlediska eGovernmentu je odkazováno na tzv. právo na řádnou správu, vycházející z článku 41 Charty základních práv EU, kdy má každý občan EU právo nato, *„aby jeho záležitosti byly orgány, institucemi a jinými subjekty Unie řešeny nestranně, spravedlivě a v přiměřené lhůtě.“*[88] eGovernment zde sice opět výslovně zmíněn není z důvodů již rozebíraných v jiné kapitole této práce a je ponechávána širší

[87] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 285.
[88] Listina základních práv Evropské unie, Článek 41, Odstavec 1

interpretaci daných ustanovení, na základě které může být tento článek považován za základ pro elektronickou činnost veřejné správy.[89]

Z hlediska veřejné správy se lze taktéž odvolávat na odstavec 2, písmeno b tohoto článku, který deklaruje *„právo každého na přístup ke spisu, který se jej týká, při respektování oprávněných zájmů důvěrnosti a profesního a obchodního tajemství;“*[90] Na základě interpretace lze dovodit, že přístup může být i elektronický, protože jeho forma zde není výslovně stanovena. Z tohoto článku tedy vyplývá právo na možný elektronický přístup ke spisům vedených veřejnou správou.

Příklad fungující digitální veřejné správy v oblasti zaručené komunikace lze nalézt například ve Francii, kde od roku 2009 fungují zvláštní síťové systémy (pro soudy a pro státní zastupitelství), kdy jsou již veškerá podání realizována pouze elektronicky.[91]

[89] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 290.
[90] Listina základních práv Evropské unie, Článek 41, Odstavec 2, Písmeno b
[91] Réseau privé virtuel justice (RPVJ) a Réseau privé virtuel avocat [online] [cit. 25.3.2019]. Dostupné z: http://www.textes.justice.gouv.fr/art_pix/boj_20090005_0000_0001.pdf

4 POPIS A ZHODNOCENÍ STÁVAJÍCÍ PRÁVNÍ ÚPRAVY

Po abstraktnějším úvodu a popisu evropské politiky, záměrů a základních zásad v oblasti eGovernmentu se nyní budu konkrétněji zabývat některými předpisy a jejich praktickými dopady v členských státech. Pochopitelně nelze v rámci rozsahu této diplomové práce podrobně popsat veškerá nařízení, směrnice, rozhodnutí a další dokumenty, týkající se digitalizace veřejné správy, a ani to není cílem. Pro následující části jsem tedy vybral ty předpisy, které považuji za nejzásadnější a nejaktuálnější. Ani tyto předpisy však nelze podrobně popsat, kdy každý z nich samostatně by byl vhodným tématem na kvalifikační práci. Mým záměrem je obecně popsat, co je cílem daného předpisu a jak ovlivňuje právě eGovernment. Dále zhodnotím implementaci těchto předpisů v České republice a Německu.

4.1 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) Č. 910/2014 „EIDAS“

Důvěryhodná identifikace je esenciální pro rozvoj digitalizace veřejné správy. Pokud bude zaručena totožnost jednajícího, bude možné téměř veškerou komunikaci s úřady realizovat elektronicky

Průlomovým předpisem EU v oblasti elektronické identifikace a elektronické autentizace je Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, e elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, zkráceně známé jako nařízení „eIDAS“. Značná část tohoto předpisu začala být účinná již 1. 7. 2016, přičemž však účinnost některých dalších ustanovení byla pozdržena, a to i na základě výjimek, vyjednaných členskými státy.

Nařízení odkazuje na článek 114 Smlouvy o fungování Evropské Unie. Lze konstatovat, že budování důvěryhodného online prostředí je základem pro další hospodářský a sociální rozvoj. Elektronické transakce musí být důvěryhodným způsobem právní komunikace. Tato důvěryhodnost má být konstantně posilována a prohlubována, přičemž má být kladen důraz na zajišťování požadavku právní

jistoty elektronických transakcí, aby orgány veřejné moci a samozřejmě také občané a podniky využívali potenciálu digitálních technologií.[92]

V nařízení jsou cíle a záměry jasně definovány: *„Toto nařízení má zvýšit důvěryhodnost elektronických transakcí na vnitřním trhu tím, že poskytne společný základ pro bezpečnou elektronickou komunikaci mezi občany, podniky, orgány veřejné moci, čímž posílí efektivnost veřejných a soukromých on-line služeb, elektronického podnikání a elektronického obchodu v Unii.“*[93]

Cílem je také odstranění hraničních překážek a zajištění přeshraničního přístupu k elektronickým službám v rámci celé Evropské Unie, a to především pro účely veřejných služeb.[94] Lze odkázat na několik souvisejících základních zásad a výchozích bodů pro eGovernment, především „standardně digitalizované, interoperabilita a „jednotný přístup“. Harmonizace národních úprav má přispět ke společnému postupu v celé EU. Z těchto a dalších důvodů byla pravděpodobně také proto zvolena forma nařízení s přímým účinkem, aby byl zajištěn společný postup ve všech členských státech v co nejvyšší možné míře.

Aby bylo dosaženo výše uvedených cílů, je nařízení eIDAS zaměřeno na úpravu podmínek pro přeshraniční uznávání prostředků pro elektronickou identifikaci právnických a fyzických osob v rámci elektronického systému členských států. Zajištěna má být identifikovatelnost takových osob ve všech členských státech bez ohledu na státní příslušnost těchto osob, sídlo těchto osob nebo místo, kde tyto osoby právně jednají. Dále obsahuje regulaci pro služby vytvářející důvěru, zejména u elektronických transakcí.

Nařízení eIDAS také zavádí jednotná pravidla pro identifikační prostředky, kterými jsou elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.

[92] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, e elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, Důvod 1
[93] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, e elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, Důvod 2
[94] DONÁT, Josef. Nařízení eIDAS: komentář. V Praze: C.H. Beck, 2017. Beckovy komentáře. ISBN 978-80-7400-633-3. S. 45.

Nařízení eIDAS se snaží být moderním předpisem, reflektující naléhavou potřebu usnadnit a zároveň zaručit právní komunikaci, a to jak s ohledem na užívání této komunikace v rámci eGovernmentu, tak s ohledem na vnitřní trh a ekonomický prospěch. Je zde však několik problematických ustanovení, které se lépe demonstrují až v rámci implementace v jednotlivých členských státech.

4.1.1 ÚROVNĚ ZÁRUKY V NAŘÍZENÍ EIDAS

Nařízení stanoví tři úrovně záruk, nízká úroveň záruky, značná úroveň záruky a vysoká úroveň záruky. Nízká úroveň označuje prostředek pro elektronickou identifikaci, který nabízí omezenou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby. V rámci značné úrovně záruk je používán prostředek pro elektronickou identifikaci, který nabízí značnou míru spolehlivosti. Vysoká úroveň záruky je pak garantována prostředkem pro elektronickou identifikaci, který nabízí vyšší míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby než prostředek pro elektronickou identifikaci se značnou úrovní záruky. Komise stanoví podrobnosti v prováděcím nařízení z roku 2015.[95]

Úroveň záruky ve své podstatě závisí na formě a účelu daného jednání. Při některých elektronických právních transakcích není nutné vyžadovat vysokou úroveň záruky.

4.1.2 IDENTIFIKAČNÍ PROSTŘEDKY V NAŘÍZENÍ EIDAS

Mezi elektronické identifikační prostředky dle nařízení patří elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek. Elektronický podpis je z technického hlediska souborem binárních dat, které slouží k ověření totožnosti jednajícího, kterým může být pouze fyzická osoba. Nařízení eIDAS přiznává elektronickému podpisu rovnocenný právní účinek jako podpisu vlastnoručnímu, pokud je kvalifikovaný.[96]

[95] Prováděcí nařízení Komise 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014

[96] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, e elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, Článek 25, odstavec 2

Kvalifikovaný elektronický podpis musí splňovat nejvyšší nároky dle nařízení eIDAS a je uznáván jako nejvyšší možný způsob autentizace podepisujícího subjektu. Právní jistotu a důvěryhodnost takového podpisu z hlediska právního jednání zaručuje tzv. kvalifikovaný certifikát a to, že je podpis vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů. Kvalifikovaný certifikát je vydáván oprávněnou certifikační autoritou a jde o speciální součást podpisu. Kvalifikovaný prostředek pro vytváření elektronických podpisů může být například zvláštní USB token. Zde lze polemizovat, zda by v době digitálního rozmachu nebylo vhodné přiznat kvalifikovanému elektronickému podpisu rovnocenný právní účinek jako podpisu úředně ověřenému. Kombinace opatření zajišťuje dostatečný stupeň ochrany i garanci autentizace.

Elektronickou pečeť mohou oproti elektronickému podpisu užívat pouze právnické osoby. Elektronická pečeť slouží jako určitý garanční prostředek, kdy potvrzuje, že určitý dokument vytvořila určitá právnická osoby. Touto osobou je nejčastěji právě úřad, který takto potvrzuje platnost daného dokumentu.[97]

Je zde jasně specifikovaný požadavek, že identifikačním prostředkům nelze upírat jejich právní účinky jen z toho důvodu, že má elektrickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy. Také jej nelze ze stejných důvodů odmítat jako důkaz v soudním a správním řízení.[98]

V rámci rozvoje vnitřního trhu je zde požadavek na uznání takových identifikačních prostředků na území celé Evropské Unie. Tedy, že identifikační prostředek vydaný v jednom členském státě, bude uznatelný i v členském státě jiném a oprávněná osoba bude moci přistupovat k online službám eGovernmentu i s tímto prostředkem (například s elektronickým občanským průkazem). Také například zaručený elektronický podpis, nahraný na elektronickém občanském průkazu občana určitého členského státu, by měl být plně uznatelný ve všech ostatních členských státech Evropské unie. Tato uznatelnost je však závislá na několika podmínkách, které musí členský stát splňovat.

[97] Security guidelines on the appropriate use of qualified electronic seals — ENISA. ENISA [online]. Copyright © 2005 [cit. 25.03.2019]. Dostupné z: https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-seals

[98] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, e elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, Článek 25, Odstavec 1

4.1.3 VZÁJEMNÉ UZNÁVÁNÍ

V rámci zajištění vzájemného uznávání prostředků elektronické identifikace ve všech členských státech, upravuje nařízení eIDAS právě přeshraniční uznávání, kdy každý z členských států má notifikovat svůj elektronický systém. *„Pokud se podle vnitrostátního práva nebo správní praxe pro přístup ke službě poskytované on-line subjektem veřejného sektoru v určitém členském státě vyžaduje elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizace, je pro účely přeshraniční autentizace pro danou on-line službu uznán v tomto členském státě prostředek pro elektronickou identifikaci vydaný v jiném členském státě, pokud jsou splněny tyto podmínky:…*[99] . Tedy povinnost vzájemného uznání prostředku pro elektronickou komunikaci vydaném v jiném členském státě se týká jen prostředků, které splňují dále stanovené podmínky. Těmito podmínkami jsou:

1) Notifikace daného prostředku Evropskou komisí – prostředek je zkoumán odborníky a až poté uznán
2) Dostatečná úroveň záruky prostředku – úroveň musí být značná nebo vysoká
3) Užití značné nebo vysoké úrovně záruky příslušným subjektem veřejného sektoru

Účinný začal být článek 6 nařízení eIDAS dne 29.9.2018. Členské státy splňující podmínky lze nalézt na oficiálních stránkách Evropské komise. Německo dané podmínky splňuje již od 26.9.2017, Česká republika dané podmínky v současné době stále nesplňuje.[100] Nařízení eIDAS však nestanoví žádné sankce za to, že určitý členský stát nesplní podmínky pro elektronickou identifikaci a neoznámí svůj elektronický systém, tedy nebude notifikován.[101]

Nařízení eIDAS vyžaduje vzájemné uznávání prostředků elektronické identifikace jen od subjektů veřejné sféry. Fyzickým a právnickým osobám je

[99] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, e elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, Článek 6, odstavec 1
[100] CEF Digital. [online] European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[101] DONÁT, Josef. Nařízení eIDAS: komentář. V Praze: C.H. Beck, 2017. Beckovy komentáře. ISBN 978-80-7400-633-3.

ponechána pouze možnost, nikoliv povinnost užití daných prostředků pro elektronickou identifikaci.[102]

4.1.4 Implementace nařízení eIDAS v České Republice a ve Spolkové republice Německo

V České republice byly přijaty dva adaptační zákony, kdy jeden obsahuje úpravu především elektronického podepisování a druhý úpravu elektronické identifikace, ačkoliv jsou tyto pojmy obsahem jednoho nařízení. Adaptační zákon č. 297/2016 Sb. „o službách vytvářejících důvěru“, byl přijat 24.8.2016. Upravuje některé procesy, které souvisejí s poskytovateli elektronických podpisů, pečetí a dále přestupky na úseku tohoto zákona.

Druhý adaptační zákon byl přijat 19. července 2017 pod označením zákon 250/2017 Sb. o „elektronické identifikaci.“ Jeho ustanovení regulují právě oblast elektronické identifikace, kdy v souladu s novelou zákona č. 328/1999 Sb., o občanských průkazech tak mohl být zavedena tzv. elektronický občanský průkaz neboli eObčanka. Je vydáván od 1.8.2018 a obsahuje elektronický čip. S pomocí eObčanky se každý občan může přihlásit na portál veřejné správy (https://portal.gov.cz/obcan/) a využívat služeb veřejné správy bez nutnosti fyzické návštěvy úřadu. Elektronická občanka splňuje nejvyšší nároky nařízení, a tedy slouží jako identifikační prostředek s vysokou úrovní záruky dle nařízení eIDAS. Umožňuje zaručené právní jednání, provádění elektronických online transakcí a zaručuje identifikaci jednajícího. Elektronický občanský průkaz lze také využít jako prostředek pro vytváření elektronického podpisů.

Elektronický občanský průkaz však stále nelze užít k identifikaci ve všech jednáních. Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, který zapracovává a zároveň navazuje na příslušné předpisy Evropské Unie v oblasti ochrany proti „praní špinavých peněz“ a financování terorismu[103], vytváří v právní úpravě jistou dvojkolejnost.

[102] DONÁT, Josef. Nařízení eIDAS: komentář. V Praze: C.H. Beck, 2017. Beckovy komentáře. ISBN 978-80-7400-633-3.
[103] Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz a financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES

Zákon č. 253/2008 Sb. kromě jiného vymezuje povinné subjekty (například banky, auditory a podobně), kterým ukládá v případě provádění obchodní transakce s jiným subjektem (klientem) povinnost identifikace tohoto subjektu. K této identifikaci je elektronický občanský průkaz nedostačující a nelze jej pro tento účel užít. Zákon vyžaduje specifickou identifikaci zaručeným elektronickým podpisem nebo kvalifikovaným elektronickým podpisem ve spojení s certifikátem či časovým razítkem, tedy službou vytvářející důvěru pro takovou transakci. Elektronický občanský průkaz je však kvalifikovaným systémem. [104] Poměrně aktuální směrnice (EU) č. 2018/843 by měla daný rozpor vyřešit (do 10. 1. 2020) a vhodnou transpozicí umožnit elektronickou identifikaci pomocí elektronických občanských průkazů i v těchto případech.

Spolková republika Německo přijala adaptační zákon 18.7.2017 pod označením Vertrauensdienstegesetz[105] V kombinaci s novelizovaným zákonem upravující elektronické občanské průkazy (Personalausweisgesetz)[106] zajistil plošné vydávání elektronických občanských průkazů, umožňující interakci s veškerými funkcemi eGovernmentu.

Nařízení neponechává mnoho prostoru pro odlišnou úpravu, lze tedy spíše hodnotit, v jakém stádiu realizace jsou zatím konkrétní ustanovení.

Česká republika si vyjednala výjimku v rámci nutnosti užití kvalifikovaného elektronického podpisu veřejnou správou.[107] Nařízení eIDAS předpokládá, že veřejná správa bude v rámci svých jednání užívat nejvyšší formu elektronického podpisu, tedy podpis kvalifikovaný. Výjimka umožňovala pro taková jednání veřejnou správou užívat také podpis s menší úrovní záruky, tedy pouze podpis zaručený. Od 19.9.2018 je však nutnost vždy užívat právě elektronický podpis kvalifikovaný.[108] Vyjednávání výjimek má jistě

[104] Výzvy a milníky nařízení eIDAS | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 25.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/vyzvy-a-milniky-narizeni-eidas-108441.html
[105] Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014des Europäischen Parlaments und des Rates vom 23. Juli 2014über elektronische Identifizierung und Vertrauensdienste für elektronischeTransaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (BGBl. I S. 2745 (Nr. 52)
[106] Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 18.7.2017 (BGBl. I S. 1346)
[107] v §19, odst. 1 zákona č. 297/2016 Sb.

[108] Elektronické podpisy: v září skončí výjimka, budou úředníci připraveni? - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 25.03.2019]. Dostupné z:

v odůvodněných případech smysl, lze však polemizovat nad obecnou nutností takto činit. Pokud nebyla připravena technická infrastruktura, lze toto samozřejmě pochopit, nicméně obecně podobné výjimky svým způsobem právě zbržďují pokračující digitalizaci a rozvoj. Trend by měl být spíše obrácený, a to konkrétně snaha kvalitně implementovat předpisy a realizovat předpokládané cíle co nejdříve. Samozřejmě tak nelze činit na úkor kvality daných předpisů.

Pokud se týče vzájemného uznávání mezi členskými státy, kde jsou rozdíly na evropské úrovni snad nejmarkantnější, jak již bylo řečeno, Česká republika stále nesplňuje podmínky pro vzájemné uznávání elektronické identifikace ke službám online, notifikace je v přípravě. Občan jiného členského státu tedy nemůže pro přístup k českým online službám veřejné správy užít svého zaručeného prostředku elektronické identifikace, i když zde byla povinnost adaptovat národní systémy již 29.9.2018, kdy článek 6 nařízení eIDAS vstoupil v účinnost. Stejně tak není eObčanku možno užít k přístupu k veřejným online službám v jiném členském státě. Spolková republika Německo naopak jako první členská země Evropské Unie již od 20.2.2017 splnila podmínky dané nařízením a dle článku 9 nařízení eIDAS notifikovala svůj kvalifikovaný systém elektronické identifikace.[109]

https://www.lupa.cz/clanky/elektronicke-podpisy-v-zari-skonci-vyjimka-budou-urednici-pripraveni/

[109] Úřední věstník Evropské unie, C 319, 26. září 2017

4.2 KYBERNETICKÁ BEZPEČNOST

Odpovědná kyberbezpečnostní politika a důsledná regulace jsou základními předpoklady pro rozvoj eGovernmentu. *„Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i soukromém sektoru a současně jsou schopny vyvolat negativní politické důsledky, a to jak v národním měřítku, tak v měřítku globálním. V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu.“*[110]

Rizika v oblasti eGovernmentu jsou značná, protože ze své podstaty je jeho fungování založeno na komunikačních a informačních technologiích, které jsou propojené se základními databázemi a dalšími registry státu. Hrozba nespočívá pouze v tom, že útočník dané systémy vyřadí z provozu, ale také v tom, že dojde ke krádeži citlivých dat, jejich poškození nebo zničení. Dále hrozba spočívá také v tom, že může dojít k jejich modifikaci či jiné manipulaci. Vzhledem k rozšiřující se digitalizaci, „internetu věcí“ a dalšímu rozvoji, kdy v podstatě již nejsou zařízení klíčové infrastruktury v oblasti státní správy, energetiky, dopravy, ke kterým by nebyl možný přístup přes síť, je kompletní ochromení fungování státu zcela reálným rizikem.

Celoevropský společný postup v oblasti kyberbezpečnosti byl tedy logickým vyústěním pokračující digitalizace a s ní spojených hrozeb. V rámci Evropské unie byla vypracována Strategie kybernetické bezpečnosti EU: Otevřený, bezpečný a chráněný kyberprostor. K provádění kyberbezpečnostní agendy je v Evropské Unii příslušná především Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) a Vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku. Právě ENISA je hlavním iniciátorem návrhů politiky a právních předpisů, které mají zajistit ochranu evropských sítí a informačních a komunikačních technologií.[111] Dále působí v rámci Evropské Unie specializovaný CERT, neboli

[110] MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8., strana 1

[111] European Union Agency for Network and Information Security (ENISA) | European Union [online]. EUROPA - European Union website, the official EU website [cit. 25.3.2019]. Dostupné z: https://europa.eu/european-union/about-eu/agencies/enisa_en

Computer Emergency Response Team[112], který přímo chrání evropské sítě, vyhodnocuje rizika a již provedené narušení bezpečnosti.

V roce 2013 předložil Evropská komise návrh směrnice o potřebných opatřeních, jedná se o Směrnici Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Přijata byla dne 6. 7. 2016 a hned v prvním důvodu přijetí (které je opět primárně odůvodněno především odkazem na článek 114 SFEU) je konstatováno: *„Sítě, informační systémy a informační služby hrají ve společnosti zcela zásadní roli. Jejich spolehlivost a bezpečnost je nezbytná pro ekonomické a společenské činnosti, a především pak pro fungování vnitřního trhu.“*[113] Vzhledem k neustálé potřebě reagovat na nové hrozby byla již v roce 2017 předložen Evropskou komisí návrh reformního balíčku, který byl v prosinci 2018 schválen Evropskou radou.[114] *„Tento akt umožní zavedení celounijní certifikace kybernetické bezpečnosti a povede rovněž ke konsolidaci stálé Agentury EU pro kybernetickou bezpečnost.“*[115]

4.2.1 KLÍČOVÉ PRVKY SMĚRNICE

Od všech členských států je vyžadováno přijetí národní strategie pro bezpečnost informačních systémů a sítí, každý stát musí zároveň určit, který orgán bude působit jako jednotné kontaktní místo. Je zde požadavek na vytvoření týmů pro celounijní spolupráci v dané oblasti.

Směrnice má zajistit jednotnou evropskou úroveň ochrany před kybernetickými útoky, tzn. útoky na klíčovou počítačovou infrastrukturu. Chráněny podle směrnice mají být sítě, servery, portály poskytující veřejné služby, technologie a další klíčové body. Konkrétní subjekty pak mají povinnost hlásit závažné incidenty, kdy došlo k narušení kybernetické bezpečnosti za účelem varování ostatních spolupracujících subjektů, společné koordinace a efektivní zvyšování ochrany.

[112] CERT-EU News Monitor [online]. CERT-EU [cit. 25.3.2019]. Dostupné z: https://cert.europa.eu/cert/plainedition/en/cert_about.html
[113] 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
[114] Interinstitucionální dohoda 2017/0225(COD) ze dne 20.12.2018
[115] Reforma v oblasti evropské kybernetické bezpečnosti - Consilium [online]. Consilium [cit. 25.3.2019]. Dostupné z: https://www.consilium.europa.eu/cs/policies/cyber-security/#

4.2.2 KYBERNETICKÁ BEZPEČNOST V ČESKÉ REPUBLICE A VE SPOLKOVÉ REPUBLICE NĚMECKO

V České republice byla směrnice transponována zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, který je průběžně novelizován. Centralizovaným orgánem státní správy, mající povahu ústředního správního úřadu dle zákona 2/1969 Sb., je pro oblast kyberbezpečnosti Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)[116] se sídlem v Brně. Mezi úkoly NÚKIB konkrétně patří tvorba a stanovení bezpečnostních standartů pro tzv. kritickou informační infrastrukturu. Jedná se o systémy, které jsou zásadní pro chod státu a jsou definovány ve zvláštním zákoně a nařízení pomocí průřezových kritérií v závislosti na hlediscích jako je počet obětí při ohrožení určitého prvku nebo ekonomickými dopady[117]. Zařízením kritické infrastruktury jsou kromě jiného komunikační a informační systémy a zařízení pro výkon veřejné správy, především pro správu veřejných financí, sociální ochrany a zaměstnanosti a další státní správa.

Ve Spolkové republice Německo byla v rámci transponování směrnice o kybernetické bezpečnosti nutná jen částečná doplnění příslušných zákonů. Příslušným úřadem pro záležitosti kybernetické bezpečnosti je Bundesamt für Sicherheit in der Informationstechnik (Spolkový úřad pro bezpečnost v informační technologii). Na rozdíl od České republiky byl tento úřad zřízen speciálním samostatným zákonem „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, zkráceně označován jako BSI-Gesetz.[118] Spadá pod ministerstvo vnitra. Hlavním zákonem reflektující obsah směrnice je pak zákon ze 17. července 2015, zkráceně označován jako IT-Sicherheitsgesetz.[119] Velmi se podobá českému zákonu v návaznosti na společnou reflexi směrnice.

[116] Národní úřad pro kybernetickou a informační bezpečnost vznikl na základě zákona číslo 205/2017 Sb., který novelizoval zákon č. 181/2014 Sb.
[117] Zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.
Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
[118] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821)
[119] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (BGBl. I S. 1324)

4.2.3 KYBERBEZPEČNOST A DIGITALIZACE – KOMENTÁŘ AUTORA

Rád bych v této podkapitole prezentoval svůj názor na související problematiku. Za největší překážku digitalizace nepovažuji roztříštěnost úpravy nebo celkové zanedbávání této oblasti vládami členských států, ale právě tato bezpečnostní rizika spojené s užíváním informačních a komunikačních technologií. Základem je právní regulace, která umožňuje zavedení a aplikaci odpovídající úrovně zabezpečení. Dále jsou to samozřejmě lidské zdroje. Pracovní uplatnění ve státní správě by mělo být atraktivní, a to nejen platově, ale i v rámci nejrůznějších benefitů a dalších výhod.

Považuji za nezbytné zdůraznit, že Česká republika v oblasti kyberbezpečnosti nezaspala, je dokonce na první příčce indexu dle expertů z estonské neziskové organizace e-Governance Academy[120] Jedním z kritérií hodnocení členského státu je i legislativa, která je v České republice velmi kvalitní a dokonce „přísnější“ než vyžaduje celoevropská úroveň.[121] Národní úřad pro kybernetickou a informační bezpečnost sídlí v Brně a čeští experti, kteří zde působí, svoji vysokou odbornost a kompetentnost dokazují například pravidelnými úspěchy na největším světovém technickém cvičení Locked Shields, které pořádá kybernetické centrum NATO.[122] Velice aktuálním a diskutovaným je v současné době varování Národního úřadu pro kybernetickou a informační bezpečnost ze dne 17. 12. 2018.[123] Česká republika tímto jako vůbec první varovala před užíváním technologií čínských společností Huawei a ZTE ve veřejné správě. Česká republika má dokonce své speciální diplomatické atašé ve světových centrech kybernetické ochrany. Působí ve Washingtonu, Tel Avivu a Bruselu. Cílem je konstantní zlepšování už tak úzké spolupráce a společné zvyšování schopnosti čelit hrozbám.

O neustálých bezpečnostních hrozbách svědčí i nedávný hackerský útok v Německu, kdy byla zveřejněna data stovek německých politiků, včetně Spolkové

[120] NCSI:Ranking Index [online]. e-Governance Academy Foundation [cit. 25.3.2019]. Dostupné z: https://ncsi.ega.ee/ncsi-index/
[121] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
[122] Čeští experti na kyberbezpečnost zabodovali. Z mezinárodní soutěže v Estonsku si vezou první místo - Aktuálně.cz. Zprávy - Aktuálně.cz [online]. Copyright © Economia, a.s. [cit. 28.03.2019]. Dostupné z: https://zpravy.aktualne.cz/zahranici/estonsko/r~19648ab62c1311e7b58d0025900fea04/
[123] Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation [online]. NÚKIB [cit. 25.3.2019]- https://nukib.cz/download/uredni-deska/Varov%C3%A1n%C3%AD%20N%C3%9AKIB%202018-122-17.pdf

kancléřky Angely Merkel.[124] Spolková republika Německo přitom svou kyberbezpečnostní politiku taktéž nezanedbává, kdy se ve stejném indexu jako Česká republika umístila na 7. pozici.[125]

Na základě výše uvedených rizik, ačkoliv jsem zastáncem a podporovatelem pokračující digitalizace a užívání ICT technologií jak ve veřejném, tak v soukromém sektoru, existuje oblast, kde mám na využívání informačních technologií odlišný názor - E-Voting neboli elektronické volby. Je všeobecně známo, že přímé, svobodné a rovné volby jsou pilířem demokratického právního státu. Demokracie potřebuje pro svou existenci legitimní volby, na jejichž základě vzejdou dočasně zvolení zástupci z lidu. Vzhledem k současné situaci ve světě a bezpečnostním rizikům považuji za více než vhodné setrvat u voleb „klasických", tedy takového způsobu jejich provedení, který je praktikován nyní například v České republice. Tyto volby jsou i tak zatíženy možnými riziky, jak jsme se mohli poměrně nedávno přesvědčit v roce 2017, kdy Nejvyšší správní soud v rámci voleb v České republice zjistil závažná pochybení při sčítání preferenčních hlasů, na základě čehož dále poukázal na nedokonalost provádění voleb a na možnou manipulaci s hlasovacími lístky.[126] Rizikovým je samozřejmě samotné elektronické shromažďování výsledků na Českém statistickém úřadě, avšak stále si myslím, že riziko nedosahuje takové míry, jako v případě voleb plně digitalizovaných. V neposlední řadě považuji volby za celospolečenskou událost, a za občanskou tradici právě osobní účast ve volbách.

Lze konstatovat, že politika i legislativní snahy na celoevropské i vnitrostátní úrovni odpovídají rizikům a zajišťují postupnou digitalizaci a fungování eGovernmentu v Evropské unii a členských státech.

[124] Bundes- und Landesebene: Hackerangriff auf Hunderte Politiker | tagesschau.de. Aktuelle Nachrichten - Inland Ausland Wirtschaft Kultur Sport - ARD Tagesschau | tagesschau.de [online]. Copyright © ARD [cit. 28.03.2019]. Dostupné z: https://www.tagesschau.de/inland/deutsche-politiker-gehackt-101.html

[125] NCSI:Ranking Index [online]. e-Governance Academy Foundation [cit. 25.3.2019]. Dostupné z: https://ncsi.ega.ee/ncsi-index/

[126] Usnesení volebního senátu Nejvyššího správního soudu ve věci sp.zn. Vol 58/2017

4.3 OCHRANA OSOBNÍCH ÚDAJŮ

Zpracovávání osobních údajů je základním předpokladem pro fungování státní správy. V digitální době stát tyto údaje zpravidla uchovává a spravuje v rozsáhlých databázích na určitých serverech, kdy k těmto údajům mají dle své příslušnosti přístup nejrůznější subjekty a vykonatelé státní moci, jako ústřední orgány státní správy, úřady a další orgány veřejné správy. Osobní údaje jsou ve výsledku vyžadovány pro činnost obecního úřadu, ministerstva, nebo Interpolu. Při realizaci veškerých činností veřejné správy tedy dochází k rozsáhlému zpracovávání osobních údajů značným počtem úředníků a dalších zaměstnanců státu.

K právní regulaci ochrany osobních údajů v moderním světě na celoevropské úrovni bylo přijato nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), zřejmě nejvíce známé pod označením „GDPR“.

Osobním údajem jsou dle nařízení GDPR „veškeré informace o identifikované nebo identifikovatelné fyzické osobě.“[127] Může to být jméno, rodné číslo a další základní údaje o každé fyzické osobě, stejně tak zvláštní prvky fyzické, genetické, psychické, tvořící identitu této fyzické osoby. V době digitálního světa je zvlášť důležité zdůraznit, že osobním údajem může být i síťový identifikátor – tedy IP adresa (jedinečný identifikátor každého elektronického zařízení, připojeného do sítě), která umožňuje identifikaci každého elektronického zařízení, které je připojeno do internetové sítě, lokační údaje (GPS), e-mailová adresa a další prvky, na základě kterých je možno přímo či nepřímo identifikovat konkrétní fyzickou osobu.

Evropská Unie přisuzuje ochraně osobních údajů velký význam. Svědčí o tom mimo jiné i zakotvení základních zásad ochrany osobních údajů v Listině základních práv Evropské unie. Listina základních práv Evropské unie garantuje v článku 8 každému právo na ochranu osobních údajů. Upřesňuje také postup

[127] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), Článek 4, odstavec 1

zpracovávání, kdy tyto údaje musí být zpracovány „korektně“, „k přesně stanoveným účelům“ a na „základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu“, který je stanoven zákonem.[128]

Ochranu osobních údajů dále reflektují další orgány Evropské unie. Základními principy, které Evropská komise považuje za klíčové nejen pro úspěšnou digitální transformaci digitalizaci veřejné správy, ale pro fungování moderní evropské společnosti, je důvěryhodnost a bezpečnost. V Akčním plánu pro eGovernment 2016-2020 je pro zajištění této důvěryhodnosti a bezpečnosti výslovně zdůrazněno: *„Všechny iniciativy by měly přesahovat pouhé dodržování právního rámce pro ochranu osobních údajů a soukromí a bezpečnost informačních technologií a měly by tyto prvky zahrnout již do fáze přípravy“*[129] Výslovně je zde zmíněn určitý požadavek (z právního hlediska spíše doporučení) na zachovávání ještě vyšší míry ochrany osobních údajů, než je právně stanoveno především v nařízení 2016/679 GDPR.

Právním základem pro nařízení 2016/679 GDPR dle primárních Smluv je především Článek 16, odstavec 2 Smlouvy o fungování Evropské unie. Článek 16 počítá s přijetím pravidel *„o ochraně fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů.“*[130] Nařízení má ze své podstaty přímý účinek ve všech členských státech a účinné je od 25. 5. 2018. Nařízení obsahuje početné klauzury, které umožňují členským státům doplnění a odchylky v rámci vnitrostátního práva národním zákonem.[131] Z podstaty povahy nařízení samozřejmě nemohou tyto odchylky být značné nebo podstatné. Nařízení GDPR bylo dnem účinnosti přímo použitelné a povinnosti z něj plynoucí vynutitelné na celém území Evropské unie bez ohledu na přijetí či nepřijetí adaptačních zákonů. Členské státy se opožděnou adaptací nařízení ve vnitrostátní úpravě jen ochuzují o včasnější možnost úpravy dispozitivních ustanovení a odchylek.

[128] Listina základních práv Evropské unie, Úřední věštník C 326, 26.10.2012, Článek 8
[129] Akční plán EU pro „eGovernment“ na období 2016–2020 Urychlování digitální transformace veřejné správy, COM/2016/0179 final, strana 4
[130] Smlouva o fungování Evropské unie, Článek 16, odstavec 2
[131] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 375.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, známé jako GDPR, usiluje o moderní regulaci ochrany osobních údajů a přizpůsobení této ochrany novým změnám a výzvám, které digitalizace přináší, a to na celoevropské úrovni. Spíše než za zásadní je však v odborných kruzích nařízení GDPR zkrátka považováno za předpis určitým způsobem odrážející několikaletý vývoj v této oblasti. Zaznívají i názory, že již v době, kdy bylo nařízení schvalováno a přijato, bylo zastaralým a nedostatečným předpisem vzhledem k současnému stavu, natož k budoucnosti. Zde lze opět poukázat na vztah práva a technologií, nebo ještě lépe na vztah práva a technologického pokroku, kdy i při zjevných snahách nelze dosáhnout zamýšleného a zcela uspokojivého výsledku.

4.3.1 Ochrana osobních údajů v České republice a ve Spolkové republice Německo

Ve Spolkové republice Německo byla s účinností od 25. 5. 2018 přijata novelizace Spolkového zákona na ochranu osobních údajů (Bundesdatenschutzgesetztes, BDSG-neu).[132] Zákon však bývá kritizován právě pro chybějící využití možnosti doplnění a zavedení odchylek některých institutů, které nařízení umožňuje.[133]

V České republice byl adaptační zákon schválen teprve 12. března 2019 poté, co byl Poslanecké sněmovně vrácen senátem.[134]

Adaptační zákon byl již jinak přijat ve většině členských států. Například v Rakousku byl adaptační zákon přijat 31. 7. 2017. Zákon například garantuje základní právo na ochranu osobních údajů i pro právnické osoby, což je téměř unikum.

[132] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)
[133] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 376.
[134] USNESENÍ Poslanecké sněmovny z 27. schůze ze dne 12. března 2019 k návrhu zákona o zpracování osobních údajů /sněmovní tisk 138/14/ - vrácenému Senátem

5 BUDOUCNOST A PERSPEKTIVA EGOVERNMENTU A EVROPSKÉ UNIE

V této kapitole je pojednáno o perspektivě digitalizace a eGovernmentu. Taktéž je přiblížen zajímavý fenomén, totiž společenská (či občanská) akceptace eGovernmentu, která je podstatným kritériem snahy o digitální transformaci veřejné správy. Dále je popisován zřejmě nejrelevantnější ukazatel rozvoje eGovernmentu ve světovém měřítku, a to E-Government Development Index (EGDI) Organizace spojených národů (UN) a obdobný evropský The Digital Economy and Society Index (DESI).

5.1 PERSPEKTIVA DIGITALIZACE A EGOVERNMENTU

Digitalizace a eGovernment jsou pojmy dnešní doby. Tyto oblasti jsou předmětem nejen vědeckého bádání, ale čím dál tím více praktickou součástí života. Státní instituce i regionální úřady se pokoušejí zajistit fungování digitálních služeb, které by občanům umožnily snadný a rychlý způsob vyřizování úředních záležitostí, zvýšili transparentnost a pohodlí. Evropská unie si uvědomuje potenciál digitální revoluce a vyvíjí snahy odpovídajícím způsobem reagovat na digitální vývoj a využít možností, co pokračující digitalizace nabízí.

Oblast eGovernmentu je jen dílčí oblastí, kterou je v rámci digitalizace třeba rozvíjet, nicméně velmi zásadní. Jedním z hlavních cílu eGovernmentu je zprostředkovat občanům veřejnosprávní služby, které jim budou blízké, budou umožňovat občanské zapojení do státní správy a zvyšovat transparentnost veškerých jednání.[135] S tím přímo souvisí samotné zefektivnění fungování veřejné správy, které by mělo být přehlednější, méně komplikovaná a v neposlední řadě také méně náročné, a to jak z finančního, tak z personálního hlediska.

Dosažení těchto cílů kromě jiného nezávisí jen na implementaci digitálních technologií ve veřejné správě, ale také na akceptaci nabídky těchto elektronických služeb obyvatelstvem a podnikateli, jakožto adresáty veřejné správy. Jinými slovy, adresáti, kterým jsou elektronické veřejné služby určeny, by měly těchto služeb v rámci možností aktivně využívat. V zásadě právě ti, kterým jsou služby určeny,

[135] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 659.

mohou posoudit jejich potřebnost a kvalitu a poskytnout případnou zpětnou vazbu a případně i konstruktivní kritiku. Bez akceptace nabídky těchto služeb adresáty veřejné správy se snahy o zavádění těchto nových technologií stávají mnohem obtížnějšími a taktéž se nabízí otázka o samotném smyslu těchto záměrů. Samotný fakt, že internet se stává stále dostupnějším, nutně neznamená, že občané budou jeho možností plně využívat. Překážkou může být nejen technická negramotnost, ale také určité odmítání celkových společenských změn, které digitální revoluce přináší.[136]

Pro úvahy o perspektivě a budoucnosti je nejprve nutné zhodnotit současný stav. Poměrně relevantním ukazatelem, který je určitým zhodnocením úspěšnosti rozvoje eGovernmentu v jednotlivých zemích světa, je E-Government Development Index (EGDI), který je spravován a vyhodnocován Organizací spojených národů a v rámci Unie The Digital Economy and Society Index (DESI).

Databáze EGDI byla vytvořena odborem pro veřejné instituce a eGovernment za účelem poskytnutí všem členům občanské společnosti hodnotné informace pro výzkum, vzdělávání a plánování do budoucna. Index je aktualizován každé dva roky, poslední aktualizace proběhla v roce 2018, další hodnocení a výsledky současného období budou dostupné v roce 2020.[137]

Index je založen především na analýze tří základních dimenzí eGovernmentu. Kvalitě online služeb, rozvoji telekomunikační infrastruktury a tzv. Human capital indexu, což je zvláštní index zpracovávaný Světovou bankou, který je měřítkem ekonomické úspěšnosti jednotlivých států.

Na základě globálních výsledků z roku 2018 je v rámci kontinentů Evropa v rozvoji služeb eGovernmentu ve světě nejdále. Druhé místo obsadila Amerika, třetí Asie, dále Oceánie a Afrika. Rozvoj eGovernmentu je samozřejmě závislý na celkové hospodářské vyspělosti a obecné výši HDP na daném kontinetu.

Absolutní prvenství mezi státy drží Dánsko s indexem 0.91. V první desítce se také umístili státy jako Austrálie, Jižní Korea nebo Švédsko. Spolková republika Německo jen těsně nepatří do první desítky s indexem 0.87. Česká republika obsadila ze 193 hodnocených zemí 54. místo s indexem 0.70. Hodnocení dle indexu

[136] SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1, S. 660.
[137] EGOVKB | United Nations [online]. United Nations [cit. 25.3.2019]. Dostupné z: https://publicadministration.un.org/egovkb/en-us/

nelze považovat za absolutní a jednoznačný ukazatel rozvoje eGovernmentu v tém kterém konkrétním státu, nicméně je zcela jistě určitým vodítkem a odrazem vývoje v jednotlivých státech a na světových kontinentech.

DESI je evropskou obdobou indexu Organizací spojených národů. Na základě relevantních kritérií a indikátorů hodnotí digitální konkurenceschopnost jednotlivých států a celé Evropské unie. Kritérii pro hodnocení jsou zejména konektivita, digitální dovednosti občanů, využívání internetových služeb občany, integrace digitálních technologií v podnikání, stupeň rozvoje elektronické veřejné správy (eGovernment) a výzkum a vývoj v oblasti informačních a komunikačních technologií.

Kritérium konektivity hodnotí celkovou dostupnost telekomunikačních sítí. Kritérium digitální dovednosti občanů ve své podstatě zkoumá počítačovou gramotnost a její rozvíjení v jednotlivých státech. Kritérium využívání internetových služeb občany zkoumá, do jaké míry jsou digitální služby využívány a do jaké míry jsou upřednostňovány před analogovým způsobem komunikace. Integrace digitálních technologií v podnikání hodnotí digitalizaci v byznysu a využívání informačních a komunikačních technologií ve vzájemném obchodu. Kritérium rozvoje eGovernmentu reflektuje úroveň digitální transformace a elektronizace veřejné správy. V roce 2018 byly dle indexu v Evropské unii v oblasti digitalizace nejdále státy jako Dánsko, Švédsko, Finsko a Holandsko. Česká republika je na 17. místě, Spolková republika Německo na 13. místě. Další aktualizaci indexů lze očekávat v roce 2020.[138]

Na základě výše uvedeného lze konstatovat, že se úroveň mezi jednotlivými státy Evropské Unie poměrně liší, nicméně je vývoj v rámci celé Evropské unie konstantní a lze jej hodnotit pozitivně. Každý rok dochází k určitému zlepšení daných segmentů a v současné době není důvod, proč by tato tendence neměla pokračovat v podobném duchu. Komplexní snahy do budoucna směřují k dosažení stanovených cílů a vizí, avšak bude zcela jistě potřeba ještě mnoho času, financí, chnologických vylepšení a také zmiňované akceptace digitální revoluce od samotných občanů.

[138] The Digital Economy and Society Index (DESI) [online]. European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/digital-single-market/en/desi

5.2 PERSPEKTIVA EVROPSKÉ UNIE

Německý sociolog Ralf Dahrendorf se společenskými, sociálními a ekonomickými problémy současnosti zabýval ve své úvaze Kvadratura kruhu. Název odkazuje na slavný konstrukční matematický problém, kterým se zabývali již antičtí matematici, než bylo po roce 1800 dokázáno, že tento problém nemá řešení.

Dahrendorf konstatuje, že je principiálně souběžně nemožné dosáhnout hospodářského blahobytu, sociální sounáležitosti a politické svobody. Jako příklad pro svá tvrzení uvádí země, kde jsou rozdíly mezi těmito složkami enormní, a to Spojené státy americké (blahobyt a svoboda, avšak velice rozvrstvená, silně nesolidární společnost), Singapur (blahobyt na úkor svobody) a Indie (svoboda, avšak výrazná ekonomická zaostalost).[139]

Evropská unie však našla mezi třemi zásadními oblastmi fungování společnosti jistou rovnováhu. Soustavnou a usilovnou snahou bylo docíleno velmi vysoké úrovně ve všech aspektech moderní společnosti. Evropská unie je jednou z největších ekonomik světa, kdy celková hodnota vytvořených statků a služeb (HDP) byla pro rok 2018 18,8 bilionů euro. Na základě objektivních i subjektivních kritérií lze konstatovat, že je životní standard v Unii velmi vysoký, sociální politika je solidární a právní i faktická svoboda každého jedince zaručena.[140]

Nicméně je v současné době ve světle posledních událostí cítit jistá vratkost a ohrožení této dosažené rovnováhy. Evropská unie musela a stále musí v posledních letech čelit několika závažným celospolečenským krizím, které jsou ještě umocněny právě globalizací a digitální revolucí. Světová finanční krize v roce 2008 zasáhla všechny státy světa a způsobila ekonomickou depresi. Recese se negativně podepsala na obchodu i životní úrovni obyvatel. Na druhou stranu vedla krize k přijetí několika zásadních opatření, která by pro případ příští finanční deprese měla do značné míry zmírnit její negativní důsledky.

---

[139] LOPATKA, Reinhold. Die EU und die Mitgliedstaaten: Subsidiarität. Proportionalität. Weniger, aber eizienteres Handeln [online]. Vienna: Austrian Institute for European and Security Policy 2018 [cit. 25.3.2019]. Dostupné z https://www.aies.at/publikationen/2018/studien-07.php

[140] Eurostat - Tables, Graphs and Maps Interface [online].European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/eurostat/tgm/refreshTableAction.do;jsessionid=9ea7d07e30dd3bf0a52b9a8a474c872db039e243c026.e34OaN8Pc3mMc40Lc3aMaNyTa3eQe0?tab=table&plugin=1&pcode=tec00001&language=en

Migrační krize 2015 byla další těžkou zkouškou pro Evropskou unii, kterou zasáhla nejvíce. Mezi členskými státy se objevily velice rozporuplné názory a návrhy na její řešení a ostré debaty o podobě evropské sounáležitosti, které krize vyvolala, trvají v podstatě dodnes.

Brexit, neboli vystoupení Velké Británie z Evropské unie, je současnou krizí, se kterou se Evropská unie potýká. Možná není krizí v pravém slova smyslu co do svého rozsahu, nicméně vyvolává závažné otázky, týkající se integrace a politického směřování Evropské unie. Ekonomická hlediska také nejsou zanedbatelná.

Negativní vnímání Evropské unie v členských zemích za poslední léta vzrostlo. Protiunijní nálady demonstrují kromě jiného i nebývalé úspěchy krajních až extremistických stran. Populistické požadavky na vystoupení z Evropské unie se setkávají s ohlasem v mnoha členských státech. Kde však hledat příčinu a lze tomuto stavu čelit, popřípadě jej napravit?

Pravděpodobně bude třeba lidem navrátit důvěru v Evropské společenství, v Unii jako takovou. Evropská unie vznikla, protože si lidé kromě jiného uvědomili, že obchod a blahobyt je více než válka a bída, že demokracie a svoboda je více než diktatura a totalitní represe. Po hrůzostrašných celosvětových válečných konfliktech 20. století, při kterých přišlo o život desítky milionů lidí, civilní obyvatelstvo trpělo a země byly rozmetány, zkrátka evropští obyvatelé dospěli k tomu, že podobné hrůzy již nelze nikdy připustit a že je třeba vyvinout veškeré úsilí k zachování míru a svobody. Od těchto konfliktů již ale uplynulo řadu let a lidstvo má tendenci zapomínat. Příčinou může být čas, globalizace, ale také jistá neschopnost unést svobodu, poradit si v novém světě, neztotožnění se s principy fungování moderní společnosti, rezignování na politiku.

Zcela jistě jsou chyby i na straně Evropské unie, respektive členských států s největším vlivem na její podobu. Debaty o „dvourychlostní Evropě“, zákulisní sbližování jen některých členských států, vyhrožování postihy při odmítavém názoru a stanoviscích ke konkrétní problematice jsou jen některé příklady kroků, které ke zlepšení situace jistě nepřispějí.

Jak danou situaci řešit? Možná pozitivními kroky, pozitivní politikou. Více respektu pro názory členských států, pochopení odlišných tradic, zvyklostí,

společenských nálad. Jednání se všemi na stejné úrovni, bez ohledu na velikost a počet mandátů v Evropském parlamentu, slušnost a asertivita.

V každém případě tuto ani budoucí krize nelze přecházet, je třeba aktivně analyzovat veškeré aspekty a navrhovat možná řešení při zachování základních hodnot Evropské unie a respektování cílů její existence.

6 ZÁVĚR

V této diplomové práci obecně popisuji základní problematiku týkající se digitalizace veřejné správy v Evropské unii.

V kapitole Úvod do problematiky jsem se zabýval digitální revolucí jako takovou, kde jsem přiblížil některé aspekty technologického rozvoje, vztahu práva a technologií a elektronických online voleb. Zabýval jsem se pojmem eGovernment, především pak jeho obsahem, kterým je v podstatě veškerá digitální činnost veřejné správy. Digitální transformace veřejné správy je kromě jiného podmíněna technologickým zabezpečením potřebných prostředků, které má vysoké nároky na kvalitu provedení a na všeobecnou erudici. V neposlední řadě má svůj vliv také finanční náročnost celého procesu.

V části Evropská unie v současnosti jsem popisoval Evropskou unii jako celek, orgány Evropské unie, hodnoty a zásady, na kterých je Unie postavena a základní principy jejího fungování. Dále jsem se zabýval pravomocí Evropské unie, konkrétně pak pravomocemi pro právní regulaci eGovernmentu. Dospěl jsem ke zjištění, že Evropská unie nedisponuje na základě primárního práva odpovídající pravomocí regulovat oblast veřejné správy jednotlivých členských států, a tedy ve výsledku chybí také kompetenční základ pro prosazování jednotné strategie v oblasti eGovernmentu. Nicméně se však daří, při respektování zásady subsidiarity, přijímat právní úpravu na celoevropské úrovni, která poměrně vhodně reguluje dílčí oblasti eGovernmentu. Řešení těchto dílčích oblastí pak v souhrnu zajišťuje konstantní realizaci a směřuje k naplňování daných cílů. Primární zmocnění pro sekundární právní akty práva EU v této oblasti jsou především články SFEU o vnitřním trhu, sbližování právních předpisů a další. Dále lze dle prohlášení a dalších kroků představitelů členských států soudit, že snahy o právní úpravu eGovernmentu jsou legitimním a společným záměrem a výsledkem demokratického konsenzu. Samostatné iniciativy členských států, jejichž následkem může být nekompatibilita právních předpisů a také informačních a komunikačních systémů se daří moderovat společnými postupy, které jsou deklarovány v prohlášeních, akčních plánech a strategiích.

V kapitole Zhodnocení stávající právní úpravy jsem popisoval vybrané právní předpisy. Elektronické právní transakce, kyberbezpečnost a ochrana osobních údajů jsou zásadní oblasti, které jsou pilíři digitální transformace veřejné správy. Na celoevropské úrovni je pro zajištění společné a komplexní úrovně elektronických právních transakcí užito právního předpisu sekundárního práva EU ve formě nařízení, které zajišťuje přímý účinek ve všech členských státech a umožňuje pouze částečné odchylky. Snahy jednotlivých států o budování systémů elektronické identifikace a jejich následná notifikace pro účely vzájemného uznávání jistě pokročily, stále se však nejedná o samozřejmost a celý projekt je v počátku. V oblasti kyberbezpečnosti si všechny členské státy drží poměrně vysokou úroveň implementace daných institutů. Kyberbezpečnostní politika není důležitá jen pro eGovernment, ale především pro schopnost států čelit nejzávažnějším hrozbám v digitálním světě. Tyto hrozby mohou v krajním případě mít následky v podobě narušení nebo zničení státní integrity a suverenity ve spojení s ohrožením samotných demokratických zřízení. S kyberbezpečností nepochybně souvisí i schopnost členských států, Evropské unie i států NATO čelit propagandě a dezinformacím, které je v době internetu tak snadné masivně a anonymně šířit. Zde hraje klíčovou roli kromě jiného občanská aktivita, kritický přístup k hodnocení informací a v neposlední řadě také důvěra ve stát a státní aparát. Ochrana osobních údajů je dalším klíčovým institutem, který je regulován na celoevropské úrovni.

Neméně důležitým předpokladem rozvoje digitální veřejné správy je digitální politika každého členského státu. Funkčnost digitální veřejné správy se přímo odvíjí od centralizovaného orgánu státní správy, do jehož působnosti digitalizace a eGovernment spadá. Domnívám se, že je vzhledem k digitální revoluci zcela vhodné mít specializované ministerstvo pouze pro digitální agendu. Ministerstvo informatiky, zřízené v České republice zákonem č. 517/2002 Sb. 1.ledna 2003, působilo jistou nadčasovostí a moderností. Oblasti působnosti ministerstva reflektovaly klíčové body digitalizace, avšak místo rozvoje úřadu a postupného personálního zajišťování odborů experty došlo ke zrušení tohoto ministerstva a rozdělení agendy mezi tři jiná ministerstva. Je vhodné doplnit, že mnoho členských států, které obsazuji v indexu rozvoje eGovernmnetu vyšší příčky, nemá specializované ministerstvo pro oblast informačních a komunikačních technologií a tato agenda spadá pod obdoby ministerstva vnitra, dopravy a podobně.

Poměrně relevantním ukazatelem úrovně eGovernmentu v jednotlivých zemích je eGovernment Development Index, zpracovávaný a vyhodnocovaný Organizací spojených národů, respektive The Digital Economy and Society Index (DESI), vyhodnocovaný Evropskou unií.

Digitální revoluci se nelze vyhnout. Právo musí co možná nejpružněji reagovat na změny a nové výzvy, které přináší. Nelze tak však v žádném případě činit na úkor nebo kvalitu zachování základních demokratických hodnot, zásad a postupů. Zásady právního státu a ochrana základních lidských práv a svobod musí vždy stát na absolutním vrcholu požadavků na fungování moderní společnosti.

RESUMÉ

Kvalifikační práce s názvem Právní aspekty digitalizace v Evropské unii se zaměřením na eGovernment se zabývá problematikou digitalizace a digitální transformace veřejné správy. Téma je zpracováno převážně obecně, v evropské rovině, kdy jsou popisovány základní pojmy a instituty týkající se digitalizace, eGovernmentu a konkrétních právních předpisů. V práci je řešena kompetence EU pro právní regulaci oblasti eGovernmentu a jednotlivé zásady a výchozí body pro digitální transformaci veřejné správy. Dále se práce zabývá třemi stěžejními oblastmi, které jsou klíčové pro rozvoj eGovernmentu, a to elektronickou právní komunikací, kyberbezpečností a ochranou osobních údajů. Popisovány jsou základní záměry v rámci Evropské unie v těchto oblastech a klíčové předpisy, obsahující právní úpravu těchto institutů. Tyto vybrané předpisy jsou pak reflektovány v kontextu jejich aplikace v České Republice a Spolkové republice Německo. V práci je také nastíněna možná perspektiva a budoucnost digitalizace, eGovernmentu a Evropské unie.

Thesis titled Legal Aspects of Digitalization in the European Union with Focus on eGovernment deals with the problematics of digitalization and digital transformation of public administration. The topic is primarily covered generally, within the scope of the European Union, with description of basic terms and sets of legal norms related to digitalization, eGovernment and specific law regulations. The paper addresses the European Union's competence over legal regulation within the realm of eGovernment, and individual principles and starting points necessary for digital transformation of public administration. Further, the thesis examines three crucial domains key for the development of eGovernment: electronic legal communication, cyber security and personal data protection. Fundamental intents of these spheres within the European Union's purview are characterized along with indispensable regulations, containing legislation of aforementioned sets of legal norms. These selected legislations are then reflected in the context of their application in the Czech Republic and the Federal Republic of Germany. The paper also outlines a possible prospect of digitalization, eGovernment and the European Union.

Die Diplomarbeit Rechtsaspekte der Digitalisierung in der Europäischen Union mit der Richtung auf eGovernment beschäftigt sich mit der Problematik der Digitalisierung und digitaler Transformation der öffentlichen Verwaltung. Das Thema wird überwiegend allgemein, in der europäischen Ebene bearbeitet. Es wird die Grundbegriffe und Grundinstituten beschrieben, die die Digitalisierung, eGovernment und die konkreten Rechtsvorschriften betreffen. In der Diplomarbeit wird die Kompetenz der Europäischen Union für die Rechtsregelung des eGovernments und die einzelnen Prinzipe und Ausgangpunkte für die Entwicklung des eGovernments gelöst. Die Diplomarbeit befasst sich dann mit drei tragenden Instituten und zwar mit der elektronischen Rechtskommunikation, mit der Cybersicherheit und mit dem Datenschutz. Es werden die Vorhaben der Europäischen Union in diesem Gebiet beschrieben und auch die Schlüsselvorschriften, die die Regelung der elektronischen Rechtskommunikation, der Cybersicherheit und des Datenschutzes enthalten. Diese ausgewählten Vorschriften werden dann im Kontext ihrer Applikation in der Tschechischen Republik und Bundesrepublik Deutschland reflektiert. Die Perspektive und die Zukunft des eGovernments und der Europäischen Union wird auch in der Arbeit andeutet.

POUŽITÁ LITERATURA A DALŠÍ PRAMENY

Monografie

DONÁT, Josef. Nařízení eIDAS: komentář. V Praze: C.H. Beck, 2017. Beckovy komentáře. ISBN 978-80-7400-633-3.

FLORIDI, Luciano. The 4th revolution: how the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014. ISBN 9780199606726.

HENDRYCH, Dušan, a kol. Právnický slovník. Praha: C. H. Beck, 2009. ISBN 978-80-7400-059-1.

JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. Internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

SAVIN, A. (2017). EU internet law. Northampton, MA: Edward Elgar Pub. ISBN: 9781784717957.

SECKELMANN, Margit. Digitalisierte Verwaltung - Vernetztes E-Government. Berlin: ESV, 2019. ISBN 978-3-503-18139-1.

TOMÁŠEK, Michal, Vladimír TÝČ a Jiří MALENOVSKÝ. Právo Evropské unie. Praha: Leges, 2013. Student (Leges). ISBN 9788087576533.

VANÍČEK, Zdeněk a Stanislav A. MARCHAL. Právní aspekty eGovernmentu v ČR. Praha: Linde, 2011. ISBN 9788072018550.

Právní předpisy a judikatura

a) Předpisy práva EU

Listina základních práv Evropské unie

Smlouva o Evropské unii

Smlouva o fungování Evropské unie

Nařízení (EU) 2015/848, o insolvenčním řízení

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

Nařízení Evropského parlamentu a Rady (EU) 2018/1724 ze dne 2. října 2018,

kterým se zřizuje jednotná digitální brána pro poskytování přístupu k informacím, postupům a k asistenčním službám a službám pro řešení problémů a kterým se mění nařízení (EU) č. 1024/2012

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

Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014

Směrnice Evropského parlamentu a Rady 2013/37/EU ze dne 26. června 2013, kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru

Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz a financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES

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

Rozhodnutí (EU) 2015/2240 ze dne 25. listopadu 2015, kterým se zavádí program pro řešení interoperability a společné rámce pro evropské orgány veřejné správy, podniky a občany (program ISA2) jako prostředek modernizace veřejného sektoru

b) České právní předpisy a judikatura

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon č. 480/2004 Sb., o některých službách informační společnosti

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru

Zákon č. 250/2017 Sb., o elektronické identifikaci

Zákon č. 328/1999 Sb., o občanských průkazech

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Usnesení volebního senátu Nejvyššího správního soudu ve věci sp.zn. Vol 58/2017

c) Německé právní předpisy a judikatura

BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821)

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (BGBl. I S. 1324)

Grundgesetz vom 23. Mai 1949 (BGBl. S. 1)

Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014über elektronische Identifizierung und Vertrauensdienste für elektronischeTransaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (BGBl. I S. 2745 (Nr. 52)

Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 18.7.2017 (BGBl. I S. 1346)

BVerfG, Urteil des Zweiten Senats vom 03. März 2009 - 2 BvC 3/07 - Rn. (1-163)

Dokumenty EU

Akční plán EU pro „eGovernment“ na období 2016–2020 Urychlování digitální transformace veřejné správy, COM/2016/0179 final

Evropský rámec interoperability – Strategie provádění – Akční plán interoperability, COM(2017) 134 final

Evropský rámec interoperability – Strategie provádění – Akční plán interoperability, COM(2017) 134 final, Annex 1

Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017

Strategie pro jednotný digitální trh v Evropě, COM(2015) 192 final, Úvod

Závěry Evropské rady, 18. října 2018 (EUCO 13/18)

Internetové zdroje

A) Odborné články a studie

Buhl, H.U., Hirsch, T. & Loeffler, M. Wirtsch[online]. Inform Manag (2012) 4: 28. [cit. 25.3.2019]. Dostupné z: https://doi.org/10.1365/s35764-012-0122-1

Elektronické podpisy: v září skončí výjimka, budou úředníci připraveni? - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 25.03.2019]. Dostupné z: https://www.lupa.cz/clanky/elektronicke-podpisy-v-zari-skonci-vyjimka-budou-urednici-pripraveni/

Huesmann, J. & Galbis, A. Wirtsch [online]. Inform Manag (2015) 7: 18. [cit 25.3.2019]. https://doi.org/10.1007/s35764-015-0535-8

J. Alex Halderman [online]. Copyright © [cit. 25.03.2019]. Dostupné z: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

Jörn von Lucke/Heinrich Reinermann[online]. Speyerer Definition von E-Government, 2000, S. 1[cit. 25.3.2019]. Dostupné z: http://www.joernvonlucke.de/ruvii/Sp-EGov.pdf

LOPATKA, Reinhold. Die EU und die Mitgliedstaaten: Subsidiarität. Proportionalität.Weniger, aber eizienteres Handeln [online]. Vienna: Austrian

Institute for European and Security Policy 2018 [cit. 25.3.2019]. Dostupné z https://www.aies.at/publikationen/2018/studien-07.php

MALAST, Jan. Správní právo přehledně [online]. JUDr. PhDr. Jan Malast, Ph.D., 2018 [cit. 25.3.2019]. Dostupné z: https://www.spravko.cz/produkty/ebook-spravni-pravo-prehledne/

Security guidelines on the appropriate use of qualified electronic seals — ENISA. ENISA [online]. Copyright © 2005 [cit. 25.03.2019]. Dostupné z: https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-seals

Výzvy a milníky nařízení eIDAS | epravo.cz. EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 25.03.2019]. Dostupné z: https://www.epravo.cz/top/clanky/vyzvy-a-milniky-narizeni-eidas-108441.html

Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation [online]. NÚKIB [cit. 25.3.2019]- https://nukib.cz/download/uredni-deska/Varov%C3%A1n%C3%AD%20N%C3%9AKIB%202018-122-17.pdf

ZLATUŠKA, Jiří. Informační společnost [online]. Zpravodaj ÚVT MU. 1998, roč. 8., č. 4, s. 1–6. ISSN 1212-0901[cit. 25.3.2019]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/122.html.

B) Další internetové zdroje

Bundes- und Landesebene: Hackerangriff auf Hunderte Politiker | tagesschau.de. Aktuelle Nachrichten - Inland Ausland Wirtschaft Kultur Sport - ARD Tagesschau | tagesschau.de [online]. Copyright © ARD [cit. 28.03.2019]. Dostupné z: https://www.tagesschau.de/inland/deutsche-politiker-gehackt-101.html

CEF Digital. [online] European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

CERT-EU News Monitor [online]. CERT-EU [cit. 25.3.2019]. Dostupné z: https://cert.europa.eu/cert/plainedition/en/cert_about.html

Čeští experti na kyberbezpečnost zabodovali. Z mezinárodní soutěže v Estonsku si vezou první místo - Aktuálně.cz. Zprávy - Aktuálně.cz [online]. Copyright © Economia, a.s. [cit. 28.03.2019]. Dostupné z: https://zpravy.aktualne.cz/zahranici/estonsko/r~19648ab62c1311e7b58d0025900fea04/

EGOVKB | United Nations [online]. United Nations [cit. 25.3.2019]. Dostupné z: https://publicadministration.un.org/egovkb/en-us/

Eurostat - Tables, Graphs and Maps Interface [online].European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/eurostat/tgm/refreshTableAction.do;jsessionid=9ea7d07e30dd3bf0a52b9a8a474c872db039e243c026.e34OaN8Pc3mMc40Lc3aMaNyTa3eQe0?tab=table&plugin=1&pcode=tec00001&language=en

Digital economy and society statistics - households and individuals - Statistics Explained [online]. European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals

eGovernment & Digital Public Services | Digital Single Market [online]. European Commission [cit. 25.3.2019]. Dostupné z: https://ec.europa.eu/digital-single-market/en/policies/egovernment

EU-wide digital Once-Only Principle for citizens and businesses:Policy options and their impacts [online]. European Commission [cit. 25.3.2019]. Dostupné na http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42301

IT Slovník [online]. [cit. 25.3.2019]. Dostupné z: https://it-slovnik.cz/pojem/digitalizace

Internet of Things Global Standards Initiative [online]. Copyright © ITU [cit. 25.03.2019]. Dostupné z: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

Internet voting in Estonia[online]. Elections in Estonia. [cit 25.3.2019]. Dostupné z: https://www.valimised.ee/en/internet-voting/internet-voting-estonia

Interoperabilita mezi informačními systémy EU: Předsednictví Rady a Evropský parlament dosáhly předběžné dohody - Consilium[online]. Home - Consilium [cit.

25.3.2019]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2019/02/05/interoperability-between-eu-information-systems-council-presidency-and-european-parliament-reach-provisional-agreement/

NCSI:Ranking Index [online]. e-Governance Academy Foundation [cit. 25.3.2019]. Dostupné z: https://ncsi.ega.ee/ncsi-index/

Reforma v oblasti evropské kybernetické bezpečnosti - Consilium [online]. Consilium [cit. 25.3.2019]. Dostupné z: https://www.consilium.europa.eu/cs/policies/cyber-security/#

Réseau privé virtuel justice (RPVJ) a Réseau privé virtuel avocat [online] [cit. 25.3.2019]. Dostupné z: http://www.textes.justice.gouv.fr/art_pix/boj_20090005_0000_0001.pdf

Soudní dvůr Evropské unie | Evropská unie[online]. EUROPA - European Union website, the official EU website [cit. 25.3.2019]. Dostupné z: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_cs