Univerzita Karlova

Právnická fakulta

Jan Nešpor

Právní úprava eGovernmentu v České republice

Diplomová práce

Datum vypracování práce:
24. června 2022

Vedoucí diplomové práce:
JUDr. Ing. Josef Staša, CSc.

Katedra:
Správní právo a správní věda

Čestné prohlášení a souhlas s publikací práce

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny, že práce nebyla využita k získání jiného nebo stejného titulu a že část textu práce vychází z práce obhájené v rámci Studentské vědecké odborné činnosti v roce 2021 na téma „Aktuální legislativní změny a budoucnost eGovernmentu v České republice“. Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 304 810 znaků včetně mezer.

_____

Jan Nešpor

V Praze dne 30. června 2022

Poděkování

V souvislosti s touto prací tímto předně děkuji JUDr. Ing. Josefovi Stašovi, CSc. za jeho cenné rady a drahocenný čas, který mi byl ochotný věnovat jako konzultant této práce. Současně moc děkuji Ing. Barboře Červenkové, DiS. za konzultaci týkající se některých technických aspektů elektronizace a digitalizace a Mgr. Danielu Burdovi za jeho oponentní věcné připomínky k mé práci na téma „Aktuální legislativní změny a budoucnost eGovernmentu v České republice“ obhájené v rámci SVOČ, která tvoří základ této diplomové práce. Dále chci poděkovat i Mgr. Radimu Karáskovi za umožnění absolvování stáže na odboru hlavního architekta eGovernmentu Ministerstva vnitra a jeho konzultace, které mi byl ochoten poskytnout.

Obsah

Seznam použitých zkratek

AIFO	Agendový identifikátor fyzických osob
AVG	(Rakouský) zákon BGBl. č. 51/1991, všeobecný správní řád (*Allgemeines Verwaltungsverfahrensgesetz*)
AvTeS	(Estonský) zákon o veřejných informacích (*Avaliku teabe seadus*, RT I 2000, 92, 567)
Benchmark	eGovernment Benchmark
BIM	Building Information Modeling
Cesta k digitální dekádě	Návrh rozhodnutí Evropského parlamentu a Rady, kterým se zavádí politický program 2030 „Cesta k digitální dekádě“, ze dne 15. září 2021, COM(2021), 574 final
CMS	Centrální místo služeb
DaňŘ	Zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů
DEPO	Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, ve znění pozdějších předpisů
DESI	Index digitální ekonomiky a společnosti
Digi Peněženka	Evropská digitální peněženka
E-GovG	(Rakouský) zákon BGBl. č. 10/2004, o předpisech pro usnadnění elektronické komunikace s orgány veřejné moci (zákon o eGovernmentu – E-GovG), ve znění pozdějších předpisů [*Bundesgesetz über Regelungen zur Erleichterung des*

	elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz)]
eIDAS	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
eIDAS II	Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, COM(2021) 281 final
eObčanka	Občanský průkaz s aktivovaným kontaktním čipem vydaným po 1. červenci 2018
Evropské digitální zásady	Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výrobu regionů o Evropském prohlášení o digitálních právech a zásadách pro digitální dekádu, ze dne 26. ledna 2022, COM(2022) 27 final
Evropský kompas	Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Digitální kompas 2030: Evropské pojetí digitální dekády, ze dne 9. března 2021, COM(2021), 118 final
HalS	(Estonský) zákon o správním řízení (*Haldusmenetluse seadus,* RT I 2001, 58, 354)
ICT	Informační a komunikační technologie
IMA	Identity Malta Agency
ITDS	(Estonský) zákon o dokladech totožnosti (*Isikut tõendavate dokumentide seadus,* RT I 1999, 25, 356)

KIVS	Komunikační infrastruktura veřejné správy
Koncepce BIM	Koncepce zavádění metody BIM v České republice
KontrolŘ	Zákon č. 255/2012 Sb., o kontrole, ve znění pozdějších předpisů
Legislativní pravidla vlády	Usnesení vlády č. 188 ze dne 19. března 1998 ve znění pozdějších změn
NAKIT	Státní podnik Národní agentura pro komunikační a informační technologie založen zakládací listinu Ministerstva vnitra ze dne 21. ledna 2016
NIA	Národní bod pro identifikaci a autentizaci (tzv. národní identitní autorita)
NStavZ	Zákon č. 283/2021 Sb., (nový) stavební zákon, ve znění pozdějších předpisů
NZIS	Národní zdravotnických informační systém
ReUseAct	(Maltský) zákon o opakovaném použití informací veřejného sektoru z roku 2015, ve znění pozdějších předpisů [Cap. 546] (*Re-Use of Public Sector Information Act*)
ROB	Základní registr obyvatel
ROS	Základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci neboli registr osob
RPP	Základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností neboli registr práv a povinností neboli registr práv a povinností

RÚIAN	Základní registr územní identifikace, adres a nemovitostí neboli registr územní identifikace
Sbírka	Sbírka zákonů a mezinárodních smluv
SDGR	Nařízení Evropského parlamentu a Rady (EU) č. 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
SFDI	Státní fond dopravní infrastruktury
SlovSpŘ	(Slovenský) zákon č. 71/1967 Zb., o správním řízení (správní řád) [*o správnom konaní (správny poriadok)*]
SměrPřWeb	Směrnice Evropského parlamentu a Rady (EU) č. 2016/2102 ze dne 26. října 2016 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru
SouvisZoEI	Zákon č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci, ve znění pozdějších předpisů
SpŘ	Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
SŘS	Zákon č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů
SÚKL	Státní ústav pro kontrolu léčiv
SVG	(Rakouský) zákon BGBl. č. 50/2016, o elektronickém podpisu a službách vytvářejících důvěru v elektronických transakcích [Bundesgesetz über elektronische Signaturen und

	Vertrauensdienste für elektronische Transaktionen (Signatur – und Vertrauensdienstegesetz – SVG)]
SZeGOV	(Slovenský) zákon č. 305/2013 Zb., o elektronické podobě výkonu působnosti orgánů veřejné moci a o změně a doplnění některých zákonů (zákon o e-Governmentu) [*o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)*]
SZoIT	(Slovenský) zákon č. 95/2019 Zb., o informačních technologiích ve veřejné správě a o změně a doplnění některých zákonů [*o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov*]
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚZIS	Ústav zdravotnických informací a statistiky ČR
ZeRecept	Zákon č. 262/2019 Sb., kterým se mění Zákon o léčivech, ve znění pozdějších předpisů
ZeZdrav	Zákon č. 325/2021 Sb., o elektronizaci zdravotnictví ve znění pozdějších
ZeZnám	Zákon č. 227/2019 Sb., kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů
ZIFO	Zdrojový identifikátor fyzické osoby
ZoAML	Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů
ZoBank	Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů

ZoBI	Zákon č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů
ZoCzechPOINT	Zákon č. 269/2007 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a další související zákony
ZoEI	Zákon č. 250/2017 Sb., o elektronické identifikace, ve znění pozdějších předpisů
ZoEÚAK	Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
ZoISVS	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně dalších zákonů, ve znění pozdějších předpisů
ZoLéč	Zákon č. 378/2007 Sb., o léčivech a o změnách souvisejících, ve znění pozdějších předpisů
ZoOdpŠk	Zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů
ZoOP	Zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů

ZoOvěř	Zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů, ve znění pozdějších předpisů
ZoPozKom	Zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů
ZoPřWeb	Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
ZoSbírce	Zákon č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv, ve znění pozdějších předpisů
ZoSVD	Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
ZoUtajInf	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
ZoVOP	Zákon č. 349/1999 Sb., o Veřejném ochránci práv, ve znění pozdějších předpisů
ZoZR	Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
ZoZS	Zákon č. 372/2011 Sb., o zdravotnických službách a podmínkách jejich poskytování, ve znění pozdějších předpisů
ZPDS	Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů

ZustG	(Rakouský) zákon BGBl. č. 1982/200, o doručování písemností [Bundesgesetz über die Zustellung behördlicher Dokumente (Zustellgesetz – ZustG)]

Úvod

Téma eGovernmentu je v právním prostředí novým a doposud neprozkoumaným tématem. Samotný pojem eGovernment je poměrně obsáhlý koncept, jehož součástí je zapojování informačních a komunikačních technologií (dále jen „**ICT**“) do veřejné správy a její digitalizaci uvnitř i navenek. Nedílnou součástí jsou služby, které veřejná správa poskytuje svým adresátům. Tato práce se ovšem nebude zabývat pouze eGovernmentem jako takovým. Pozornost bude věnována zejména právní úpravě toho, co je v České republice nazýváno eGovernmentem. Práce bude též pracovat i s některými technickými a technologickými aspekty eGovernmentu, kterých se však dotknu spíše okrajově.

V práci se naopak nebudu zabývat právní úpravou tzv. eJustice, která bývá často řazena pod pojem eGovernment. Cílem eJustice je primárně modernizace soudnictví a dílčích procesů v něm. Řadu institutů, jako jsou datové schránky nebo elektronické podpisy, které jsou součástí eGovernment, lze jistě využívat i v rámci soudního řízení. To lze ostatně říct, ale i o dalších právních odvětvích, jako je např, závazkové právo, které bezpochyby součástí eGovernmentu není. V této práci se soustředím především na eGovernment jakožto institut veřejné správy, jejíž součástí soudní moc v zásadě není. Téma eJustice si jistě pozornost zaslouží a při extenzivním výkladu jej lze zřejmě pod eGovernment v širším pojetí zařadit lze. Z výše uvedených důvodů mu však nebude věnována větší pozornost.

Mou motivací pro toto téma byla jednak jeho aktuálnost a jak jsem již zmínil, to, že právní teorie tomuto tématu doposud příliš pozornosti nevěnovala. Jistě lze namítnout, že některé dílčí části eGovernmentu jako jsou datové schránky, elektronické podpisy nebo právo na digitální služby byly předmětem celé řady publikací. Co ovšem dle mého názoru právní teorie postrádá je právě snaha o výzkum tohoto dynamicky se rozvíjejícího tématu jako celku a vytvoření základu pro další výzkum právní úpravy eGovernmentu. Dalším důvodem, proč jsem rozhodnul toto téma zpracovat v diplomové práci, je má profesní zkušenost. Jako legislativní asistent v Poslanecké sněmovně jsem měl možnost sledovat přijímání dvou pro eGovernment zásadních předpisů. Jednalo se o zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, někdy též nazývaný jako „digitální ústava“ (dále jen „**ZPDS**“), a zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (dále jen „**DEPO**“). Tato zkušenost mě motivovala k absolvování stáže na odboru hlavního architekta eGovernmentu v rámci Ministerstva vnitra a později k vypracování práce, kterou jsem úspěšně obájil v rámci fakultního kola SVOČ 2021 na téma „Aktuální legislativní

změny a budoucnost eGovernmentu v České republice“. V této diplomové práci dále navazuji na zjištění v rámci SVOČ a rozvíjím v ní uvedené koncepty a myšlenky. Text původní SVOČ tedy tvoří částečně i text této diplomové práce.

Cílem této práce je především doktrinální a kvalitativní analýza jednotlivých právních předpisů českého, ale i evropského práva, které tvoří právní rámec eGovernmentu v České republice. V rámci analýzy budu pro snazší interpretaci jednotlivých předpisů vycházet z textu právních norem, ale i z úmyslu zákonodárce, který je vtělen do dílčích důvodových zpráv. Součástí bude i doplnění o doktrinální komentářový výklad a soudní interpretaci v relevantní judikatuře. Pozornost bude kromě analýzy předpisů zaměřena na přístup Evropské unie ve snaze regulovat dílčí části eGovernmentu, ale i na snahu o harmonizaci úpravy eGovernmentu v evropském prostoru. Součástí této práce bude i komparace s právní úpravou eGovernmentu v některých evropských státech, jejichž eGovernmenty jsou v evropském prostoru pozitivně hodnoceny nebo jejichž právní systém je podobný České republice. Kromě právních předpisů budu pracovat i s odbornou literaturou v oblasti správního práva a eGovernmentu, odbornými analýzami a koncepcemi, které byly zpracovány orgány EU, vládními a obdobnými orgány členských států.

Současně je cílem této práce potvrzení nebo vyvrácení níže uvedené hypotézy: „*Právo eGovernmentu je specifické právní odvětví, které je tvořeno konkrétními právními předpisy a stojí na konkrétních právních zásadách jak pro jeho tvorbu, tak i aplikaci. Součástí práva eGovernmentu jsou i specifická práva a povinnosti všech zúčastněných subjektů.“* Potvrzením této hypotézy by došlo k naplnění obecného cíle této práce, a to sice systematizaci roztříštěné právní úpravy do uceleného právního odvětví. Systematizace umožní dle mého názoru snazší orientaci v této právní úpravě a vytvoří podklad pro další rozvoj oboru práva eGovernmentu. Zároveň si kladu i ambice, že poslouží jako zdroj pro budoucí zákonodárství v této oblasti.

První dvě kapitoly budou tvořit převážně teoretickou část práce, ve které budu deskriptivní metodou zkoumat samotný pojem eGovernment včetně souvisejících jevů a institutů. V druhé kapitole budu analyzovat jednotlivé právní předpisy a související instituty, které tvoří páteř českého eGovernmentu a další oblasti správního práva, ve kterých dochází k digitalizaci. Na závěr druhé kapitoly budu hledat odpověď na otázku, zda mají adresáti veřejné správy právo domáhat se využívání zákonem předpokládaného projektu eGovernmentu a zda tomuto právu koresponduje povinnost státu realizovat zákonem předpokládané projekty eGovernmentu. Jinými slovy, zda existuje veřejné subjektivní právo na využívání jednotlivých projektů, které by adresátům veřejné správy náleželo. Analytickou část tvoří část druhé kapitoly, ale především

třetí a čtvrtá kapitola. Ve třetí kapitole budu analyzovat klíčové předpisy a politiky na evropské úrovni a právně komparovat tuzemskou právní úpravu s právní úpravou Estonska, Malty, Rakouska a Slovenska. Ve čtvrté kapitole pak na základě získaných poznatků plánuji vytvořit jednotnou funkční systematiku právních předpisů, které souvisí s eGovernmentem a potvrdím nebo vyvrátím výše uvedenou hypotézu.

1 Pojem eGovernment a digitalizace veřejné správy[1]

„Myšlenkou eGovernmentu je správa věcí veřejných za využití moderních elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější.“[2]

Definice samotného pojmu eGovernment se můžou lišit. David Špaček jej definuje jako „*zapojování ICT (informačních a komunikačních technologií pozn. autora) do činnost veřejné správy*“[3], Mates se Smejkalem jako „*různé úkoly, které se zabývají elektronizací výkonu činnosti veřejné správy nebo v širším pojetí spíše orgánů veřejné moci vůbec*“[4] a např. Ministerstvo vnitra tak, že „*samotný eGovernment zahrnuje nejen samotné informační technologie, ale také optimalizaci a zjednodušování služeb veřejné správy vázané na legislativní prostředí.“*[5] Každopádně jak popisuje Mates a Smejkal: „*výraz e-government se stal součástí newspeaku moderní společnosti natolik, že se k němu snad ani nehledá odpovídající překlad v žádném jazyce*“[6], proto lze předpokládat, že se jedná o takový pojem, pod kterým si každý dokáže představit něco, co se alespoň přibližuje skutečnému obsahu tohoto fenoménu. Mates dále uvádí, že eGovernment je „*fenomén, který je označován poněkud technicistní, dnes však již všeobecně používanou zkratkou e-government, je produktem moderní doby, stejně tak jako jejím výrazem. Zahrnuje rozsáhlou škálu otázek od přístupu adresátů veřejné správy k informacím, přes elektronickou komunikaci s úřady, po vytváření potřebných organizačních a technických infrastruktur v rámci veřejné správy, jejichž společným jmenovatelem je zavádění a využívání elektronických informačních a komunikačních technologií.*“[7]

---

[1] Část tohoto textu vychází z NEŠPOR, Jan, 2021. Aktuální legislativní změny a budoucnost eGovernmentu v České republice. Praha. Práce v rámci Studentské vědecké odborné činnosti (SVOČ). Univerzita Karlova, Právnická fakulta. Vedoucí práce STAŠA, Josef, str. 5-8

[2] MINISTERSTVO PRŮMYSLU A OBCHODU. *Koncepce zavádění metody BIM v České republice* [online]. Praha: Ministerstvo průmyslu a obchodu, 2017. [cit. dne 2022-05-05]. str. 19. Dostupné z: https://www.koncepcebim.cz/uploads/inq/files/Koncepce%20zaváděn%C3%AD%20metody%20BIM%20v%20ČR.pdf

[3] ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. V Praze: C.H. Beck, 2012. Beckova edice ekonomie. str. 1. ISBN 978-80-7400-261-8

[4] MATES, Pavel a Vladimír SMEJKAL. *E-government v českém právu*. Praha: Linde, 2006. str. 9. ISBN 80-7201-614-8

[5] MINISTERSTVO VNITRA. Agenda odboru hlavního architekta eGovernmentu. *Ministerstvo vnitra* [online]. [cit 2022-05-05]. Dostupné na https://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu-agenda-odboru-hlavniho-architekta-egovernmentu.aspx

[6] MATES, Pavel a Vladimír SMEJKAL. *E-government v českém právu.* Praha: Linde, 2006. str. 9. ISBN 80-7201-614-8

[7] MATES, Pavel. *E-government v české veřejné správě*. Praha: Právní rozhledy, 2005, č. 8, str. 283–286. ISSN: 1210-6410

Výsledná definice není dle mého názoru natolik zásadní. Naopak podstatné je odlišení pojmu eGovernment od pojmu eGovernance. Robert Keohane uvádí, že „*Governance* (v překladu vládnutí/řízení/správa pozn. autora) *znamená procesy a instituce, formální i neformální, které řídí a omezují kolektivní aktivity skupiny. Vláda je podmnožinou, která jedná autoritativně a vytváří formální povinnosti. Governance ovšem nemusí být výhradně vykonáváno jenom Vládou jako takovou. Soukromé firmy, sdružení firem, nevládní organizace a sdružení nevládních organizací se do něj zapojují, často ve spolupráci s vládními orgány, čímž vytvářejí governance; někdy ovšem bez vládní autority.“* Keohane se tedy jinými slovy podle Shailendra C. Jain Palvia a Sushil S. Sharma snaží říct, že governance, potažmo eGovernance nemusí být nutně spojeno s veřejným sektorem. Zahrnuje řízení a správu politik a postupů i v soukromém sektoru.[8]

Palvia a Sharma dále konstatují, že hlavním rozdílem mezi zmíněnými pojmy je, že eGovernment je poskytování informací a služeb souvisejících s veřejnou správou prostřednictvím internetu a jiných digitálních prostředků mezi orgány veřejné správy, občany a podnikateli. Je to také prostředek snížení byrokracie a veřejných výdajů. Na druhou stranu eGovernance je širším pojmem, který je obecně uplatnitelný i mimo veřejnou správu a který souvisí se správou, koordinací, plánováním, dohledem a využíváním digitálních technologií pro zefektivnění procesů.[9] Dle mého názoru lze shrnout, že eGovernance je cestou nebo spíše nástrojem, zatímco eGovernment je dynamicky se rozvíjejícím výsledným dílem.

Pokud tedy někteří autoři tvrdí, že eGovernment je zapojování ICT do veřejné správy, mají pravdu spíše jen z části. Jistě je to jeden ze společných jmenovatelů obou pojmů, ale samotný eGovernment má i druhou rovinou, a tou je právě poskytování různých veřejných e-služeb pro občany daného státu. Ve skutečnosti se však nejedná pouze o služby mezi státem a občanem G2C (government to citizen), mezi státem a podnikateli G2B (government to business), ale i mezi orgány veřejné moci navzájem G2G (government to government), a to „*pro účely integrace existujících procesů a dosažení větší racionality a systémovosti“*[10].

[8] PALVIA, Shailendra C. Jain, SHARMA, Sushil S. *E-Government and E-Governance: Definitions/Domain Frameworkd and Status around the World.* Karkala: Computer Society Of India, 2007. [cit. 2022-05-05]. str. 3–4. Dostupné z: http://governance40.com/wp-content/uploads/2019/06/E-Government_and_E-Governance_Definition.pdf
[9] Ibid., str. 3-4
[10] ŠPAČEK, David, op. cit. sub. 17, str. 9

Gestorem oblasti eGovernmentu je v České republice Ministerstvo vnitra. V jeho rámci je zřízen odbor Hlavního architekta eGovernmentu, který má nadresortní působnost a který zodpovídá za koordinaci a vedení rozvoje eGovernmentu ve veřejném sektoru.[11] Kromě tohoto útvaru má důležité postavení mezi orgány veřejné správy i Vláda České republiky. Ta ke konci roku 2018 v rámci programu Digitální Česko schválila Informační koncepci České republiky, ve které stanovila hlavní cíle a poslání eGovernmentu České republiky. Mezi poslání se řadí poskytování on-line služby klientům veřejné správy nejjednodušším a nejefektivnějším způsobem a zároveň poskytování standardizovaných sdílených elektronických služeb nad daty úředníkům veřejné správy při výkonu jejich působnosti. Jako vrcholný cíl si Vláda ČR vytyčila, aby v závěru pětiletého horizontu koncepce platila následující teze: „*Česká republika je jednou z předních zemí v praktickém využívání moderních služeb eGovernmentu, což významně přispívá k přívětivosti a celkové efektivitě veřejné moci*“.[12]

V každém případě se domnívám, že je zásadní, aby bylo využívání eGovernmentu a jeho služeb koncipováno jako právo, nikoliv povinnost. A to sice právo využívat služby digitálními prostředky při současném zachování úcty ke generačním rozdílům mezi občany a jejich rozdílným schopnostem ovládat moderní dostupné technologie, tj. digitální gramotnosti.[13] Právní úprava eGovernmentu by měla pozitivně motivovat občany a osoby k využívání jeho služeb, ale současně nesankcionovat ty, kteří tyto služby z objektivních důvodů využívat nebudou. V praxi je, podobně jako je tomu i soukromých elektronických služeb, využívána zejména motivace finanční a praktická – elektronické služby jsou poskytovány zdarma nebo za snížený poplatek a využíváním elektronických služeb urychlí každá osoba proces vyřizování konkrétních záležitostí, kterou by za jiných okolností vyřizovala osobně.

Jak jsem uvedl výše eGovernment je jedna ze součástí veřejné správy. Pojem veřejná správa jakožto součást výkonu státní moci, která není zákonodárstvím, soudnictvím ani vládnutím, v sobě mimo jiné obsahuje i jakýsi závazek toho, že správa je „*cíleně zaměřená činnost*

[11] Protože Ministerstvo vnitra je samo správcem klíčových informačních systémů veřejné správy, např. základního registru obyvatel, informačního systému evidence obyvatel nebo informačního systému datových schránek, plní významnou úlohu též odbor eGovernmentu a další útvary.

[12] DZURILLA, Vladimír, et al. Digitální Česko. Vládní program digitalizace České republiky 2018+. Informační koncepce. Koncepce budování eGovernmentu v ČR 2018+ a jeho IT podpory podle zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. Praha: Úřad vlády České republiky, 2020. [cit. 2022-05-05]. str. 2. Dostupné z: https://www.digitalnicesko.cz/informacni-koncepce-cr/

[13] MEDIAN. *Digitální gramotnost. Zpráva o stavu a výuce digitální gramotnosti a komparace se zahraničím.* Praha: Median, 2017. [cit. 2021-21-03]. str. 20. Dostupné z: https://www.mpsv.cz/documents/20142/225517/Digitalni_gramotnost__-_Zprava_o_stavu_a_vyuce_digitalni_gramotnosti_a_komparace_se_zahranicim.pdf/f633dd0f-e5df-c19f-7cfa-38291b31ceb4

k obstarávání nejrůznějších záležitostí“.[14] Lze jí tedy vnímat i jako službu orgánů veřejné správy, při které vykonávají své úkoly pro účely plně fungujícího a přívětivého systému veřejné správy, který občanům a osobám umožnuje plnit své povinnosti a domáhat se efektivně svých práv. Institut eGovernmentu je tedy svým způsobem službou, kterou veřejná správa poskytuje. To ovšem neznamená, že se v některých oblastech jeho úprava bude dotýkat čistě veřejné správy bez zapojení dalších orgánů veřejné moci.

Právní předpisy týkající se eGovernmentu v některých případech používají pojmy orgán veřejné moci a v některých naopak orgán veřejné správy. Není to ovšem náhodné nebo chybné zaměňování. Ačkoliv obecným pojmem správního práva je správní orgán, definován v § 1 odst. 1 SpŘ jako „*orgán moci výkonné, orgán územních samosprávných celků a jiné orgány, právnických a fyzických osob, pokud vykonávají působnost v oblasti veřejné správy*.“, řada právních předpisů používá pojem orgán veřejné správy, který je s pojmem správní orgán srovnatelný. Orgán veřejné správy je, stejně jako správní orgán, vykonavatelem veřejné správy, konkrétněji (podle svého nositele) státní správy, samosprávy nebo ostatní veřejné správy.[15] Zatímco orgánem veřejné moci je jakýkoliv orgán, který autoritativně rozhoduje o právech a povinnostech, tedy například i soud.[16] Podle kontextu tedy zákonodárce zaměňuji tyto pojmy záměrně, aby odlišil, kdy se ta která úprava týká výhradně veřejné správy a kdy naopak i orgánů stojící mimo veřejnou správu. Ve výsledku služby eGovernmentu zajišťují orgány veřejné správy, ale zároveň umožňují jejich propojení i s orgány veřejné moci. Příkladem můžou být základní registry, které spravují rozdílné orgány veřejné správy (Ministerstvo vnitra, Český zeměměřičský a katastrální úřad nebo Český statistický úřad), ale jejich editorem může být i orgán veřejné moci jako je například soudní exekutor, tedy osoba, která nevykonává veřejnou správu, ale veřejnou moc.[17]

1.1. Pilíře eGovernmentu

[14] KOPECKÝ, Martin. *Správní právo: obecná část.* V Praze: C.H. Beck, 2019. Beckovy právnické učebnice. str. 6. ISBN 978-80-7400-727-9

[15] Srovnání KOPECKÝ, Martin, op. cit. sub. 20, str. 6, HENDRYCH, Dušan. [Správní orgán] In: HENDRYCH, Dušan. *Právnický slovník*. 3.vydání. V Praze: C.H. Beck, 2009. Beckovy odborné slovníky. ISBN 978-80-7400-059-1, ustanovení § 1 odst. 1 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně dalších zákonů (dále jen „**ZoISVS**“) a JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. § 1 [Rozsah působnosti]. In: JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. *Správní řád*. 6. vydání. Praha: C. H. Beck, 2019, str. 15. ISBN 978-80-7400-751-4

[16] HENDRYCH, Dušan. [Orgán veřejné moci] In: HENDRYCH, Dušan. op. cit. sub. 20

[17] Srovnání ustanovení § 2 písm. c) zákona č. 111/2009 Sb., o základních registrech (dále jen „**ZoZR**“)

Český eGovernment tvoří dle mého názoru tři základní pilíře. Prvním jsou informační systémy obecně. Orgánům veřejné moci svěřují některé právní předpisy do správy vlastní informační systémy, ve kterých shromažďují nejrůznější údaje a data. Je podstatné, pakliže chceme přijmout tezi, že „obíhat by měly data, nikoliv lidé“, aby vůbec existovaly evidence, jakkoliv systematizovaných dat, díky kterým si mezi sebou mohou orgány data za stanovených podmínek předávat. Jedna věc je tedy existence databází, druhá zajištění propojenosti databází navzájem. Druhým pilířem je klíčová komunikační infrastruktura českého eGovernmentu, která se nazývá Komunikační infrastruktura veřejné správy (dále jen „**KIVS**“).

KIVS je často označována jako oběhová soustava eGovernmentu.[18] Je to sjednocená datová privátní síť orgánů veřejné správy určená pro bezpečné propojení informačních systémů navzájem, přičemž jejím středobodem je Centrální místo služeb (dále jen „**CMS**“). CMS "*je základní stavební prvek celé komunikační infrastruktury veřejné správy. Zajišťuje vzájemné, řízené a bezpečné propojování subjektů veřejné a státní správy, dále zajišťuje komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích, jakými jsou internet nebo komunikační infrastruktura EU.*“[19]

Domnívám se, že existuje-li systematizovaná databáze údajů, které orgány veřejné správy vedou o subjektech veřejné správy, a tyto databáze jsou navzájem propojené tak, aby bylo možné navzájem bezpečně sdílet tyto údaje, musí existovat i možnost, jakým způsobem budou adresáti veřejné správy tyto údaje získávat pro sebe nebo jak je budou předávat státu. Proto jsem toho názoru, že třetím pilířem českého eGovernmentu jsou nástroje, které využívají adresáti veřejné správy pro komunikaci s orgány veřejné správy. Mezi ně pak lze řadit bezpochyby datové schránky, služby vytvářející důvěru (např. elektronický podpis) nebo službu elektronické identifikace.

Výše uvedené pilíře jsou pouhým obecným nástinem toho, co tvoří dle mého názoru eGovernment v České republice. Přesto se domnívám, že toto rozdělení lze aplikovat i na obecnou nauku o eGovernmentu jako takovém. Pokud bych tedy měl výše uvedené shrnout,

[18] FELIX, Ondřej, KAUCKÝ, Jiří, KOLÁŘ, Jindřich, et al. *Jak se (z)rodil eGON: reforma a elektronizace veřejné správy*. Praha: CEVRO Institut, 2015. ISBN 978-80-87125-28-1.
[19] NÁRODNÍ AGENTURA PRO KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE. Podrobnější popis projektů. *Národní agentura pro komunikační a informační technologie* [online]. [cit. dne 2022-05-05]. Dostupné z: https://nakit.cz/projekty-popis/

tak pro adekvátně funkční eGovernment je dle mého názoru nutné podle dosavadních technických možností zajistit:

a) průběžně aktualizované databáze údajů o subjektech i orgánech veřejné správy,
b) komunikační síť, která údaje z databází propojuje a z nich vyvozuje fakticky ověřitelné závěry, a
c) nástroje, díky kterým může adresát veřejné správy s veřejnou správou komunikovat a předávat jí a získávat od ní údaje.

Konkrétní provedení výše uvedených pilířů pak záleží na praktické aplikaci dosavadních dostupných technologií a vůbec vůli efektivně modernizovat infrastrukturu ICT, kterou veřejná správa využívá.

1.2. Elektronizace a digitalizace

Při debatě o eGovernmentu rozlišujeme mezi pojmy digitalizace a elektronizace. Často jsou tyto pojmy zaměňovány, čemuž se snad nelze ani podivovat, jelikož hranice mezi nimi je dosti neostrá. Tyto pojmy nejsou ve hierarchickém vztahu, v řadě případů se navzájem propojují a splývají v jedno, někdy naopak znamenají poměrně odlišné věci. Pro lepší představu je vhodné nejprve vymezit co znamenají původní slova, od nichž jsou oba procesy odvozeny, tedy elektronický a digitální.

Elektronický je velmi zjednodušeně adjektivum poukazující na objekt, který využívá pro svou činnost tok elektronů, tedy subatomárních částic, které tvoří obal atomu se záporným elektrickým nábojem.[20] Elektronické mohou být různé spotřebiče, vedení vysokého napětí, ale i například analogové hodinky. Záměrně jsem zmínil analogové hodinky, tyto hodinky jsou totiž elektronické, jelikož jsou napájené elektrickou baterií. Přesto nejsou digitální. Naopak digitální hodinky jsou digitální i elektronické zároveň.

[20] SPENCER, Matthew. *What`s the difference between „electronic“ and „digital“?* Quora.com [online]. [cit. 2022-05-05]. Dostupné z: https://www.quora.com/Whats-the-difference-between-electronic-and-digital

Pojem digitální[21] je totiž opak pojmu analogový a vyjadřuje informaci v diskrétní (nespojité) číselné podobě. Typickým příkladem digitálního systému jsou například binární soustava, Morseova abeceda nebo kouřové signály. [22]

Abych výše uvedené shrnul. Elektronizace je proces převodu neelektronických institutů (například vyplnění listinného formuláře) do elektronické podoby (vyplnění formuláře na počítači online). Digitalizace je převod analogového systému do systému vyjadřujícího informaci strojově čitelnou formou nespojitých sérií číslic jako je například vytvoření alternativy pro doručování písemností standardní (analogovou) metodou prostřednictvím držitele poštovní licence, a to sice doručování skrze datové (digitální) schránky. Výše uvedené si lze ukázat na jednoduchém příkladu v praxi veřejná správě hojně využívané archivace listinných dokumentů.

Za předpokladu, že bude z listinného dokumentu vytvořena pouze elektronická kopie pomocí klasického scaneru nebo fotoaparátu, bude se jednat velmi pravděpodobně pouze o elektronizaci. Samo nafocení, chceme-li scanování, je pouhým převodem do elektronické podoby, ale jako takové neumožňuje strojové čtení textu.

V případě, že by byl scan vytvořen za pomocí OCR (optical character recognition) programu pro rozpoznávání textu „scanů“, díky čemuž dojde k vytvoření strojově čitelného textu z takových obrázků, bude se jednat pravděpodobně o digitalizaci.

Pokud se tedy hovoří o tvorbě eGovernmentu, byť samotný pojem eGovernment znamená v doslovném překladu „elektronická vláda“, domnívám se, že je vhodnější používat pojem digitalizace namísto elektronizace. Při digitalizaci se nezřídka může stát, že dílčí změny jsou pouhou elektronizací, jako je například možnost elektronického podání (ve své podstatě se jedná pouze o odeslání klasického scanu dokumentu). Ponechávám stranou případy, kdy je nutné takové podání opatřit elektronickým podpisem, případně odeslat datovou schránkou. Pokud se ovšem zamyslím nad smyslem tvorby eGovernmentu, mělo by být smyslem zjednodušení komunikace mezi státem a občanem a mezi orgány státu navzájem za použití ICT. To tedy znamená převod analogových metod (např. listinných formulářů nebo listinných

[21] Pojem digitální je odvozen ze slova „*digit“* anglicky číslice nebo prst a z latinského „*digitus“*, tedy prst. Někdy se uvádí, že digitální jsou ty systémy jejichž prvky se dají spočítat „na prstech“.
[22] UNIVERSITY OF CAMBRIDGE. Význam slova „Digital“ v Cambridge English Dictionary. *Cambridge Dictionary. English Dictionary, Translations & Thesaurus* [online]. Copyright © Cambridge University Press [cit. 2022-05-05]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/digital

evidencí) do formulářů a evidencí vyjádřených „jedničkami a nulami“, tj. do digitální podoby. Proto jsem toho názoru, že přiléhavějším obecným pojmem je digitalizace, nikoliv elektronizace.

1.2.1. Smysl, proces a úskalí digitalizace

K čemu digitalizace slouží a jaké jsou její benefity? Usnadňuje život i osobám, které například neumí zacházet s počítačem, a to za situace, kdy jediný možný kontakt s veřejnou správou je elektronicky a možnosti písemné nebo osobní komunikace jsou limitovány? Nebo osobám, které sice s počítačem zacházet dokáží, ale žijí v oblasti České republiky, kde není dostatečné pokrytí internetové sítě? Je pro výše zmíněné subjekty skutečně snazší digitální veřejná správa, oproti „analogové“ veřejné správě? Spíše nežli nalezení odpovědi na výše uvedené otázky, pokládám za důležité poskytnout i jiný úhel pohledu než ten, že je nutné veřejnou správu digitalizovat za každou cenu. Je nutné zdůraznit, že by nemělo být cílem digitalizovat jenom proto, aby se digitalizovalo, protože je po tom společenská poptávka.

Při procesu digitalizace je nutné brát v potaz i výše zmíněné otázky. Stále existuje celá řada ohrožených skupin, kterým dělá práce s ICT zásadní potíže, jako jsou senioři, lidé se základním vzděláním nebo lidé žijící v regionech s nedostatečným pokrytím.[23] Těmto osobám je nutné poskytnout určité formy záruky alternativ k digitálnímu světu, možnosti bezplatného digitálního vzdělávání nebo jiné formy kompenzací. Tento problém právo nevyřeší, ale může mu zcela jistě jít naproti a vytvářet rámce pro vhodné nástroje.

Digitalizace zcela určitě s sebou přináší časovou úsporu pro občany, kteří využijí služby eGovernmentu tím, že nebudou muset být fyzicky přítomni při kontaktu s veřejnou správou. Časovou úsporu přinese i naplnění „once only“ zásady (česky „jenom jednou“), díky které veřejná správa nevyžaduje po subjektu data, která již má k dispozici a která je schopná si navzájem předat prostřednictvím informačních systémů.

Dalším benefitem je i možnost „elektronické participace“ tj. zapojení subjektů do rozhodovacích a jiných procesů veřejné správy za pomocí ICT. Øystein Sæbø a kolektiv též hovoří o elektronické participaci, nebo chceme-li e-participaci jako o „*technologicky zprostředkované interakci mezi občanskou sférou a politickou sférou a občanskou sférou a*

[23] MEDIAN, op. cit. sub. 19, str. 21

veřejnosprávní sférou“[24]. Organizace spojených národů prostřednictvím e-Participation indexu (EPI) analyzuje kvalitu „politických institucí“ daného státu v souvislosti s elektronickou participací svých občanů. Kolektiv autorů Antonio F. Tavares, Joao Martins a Mariana Lameiras zkoumal, zda se potvrzuje hypotéza, že s mírou elektronické participace roste kvalita politických institucí. Závěrem jejich výzkumné práce s názvem „*Electronic Participation in a Comparative Perspective: Institutional Determinants of Performace*“ byl, že demokratické státy s efektivnější vládou a nízkou mírou korupce mají zároveň vyšší EPI výsledek (tj. více občanů se zapojuje elektronicky do rozhodovacích a jiných procesů veřejné moci). Samozřejmě je nutné vzít v potaz i další důležité aspekty, a to zapojení technologií do rozhodovacích a jiných procesů a socioekonomický vývoj obyvatelstva. Zásadní však je, že míra e-participace (a v širším kontextu i digitalizace pozn. autora) má menší či větší vliv na posilování „demokratičnosti“ státu a zvýšení efektivity výkonu veřejné správy.[25]

Ať už v České republice nebo i v ostatních zemích lze pozorovat trend v oblasti digitalizace. Z tohoto trendu ostatně plyne i pro eGovernment klíčová zásada, která se více či méně naplňuje, a to sice zásada primární digitalizace (*digital by default*). Jedná se jednak o vytváření legislativního prostředí pro digitalizaci, tak ale i o snahu maximálně digitalizovat relevantní odvětví a jejich služeb. Ostatně k této zásadě se veřejně přihlásila i Česká republika.[26] Současně je klíčové, aby všechny subjekty, které by potenciálně mohly digitálních služeb využívat, byly schopné bez větších obtížích komunikovat s veřejnou správou elektronicky a byly digitálně gramotné. Druhu důležitou komponentou je zajištění infrastruktury, která umožní všem bez rozdílu digitální služby veřejné správy využívat. To znamená minimálně zajistit adekvátní připojení k internetu ve všech obydlených částech České republiky. Nemluvě o faktu, že stále není samozřejmostí, že každý jeden subjekt vlastní zařízení, skrze které může elektronické služby využívat. Čím více budou naplňovány výše uvedené náležitosti, tím se domnívám, že bude více přibývat důvodů proč veřejnou správu digitalizovat, spíše než proč nedigitalizovat. Ovšem je nutné brát v potaz výše uvedené faktory a v rámci digitalizace se držet další klíčové zásady, a to zásady dobrovolnosti využívání eGovernmentu. Je jistě na místě vytvářet pozitivní

[24] SAEBØ, Øystein et al. *The Shape of Eparticipation: Characterizing an Emerging Research Area* [online]. Amsterdam: Elsevier, 2007. [cit. 2022-05-05] str. 402. Dostupné z: DOI:10.1016/j.giq.2007.04.007

[25] TAVARES, António, MARTINS, João, LAMEIRAS, Mariana. [Electronic Participation in a Comparative Perspective: Institutional Determinants of Performance] In: BOLIVAR, Manuel Pedro Rodriguez, et al. *Digital Government and Achievieng e_Public Participation: Emerging Research and Opportunities.* [online]. Hershey: IGI Global, 2020. [cit. 2022-05-05]. str. 99. ISBN: 978-1-7998-1529-7. Dostupné z: DOI:10.4018/978-1-7998-1526-6.ch005

[26] DZURILLA, Vladimír, et al, op. cit. sub. 19, str. 6

motivaci pro účast v digitálním světě, nikoliv však sankcionování za neúčast. Nikdo by neměl být omezován na svém právu „nežít v digitálním světě“, pokud zde nepřevažuje veřejný zájem, který by takové omezení dostatečně ospravedlňoval.

Určitým vzorem eGovernmentu je Estonská republika, které se blíže věnuji v kapitole 3.2.1. Úspěch Estonska na poli digitální revoluce se stal objektem řady studií. Jednou z takových studií je case report Evropské komise, která shrnula, co stojí za estonským úspěchem a jaká zjištění můžou sloužit jako vzor pro další státy při budování nebo zlepšování svého eGovernmentu. Ve svých zjištěních shrnula, že je klíčové, aby stát veřejně podporoval propojování ICT s veřejnou správou, úzce spolupracoval při tvorbě se soukromým sektorem a vytvářel a udržoval optimální právní rámec, který bude výše uvedené umožňovat.[27]

Není žádným překvapením, že moderní ICT jsou dynamicky se rozvíjejícím odvětvím současných technologií. Jsou součástí každodenního života prakticky všech subjektů. Jak ale docílit toho, aby byl právní rámec „optimální“ a zbytečně „neházel klacky pod nohy“ nově se objevujícím technologiím nebo efektivnějším řešením? Jakým způsobem docílit toho, aby právní úprava „využívání moderních ICT ve veřejné správě“ byla vždy aktuální a nemusela se s každou novou technologií měnit a tím se vystavovat riziku „zastaralosti“? Tuto problematiku řeší tzv. technologická neutralita.

Technologická neutralita je poměrně komplexní koncept, který nelze vyjádřit jednoduchou definicí. Jak shrnuje Harašta ve dvé dizertační práci „*První analýzy pojmu technologická neutralita jsme se dočkali až v roce 2006, kdy Bert-Jaap Koops uvedl, že na jednu stranu je tento tvrzený princip složen z mnoha různých složek, které si navzájem mohou odporovat, na druhou stranu ale, jak z jeho práce vyplynulo, je technologická neutralita do značné míry odrazem běžných požadavků kladených na právo i jinak, než jen ve vztahu k technologiím. Jedná se např. o obecnost právních norem a zákaz diskriminace nebo o možnost využití teleologického výkladu v určitých situacích. Každý z těchto požadavků se projevuje v kontextu technologického vývoje jinak – obecnost právních norem zajišťuje udržitelnost práva tváří v tvář měnícímu se technologickému prostředí, zákaz diskriminace zapovídá právu vybírat technologické vítěze a teleologický výklad umožňuje interpretaci fixovanou na účel normy a*

[27] CASTAÑOS, Virgina. *Case Study Report: e-Estonia.* [online]. Brusel: Evropská komise, 2018. [cit. 2022-05-05]. Dostupné z: https://jiip.eu/mop/wp/wp-content/uploads/2018/10/EE_e-Estonia_Castanos.pdf

nikoli na projevy okolní technologické reality. Technologická neutralita tak má zajistit, že se statický text nestane zastaralým a neefektivním tváří v tvář technologickému vývoji.“ [28]

J. Harašta dále uvedl s odkazem na Paula Ohma, že sama technologická neutralita není principem, ale spíše jedna ze dvou cest, kterou se lze vydat při tvorbě regulací technologií. Tou druhou cestou je pak tzv. technologická specifita. To ovšem není zcela úplně záležitostí týkající se eGovernmentu.

Právní úprava eGovernmentu se jako taková nezabývá regulací technologií, které jsou pro eGovernment využívány, spíše využívá dostupných technologií tím, že je zapojuje do své činnosti, a pro tyto účely připravuje právní rámec. Jak uvádí Koops, technologická neutralita má směrem k legislativě čtyři hlavní účely:

a) regulovat chování subjektů, nikoliv prostředky jejich chování;

b) zajištění funkční ekvivalence mezi různými způsoby realizace určitého chování (např. elektronický podpis je ekvivalent standardního podpisu pozn. autora);

c) nediskriminovat technologie s ekvivalentním efektem, tedy, že nebude upřednostňována jedna technologie oproti druhé; a

d) zajistit udržitelnost práva a přizpůsobit ho budoucímu vývoji.[29]

Všechny výše uvedené účely by se dle mého názoru měly více či méně promítnout i do tvorby právního rámce eGovernmentu, a proto jsem přesvědčen, že je zapotřebí, aby byl samotný přístup normotvorby technologicky neutrální. Představa, že je právní rámec institutů eGovernmentu přesně spojen s konkrétně definovanou technologií, by v budoucnu vedla ke kolapsu eGovernmentu jako takového. A to z toho důvodu, že se vznikem nové technologie by se technologicky specifikovaná právní úprava eGovernment okamžitě stala neaktuální a zastaralou, což vzhledem ke specifičnosti dalších různých ICT způsobí, že nebude eGovernment interoperabilní. Interoperabilitou se rozumí „*schopnost systémů vzájemně si*

[28] HARAŠTA, Jakub, 2017. *Princip technologické neutrality v kybernetické bezpečnosti*. Brno. Diertační práce. Masarykova univerzita v Brně. Právnická fakulta. Vedoucí práce POLČÁK, Radim. str. 7

[29] KOOPS, Bert-Jaap. [Should ICT Regulation be Technology-Neutral?] In: KOOPS, Bert-Jaap, Miriam LIPS, Corien PRINS a Maurice SCHELLEKENS et al. *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. The Hague: T.M.C. Asser Press, 2006. str. 103-108. ISBN: 978-90-6704-216-1

poskytovat služby a efektivně spolupracovat.“ [30] jinými slovy interoperabilita „*umožňuje správním subjektům, aby si elektronicky vyměňovaly mezi sebou a s občany a podniky smysluplné informace způsoby, které budou pro všechny strany srozumitelné.*“[31] Nemyslím si proto, že by měla být nastavena polemika o tom, jakou cestou by se měla právní úprava eGovernmentu vydat, ale postavit najisto, že jedinou možnou cestou je cesta technologické neutrality.

Na tomto základě bych si dovolil definovat zásadu, která úzce souvisí s technologickou neutralitou, která ale, jak jsem uvedl výše, není zásadou sama o sobě. Jedná se o *zásadu technologicky neutrální normotvorby*. Zásada, která zajistí, že se zákonodárce bude vydávat jedinou cestou, cestou technologické neutrality. Jakákoliv jiná cesta by se dle mého názoru dříve či později projevila jako neefektivní či dokonce kontraproduktivní. Taková zásada do budoucna zajistí samotnou podstatu technologické neutrality, a to, jak jsem již výše citoval, že *„se statický text nestane zastaralým a neefektivním tváří v tvář technologickému vývoji.“*[32]

[30] Usnesení Vlády ČR ze dne 8. října 2014 č. 815, o strategii rozvoje infrastruktury pro prostorové informace v České republice do roku 2020

[31] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výrobu regionů. Evropský rámec interoperability – Strategie provádění, Brusel, 23. března 2017, COM (2017) 134 final

[32] HARAŠTA, Jakub, op. cit. sub. 27, str. 7

2. Instituty českého eGovernmentu a jejich právní úprava

Historie rozvoje konkrétnější právní úpravy pro elektronizaci veřejné správy a její faktickou realizaci, která vyústila v to, co se dnes nazývá eGovernment České republiky, sahá do relativně nedávné minulosti, do roku 2007. Byť před tímto obdobím existovala jistá snaha o elektronizaci některých procesů (lze zmínit například zákon č. 227/2000 Sb., o elektronickém podpisu nebo pro další vývoj stěžejní ZoISVS v původním znění), neexistovala v té době žádná klíčová legislativa, která by vyloženě usnadňovala komunikaci mezi veřejnou správou a jejími adresáty. Jedinou výjimkou byl ZoISVS. Ten byl zcela jistě přelomovou právní normou, která lapidárně řečeno, otevřela stavidla a usnadnila příliv dalších legislativních norem, které více či méně vytvářely podmínky pro naplňování cíle budování eGovernmentu. Jako takový ovšem žádné konkrétní benefity pro adresáty veřejné správy nepřinášel. Pouze usnadnil komunikaci mezi orgány veřejné správy navzájem a cílil především na vztah G2G. Z tohoto důvodu se domnívám, že by ZoISVS dal označit jako takzvaný základní kámen právní úpravy eGovernmentu, který by ovšem bez dalších předpisů nebyl tak zásadním, jako je tomu dnes.

2.1. Informační systémy veřejné správy

Původní myšlenkou přijetí ZoISVS ve svém původním znění bylo vytvoření obecného zákonu, který stanovoval podmínky pro první kroky v oblasti elektronizace veřejné správy, zejména pro provoz informačních systémů veřejné správy[33]. „*Informační systémy veřejné správy jsou pojímány jako soubor jednotlivých informačních systémů, které slouží pro výkon veřejné správy a jsou vedeny ministerstvy, jinými správními úřady, orgány územní samosprávy v přenesené působnosti a dalšími státními orgány (souhrnné označení "orgány veřejné správy"). Východiskem je skutečnost, že jednotlivé informační systémy obsahují informace, které jsou potřebné pro jiné informační systémy, resp. pro zajištění správních činností příslušných orgánů. Cílem navrhovaného zákona je vytvoření podmínek pro zajištění kvalitních dat a bezpečné výměny informací za předem stanovených podmínek. K tomu je také nutno zajistit základní předpoklady pro tvorbu a rozvoj informačních systémů.*“[34] Jinými slovy, informační

[33] Ustanovení § 2 písm. b) ZoISVS definuje informační systém veřejné správy jako „funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy nebo plnění jiných funkcí státu anebo dalších veřejnoprávních korporací. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále technické a programové prostředky, případně jiné nástroje umožňující výkon informačních činností

[34] Důvodová zpráva ZoISVS

systémy jsou databáze jednotlivých orgánů veřejné správy navržené tak, aby mezi dílčími databázemi mohla probíhat bezpečná výměna dat a aby za stanovených podmínek mohl některý z orgánů údaje jednoduše získat. Z výše uvedených definic vyplývá, že informační systémy veřejné správy nejsou uzavřený celek konkrétních informačních systémů, ale naopak, že lze předpokládat s rozvojem dalších agend svěřených veřejné správě, že se jejich celkový počet může měnit (v některých případech bude počet narůstat, ale i klesat v důsledku zrušení některých obsolentních informačních systémů či jejich transformování do jiných systémů).

Jedním z takových informačních systémů veřejné správy je tzv. Portál veřejné správy. „*Jeho posláním je poskytnout fyzickým a právnickým osobám dálkový přístup ke všem informacím a službám v oblasti veřejné správy, zpřístupnit znalosti, fakta a záznamy veřejné správy, zvýšit efektivnost a autoritu veřejné správy, posílit důvěru občanů v ní a umožnit státní správě vystupovat jako integrální organizace. Při jeho budování byl jako významné kritérium brán v úvahu požadavek dostupnosti informací a jejich aktuálnosti, spolehlivosti a odolnosti, bezpečnosti tam, kde se osoby musí registrovat, a přívětivosti, zajišťující možnost užívání i těm, kteří nemají potřebné znalosti.“*[35]

Po obsahové stránce ZoISVS primárně vymezuje práva a povinnosti spojené se správou a provozem jednotlivých informačních systémů, stejně jako povinnost poskytovat informace z informačních systémů dalším orgánům veřejné správy, a to v odůvodněných případech. Z tohoto ZoISVS dále negativně vymezuje ty informační systémy, které se neřadí mezi informační systémy de lege. Jedná se o systémy pro potřeby nakládání s utajovanými informacemi, systémy zpravodajských služeb, Národního bezpečnostní úřadu a Národního úřadu pro kybernetickou a informační bezpečnost. Na zmíněné systémy by totiž nemohl dopadat právní rámec ZoISVS, jelikož by se tím ohrozila bezpečnost utajovaných informací, které jsou chráněny zvláštními předpisy včetně podmínek přístupu k takovým informacím.[36] Současně se úprava nevztahuje na informační systémy jednotlivých správců informačních systémů.

Původní znění ZoISVS počítalo se stanovením působnosti Úřadu pro státní informační systém jakožto ústředního správního úřadu pro vytváření a rozvoj informačních systémů.[37] Tento úřad

[35] MATES, Pavel op. cit. sub. 17, str. 283-286
[36] Např. zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „**ZoUtajInf**“).
[37] Ustanovení § 4 odst. 1 ZoISVS v původním znění,

byl následně zrušen a jeho pravomoci zákonem č. 517/2002 Sb., transformovány na v této době existující Ministerstvo informatiky, které bylo následně zákonem č. 110/2007 Sb., zrušeno a jeho kompetence převedeny pod Ministerstvo vnitra.

„*Elektronizace veřejné správy neboli eGovernment je téma, které se dostalo na půdu Poslanecké sněmovny Parlamentu České republiky v pravém slova smyslu až v roce 2007, kdy ministerstvo vnitra a informatiky představilo svůj záměr řešení agend elektronickou cestou.“*[38] Jedná se o novelu ZoISVS vyhlášenou 31. října 2007 publikovanou jako zákon č. 269/2007 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a další související zákony s účinností od 1. ledna 2008, které se vžilo označení zákon o Czech POINT (dále jen „**ZoCzechPOINT**“). Czech POINT neboli Český Podací Ověřovací Informační Národní Terminál, je síť tzv. kontaktních míst veřejné správy, které umožňují na žádost vydat „výstup z informačního systému veřejné správy“, tedy listinný výpis ze zapsaných údajů vedených ve veřejných evidencích, který má charakter veřejné listiny. Současně se rozšířila působnost dalších správních orgánů, které můžou tyto výstupy vydávat.[39] Nově měly, kromě úřadů obcí s rozšířenou působností a notářů, pravomoc vydávat výstupy veškeré obecní úřady, zastupitelské úřady, držitelé poštovní licence a Hospodářská komora České republiky. Zmíněné úřady tak tvořily síť Czech POINT.[40] Další správně právní zajímavostí kolem názvu Czech POINT je soudní řízení o ochraně slovní ochranné známky CZECH POINT. V tomto případě byla žalobkyní CZECH POINT 101 s.r.o. podána správní žaloba proti Úřadu průmyslového vlastnictví, když prohlásil *ex tunc* ochranou známku žalobkyně ve znění „CZECH POINT“ za neplatnou z důvodu neexistence dobré víry zápisu této známky. Nejvyšší správní soud posléze zamítnul kasační stížnost a potvrdil rozhodnutí Městského soudu v Praze a vrátil věc k novému rozhodnutí Úřadu průmyslového vlastnictví.[41]

Cílem ZoCzechPOINT bylo v konečném důsledku jednak zvýšení počtu „kontaktních míst veřejné správy“ a jednak rozšíření okruhu subjektů příslušných k ověřování výpisů z veřejných

---

[38] FELIX, Ondřej, KAUCKÝ, Jiří, KOLÁŘ, Jindřich, et al., op. cit. sub. 21

[39] „Okruh obecních úřadů, které mohou vydávat ověřené výstupy z informačních systémů veřejné správy, je v současnosti omezen pouze na obecní úřady obcí s rozšířenou působností a na základě vyhlášky vydané Ministerstvem vnitra též na pověřené obecní úřady, celkem cca 400 obecních úřadů, což je velmi nízký počet vzhledem k tomu, že smyslem vydávání ověřených výstupů prostřednictvím sítě obecních úřadů (a dalších subjektů) je umožnit žadatelům snadný přístup k výpisům z informačních systémů veřejné správy“ (cit. z Důvodové zprávy k ZoCzechPOINT)

[40] Srovnání znění ZoISVS účinného k 31. prosince 2007 a k 1. lednu 2008

[41] Rozsudek Nejvyššího správního soudu ze dne 22. ledna 2021 s č.j. 5 As 112/2018-53

(např. katastr nemovitostí, obchodní rejstřík, živnostenský rejstřík), ale primárně i některých neveřejných evidencí a registrů jako např. z Rejstřík trestů.[42]

V rámci dalšího vývoje došlo k rozšíření „služeb“, které Czech POINT může poskytovat. Pro další vývoj eGovernmentu byla zásadní zejména služba zřizování datových schránek a poskytování autorizované konverze dokumentů.

ZoISVS za účelem řízení konkrétních informačních systémů veřejné správy, kromě provozních informačních systémů, zakotvuje povinnost získání atestace u subjektů, které mají zájem na dlouhodobém řízení informačních systémů veřejné správy. Atestaci udělují tzv. atestační střediska, kterým bylo uděleno pověření k provádění atestací Ministerstvem vnitra. Podmínkou pro udělení tohoto pověření je získání osvědčení o akreditaci, které vydává tzv. akreditující osoba. Akreditující osoba, obdobně jako atestační střediska, musí splňovat konkrétní podmínky pro vydání pověření k provádění akreditaci, které vydává Ministerstvo vnitra.[43]

2.2. Elektronický podpis a další služby vytvářející důvěru pro elektronické transakce

Původní úprava elektronického podpisu byla obsažena v zákoně č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, přičemž byla s účinností od 19. září 2016 zrušena zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „**ZoSVD** “). ZoSVD je předpisem, který je implementací nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu (dále jen „**eIDAS**“). ZoSVD navazuje na původní úpravu elektronického podpisu a dále upravuje postup poskytovatelů služeb vytvářejících důvěru, mezi které se řadí vydávání kvalifikovaných certifikátů pro a) elektronické podpisy a elektronické pečetě, b) autentizaci internetových stránek a pro c) časová razítka, tedy pro takzvané služby vytvářející důvěru.[44]

[42] Oprávnění vydávat výpisy z neveřejných evidencí a registrů je řešeno cestou legislativních úprav dotčených předpisů. V případě rejstříku trestů je to zákon č. 269/1994 Sb., o Rejstříku trestů.
[43] Srovnání ustanovení § 6 a násl. ZoISVS
[44] Ustanovení § 3 odst. 1 ZoSVD

Dle eIDAS má elektronický podpis tři varianty, a to **kvalifikovaný elektronický podpis** (QES, pozn. autora), **zaručený elektronický podpis** (AdES, pozn. autora) a **(další) elektronický podpis**.[45] ZoSVD rozeznává ještě čtvrtou kategorii, tzv. **uznávaný elektronický podpis**.[46]

„***Kvalifikovaný elektronický podpis*** *má právní účinek rovnocenný vlastnoručnímu podpisu*“[47] a je jednak vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů tzv. QSCD[48] a současně je založen na kvalifikovaném certifikátu pro elektronické podpisy.[49] Kvalifikovaným certifikátem se rozumí „*elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou“*[50] a může ho vydat pouze poskytovatel služeb vytvářejících důvěru podle ZoSVD, kterému orgán dohledu udělil status kvalifikovaného poskytovatele.[51] Těmto poskytovatelům stanovuje ZoSVD zvláštní práva a povinnosti, zejména povinnost přijmout vhodná technická a organizační opatření a objektivní odpovědnost za škodu vzniklou při poskytování služeb vytvářející důvěru.[52]

Zaručený elektronický podpis nemusí být vydán na kvalifikovaném prostředku, ale musí být „*jednoznačně spojen s podepisující osobou, umožňuje identifikaci podepisující osoby, je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou a je k datům, která jsou tímto podpisem podepsaná, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat*.“[53], přičemž může být „*založený na jakémkoliv, komerčním či zaměstnaneckém, certifikátu“*[54]. Kvalifikovaný elektronický podpis, je dále v souladu s eIDAS zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a je založen na kvalifikovaném certifikátu pro elektronické podpisy.[55]

---

[45] Ustanovení čl. 3 odst. 10 až 12 eIDAS
[46] Ustanovení § 6 odst. 1 ZoSVD
[47] Ustanovení čl. 25 odst. 2 eIDAS
[48] Konfigurovaný program nebo vybavení, které vytváří elektronické podpisy a splňuje „kvalifikační“ podmínky
[49] Ustanovení čl. 3 odst. 22 a 23 eIDAS
[50] Ustanovení čl. 3 odst. 14 eIDAS
[51] Srovnání ustanovení čl. 3 odst. 20 eIDAS a § 2 a násl. ZoSVD
[52] Srovnání ustanovení čl. 13 a 19 eIDAS
[53] Ustanovení čl. 26 eIDAS
[54] KORBEL, František, KOVÁŘ, Dalibor, AMLER, Petr. *Interpretace elektronického podpisu a související identifikace v soukromém právu* [online]. Praha: Právní prostor, 2020. [cit. 2022-05-05]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/interpretace-elektronickeho-podpisu-souvisejici-identifikace-v-soukromem-pravu
[55] Ustanovení čl. 3 odst. 12 eIDAS

Český zákonodárce ovšem implementaci poměrně zkomplikoval. V souladu se ZoSVD je kvalifikovaný elektronický podpis povinné využívat pouze v případech, kdy činí úkon subjekty veřejné správy uvedené v § 5 odst. 1 ZoSVD a další osoby při výkonu své působnosti. Zaručený elektronický podpis a další elektronický podpis je možné činit v jiných případech, kdy subjekt právně jedná, pokud nenaplňuje podmínky v § 5 ZoSVD, tedy v případech, kdy subjekt nejedná právně jako subjekt veřejné správy. Z tohoto důvodu zákonodárce vytvořil již zmíněnou alternativu – **uznávaný elektronický podpis**, který eIDAS výslovně nepředpokládá.[56] Uznávaný elektronický podpis je v souladu s § 6 odst. 2 ZoSVD buďto:

a) zaručený elektronický podpis, ale na rozdíl od eIDAS musí být vydán na kvalifikovaném certifikátu pro elektronický podpis, nebo

b) kvalifikovaný elektronický podpis.

Zákonodárce zde zvolil poměrně komplikovanou a nepřehlednou implementaci evropského nařízení, která vytváří interpretační problémy. Zjednodušeně řečeno je totiž uznávaný elektronický podpis a kvalifikovaný elektronický podpis téměř to samé s tím rozdílem, že kvalifikovaný elektronický podpis slouží pouze pro potřebu subjektů veřejné správy, zatímco uznávaný elektronický podpis má širší využití.

Poslední zmíněnou kategorií jsou „**další elektronické podpisy**“ někdy nazývané jako „prosté elektronické podpisy“ ve smyslu čl. 3 odst. 10 eIDAS. O těchto podpisech eIDAS stanovuje, že se jimi „*rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání*“[57], jak uvádí F. Korbel a spol., v tomto případě tedy eIDAS přistoupilo k pojetí, ve kterém zdůrazňuje vážnost projevu vůle podepisujícího a stvrzení konečnosti oproti objektivním charakteristikám toho kterého podpisu (např. zda obsahuje specifikovanou úroveň zabezpečení nebo je vydán konkrétním poskytovatelem).[58] Prostým elektronickým podpisem pak může být celá škála konkrétních forem podpisu, může se jednat o signaturu na závěr emailové zprávy nebo neověřená kopie fyzického podpisu. Zjednodušeně řečeno je to jakýkoliv

[56] Jak jsem již uvedl, podle čl. 3 odst. 12 eIDAS, se za kvalifikovaný elektronický podpis považuje i zaručený elektronický podpis založený na kvalifikovaném certifikátu, tedy to, co český zákonodárce nazývá uznávaný elektronický podpis. Ovšem samotné pojmenování uznávaný elektronický podpis je čistě český „vynález“.
[57] Ustanovení čl. 3 odst. 10 eIDAS
[58] Srovnání s KORBEL, František, KOVÁŘ, Dalibor, AMLER, Petr, op. cit. sub. 33

podpis v elektronické formě, který nesplňuje kritéria uznávaného nebo zaručeného elektronického podpisu podle eIDAS.

V rámci zjednodušení si dovolím udělat následující srovnání.

Elektronický podpisem s nejvyšší silou je na prvním místě *kvalifikovaný elektronický podpis* (dle eIDAS) a *uznávaný elektronický podpis* (dle ZoSVD).

Na druhém místě je *zaručený elektronický podpis* (bez kvalifikovaného certifikátu) a na posledním je prostý *elektronický podpis*.

Dalšími službami vytvářející důvěru jsou kvalifikované elektronické pečetění dokumentu a kvalifikované elektronické časové razítko. Formy i podmínky využívání těchto služeb jsou víceméně totožné jako u elektronického podpisu.[59]

2.3. Datové schránky a autorizovaná konverze

S rozvojem služeb Czech POINTu vznikla, v souvislosti se zvyšujícím se podílem elektronické komunikace směrem k úřadům, poptávka po tom, aby existovaly další elektronické nástroje pro zefektivnění komunikace mezi veřejnou správou a jejími adresáty. Jedním z dosavadních nástrojů byla například možnost činit úkon vůči správnímu orgánu v elektronické podobě podepsané zaručeným elektronickým podpisem ve smyslu již zrušeného zákona o elektronickém podpisu.[60] Současně zákonodárce pociťoval potřebu sjednotit možnosti elektronické komunikace mezi orgány veřejné správy a jejím adresáty a upravit převod dokumentů z listinné do elektronické podoby, takzvanou konverzi. Na tomto základě byl přijat zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (dále jen „**ZoEÚAK**“), který v době svého přijetí byl označován jako „eGovernment act“ a jako srdce „eGON“. EGON byl společným symbolem pro realizaci čtyř základních projektů eGovernmentu v České republice mezi lety 2006 a 2012.[61] S odstupem času je označení ZoEÚAK jako „eGovernment act“, tedy naznačování, že tento předpis je alfou a omegou právní úpravy eGovernmentu, spíše úsměvné. Logicky byl na dobu svého přijetí revolučním krokem

[59] Srovnání ustanovení §8 až § 10 a ustanovení § 11 s ustanovením § 5 až 7 ZoSVD

[60] V souvislosti se zrušením zmíněného zákona o elektronickém podpisu došlo k novelizaci ustanovení § 37 odst. 4 SpŘ, kdy byla odstraněna podmínka „zaručeného“ elektronického podpisu a ponechána možnost činit tak s elektronickým podpisem dále nespecifikovaným.

[61] FELIX, Ondřej, KAUCKÝ, Jiří, KOLÁŘ, Jindřich, et al., op. cit. sub. 21, str. 22

v právním řádu České republiky, nicméně záměrně zdůrazňuji, že se jednalo o revoluční krok jen pro Českou republiku. Zpětně už je úprava vyjádřená v ZoEÚAK natolik samozřejmá, že se domnívám, že označení „eGovernment act“ by se dala nazvat celá řada dalších právních předpisů, které znamenaly ve své době revoluci. Tím se však potvrzuje pouze to, že právní úprava eGovernmentu je dynamicky se rozvíjejícím oborem a s trochou nadsázky, co je dnes považováno za budoucnost, bude již zítra minulostí.

I s ohledem na to, co jsem vyjádřil výše, je nutné dodat, že právní úprava obsažená v ZoEÚAK utváří jeden ze zásadních nástrojů používaných pro komunikaci adresátů s veřejnou správou a mezi orgány veřejné správy navzájem, tzv. datové schránky.

2.3.1. Datové schránky

Datovou schránku definuje § 2 odst. 1 ZoEÚAK jako „*elektronické úložiště, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci a dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob*.“[62] Zjednodušeně řečeno se jedná o jakousi formu elektronické pošty, která má ovšem některá výrazná specifika oproti emailu, které dále rozeberu.

Jak vyplývá z definice, datová schránka je standardizovaný nástroj elektronické komunikace jak pro fyzické, fyzické podnikající a právnické osoby, tak ale i pro orgány veřejné moci. Celkem ZoEÚAK počítá se čtyřmi druhy datové schránky, přičemž s každou se pojí jiná práva a povinnosti. První je datová schránka orgánu veřejné moci.

Orgánu veřejné moci se datová schránka zřizuje povinně bez potřeby předložit žádost, a zřizuje jí Ministerstvo vnitra automaticky bezodkladně po vzniku konkrétního orgánu. V případě notářů a soudních exekutorů se datová schránka zřizuje dnem jejich zapsání do zákonem stanovené evidence.[63] Cílem povinného založení datových schránek pro uvedené subjekty souvisí s povinností orgánů veřejné moci, aby mezi sebou obousměrně komunikovaly výhradně pomocí datových schránek, pakliže to umožňuje povaha dokumentu a není-li doručováno na místě.

[62] Ustanovení § 2 odst. 1 ZoEÚAK
[63] Ustanovení § 6 ZoEÚAK

Současně tato povinnost plyne orgánům veřejné moci i v případě, kdy orgán veřejné moci komunikuje vůči všem osobám, které mají zřízenou datovou schránku, bez ohledu na to, zda je zřízena ze zákona nebo na základě žádosti. Orgán veřejné moci je totiž povinen zjistit informaci, zda ta která osoba má zřízenou datovou schránku, a činí tak prostřednictvím informačního systému datových schránek, ve které je tato informace obsažena. Pokud je zjištěno, že subjekt datovou schránku zřízenou má, je orgán veřejné moci povinen doručovat do ní.[64] Orgán veřejné moci, tedy například správní orgán nebo *„soud[65] zjišťuje z úřední povinnosti, zda má adresát soudní písemnosti zřízenou a zpřístupněnou datovou schránku a pokud zjistí, že ji zpřístupněnou má, doručuje veškeré písemnosti povinně a přednostně do datové schránky, aniž by adresát, který má právo očekávat, že mu soud bude veškeré písemnosti do datové schránky doručovat, o to požádal. Tímto způsobem soud nepostupuje jen tehdy, byly-li písemnosti doručeny při jednání nebo při jiném úkonu soudu nebo nedošlo-li k řádnému doručení do datové schránky.“*[66] Pro vyloučení všech pochybností se v uvedeném informačním systému zveřejňuje datum zřízení datové schránky (respektive i přihlášení do datové schránky nebo odeslání dokumentu) s přesností na vteřinu.

V případě, že nebude orgán veřejné moci komunikovat s konkrétním subjektem skrze datovou schránku, ačkoliv by jí měl subjekt zřízenou, nemůže dojít k fikci doručení, jestliže si subjekt písemnost fyzicky nepřevzal. S tímto názorem se ztotožnil i např. Nejvyšší správní soud ve svém rozsudku ze dne 30. listopadu 2016, č.j. 3 As 26/2016-45. Pokud si subjekt převzal písemnost doručenou např. držitelem poštovní licence, ačkoliv měl nárok na její doručení do datové schránky (tím, že jí měl zřízenou před datem odeslání písemnosti) považuje se písemnost za doručenou se všemi právními následky. „*Řádné doručení písemností v praxi znamená, že se písemnost zašle nebo odevzdá tomu, komu je určena, a že existuje důkaz o tom, že daná osoba písemnost převzala (…) Nedodržení formy tedy samo o sobě neznamená, že se doručení musí zopakovat, rozhodující je, zda se daná písemnost dostala do rukou adresáta.“*[67]

Jak jsem již zmínil, spolu s úpravou datových schránek se uplatňuje speciální fikce doručení písemnosti. Jedná se o právní fikci, která se uplatní pro doručované písemnosti do datové schránky. Pakliže je do datové schránky doručena konkrétní písemnost a subjekt, který má

[64] Ustanovení § 17 odst. 1 ZoEÚAK
[65] Obdobně lze analogicky vyložit tuto povinnost jak pro soud, tak i pro správní orgány. Správní orgány stejně jako soudy, jsou tzv. orgánem veřejné moci, kterým zákon stanovuje tuto povinnost bez rozdílu.
[66] Usnesení Nejvyššího soudu ze dne 6. listopadu 2013 sp. zn. 21 Cdo 3489/2012
[67] Rozsudek Nejvyššího správního soudu ze dne 6. března 2009, č.j. 1 Afs 148/2008-73

s ohledem na rozsah svého oprávnění přístup k dané písemnosti, se ve lhůtě 10 dnů ode dne, kdy byla písemnost dodána do datové schránky, do datové schránky nepřihlásí, uplatní se fikce doručení.[68] Stručně řečeno se v takovém případě má za to, že byla písemnost doručena do vlastních rukou danému subjektu desátým dnem od doručení do datové schránky. V souvislosti s přijetím DEPO byla zavedena do § 18a odst. 3 ZoEÚAK fikce doručení po uplynutí 10denní lhůty pro fyzické, fyzické podnikající a právnické osoby i v případě „soukromoprávní korespondence". Do přijetí DEPO platila fikce doručení pouze u písemností zaslaných orgánem veřejné moci.

Fikce doručení s sebou přináší celou řadu právních následků, jako je například počátek běhu lhůt. Subjektu oprávněnému k přístupu do své datové schránky zákon jinými slovy výrazně doporučuje, aby si pravidelně kontroloval svou datovou schránku, zda do ní nebyly doručeny jakékoliv písemnosti. ZoEÚAK počítá s tím, že subjekt, který má zřízenou datovou schránku, tím na sebe přebírá odpovědnost, že si jí bude pravidelně kontrolovat. Pokud tak činit nebude, musí být srozuměn se svou odpovědností za to, že mu budou doručovány písemnosti i „bez jeho vědomí". V této souvislosti považuji za zajímavé zmínit i velmi aktuální rozsudek rozšířeného senátu Nejvyššího správního soudu. Případ pojednával o otázce, zda se v případě doručování do datových schránek bude uplatňovat běžné pravidlo počítání času, jak je vyjádřené v § 33 odst. 4 zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů (dále jen „**DaňŘ**"). Zda v případě, kdy konec desetidenního časového intervalu připadá na sobotu, neděli nebo státní svátek, bude posledním dnem následující pracovní den, či nikoliv. Rozšířený senát zde dospěl k závěru, že „*Končí-li při doručování do datové schránky desetidenní úložní doba podle § 17 odst. 4 ZoEÚAK (o níž zákon hovoří jako o lhůtě), jejímž uplynutím dojde k doručení fikcí, v sobotu, neděli či státní svátek, je jejím posledním dnem nejblíže následující pracovní den."*[69] Není důvod pochybovat, že i v dalších procesních předpisech, jako je např. SpŘ se bude pravidlo počítání času uplatňovat stejně.

Kompromis mezi povinností orgánu komunikovat prostřednictvím datových schránek a povinností subjektu (jemuž byla zřízena) si jí pravidelně kontrolovat považuji za legitimní. Určitý úhel pohledu by mohl být, že je to bezpochyby spravedlivé u subjektů, které si zřídily schránku dobrovolně, ale že o něco méně spravedlivé je to u soukromých subjektů, kterým byla

[68] Srovnání s ustanovením § 17 odst. 4 ZoEÚAK
[69] Rozsudek Nejvyššího správního soudu č.j. 4 Afs 264/2018-85 ze dne 26. května 2022

zřízena ze zákona bez ohledu na jejich vůli. To se dotýká uživatelů datových schránek právnické osoby a některých uživatelů datových schránek podnikající fyzické osoby. V souvislosti s nejnovější vývojem v rámci DEPO, kterému se věnuji v kapitole 2.7 je ovšem tato legitimita v důsledku automatického zřizování datových schránek fyzickým osobám narušena.

Datovou schránku právnické osoby zřizuje Ministerstvo vnitra automaticky všem právnickým osobám zřízeným ze zákona, zapsaným v obchodním rejstříku a organizačním složkám podniku zahraniční osoby.[70] Datovou schránku podnikající fyzické osoby zřizuje všem advokátům, statutárním auditorům, daňovým poradcům, insolvenčním správcům, znalcům, soudním tlumočníkům a soudním překladatelům.[71]Domnívám se, že zmíněné subjekty ze svého postavení jsou povinné snášet větší míru nároků na jejich právní jednání a s nimi související práva a povinnosti. Ostatně podobný přístup zaujal i Ústavní soud, který se zabýval otázkou, zda není povinnost „kontrolovat si datovou schránku" a „hierarchie povinnosti zřizovat si datovou schránku" (respektive povinnost, v závislosti na svém postavení, snést zřízení datové schránky bez svojí vůle) protiústavní.

Ústavní soud k tomu dále dodal: „*V souladu s ustanovením čl. 4 odst. 1 Listiny mohou být povinnosti ukládány toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod. Pokud by zákonodárce ukládal povinnosti, které není možné objektivně splnit (nemožnost zřídit si internet jako službu, např. proto, že je poskytování takových služeb zákonem zakázáno), bylo by možné takové povinnosti, byť uložené zákonem, charakterizovat jako porušující základní práva a svobody. V současné globální komunikační společnosti nemůže být o objektivní nemožnosti přístupu k internetu vůbec uvažováno (...) Samotná hierarchie povinnosti zřídit si pro doručování datovou schránku je dle názoru Ústavního soudu zcela zřejmá - v zásadě je tato povinnost uložena subjektům, u nichž lze objektivně předpokládat, na základě exaktně zjistitelných dat, že objem komunikace s jinými subjekty bude rozsáhlejší, než je tomu u běžného občana - fyzické osoby, příp. drobného živnostníka (fyzické osoby podnikající).*"[72]

[70] Ustanovení § 5 odst. 1 ZoEÚAK
[71] Ustanovení § 4 odst. 3 ZoEÚAK
[72] Usnesení Ústavního soudu ze dne 21. července 2011 sp. zn. III. ÚS 1513/11

Jednoduše tedy shrnul, to, co se ostatně i já domnívám. Po určitých subjektech je legitimní požadovat vyšší nároky s ohledem na jejich právní, ale i faktickou povahu. Na závěr výše citovaného judikátu Ústavní soud poznamenal zajímavou myšlenku, která by se hezky dala vztáhnout na celé pojetí digitalizace státu, jeho komunikace prostřednictvím dílčích orgánů vůči svým občanům, cizincům, ale i vůči dalším entitám vzniklým podle právního řádu České republiky.

„Zrychlení a racionalizace soudního procesu je legitimním cílem v demokratické společnosti, neboť spravedlnost, která přichází pozdě, nemusí být již spravedlností. K tomuto legitimnímu cíli může být v demokratické společnosti užito přiměřených prostředků, které nepovedou k porušení práva na spravedlivý proces.“[73]

Jak jsem již zmínil, kromě datových schránek zřizovaných povinně ze zákona, existuje i možnost zřízení datové schránky na žádost. Na zřízení datové schránky je právní nárok a její případné nezřízení by bylo považováno za nezákonný zásah ve smyslu § 82 a násl. zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů (dále jen „**SŘS**“).[74] Zažádat si o zřízení datové schránky může kterákoliv fyzická osoba, podnikající fyzická osoba a právnická osoba, na které se nevztahují ustanovení o povinném zřízení datové schránky.[75] Na žádost si můžou datovou schránku zřídit i orgány veřejné moci, byť ZoEÚAK neumožňuje, aby existoval orgán veřejné moci bez zřízené datové schránky orgánu veřejné moci. Tuto řekněme „dodatečnou“ datovou schránku orgánu veřejné moci si můžou zřídit orgány veřejné moci například pro účely vnitřní organizační jednotky nebo pro výkon konkrétní agendy nebo činnosti daného orgánu.[76]

Datová schránka orgánu veřejné moci je tedy jedinou výjimkou, a je možné, aby orgán veřejné moci měl zřízenou tuto datovou schránku vícekrát pro různé účely. Naopak u ostatních subjektů je to výslovně vyloučeno.[77] Fakticky tedy platí pravidlo jeden subjekt, jedna datová schránka. Úprava ovšem nevylučuje, aby jedna fyzická osoba v objektivní smyslu měla zřízené, respektive měla přístup až ke čtyřem různým druhům datových schránek a komunikovala skrze

[73] Ibid.
[74] Srovnání KÜHN, Zdeněk. Díl 3 [Řízení o ochraně před nezákonným zásahem, pokynem nebo donucením správního orgánu] In: KÜHN, Zdeněk. *Soudní řád správní: komentář*. Praha: Wolters Kluwer, 2019. Komentáře (Wolters Kluwer ČR), str. 696-734. ISBN 978-80-7598-479-1
[75] Ustanovení § 4 odst. 3 ZoEÚAK a § 5 odst. 1 ZoEÚAK
[76] Ustanovení § 6 odst. 2 ZoEÚAK
[77] Ustanovení § 3 odst. 5, § 4 odst. 6 a § 5 odst. 6 ZoEÚAK

každou z nich z jiného titulu. Modelovým příkladem může být fyzická osoba se zřízenou datovou schránkou pro fyzické osoby, která je současně živnostníkem a má zřízenou datovou schránku pro podnikající fyzické osoby, je jednatelem právnické osoby, tudíž má přístup z titulu statutárního orgánu právnické osoby do datové schránky právnické osoby a ke všemu je starostou obce, a je tedy ve smyslu § 7 odst. 3 ZoEÚAK vedoucím orgánu veřejné moci, který je oprávněn k přístupu do datové schránky orgánu veřejné moci.

Důležité ovšem je, z jaké pozice daný subjekt vystupuje. Fakticky vzato výše uvedená fyzická osoba je stále stejný člověk, který má přístup do čtyř datových schránek, do každé s jinými přístupovými údaji. Při právním jednání nelze zaměňovat různé druhy datové schránky a je nutné v konkrétním postavení využívat odpovídající druh datové schránky. Zároveň nelze přijmout názor, že stačí jednomu člověku (záměrně nepoužívám spojení fyzická osoba) mít zřízenou jakoukoliv datovou schránku a že je to takto dostačující pro jakoukoliv komunikaci s ním, ať už jako s fyzickou osobou, nebo podnikající fyzickou osobu a tak dále.

Podobných případů není málo a jedním takovým se zabýval i Ústavní soud. V jednom případě měl stěžovatel zřízenou datovou schránku jenom jako podnikající fyzická osoba, ačkoliv v řízení vystupoval jako fyzická osoba. Písemnost mu nebyla doručena do datové schránky, protože jí neměl zřízenou jako fyzická osoba. Jeho stížnost spočívala v tom, že není rozhodující, v jakém postavení má zřízenou datovou schránku a že stačí, že má nějakou, která je s ním jakkoliv spojená. Ústavní soud samozřejmě stížnost odmítnul a dodal, že „*soud doručuje písemnosti vždy do takové datové schránky, která byla adresátu zřízena pro obor činnosti, s nímž doručovaná písemnost věcně souvisí, resp. která odpovídá povaze doručované písemnosti.*“[78] S tímto závěrem Ústavního soudu nelze nesouhlasit. Logicky není z hlediska práva fyzická a podnikající fyzická osoba ten samý subjekt práva a každý má odlišná práva a povinnosti. Současně by přijmutí opačného stanoviska naráželo na problém s právní jistotou, kdy by si například starosta/starostka jakožto osoba oprávněná k přístupu do datové schránky orgánu veřejné moci nechal/a zasílat soukromé písemnosti do této schránky a nebyl/a nucen/a si zřizovat oddělenou vlastní datovou schránku fyzické osoby. V takovém případě by ani odesílatel a ve skutečnosti ani příjemce nemohl legitimně očekávat, že by se písemnost určená fyzické osobě měla doručovat právě do datové schránky zřízené k jinému účelu, v tomto

[78] Usnesení Ústavního soudu ze dne 26. února 2019 sp. zn. IV. ÚS 3891/18 nebo Usnesení Ústavního soudu ze dne 31. srpna 2018 sp. zn. II. ÚS 2385/18

případě pro účel vztahující se jen a pouze na výkon veřejné moci orgánu územního samosprávného celku.

Mimo doručování a přijímání písemností v elektronické podobě nabízí datové schránky další významnou funkcionalitu, a tou je identifikace subjektů při elektronické komunikaci. Informační systém datových schránek totiž obsahuje u každé zřízené datové schránky údaj o takzvaném identifikátoru datové schránky. Tento identifikátor jednoznačně identifikuje konkrétní datovou schránku a propojuje jí i s oprávněním subjektem. Jeli z datové schránky odeslána datová zpráva, její příjemce je schopen přesně identifikovat, kdo je odesílatelem.

Odesláním datové zprávy se fakticky stanou dvě zásadní věci. Odesílatel objektivně vyjadřuje vážnou vůli být spojován s jednáním, které vyplývá z datové zprávy, projevenou například formou podání v rámci správního nebo jiného řízení a zároveň je s touto vůli jednoznačně spojen jeden konkrétní subjekt, jedna konkrétní fyzická, podnikající fyzická nebo právnická osoba. Takové odeslání tedy může mít de facto stejný účinek jako podepsání a podání standardního listinného podání. Na tuto skutečnost zákonodárce pamatoval a tzv. fikci podpisu výslovně inkorporoval do ustanovení § 18 ZoEÚAK, kdy stanovil, že osoby oprávněné k přístupu do datové schránky a jimi pověřené osoby mohou činit úkony prostřednictvím datové schránky, přičemž se má za to, že tento úkon má stejné účinky jako „*úkon učiněný písemně a podepsaný*“[79].

Problém ovšem nastává v okamžiku, kdy skrze datovou schránku činí úkony jiný subjekt než ten, kterému náleží oprávnění k té které datové schránce. „*Ten, kdo použije svou datovou schránku, může za určitých podmínek těžit z uplatnění fikce podpisu a své podání směřované k soudu (orgánu veřejné moci) nemusí elektronicky podepsat, i když příslušný procesní předpis podpis podání uznávaným elektronickým podpisem jinak vyžaduje. Kdo však využije cizí datovou schránku, musí své podání umístěné v příloze datové zprávy ISDS podepsat svým (platným) uznávaným elektronickým podpisem obdobně jako u podání v příloze elektronické pošty.“*[80] S tímto názorem J. Peterky a J. Podaného se ztotožňuje i Nejvyšší soud a Nejvyšší správní soud, kdy opakovaně oba soudy judikovaly, že úkon učinění vlastní datovou schránkou

[79] Ustanovení § 18 odst. 2 ZoEÚAK
[80] PETERKA, Jiří, Podaný, Jan. *Problematika podání k soudu prostřednictvím datové schránky*. Praha: Bulletin advokacie. spojené 1. a 2. vydání z roku 2013. str. 33. ISSN 1210-6348

nahrazuje elektronický podpis, ale jen do té míry, kdy jej činí oprávněná osoba.[81] *„Nejvyšší správní soud k citovanému ustanovení ZoEÚAK* (ustanovení § 18 odst. 2 pozn. autora) *uvádí, že zákonná fikce podpisu, který musí obsahovat každé podání ve smyslu ustanovení §37 odst. 2 SpŘ, platí pouze pro podání činěné majitelem datové schránky, nikoliv však pro případ, je-li prostřednictvím datové schránky zasláno podání osoby odlišné od majitele datové schránky (…).“*[82]

Pokud bych tedy shrnul klíčové aspekty právní úpravy práce s datovými schránkami, jednalo by se o následující. ZoEÚAK přijal tzv. fikci doručení, která stanovuje pravidlo, že bez ohledu na vůli oprávněné subjektu, bude každá písemnost automaticky doručena „do vlastních rukou“ nejpozději 10. dnem od doručení písemnosti do datové schránky, jinak je doručena okamžikem přihlášení do datové schránky. Současně je jasně stanoveno, že do datové schránky má přístup jen oprávněná osoba skrze své přihlašovací údaje, u kterých jí plyne povinnost zacházet s nimi tak, aby nemohlo dojít k jejich zneužití.[83] Osoba, která by měla přístupové údaje do datové schránky, aniž by byla osobou oprávněnou, a která by činila úkony prostřednictvím datové schránky se zlým úmyslem, by se vystavovala riziku trestněprávní odpovědnosti.[84] ZoEÚAK nicméně nestanovuje sankce za obecné porušení povinnosti chránit své přihlašovací údaje.[85] V neposlední řadě umožňují datové schránky jednoznačnou identifikaci subjektu odesílající zprávu a v některých případech i nahrazovat elektronický podpis.

2.3.2. Autorizovaná konverze

Druhou rozsahově úspornější úpravou jsou tzv. autorizované konverze. Autorizovanou konverzí se dle ustanovení § 22 ZoEÚAK rozumí převedení listinné podoby dokumentu do podoby dokumentu obsaženého v datové zprávě nebo v datovém souboru nebo naopak převedení datové formy dokumentu do listinné podoby, též s doložkou o provedení konverze.[86]

---

[81] Srovnání rozsudků Nejvyššího správního soudu ze dne 17. února 2012, č.j. 8 As 89/2011–31; Městského soudu v Praze ze dne 29. dubna 2015 č.j. 8 A 9/2015-29 a s rozsudkem Nejvyššího soudu ze dne 7. května 2014 s č.j. 8 Tdo 517/2014

[82] Rozsudek Nejvyššího správního soudu ze dne 30. ledna 2019, č.j. 6 As 22/2018-32

[83] Ustanovení § 9 odst. 2 ZoEÚAK

[84] Nejvyšší soudu ve svém usnesení ze dne 15. srpna 2018 č.j. 8 Tdo 266/2017, judikoval, že v případě, že oprávněná osoba předá dobrovolně přihlašovací údaje druhé osobě, která využije přístup do datové schránky za účelem vyhotovení datové zprávy obsahující nepravdivé informace, bude druhá osoba odpovědná za spáchání přečinu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. c) zákona č. 40/2009 Sb., trestní zákon, ve znění pozdějších předpisů, bez ohledu na to, že jí přihlašovací údaje předala oprávněná osoba dobrovolně.

[85] Srovnání ustanovení § 26a a násl. ZoEÚAK

[86] Ustanovení § 22 odst. 1 ZoEÚAK

Zkonvertovanému dokumentu (tzv. výstupu) z listinné podoby do datové podoby, či obráceně, se přiznávají stejné právní účinky jako vstupu, tedy původní formě dokumentu.[87]

Klíčovou součástí autorizované konverze je již zmíněná doložka o provedení konverze. Tato doložka v sobě de facto obsahuje právní účinky „vstupu", jelikož ověřuje, že obsah vstupu je totožný jako obsah výstupu. Bez doložky o provedení konverze by se v každém dalším případě jednalo o prostou kopii listiny v datové podobě bez právních účinků, které listinný dokument má.

Doložka současně obsahuje, kromě údajů o tom, kdo konverzi provedl, datum provedení konverze, ale i, v případě konverze do datové podoby, údaj o viditelném prvku, který nelze plně přenést do výstupu. Prakticky se jedná o různé pečetě nebo stužky. Pokud by ovšem subjekt chtěl konvertovat výstup, který obsahuje údaj o tom, že se takový prvek nepodařilo plně přenést, nebylo by to možné. Jinými slovy, pokud by byl z listinné podoby zkonvertován dokument s pevnou pečetí do datové podoby, nelze z něj následně učinit konverzi do listinné podoby. To ostatně platí pro vidimovaný[88] dokument, jehož původní vstup takový prvek obsahoval.[89] Bez viditelně „nezkonvertovatelného" prvku by to možné bylo.

ZoEÚAK dále vymezuje, v jakém případě, kromě výše uvedeného, není možné konverzi provést. Nelze například konvertovat listinné dokumenty, které jsou nenahraditelné, jako je občanský průkaz, cestovní doklad, zbrojní průkaz nebo cenný papír.[90] Dále pak, pokud není patrné, zda je listinná podoba dokumentu prvopisem, vidimovaným dokumentem, opisem nebo kopií pořízenou ze spisu nebo stejnopisem písemného vyhotovení rozhodnutí nebo jeho výroku.[91] Logicky též nelze zkonvertovat ani zvukové nebo audiovizuální záznamy.

Autorizovaná konverze je tedy srovnatelná s vidimací ve smyslu ZoOvěř s tou výjimkou, že subjekt žádající o vidimaci nežádá o potvrzení listinné kopie nebo opisu, ale žádá o úředně ověřené převedení listinného dokumentu do datové podoby nebo obráceně. Výsledný výstup

---

[87] Ustanovení § 22 odst. 2 ZoEÚAK

[88] Vidimace je proces, při kterém se ověřuje, že opis nebo kopie se doslova shoduje s předloženou listinou. Tato vidimovaná listina se někdy neformálně nazývá jako úředně ověřená kopie. Naopak legalizace je úřední ověření vlastnoručního podpisu. Srovnání ustanovení § 6 a násl. a § 10 a násl. zákona č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (dále jen „**ZoOvěř**")

[89] Ustanovení § 24 odst. 4 písm. e) a f) ZoEÚAK

[90] Ustanovení § 24 odst. 4 písm. b) ZoEÚAK

[91] Ustanovení § 24 odst. 4 písm. d) ZoEÚAK

má tedy stejné právní účinky jako vidimovaná lisitina, jen je vyjádřen objektivně v jiném formátu než jeho vstup.

2.4. Základní registry

Narůstající počet jednotlivých informačních systémů naplnil primární cíl ZoISVS, a to „*zajištění kvalitních dat a bezpečné výměny informací"*[92]. Postupem času však v důsledku absence určitého centra sdílení celé škály údajů vedených o adresátech výkonu veřejné správy docházelo k řadě komplikací. „*Bylo to náročné jak pro úředníka, tak pro občana. Data v databázích státní správy byla roztříštěná, nejednotná, multiplicitní. Neexistovala možnost sdílet údaje v evidencích. Ne vždy pro výkon veřejné správy byly k dispozici údaje, na které bylo možné se spolehnout. Občan při jednání s úřady musel údaje ke své osobě několikrát opakovaně dokládat."*[93] To vše vedlo k tomu, že byl s účinností od 1. července 2010 přijat ZoZR, jehož cílem bylo vyřešit výše uvedené problémy.

Jak uvedl ředitel Správy základních registrů Ing. Michal Pešek, před existencí základních registrů bylo zapotřebí každou změnu údajů hlásit každému úřadu zvlášť, což zatěžovalo vysokou mírou byrokracie jak občana, tak i samotnou veřejnou správou celou řadou tištěných formulářů apod.[94] Proto vznikly základní registry

Základní registry jsou čtyři informačními systémy *sui generis*. Základní registr obyvatel (dále jen „**ROB**"), základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci neboli registr osob (dále jen „**ROS**"), základní registr územní identifikace, adres a nemovitostí neboli registr územní identifikace (dále jen „**RÚIAN**") a základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností neboli registr práv a povinností (dále jen „**RPP**").[95] Jedná se tedy o informační systémy, jejichž obsahem jsou všechny referenční údaje. Referenční údaje jsou údaje nejčastěji využívány při výkonu veřejné správy, jsou aktuální, právně závazné a slouží jako jedinečné datové zdroje pro orgány veřejné moci. Orgány veřejné moci tedy nebudou muset získávat údaje z různých zdrojů, ale pouze ze základních registrů. Data ze základních registrů budou propisována do

[92] Důvodová zpráva ZoISVS
[93] FELIX, Ondřej, KAUCKÝ, Jiří, KOLÁŘ, Jindřich, et al., op. cit. sub. 21, str. 137
[94] Ibid., str. 136
[95] Ustanovení § 2 písm. a) a § 3 ZoZR

agendových informačních systémů (tj. informačních systémů zřizovaných pro výkon konkrétní agendy u konkrétního orgánu veřejné moci).

„*Orgán veřejné moci využívá při své činnosti referenční údaje obsažené v příslušném základním registru v rozsahu, v jakém je oprávněn tyto údaje využívat podle jiných právních předpisů, a to, aniž by ověřoval jejich správnost.*“[96] Využívání referenčních údajů je tedy pro orgány veřejné moci obligatorní. Jedinou výjimkou jsou taxativně vymezené důvody, a to pokud údaje v základních registrech nejsou, jsou označeny za nesprávné, případně o jejich správnosti vznikne pochybnost nebo se jedná o utajované informace podle ZoUtajInf. Zodpovědnými orgány za příslušné referenční údaje, jejich zapisování, případně za provádění změn jsou tzv. editoři, tedy konkrétní orgány veřejné moci, které jsou u konkrétních registrů specifikovány v ustanovení ZoZR.[97]

Kromě čtyř základních registrů existuje i speciální informační systém základních registrů, jehož prostřednictvím dochází ke sdílení dat mezi základními registry navzájem, stejně jako mezi základními registry a agendovými informačními systémy a agendovými informačními systémy navzájem. Správcem informačního systému základních registrů je na základě ZoZR zřízen správní úřad podřízen Ministerstvu vnitra, a to Správa základních registrů. Kromě Správy základních registrů je do výkonu veřejné správy v oblasti základních registrů významně zapojen i Úřad pro ochranu osobních údajů (dále jen „**ÚOOÚ**“).

Role ÚOOÚ spočívá jednak v dozoru nad využíváním údajů ze základních registrů, tak především v zajištění metodologie zabezpečení osobních údajů při jejich převodu mezi informačními systémy. Toto zabezpečení zajišťuje kombinace zdrojových identifikátorů fyzické osoby (dále jen „**ZIFO**“) a agendových identifikátorů fyzických osob (dále jen „**AIFO**“). Jak ZIFO, tak AIFO, jsou bezvýznamovými identifikátory, které zabraňují možnému zneužití osobních údajů mezi jednotlivými agendami. ZIFO je neveřejným identifikátorem, který generuje a výhradně používá ÚOOÚ pro vytváření AIFO. AIFO je také neveřejným identifikátorem, který též vytváří UOOÚ, ale je veden o fyzické osoby jen pro konkrétní agendu. O jedné fyzické osobě je tedy veden vždy jen jeden ZIFO v evidenci ZIFO, ale vícero AIFO, vždy pro každou agendu zvlášť. Realizaci vazeb mezi jednotlivými agendami zajišťuje ÚOOÚ prostřednictvím evidence ZIFO, kde dochází k převodu AIFO jedné agendy na AIFO

[96] Ustanovení § 5 odst. 1 ZoZR
[97] Srovnání ustanovení § 40 a násl., nebo § 51 odst. 10 ZoZR

druhé agendy. „*Pouze ÚOOÚ bude mít k dispozici funkci a další údaje, které umožní převod AIFO na ZIFO, aby následně mohl z odpovídajícího ZIFO odvodit AIFO další agendy*.“[98]

Zjednodušeně řečeno, jediný, kdo bude moci propojit údaje z dílčích agend bude ÚOOÚ. U ostatních správců agendy (orgánů veřejné moci, které mají ve své působnosti tu kterou agendu) budou údaje vedeny viditelně pouze pod AIFO, který sám o sobě je bezvýznamový a nelze z něj vyčíst vazbu na další údaje, ke kterým správce konkrétní agendy nemá vzhledem k rozsahu své působnosti přístup. Nástroj, respektive systém, který pro výše uvedenou činnost ÚOOÚ používá se nazývá informační systém ORG – převodník identifikátorů, „*který jako jediný dokáže propojit data v jednotlivých registrech, přičemž pro zajištění maximální ochrany osobních údajů využívá vygenerovaný bezvýznamový identifikátor místo rodného čísla. Samotné sdílení dat zajišťuje Informační systém základních registrů, který zároveň kontroluje oprávnění k přístupu k datům.*“[99]

Pro větší představu dále vymezím, kdo spravuje konkrétní základní registr, o kterých subjektech jsou vedeny referenční údaje, o jaké údaje se jedná, případně, kdo je oprávněným editorem ke změně nebo zápisu zmíněných údajů.

2.4.1. Registr obyvatel „ROB“

Správa ROB je svěřena do rukou Ministerstvu vnitra. Tento registr vede údaje de facto o všech fyzický osobách, které mají konkrétní vztah k České republice, konkrétněji vede údaje o:

- státních občanech České republiky,
- cizincích pobývající na území České republiky v rámci trvalého nebo dlouhodobého pobytu,
- občanech a jejich rodinných příslušnících z členských států Evropské unie, států vázaných mezinárodní smlouvou uzavřenou s Evropským společenstvím nebo smlouvou o Evropském hospodářském prostoru, kteří pobývají na území České republiky v rámci trvalého nebo přechodném pobytu delšího než 3 měsíce,
- cizincích, jímž byla udělena mezinárodní ochrana formou azylu nebo doplňkové ochrany, a

[98] Důvodová zpráva ZoZR
[99] MINISTERSTVO VNITRA. Základní registry a Správa základních registrů. *Ministerstvo vnitra* [online]. [cit. 2022-05-05]. Dostupné z: https://www.mvcr.cz/clanek/zakladni-registry-a-sprava-zakladnich-registru.aspx

- dalších fyzických osobách, u nichž jiný právní předpis vyžaduje AIFO, a který o nich stanoví, že budou vedeny v ROB.[100]

Jako referenční údaje výše uvedených subjektů jsou v ROB vedeny informace o jménu a příjmení, adrese místa pobytu (zde je referenční vazba na referenční údaje v RÚIAN), případně adrese pro doručování písemností, datu a místa narození (případně úmrtí), dále o státních občanstvích (jeli jich více), čísle a druhu elektronicky čitelných identifikačních dokladů a typ a identifikátor datové schránky (jeli zřízena).[101] Mezi tzv. provozní údaje vedené v ROB se řadí záznamy o využívání, případně o poskytnutí údajů z ROB, o datu poslední změny referenčních údajů a o záznamu o udělení nebo odvolání souhlasu s poskytnutím referenčních údajů.[102]

ROB je editován prostřednictvím agendového informačního systému evidence obyvatel (AISEO), cizinců (AISC), evidence občanských průkazů (AISEOP), evidence cestovních dokladů (AISECD) a agendového systému datových schránek.[103]

ZoZR dále například výslovně upravuje přístup k referenčním údajům pro výkon volebního práva. Opravňuje příslušný obecní úřad s rozšířenou působností využívat příslušné údaje z ROB, které sdělí neprodleně příslušné okrskové volební komisi.[104] Tyto údaje jsou potřebné pro sestavení tzv. stálého seznamu voličů.[105]

2.4.2. Registr osob „ROS“

Správcem tohoto registru je Český statistický úřad a tento registr vede referenční údaje o všech subjektech vymezených v ustanovení § 25 ZoZR. Jedná se zejména o právnické osoby, organizační složky státu, podnikající fyzické osoby a další právní entity (např. svěřenské fondy), jsou-li zapsány do evidence podle ZoZR nebo jiného právního předpisu. „*Všechny osoby zapsané do ROS jsou identifikovány jednoznačným identifikátorem, kterým je*

[100] Ustanovení § 17 ZoZR
[101] Ustanovení § 18 ZoZR
[102] Ustanovení § 18 odst. 4 ZoZR
[103] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Editační agendové systémy. *Správa základních registrů* [online]. [cit. 2022-05-05]. Dostupné z: https://www.szrcr.cz/cs/registr-obyvatel/editacni-agendove-systemy
[104] Ustanovení § 21 ZoZR
[105] Např. ustanovení § 5 zákona č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých zákonů

identifikační číslo osoby, které osobám v ROS přidělují editoři dle působnosti jimi vykonávané agendy. ROS využívají všechny orgány veřejné správy, které k tomu mají oprávnění z RPP.“[106]

Podobně jako u ROB, i u ROS jsou o subjektech vedeny referenční údaje jako jméno a příjmení (respektive název, označení nebo obchodní firma), AIFO určený pro ROB, identifikační číslo osoby tj. „IČO“, datum vzniku/zápisu do evidence, případně zániku/výmazu z evidence, informace o datové schránce, a především právní forma a právní stav té které osoby. Změnou oproti ROB jsou zaprvé informace o orgánech konkrétních osob, jako jsou statutární orgány, opatrovníci, likvidátoři, správci apod., které jsou vyjádřeny referenční vazbou na referenční údaje v ROB a za druhé informace o sídle nebo provozovně osoby vyjádřené referenční vazbou na referenční údaje v RÚIAN a související informace.[107]Editorů ROB je celá řada, mezi nim lze nalézt například některé ústřední orgány státní správy, profesní komory, rejstříkové soudy a další orgány státní správy.[108]

2.4.3. Registr územní identifikace „RÚIAN“

Smyslem RÚIAN je zprostředkování údajů o územních prvcích územně evidenčních jednotek[109], a jejich vzájemných vazbách, přičemž jednotlivé prvky lze dohledat na mapách státního mapového díla a v digitálních mapách veřejné správy.

Jako jediný registr je veřejně přístupný a spravuje jej Český úřad zeměměřičský a katastrální. Územní prvky jsou definovány v ustanovení § 31 ZoZR, ale ve stručnosti se jedná o prvky územního členění státu jako je území státu jako celku, vyšších i „klasických“ samosprávných celků, správních obvodů a vojenských újezdů, ale i katastrálních území, adresních míst, pozemků nebo stavebních objektů. „*Jako jediný registr vede také nereferenční údaje, kterými jsou tzv. „technickoekonomické atributy“ stavebních objektů (např. počet podlaží, připojení na plyn, kanalizaci, vodu, způsob vytápění aj.).“*[110]

Jak jsem již zmínil, veřejně dostupný RÚIAN je volně dostupný skrze veřejně dálkový přístup přes internetovou aplikaci určené k nahlížení na data v RÚIAN. Samotný RÚIAN nevede žádné

---

[106] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Registr osob. *Správa základních registrů* [online]. [cit. 2022-05-05]. Dostupné z: https://www.szrcr.cz/cs/registr-osob

[107] Ustanovení § 26 ZoZR

[108] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Dokumenty k problematice ROS. Seznam osob a editorů ROS. *Správa základních registrů* [online]. [2022-05-05]. Dostupné z: https://www.szrcr.cz/images/dokumenty/ROS/seznam_osob_a_editoru_ros.xlsx

[109] Definice v ustanovení § 29 odst. 1 písm. a) a b) ZoZR

[110] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Registr územní identifikace, adres a nemovitostí. *Správa základních registrů* [online]. [cit. 2022-05-05]. Dostupné z: https://www.szrcr.cz/cs/registr-uzemni-identifikace-adres-a-nemovitosti

osobní údaje jako referenční, pouze zprostředkovává údaje o vlastnictví z agendového informačního systému katastru nemovitostí.[111] Referenční údaje, které RÚIAN naopak vede, jsou údaje vztahující se čistě k územním prvků, jako jsou identifikační údaje, adresy, druh a způsob využití pozemku nebo stavebního objektu a typ a způsob ochrany nemovitosti.[112] „*RÚIAN obsahuje též údaje o účelových územních prvcích. Jediným účelovým územním prvkem vedeným v RÚIAN jsou v současnosti volební okrsky.*“[113] Editorem údajů v RÚIAN jsou podle povahy údajů správce RÚIAN, tj. Český úřad zeměměřičský a katastrální, příslušný stavební úřad, katastrální úřad nebo příslušná obec.[114]

2.4.4. Registr práv a povinností „RPP“

Čtvrtým registrem je RPP. Smyslem RPP je poskytovat údaje pro informační systémy základních registrů o přístupu jednotlivých uživatelů k údajům vedeným jak v základních registrech, tak v agendových informačních systémech. Správcem RPP je Ministerstvo vnitra. Pro RPP je klíčovým pojmem agenda, respektive registrovaná agenda. Agenda je definována v ustanovení § 2 písm. e) ZoZR jako „*ucelená oblast působení orgánu veřejné moci nebo ucelená oblast působení soukromoprávního uživatele*“, kterým je dle definice v písm. d) podnikající fyzická nebo právnická osoba oprávněná využívat údaje ze základních registrů a agendových informačních systémů, která není orgánem veřejné moci.

V RPP je obsahem každé registrované agendy ve formě referenčních údajů její název, právní předpis, na jehož základě mohou uživatelé agend[115] využívat údaje ze základních registrů nebo agendových informačních systémů stejně jako výčet a popis úkonů, které mohou uživatelé agendy v rámci agendy vykonávat. V neposlední řadě je obsahem agendy identifikace jednotlivých uživatelů agendy, ale především rozsah oprávnění k přístupu k údajům v základních registrech a agendových informačních systémech, které jsou uživatelé agendy oprávněni využívat pro účely své agendy. Poslední zmíněný údaj je klíčový. Do nedávna byl v základních právních předpisech pro jednotlivé agendy uveden taxativní výčet údajů, které jsou uživatelé agendy oprávněni využívat, tento princip byl ovšem opuštěn s nabytím účinnosti DEPO (viz kapitola 2.7).

---

[111] Ustanovení § 62 odst. 2 ZoZR
[112] Ustanovení § 38 ZoZR
[113] SPRÁVA ZÁKLADNÍCH REGISTRŮ, op. cit. sub. 49
[114] Ustanovení § 40 a násl. ZoZR
[115] V tomto případě dle kontextu pojmem „uživatelé agend“ myslím orgán veřejné moci i soukromoprávního uživatele

Správa základních registrů uvádí na svých webových stránkách, že „*informace vedené v registrovaných agendách transformují „řeč zákonů“ do řeči „IT systémů““*[116]. Systém základních registrů tedy automaticky posuzuje, zda má žadatel o přístup k údajům dostatečné oprávnění. Pro lepší představu, pokud tedy například kontaktní místo veřejné správy (Czech POINT) chce učinit vydání výpisu z rejstříku trestů na žádost žadatele, systém automaticky zjistí, zda má kontaktní místo veřejné správy přístup do rejstříku trestů podle údajů v registrované agendě a následně umožní provedení tohoto úkonu.

Kromě registrovaných agend jsou v RPP dále vedeny referenční údaje týkající se orgánů veřejné moci a soukromoprávních uživatelů údajů, které umožňují jejich identifikaci. Poslední obecnou kategorií referenčních údajů v RPP je souhrn označován v ZoZR jako práva a povinnosti, tj. práva a povinnosti fyzických a právnických osob.[117] Konkrétněji se jedná o údaje o rozhodnutích, na jejichž základě dochází ke změnám v ROB nebo ROS a o údaje o právech a povinnostech, které vyplývají z dalších právních předpisů.

2.5. Služby elektronické identifikace[118]

Elektronickou identifikaci, někdy nazývanou jako eID, lze jednoduše popsat jako prostředek ověření totožnosti s využitím elektronických prostředků. Kromě toho je elektronická identifikace zároveň i služba, kterou mohou orgány veřejné správy, ale i soukromoprávní subjekty poskytovat svým adresátům a klientům.

První modely elektronické identifikace fungovaly na bázi klasického průkazu totožnosti s elektronicky čitelným čipem. Poté, co byl tento průkaz vložen do čtečky karet, měl uživatel možnost se elektronicky identifikovat. Nejedná se však pouze o identifikaci v pravém slova smyslu. Z tohoto důvodu je nutné odlišit pojmy identifikace, autentizace a autorizace.

- Identifikace je proces zjišťování identity jako je například uvedení jména, rodného čísla či jiných identifikačních údajů. Jedná o proces, při kterém se poskytuje odpověď na otázku „Kdo jsi?“. Samotné zadání údajů však neověřuje, zda je uživatel skutečně tím, kým tvrdí že je.

[116] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Úvodní stránka. *Správa základních registrů* [online]. [cit. 2022-05-05]. Dostupné z: https://www.szrcr.cz/cs/
[117] Ustanovení § 50 odst. 1 písm. d) ZoZR
[118] Část tohoto textu vychází z NEŠPOR, Jan, op. cit. sub. 17, str. 9-14

- Autentizace (někdy nazývána jako verifikace), která je naopak procesem ověření totožnosti za pomocí hesla, bezpečností otázky, biometrických údajů nebo tokenu. Poskytuje odpověď na otázku „Jsi skutečně tím, kým tvrdíš, že jsi?“.
- Autorizace pak spíše vymezuje konkrétní oprávnění, který identifikovaný a autentizovaný uživatel má. Jinými slovy poskytuje odpověď na otázku „Co jsi oprávněn dělat?“.[119]

Název elektronická identifikace tedy může působit poněkud zavádějícím dojmem, nicméně tento nástroj umožňuje všechny tři procesy, jak identifikaci, tak ale i autentizaci a v konečném důsledku i autorizaci. Tato kapitola se bude věnovat zejména právnímu rámci pro poskytování, ale i přijímání elektronické identifikace a současným modelům tohoto nástroje/služby.

2.5.1. Nařízení eIDAS

Dne 1. července 2016 nabylo účinnosti eIDAS, jehož cílem je kromě vytvoření právního základu pro elektronické transakce na vnitřním trhu EU i upravení podmínek pro vzájemné uznávání prostředků elektronické identifikace subjekty veřejné správy členských států. Obsahem eIDAS je kromě již zmíněných služeb vytvářejících důvěru, harmonizovaná úprava poskytování služby elektronické identifikace.

„Jedním z cílů tohoto nařízení (eIDAS pozn. autora) *je odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, které se v členských státech používají k autentizaci, alespoň pro účely veřejných služeb. Toto nařízení nemá za cíl zasahovat do systémů správy elektronické identity a souvisejících infrastruktur zřízených v členských státech. Jeho cílem je zajistit, aby u přístupu k přeshraničním on-line službám poskytovaným členskými státy byla možná bezpečná elektronická identifikace a autentizace.“*[120] Předpokladem pro zajištění bezpečné přeshraniční elektronické identifikace a autentizace je nutné, aby daný prostředek pro elektronickou komunikaci splňoval podmínky vzájemného uznávání podle čl. 6 eIDAS. Jednou z podmínek je, aby prostředek pro elektronickou identifikaci, vydávaný v rámci systému pro elektronickou identifikaci, byl uveden podle čl. 9 eIDAS v Úředním věstníku Evropské unie včetně předcházejícího posouzení Evropskou

[119] ZVIRAN, Moshe, ERLICH, Zippy. *Identification and Authentication: Technology and Implementation Issues* [online]. Tallahassee: Association for Information Systems, 2006. [cit. 2022-05-05]. str. 90. ISSN: 1529-3181. Dostupné z: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=2969&context=cais

[120] Bod 12 recitálu eIDAS

komisí.[121] Druhou důležitou podmínkou je požadavek, aby pro přístup k dané on-line službě veřejného sektoru byla vyžadována značná nebo vysoká úroveň záruky prostředků k elektronické identifikaci ve smyslu čl. 8 eIDAS.[122] Jednotlivým členským státům zůstává ponechána pravomoc uznat i prostředek elektronické identifikace, který dosahuje pouze nízké úrovně záruky.[123]

Kromě výše uvedeného klade eIDAS požadavek na členské státy, aby jednotlivé systémy elektronické identifikace byly interoperabilní. Pro zajištění interoperability systémů elektronické identifikace byl na základě eIDAS vytvořen „rámec interoperability", který musí splňovat jasně daná kritéria, jako je technologická neutralita a zajištění zpracování osobních údajů v souladu s evropským právem.[124] Rámec interoperability dále obsahuje například minimální technické požadavky splňující úroveň záruky, procesní pravidla nebo opatření pro řešení sporů.

2.5.2. Zákon o elektronické identifikaci a související předpisy

Ačkoliv jsou evropská nařízení přímo použitelným a závazným právním předpisem, v návaznosti na vstoupení eIDAS v platnost bylo v této souvislosti v České republice přijato několik zásadních právních předpisů. Kromě již zmíněného ZoSVD byly přijaty i zákon č. 250/2017 Sb., o elektronické identifikaci (dále jen „**ZoEI**") a změna souvisejících předpisů v zákoně č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci (dále jen „**SouvisZoEI**"). ZoEI a SouvisZoEI tvoří další vývoj právního rámce eGovernmentu v České republice.

Před přijetím ZoEI nebyl v právním řádu České republiky dostatečně obecně, kromě dílčích úprav v některých právních předpisech,[125] upraven institut elektronické identifikace. V návaznosti na přijetí eIDAS byla proto do ZoEI a SouvisZoEI promítnuta širší úprava prostředků elektronické identifikace občanů, „*což je klíčový předpoklad pro to, aby mohlo dojít k dalšímu rozvoji on-line služeb nebo jiných činností především veřejného sektoru*"[126]. Samotný

[121] Ibid.
[122] Ibid.
[123] Ustanovení čl. 8 eIDAS rozlišuje tři druhy úrovně záruky. Nízkou, značnou a vysokou.
[124] Ustanovení čl. 12 odst. 3 eIDAS
[125] Samostatná identifikace podle zákona č. 187/2006 Sb., o nemocenském pojištění ve znění účinném k 1. 3. 2017, nebo identifikace za využití systému datových schránek podle zákona č. 235/2004 Sb., o dani z přidané hodnoty ve znění účinném k 1. 3. 2017
[126] Důvodová zpráva návrhu ZoEI

ZoEI přináší obecný rámec pro způsoby prokazování totožnosti elektronickými prostředky. Pro tyto účely ZoEI vytvořil institut Národního bodu pro identifikaci a autentizaci (dále jen „**NIA**“)[127], který „*slouží jako nástroj pro bezpečné a zaručené ověření totožnosti uživatele on-line služeb poskytovaných zejména veřejnou správou.“*[128] Dále ZoEI umožňuje prostřednictvím akreditačního mechanismu, aby nestátní subjekty mohly zažádat o udělení akreditace pro správu kvalifikovaného systému elektronické identifikace, tj. aby mohly i jiné subjekty, kromě státních orgánů, poskytovat službu elektronické identifikace. O žádosti rozhoduje Ministerstvo vnitra, které akreditaci udělí osobám splňující podmínky podle § 5 odst. 2 ZoEI. S udělením akreditace jsou spjatá práva a povinnosti, mezi které se řadí oprávnění spravovat kvalifikovaný systém elektronické identifikace a povinnost zřízení pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému společně s odpovědností za přestupky na úseku elektronické identifikace.[129] Zřízený institut akreditace je příkladem propojení osob soukromého práva se státními orgány, který je dle mého názoru klíčovým atributem fungujícího eGovernmentu.

Mimo legislativně technická opatření a nezbytné změny vyvolané v souvislosti s přijetím ZoEI a eIDAS se jádro novelizace celkem 6 různých právních předpisů, obsažené v SouvisZoEI, opírá o úpravu zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů (dále jen „**ZoOP**“).

Pro účely elektronické identifikace je u vydávání občanského průkazu zakotveno, že jeho vydavatelem je Ministerstvo vnitra. „*Tímto bude vyjasněna úloha Ministerstva vnitra v tom smyslu, že na něj bude možné pohlížet jako na kvalifikovaného správce systému elektronické identifikace podle § 4 písm. a) ZoEI.“*[130] ZoEI a úprava SouvisZoEI společně se zákonem č. 195/2017 Sb., kterým se mění ZoOP a který plošně zavádí občanské průkazy se strojově čitelnými údaji a s kontaktním elektronickým čipem[131], vytvářejí právní rámec pro tzv.

[127] Ustanovení § 20 a násl. ZoEI
[128] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Portál národního bodu pro identifikaci a autentizaci. *Identita občana* [online]. [cit. 2021-21-03]. Dostupné z: https://www.eidentita.cz/Home
[129] Ustanovení § 25 a násl. ZoEI
[130] Důvodová zpráva SouvisZoEI.
[131] Zákon č. 195/2017 Sb., kterým se mění zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a další související zákony

„eObčanku“, tedy občanský průkaz s aktivovaným kontaktním čipem vydaným po 1. červenci 2018 (dále jen „**eObčanka**“).[132]

„*Spolu s eObčankou Ministerstvo vnitra spouští Portál Občana, kde si občané budou moci vyřídit z jednoho místa řadu záležitostí jednoduše bez obíhání úřadů, zbytečného čekání, front a průtahů.“*[133] Portál Občana je transakční částí Portálu veřejné správy ve smyslu ZoISVS. Je to on-line služba veřejné správy založená na osobním přístupu prostřednictvím identifikace subjektu, přičemž pro přístup k této službě je zapotřebí ověření totožnosti identifikačními prostředky vydanými v souladu se ZoEI

Jedním z těchto prostředků je právě eObčanka, NIA ID[134] nebo například bankovní identita a další systémy soukromoprávních kvalifikovaných poskytovatelů podle ZoEI. Skrze službu Portál Občana je možné dálkově, po ověření identity, činit některé zákonem předpokládané úkony, jako je například daňové tvrzení DaňŘ, získávání výstupů z živnostenského rejstříku podle Živnostenského zákona, nebo získávání údajů z Centrálního registru řidičů ČR podle zákona č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů, ve znění pozdějších předpisů a další úkony předpokládané právním řádem.

2.5.3. Bankovní identita

Banky jsou ze své podstaty subjekty soukromého práva, přesto však veřejný zájem klade maximální důraz na důvěru v banky jako instituce. Vysoká míra regulace bankovní činnosti je potřebná jednak z důvodu udržení finanční stability trhu, prevence protiprávních činností, např. legalizace výnosů z trestné činnosti, jakož i z důvodu ochrany klientů. Banky jsou tedy významnými adresáty povinností nejen soukromoprávních, ale též veřejnoprávních. V kontextu elektronické identifikace je podstatná především stanovená povinnost bank zjišťovat totožnost svých klientů, jakož i možnost bank garantovat zjištěnou identitu klienta vůči jiným osobám.[135]

---

[132] VITNEROVÁ, Marika. *První eObčanky se začnou vydávat od července.* Tisková zpráva. Praha: Ministerstvo vnitra, 2018 [online]. [cit. 2021-22-03]. Dostupné z: https://www.mvcr.cz/clanek/prvni-eobcanky-se-zacnou-vydavat-od-cervence.aspx

[133] Ibid.

[134] „NIA ID je identifikační prostředek umožňující zaručené prokazovaní totožnosti při přihlašování k online službám, které požadují alespoň značnou úroveň důvěry prostředků identifikace.“ (SPRÁVA ZÁKLADNÍCH REGISTRŮ, op. cit. sub. 54)

[135] Povinnosti vyplývají ze zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dáel jen „**ZoAML**“).

V roce 2019 skupina poslanců předložila návrh novely zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů (dále jen „**ZoBank**“) a dalších souvisejících předpisů, jejímž hlavním cílem bylo vytvoření právních podmínek pro tzv. bankovní identitu. Tato novela navazuje na právní úpravu v oblasti elektronické identifikace představovanou eIDAS a ZoEI. Bankovní identita je službou, kterou banky poskytují svým klientům a která zároveň má účinky prostředku pro elektronickou identifikaci podle ZoEI. Zjednodušeně řečeno se jedná o možnost elektronické identifikace skrze přihlášení se do internetového bankovnictví. Tento institut se zároveň řadí mezi tzv. digitální identity, tedy prostředky využití technologie k tvrzení a ověření identity.[136] Novela ZoBank prošla legislativním procesem a byla přijata jako zákon č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dále jen „**ZoBI**“).

V rámci přípravy ZoBI bylo nutné zohlednit některá specifika činnosti bank. Bankovní identita tedy oproti jiným prostředkům elektronické identifikace funguje poněkud odlišně. Protože platilo, že *„§ 1 ZoBank taxativně vymezuje činnosti, které banka může v rámci své podnikatelské činnosti vykonávat, přičemž mezi těmito činnostmi není zahrnuto poskytování elektronické identifikace*.“[137], bylo zakotveno do ZoBank výslovné oprávnění bank poskytovat služby elektronické identifikace v nových ustanovení § 38aa až 38af. Zároveň s ohledem na povinnosti zejména v oblasti řízení rizik bylo použití bankovní identity v rámci NIA omezeno tak, že je možné ji v rámci NIA, na rozdíl od ostatních prostředků elektronické identifikace, použít jen vůči státním orgánům veřejné moci.[138] Použití vůči jiným příjemcům bankovní identity, ač jde o prostředky vydané v rámci NIA, probíhá mimo rámec NIA a jedině tehdy, pokud se na tomto použití vydávající banka s příjemcem bankovní identity dohodnou.[139] Pro použití mimo rámec NIA se vžilo označení SONIA (soukromoprávní NIA). Kromě možnosti výkonu podnikatelské činnosti spočívající v poskytování elektronické identifikace novela upravuje možnost přístupu bank k údajům ze základních registrů a využití elektronické identifikace pro splnění povinností podle ZoAML.[140]

---

[136] FINANCIAL ACTION TASK FORCE. *FATF Guidance on digital identity In brief* [online]. Paříž: Financial Action Task Force, 2020. [cit. 2021-22-03]. Dostupné z: https://www.fatf-gafi.org/media/fatf/documents/reports/Digital-ID-in-brief.pdf
[137] Důvodová zpráva ZoBI
[138] Ustanovení § 38ad odst. 3 ZoBank
[139] Ustanovení § 38ab a násl. ZoBank
[140] Zejména promítnutí principu „KYC“ – know your customer v § 7 a násl. ZoAML

Bankovní identita tak vedle např. eObčanky funguje jako jeden z dalších prostředků, jak využívat služby eGovernmentu pro širší okruh občanů České republiky. „*Mluví se o 5,5 milionu, což by ale měl být počet klientů všech bank dohromady. Takže až „veřejnoprávní" bankovní identitu spustí opravdu všechny naše banky, budou mít všichni klienti bank možnost přihlašovat se „přes NIA" k těm službám, které jsou touto cestou dostupné (což jsou především služby eGovernmentu).* "[141]. Podle portálu bankid.cz provozovaného Českou bankovní asociací současně spustilo službu bankovní identity 7 různých komerčních bank a do konce roku 2022 se očekává spuštění u dalších 2 bank.[142]

Zkušenosti, zejména s ohledem na zakotvení bankovní identity, ukazují, že pokud bude veřejná správa spolupracovat se soukromými subjekty, lze na straně příjemců služeb eGovernmentu očekávat větší zájem o jejich využití. Dle mého názoru jsou hlavními argumenty flexibilnější rozhodování, dostupné finance a vůle soukromých subjektů své klienty do těchto služeb zapojovat. Ponechávám stranou, zda veřejná správa nedostatečně motivuje a informuje navenek o svých dostupných službách, a proto musí využívat propagačně „schopnější" soukromé subjekty. Zatímco u veřejné správy je jakýkoliv pokrok odkázán vedle finančních možností primárně na politickou vůli zákonodárce, soukromé subjekty jsou přirozeně motivovány poskytováním nejlepších dostupných služeb a ve výsledku maximalizací svých zisků. Zároveň jakékoliv změny nejsou většinou na rozdíl o veřejné správy odkázány na regulované procesy, čímž můžou ve výsledku soukromé subjekty reagovat daleko efektivněji. V případě bankovní identity bylo zapotřebí „odblokovat" ustanovení, která bankám doslova zakazovala poskytovat služby elektronické identifikace, proto musí jít legislativa ruku v ruce s dalším vývojem eGovernmentu. Doporučení pro budoucí zákonodárce tak v případě další legislativy je, dle mého názoru, umožňovat v co možná největším množství případů zapojení soukromých subjektů jakožto garanty nebo poskytovatele služeb eGovernmentu, ať už skrze systém akreditace, jako v případě elektronické identifikace, nebo formou koncese.

2.6. Právo na digitální služby[143]

[141] PETERKA, Jiří. *Bankovní identita: 1,6 milionu aktivovaných identit, (snad) jen jedna SONIA a první ceník jejích služeb* [online]. Praha: Lupa.cz, 2021. [cit. 2021-21-03]. Dostupné z: https://www.lupa.cz/clanky/bankovni-identita-1-6-milionu-aktivovanych-identit-snad-jen-jedna-sonia-a-prvni-cenik-jejich-sluzeb/

[142] BANKID. Jak bankovní identitu získat? *BankID* [online]. [cit. 2022-24-05]. Dostupné z: *https://www.bankid.cz*

[143] Část tohoto textu vychází z NEŠPOR, Jan, op. cit. sub. 17, str. 15-18

Některé z přijatých právních předpisů zmíněné v předchozích kapitolách „*se vždy týkaly jen určitého výseku služeb eGovernmentu. Před existencí právní úpravy ZPDS tak právní řád České republiky neobsahoval ucelenou úpravu digitálních služeb a postavení, resp. práv příjemců digitálních služeb při jejich poskytování ze strany orgánů veřejné moci. Zároveň neexistoval ani žádný relevantní a státem garantovaný přehled služeb veřejné moci, na které má každý občan právo a které je veřejná správa povinna mu poskytnout (navíc bez rozdílu formy, v jaké jsou takové služby občanovi poskytovány). Stát navíc dlouhodobě neumí občany vhodně informovat o jejich možnostech v rámci právní úpravy eGovernmentu a tyto možnosti tak zůstávají povětšinou tématem odborných debat úzkého okruhu odborné i laické veřejnosti.“*[144]

Podstatou ZPDS je garance práva fyzických a právnických osob využívat digitální služby a povinnost orgánů veřejné moci:

a) poskytovat digitální služby;
b) zveřejňovat poskytované digitální služby a přijímané úkony v katalogu služeb;
c) přijímat digitální úkony; a
d) zveřejňovat poskytované digitální služby a přijímané úkony v katalogu služeb spolu s dalšími souvisejícími právy a povinnostmi.[145]

Z dalších povinností je nutné zmínit zejména zákonný závazek digitalizovat veškeré úkony (jejichž povaha nevylučuje digitální poskytování) do roku 2025, a to i za předpokladu, že nejsou obsaženy v katalogu služeb.[146] Kromě práv a povinností zakotvených v ZPDS vychází předpis z předpokladu vyšší efektivity procesu digitalizace, pozitivní motivace osob k činění úkonů

[144] KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel, ZAJÍČEK, Zdeněk. § 1 [Předmět úpravy] In: ZAJÍČEK, Zdeněk a kol. *Zákon o právu na digitální služby: komentář*. V Praze: C.H. Beck, 2021. Beckovy komentáře. str. 7. ISBN 978-80-7400-822-1

[145] Digitální službou se rozumí podle § 2 odst. 2 ZPDS: „úkon vykonávaný orgánem veřejné moci vůči uživateli služby v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě; za digitální službu se považuje i úkon vykonávaný vůči uživateli služby kontaktním místem veřejné správy v rámci agendy“.
Digitálním úkonem se rozumí podle § 2 odst. 3 ZPDS: „úkon vykonávaný uživatelem služby vůči orgánu veřejné moci v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě.“
Katalogem služeb se rozumí podle ustanovení § 2 odst. 4 ZPDS: „část údajů vedená v základním registru agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností, které se týkají úkonů orgánů veřejné moci vykonávaných v rámci agendy vůči subjektům, které přitom nemají postavení orgánů veřejné moci, a úkonů subjektů, které při jejich vykonávání nemají postavení orgánů veřejné moci, vůči orgánům veřejné moci.“

[146] Srovnání ustanovení § 14 odst. 5 ZPDS

digitálně namísto „papírově“ [147] nebo rozšíření možnosti sdílení údajů mezi orgány státní správy.[148]

ZPDS slouží jako jakýsi rámcový nebo „*umbrella*“ právní předpis v oblasti digitalizace. V obecné rovině je povinností každého orgánu veřejné správy zajistit, aby splnil povinnosti, které mu ZPDS ukládá. Současně musejí orgány veřejné správy umožnit výkon práv ostatních subjektů, která jsou obsažena v katalogu práv, jež je součástí ZPDS. Jedná se o následující práva:

- (§ 3) *právo na digitální službu,* které je právo zastřešující práva a povinnosti obsažené v ZPDS;
- (§ 4) *právo činit digitální úkon*, tedy činit úkony prostřednictvím vymezených prostředků, jako jsou datové schránky, kontaktní místa veřejné správy nebo systém veřejné správy s využitím elektronické identifikace podle ZoEI;
- (§ 5) *právo na osvědčení digitálního úkonu* a z toho plynoucí povinnost orgánů veřejné moci poskytnout uživateli služby bezodkladné osvědčení o učinění úkonu;
- (§ 6) *právo na nahrazení úředně ověřeného podpisu nebo uznávaného elektronického podpisu*, které zakotvuje možnost nahradit zmíněné typy podpisů jakoukoliv formou elektronického podpisu. Při splnění zákonných požadavků na úředně ověřený podpis (uznávaný elektronický podpis) se uplatní právní fikce takového podpisu u ostatních, i prostých, forem elektronického podpisu*;*
- (§ 7) *právo na využívání údajů*, které je projevem once only zásady, tedy povinnosti orgánu veřejné moci využívat údaje, které jsou o uživateli služby již dostupné ze základního registru nebo z agendového informačního systému;
- (§ 8) *právo na zápis práva, povinnosti nebo právní skutečnosti* je též projevem once only zásady spojené s povinností orgánů veřejné moci zapisovat práva, povinnosti nebo právní skutečnosti do registru práv a povinností, a tedy povinnost orgánů mezi sebou takové údaje sdílet;
- (§ 9) *právo na prokázání právní skutečnosti* uzavírá spolu s § 7 a 8 pomyslnou trojici „once only práv“, kdy toto právo garantuje uživateli služeb právo odkázat se na zapsané údaje v registrech při prokazování nebo osvědčování určitých právních skutečností;

[147] Např. sleva 20 %, maximálně však 1000 Kč, na poplatek v případě provedení úkonu na elektronickém formuláři (srovnání s ustanovením § 9 zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů)
[148] Z různých titulů např. na základě zákonné povinnosti nebo v případě činění digitálního úkonu konkrétní osobou.

- (§ 10) *právo na zápis kontaktního údaje,* tedy právo zapsat údaje o elektronické adrese nebo telefonním čísle do příslušného registru;
- (§ 11) *právo na informace v souvislosti s poskytováním digitálních služeb* a posílení informovanosti uživatelů v této souvislosti;
- (§ 12) *právo na elektronickou identifikaci a autentizaci* zaručuje možnost uživatele se identifikovat jakýmkoliv prostředkem elektronické identifikace s úrovní záruky značná i za předpokladu, že nebude u služby stanovena úroveň záruky v katalogu služeb; a
- (§ 13) *právo na technologickou neutralitu,* tedy *„uživatel služby tak má právo získat přístup k digitální službě bez ohledu na konkrétní jím použitý software i hardware. Jinými slovy uživatel služby je oprávněn volit technologické prostředky přístupu k digitální službě dle vlastního uvážení*“.[149][150]

Využití konkrétních forem nebo způsobů, jakými jsou orgány veřejné moci povinny poskytovat služby a umožňovat výkon práv obsažených v ZPDS, jsou ponechány v jejich kompetenci. ZPDS je tedy ze své podstaty blanketní právní normou. Ustanovení § 3 odst. 2 stanovuje, že „*práva a povinnosti podle jiných zákonů nejsou tímto zákonem dotčena*“, z čehož vyplývá, že může být stanovena jiná zákonná úprava, která poskytnutí určité digitální služby vyloučí. Toto ustanovení ZPDS je tedy ze své podstaty *lex generalis* a umožňuje odlišnou úpravu prostřednictvím *lex specialis*.

Ustanovení § 5 až § 8 a § 10 ZPDS stejně jako vyloučení povinnosti využívat digitální služby a úkony nepodnikajícími fyzickými osobami v přechodných ustanoveních[151], bylo do znění návrhu zákona dodáno až na základě komplexního pozměňovacího návrhu výboru pro veřejnou správu a regionální rozvoj Poslanecké sněmovny Parlamentu České republiky.[152] Vzhledem k absenci důvodové zprávy k těmto změnám se lze jen domnívat pro jaké důvody navrhovatelé spatřovali potřebu zmíněných ustanovení. Ochrana nepodnikajících fyzických osob bude pravděpodobně vyvažovat rozdílnou technologickou gramotnost u potenciálních uživatelů služeb v České republice. Jinými slovy není nutné požadovat po každém, aby si s technologiemi „rozuměl“ natolik, aby byl nucen je používat při běžném kontaktu s veřejnou správou. Jiný případ ovšem nastane, pokud se jedná o podnikající fyzickou nebo právnickou osobou, u

[149] Ustanovení § 3 až § 13 ZPDS
[150] DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. § 13 [Právo na technologickou neutralitu] In: ZAJÍČEK, Zdeněk et al., op. cit. sub. 58, str. 138
[151] Ustanovení § 14 odst. 1 ZPDS
[152] Usnesení č. 133 Výboru pro veřejnou správu a regionální rozvoj ze dne 5. září 2019

kterých je zájem na využívání digitální služeb prostřednictvím digitálních úkonů vyšší viz například povinné zřízení datových schránek u těchto subjektů.

V rámci ZPDS byla novelizována i celá řada dalších předpisů, přičemž jednou z nejvýznamnějších změn v kontextu eGovernmentu byla změna ZoISVS, kde došlo k „*zakotvení průřezové úpravy využívání cloud computingu*[153] *veřejnou správou a nákupu cloudových služeb v § 6i a násl. ZoISVS (úprava působnosti, zřízení informačního systému, katalogu cloud computingu, využívání, zápisů poptávky a související*).“[154]

Ačkoliv je ZPDS ze své podstaty obecný právní předpis, jeho přijetím došlo k přímé i nepřímé novelizaci zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „**SpŘ**“). Nejvýraznější nepřímou změnou procesních norem správního práva je dle mého názoru jasně deklarované právo činit úkony vůči orgánům veřejné správy digitálně. Byť předcházející úprava tomu vyloženě v některých ohledech nebránila, ZPDS to stanovil najisto. Přímá novela je pak zdánlivě nenápadná, přesto zásadní změna samotného SpŘ. V základních zásadách SpŘ bylo před přijetím ZPDS stanoveno, že správní orgán může získat potřebné údaje z evidence, kterou sám vede, jen pokud o to dotčená osoba požádá.[155] Tedy úprava nebránila správním orgánům údaje využívat, ale nebyla to výslovná povinnost. Lze se domnívat, že právě možnost diskrece správních orgánů k využívání údajů z registrů vedla k tomu, aby údaje ze svojí iniciativy nevyužívaly. Zákonodárce tak přistoupil k novelizaci, která jasně stanovuje, že „*správní orgán opatřuje podklady přednostně s využitím úřední evidence, do níž má přístup. Podklady od dotčené osoby vyžaduje jen tehdy, stanoví-li tak právní předpis.“*[156] Došlo tedy k odstranění diskrece a ke stanovení jednoznačné povinnosti správních orgánů využívat údaje z jakékoliv evidence, do které má přístup. Nikoliv pouze z evidence, kterou sám správní orgán zřizoval, jako tomu bylo před přijetím novely. Právě přístup správních orgánů do jednotlivých rejstříků a evidencí se ukázal jako značně problematický. Z tohoto důvodu došlo od přijetí ZPDS k dalším legislativním změnám (viz DEPO v kapitole 2.7).

---

[153] Cloud computing je model umožňující pohodlný přístup „on demand“ (česky na vyžádání) a v reálném čase ke sdíleným datům uložených na konfigurovatelných výpočetních zdrojích jako jsou sítě, servery, datová úložiště, aplikace, služby aj. (srovnání KORBEL, František, KOVÁŘ, David, AMLER, Pavel. § 15 až 25 [Změnová ustanovení] In: ZAJÍČEK, Zdeněk, et al. op. cit. sub. 58, str. 155 a EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. *Cloud Computing Risk Assessment*. Hérakleion: European Network and Information Security Agency, 2009 [online]. [cit. 2021-01-04]. str. 14. Dostupné z: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment)

[154] KORBEL, František, KOVÁŘ, David, AMLER, Pavel. § 15 až 25 [Změnová ustanovení] In: ZAJÍČEK, Zdeněk, et al. op. cit. sub. 58, str. 155

[155] Ustanovení § 6 odst. 2 SpŘ ve znění účinném do 31. ledna 2020

[156] Ustanovení § 6 odst. 2 SpŘ

Na závěr analýzy úpravy ZPDS je důležité poznamenat, že ačkoliv ZPDS nezakotvuje postup vymáhání práv uživatelů v oblasti práva na digitální služby, právo na digitální služby a související práva nejsou pouhou proklamací. Právo na digitální služby má charakter veřejného subjektivního práva, které požívá ochrany i prostřednictvím norem správního práva.[157] Podle Zajíčka by se jednalo v případě nezákonného neposkytnutí digitální služby o nesprávný úřední postup podle § 13 zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů (dále jen „**ZoOdpŠk**"). Ustanovení § 13 odst. 1 ZoOdpŠk rozumí nesprávným úředním postupem „*porušení povinnosti učinit úkon nebo vydat rozhodnutí v zákonem stanovené lhůtě"*. ZoOdpŠk jako takový řeší až samotnou kompenzaci, kterou je možné po státu požadovat v rámci civilního řízení. Nabízí se tedy otázka, jakým způsobem se bude postupovat v případě obrany ve správním řízení, respektive v soudním řízení správním, zda se bude jednat o nezákonnou nečinnost nebo naopak o nezákonný zásah a jak získat vykonatelný titul (je-li nutný) pro postup podle ZoOdpŠk.

V případě, že nastane situace, kdy dojde k neposkytnutí určité služby, které má charakter nevydání rozhodnutí podle ustanovení SpŘ, lze usuzovat, že má žadatel právo uplatnit prostředky ochrany před nečinností podle ustanovení § 80 a násl. SpŘ (tj. žádost o uplatnění opatření proti nečinnosti). Při bezvýsledném vyčerpání prostředků SpŘ pak přichází v úvahu žaloba proti nečinnosti podle ustanovení § 79 a násl. SŘS. Komentářová literatura doplňuje, že nečinnost je potřeba vnímat především jako průtahy s rozhodnutím v aktuálně „živém" řízení nebo i průtahy tzv. „již odeznělé" v řízení, ve kterém bylo rozhodnutí již vydáno.[158]

Současně lze předpokládat, že může dojít k takové „nečinnosti" orgánu veřejné správy, která nespočívá v nevydání rozhodnutí, jak je uvedeno výše, a která je způsobilá zasáhnout sféru práv a povinností jednotlivce. V takovém případě se nebude jednat o nečinnost ve smyslu § 80 SpŘ, nýbrž o nezákonný zásah ve smyslu § 82 a násl. SŘS. Zásahem dle platné judikatury *„může být i nezákonná nečinnost spočívající v neučinění nějakého úkonu jiného než rozhodnutí ve smyslu § 65 odst. 1 SŘS (usnesení rozšířeného senátu NSS ze dne 16. 11. 2010, sp. zn. 7 Aps 3/2008*

[157] Srovnání KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel, ZAJÍČEK, Zdeněk. § 3 [Právo na digitální službu] In: ZAJÍČEK, Zdeněk, et al. op. cit. sub. 58, str. 39 a KOPECKÝ, Martin, op. cit. sub. 20, str. 41 an.
[158] POTĚŠIL, Lukáš. § 80 [Opatření proti nečinnosti]. In: POTĚŠIL, Lukáš, HEJČ, David, RIGEL, Filip, MAREK, David. Správní řád. 2. vydání. Praha: C. H. Beck, 2020, str. 430. ISBN 978-80-7400-804-7

[2206/2011 Sb. NSS]; rozšířený senát zde překonal dřívější názor, že nezákonným zásahem může být toliko konání, ne však opomenutí, viz rozsudek NSS ze dne 16. 1. 2008, sp. zn. 3 Aps 3/2006).“ [159]

Do nabytí úplné účinnosti ZPDS (tj. 1. ledna 2025) bude povinností orgánů veřejné správy, aby vnitřními administrativními opatřeními splnily požadavky kladené ZPDS. V případě, že by se ukázalo, že je zapotřebí přijmout příslušnou prováděcí legislativu k ZPDS, nebyla by samotná absence konkrétní legislativy nečinností zákonodárce ve smyslu SpŘ, respektive SŘS. V této otázce konstantně judikuje Ústavní soud, že by se soud přijmutím takového narativu stavěl do role pozitivního zákonodárce, kdy by „sankcionoval“ nečinnost zákonodárce. K tomu např. v usnesení sp. zn. I. ÚS 1537/14 dodal, že „*kdokoliv by mohl kdykoliv a bez dalšího protestovat proti jakékoliv právní úpravě nebo absenci této právní úpravy a obcházet tak pravidla legislativního procesu*“. Může nastat situace, kdy bude jednotlivci zasaženo orgánem veřejné správy do jeho práv vyplývajících z ZPDS z toho důvodu, že zákonodárce včas nereagoval a nepřijmul příslušnou legislativu. Orgán veřejné správy by se tak bez svého zavinění dostal do právně zajímavé situace, kdy musí nést následky za nekonání zákonodárce, který není ze své funkce odpovědný za nečinnost. V takovém případě se nicméně domnívám, že by neměla být jedinci upřena možnost obrany prostředky správního práva, jelikož nekonání zákonodárce nezavinil a v dobré víře předpokládal, že bude výkon jeho práv neohrožen třetím subjektem.

V současné době lze s povděkem sledovat, že se naopak zákonodárce snaží „transformaci“ veřejné správy na systém v souladu s ZPDS spíše pomáhat a být o krok napřed, jako tomu bylo v případě přijetí DEPO.

2.7. Další elektronizace postupů orgánů veřejné moci „DEPO“[160]

DEPO v sobě zahrnuje novelu celkem 169 různých právních předpisů. Hlavní princip této úpravy je, kromě zakotvení elektronizace petičního práva, dálkového přístupu do centrálního registru zbraní, zmírnění požadavků pro využívání cloud computingu ve veřejné správě a

[159] JIRÁSEK, Jan. § 82 [Žalobní legitimace] In: BLAŽEK, Tomáš, JIRÁSEK, Jan, MOLEK, Pavel, POSPÍŠIL, Petr, SOCHOROVÁ, Vendula, ŠEBEK, Petr. *Soudní řád správní – online komentář*. 3. vydání. V Praze: C. H. Beck, 2016 [online]. [cit. 2021-08-11]. Dostupné z: https://www-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembrgzpw62zsl4zs443cl4zdambsl4ytkma

[160] Část tohoto textu vychází z NEŠPOR, Jan, op. cit. sub. 17, str. 18-20

dalších změn, především úprava sdílení dat mezi orgány veřejné správy a odstranění souvisejících překážek.

Hlavní problém právní úpravy před přijetím DEPO byl v disproporci právních titulů pro využívání údajů v agendových informačních systémech. Jejich zřízení nevyplývalo vždy přímo ze zákona a „*využití údajů v nich uvedených pro výkon jiných agend se právně opírá* (opíralo pozn. autora) *o více, či méně obecná ustanovení v obecných kompetenčních normách, obecných procesních normách i v zákonech upravujících konkrétní agendy* (…)“.[161] Správci agendových systémů tak v řadě případů nebyli výslovně povinni údaje zveřejňovat a vše ve výsledku záleželo na jejich subjektivním posouzení. Kromě 4 základních registrů[162] existuje v České republice cca 4 300 agendových informačních systémů. Dá se tedy říct, že existuje veřejný zájem na zpřístupnění údajů i z těchto systémů pro cílenou koordinaci digitálních služeb.[163] Tvrzená disproporčnost pak spočívala ve skutečnosti, že oprávnění poskytovat a využívat údaje z agendových informačních systémů byla v právním řádu řešena taxativním výčtem údajů, ke kterým orgán veřejné moci mohl získat přístup. Oprávnění k využívání údajů bylo vzhledem k výše uvedené citaci poměrně nepřehledné, z čehož plynul nejednotný přístup správců systémů ke sdílení údajů. Zároveň v souvislosti s přijetím ZPDS nebyla tehdejší koncepce (tj. výčet údajů, které byli správci registrů oprávněni využívat) nadále kompatibilní s podmínkami kladenými ZPDS.[164]

Úprava sdílení dat mezi orgány veřejné moci v kontextu DEPO se ze 169 různých právních předpisů dotýká 144. Navrhovaná změna pak z těchto 144 právních předpisů vypouští taxativní výčty údajů, které jsou orgány veřejné moci oprávněné využívat. „*Cestou přechodných ustanovení k ZPDS je zabezpečeno, že orgánům veřejné moci bude zachována kompetence využívat údaje z informačních systémů veřejné správy za dosavadních (technických) podmínek jejich poskytování a v rozsahu stanoveném zrušenými ustanoveními zákonů upravujících jednotlivé agendy, a to až do okamžiku, kdy ohlašovatel agendy dospěje k závěru, že je nutno rozsah modifikovat. Po této modifikaci bude orgán veřejné moci využívat údaje z informačních systémů veřejné správy v rozsahu stanoveném v RPP.*“[165][166] DEPO tedy zjednodušeně řečeno

[161] Důvodová zpráva DEPO
[162] Registry zřízené na základě ZoZR
[163] Důvodová zpráva DEPO
[164] Srovnání s ustanovením § 7 ZPDS
[165] Ibid.
[166] Srovnání s Důvodová zpráva k ZPDS, zvláštní část § 14

opouští původní princip, kdy správci agend využívaly údaje na základě zákonných ustanovení a přesouvá se k principu využívání údajů na základě registrace agendy v RPP.

„*Oprávnění jednotlivých orgánů veřejné moci k čerpání údajů ze základních registrů a agendových informačních systémů se bude nově odvíjet od registrace agendy v RPP a registrace působnosti konkrétního orgánu veřejné moci v agendě. Ústřední správní úřad ohlašující agendu (gestor agendy) vyhodnotí, které údaje, ze kterých informačních systémů veřejné správy, bude potřeba pro výkon jím ohlašované agendy využívat, přičemž potřebu těchto údajů odůvodní* (…) *Správce příslušného základního registru nebo agendového informačního systému posoudí vhodnost zpřístupnění navrhovaných údajů a v případě nutnosti navrhne redukci či naopak rozšíření. Nebude-li ohlašovatel agendy s touto modifikací souhlasit, rozhodne v případě těch ohlašovatelů, kteří jsou podřízeni vládě, o konečném rozsahu údajů vláda jako vrcholný orgán moci výkonné a subjekt odpovědný Poslanecké sněmovně mj. za výkon veřejné správy, a to s využitím stanoviska ÚOOÚ.*“[167]

Zachová se tedy princip právní jistoty v tom smyslu, že subjekt těchto údajů si může ověřit, ke kterým jeho údajům má který orgán veřejné moci přístup. Zároveň je ale přístup daleko flexibilnější, jelikož jakákoliv potřeba změny není odkázána na vůli zákonodárce, kdy lze očekávat náročný a dlouhý legislativní proces, který ne vždy dokáže účinně reagovat na poptávku po úpravě. Namísto toho bude, jak jsem již výše uvedl, rozsah využívaných údajů stanoven v rámci registrace agendy ve smyslu ustanovení § 53 a násl. ZoZR. „*Využívání osobních údajů ze základních registrů a agendových informačních systémů je zpracováním osobních údajů ve smyslu GDPR. Zpracování je zákonné, neboť je prováděno při výkonu veřejné moci, kterým je správce pověřen, a zároveň je nezbytné pro splnění právní povinnosti správce. Zpracování osobních údajů ve formě jejich využití ze základního registru nebo agendového informačního systému bude mít právní základ v zákonech upravujících konkrétní agendu ve spojení s úpravou v ZoZR.*“[168]

Kromě výše uvedeného byla v souvislosti s přijetím DEPO novelizována i úprava datových schránek, respektive bylo zakotveno automatické zřizování datových schránek některým osobám. V případě, že svéprávná fyzická osoba (zapsaná v ROB k 1. lednu 2023) využije některý z kvalifikovaných prostředků elektronické identifikace (např. bankovní identitu) před

[167] Důvodová zpráva DEPO
[168] Ibid.

31. prosincem 2022, zřídí této osobě Ministerstvo vnitra automaticky datovou schránku k 1. lednu 2023. Všem dalším fyzickým osobám, které použijí kvalifikovaný prostředek elektronické identifikace po roce 2022, bude zřízena bezodkladně.[169] Jinými slovy, každá fyzická osoba, která se elektronicky identifikovala nebo se elektronicky identifikuje je dříve či později „odsouzena" k tomu, využívat službu datové schránky fyzické osoby. Podnikajícím fyzickým osobám a právnickým osobám bude datová schrána zřízena bez dalšího k 1. březnu 2023.[170] Tato úprava byla do samotného návrhu vtělena až v rámci komplexního pozměňovacího návrhu Výboru pro veřejnou správu Poslanecké sněmovny, který byl posléze modifikován pozměňovacím návrhem Senátu, v jehož znění byl návrh schválen a následně publikován. Vzhledem k absenci důvodové zprávy lze vycházet ze stenozáznamu jednání Poslanecké sněmovny případně Senátu, kde ovšem chybí ucelené odůvodnění této změny.[171]

Na jednu stranu se dá rozumně předpokládat, že cílem zákonodárce bylo aktivování datových schránek pro co možná největší objem osob, čímž se sleduje vcelku racionálně zefektivnění komunikace mezi osobami a orgány veřejné správy a ve výsledku usnadnění modernizace veřejné správy a snížení potenciálních výdajů ze státního rozpočtu. Na druhou stranu, byť může být sledovaný cíl legitimní, domnívám se, že není naplňován legitimními prostředky. Zákonodárce zde nachystal jakousi past pro fyzické osoby, které nemají zřízenou datovou schránku. V okamžiku, kdy fyzická osoba využije prostředek elektronické identifikace, automaticky si sama způsobí to, že jí bude (vědomě i nevědomě) zřízena datová schránka.

Nabízí se dva argumenty ve prospěch této změny. První stojí na základní právní zásadě *ignorantia iuris non excusat*, zároveň je však zapotřebí zdůraznit, že i tato zásada má své limity, zejména u tak komplexních a rozsáhlých změn, jakou DEPO bezpochyby je. Druhým argumentem je pak právo fyzické osoby podat žádost o znepřístupnění datové schránky, bez ohledu na to, zda byla zřízená na žádost nebo automaticky na základě § 3 odst. 1 ZoEÚAK.

Ovšem samotné zřízení datové schránky vytváří konkrétní právní rámec, ve kterém se fyzická osoba musí nutně pohybovat. Fyzická osoba tak v dobré víře může například očekávat doručování (nikoliv prostřednictvím datové schránky) zatímco jí může v důsledku fikce

[169] § 3 odst. 1 ZoEÚAK ve znění účinném od 1. ledna 2023 a Přechodná ustanovení k ZoEÚAK zavedena DEPO Čl. CXLIII, bod č. 2
[170] Ibid, bod č. 3 a 4
[171] Srovnání stenozáznamů z 87. schůze Poslanecké sněmovny ze dne 5. března 2021 a z 10. schůze Senátu ze dne 29. dubna 2021.

doručení do datové schránky uplynout lhůta pro ten který úkon, který je po osobě vyžadován v rámci konkrétní lhůty. Bez ohledu na to, zda si fyzická osoba může datovou schránku znepřístupnit, bude existovat okamžik (byť jen nepatrný), ve kterém bude fyzická osoba muset „strpět" nová práva, ale primárně povinnosti vyplývající se zřízené datové schránky. Realitou též je, že ne každá fyzická osoba bude se zřízením datové schránky vědomě obeznámena,[172] což pro tu kterou osobu může mít výše zmíněné důsledky.[173]

Povinné zřízení datových schránek je nutné vnímat v kontextu i dalších právních předpisů, které s eGovernmentem souvisí, zejména pak s ustanovením ZPDS. Jak jsem již zmínil v kapitole 2.6, závěrečná a přechodná ustanovení v § 14 odst. 1 stanovují, že „*Nepodnikající fyzické osoby nemohou být nuceny využívat digitální služby nebo činit digitální úkony podle tohoto zákona."* Jinými slovy výslovně zakotvuje zásadu dobrovolnosti ve vztahu k digitálním službám a eGovernmentu. Digitální službou podle tohoto zákona se rozumí v souladu s § 2 odst. 2 „*úkon vykonávaný orgánem veřejné moci vůči uživateli služby v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě*".

Mezi agendu Ministerstva vnitra patří zřizování datových schránek jakožto úkon číslo U1907 v rámci agendy pod kódem A119.[174] Ministerstvo vnitra je současně orgánem veřejné moci, který vykonává úkon vůči uživateli služby (fyzické nepodnikající osobě, která použila prostředek elektronické identifikace) v rámci agendy (zřizování datových schránek), který je vedený v katalogu služeb jako úkon v elektronické podobě (datovou schránku lze zřídit i elektronicky).[175] Ve své podstatě tedy úkon Ministerstva vnitra, kterým zřídí datovou schránku všem fyzickým osobám (bez datové schránky), které použily nebo použijí prostředek elektronické identifikace po účinnosti DEPO, naplňuje definici digitální služby podle ZPDS.

Jak jsem výše zmínil, sama existence datové schránky přináší řadu práv, ale zejména i povinností pro oprávněnou osobu. Jinými slovy, fyzická osoba je donucena k tomu, aby využívala digitální služby. V tomto případě se však nejedná pouze o povinnost využívat službu zřízení datové schránky, ale také například i o již zmíněnou povinnost využívat službu

[172] Doposud nejsou známy konkrétní kroky, jakým budou fyzické osoby o tomto zřízení informovány.
[173] Nutno dodat, že nastavení notifikací pomocí SMS apod. si musí daný uživatel ve své datové schránce nastavit, což logicky nelze udělat v případě, že daná osoba o existenci své schránky neví.
[174] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Rozcestník vygenerovaných agend. *Registr práv a povinností – agendové informační systémy* [online]. [cit. 2022-16-06]. Dostupný z: https://rpp-ais.egon.gov.cz/gen/agendy-detail/
[175] MINISTERSTVO VNITRA. Zřízení datové schránky. *Portál veřejné správy* [online]. [cit. 2022-05-05]. Dostupné z: https://portal.gov.cz/sluzby-vs/zrizeni-datove-schranky-S5692

elektronického podání daňového přiznání (datovou schránkou zřízenou ze zákona) [176] nebo službu elektronického doručování do datové schránky, ke kterému jsou orgány veřejné moci povinné.

Na druhou stranu je potřeba zvážit již zmiňované ustanovení marginální rubriky § 3 Právo na digitální službu odst. 2 ZPDS, které stanovuje, že „*práva a povinnosti podle jiných zákonů nejsou tímto zákonem dotčena*“. Ovšem, jak uvádí F. Korbel a spol., smyslem tohoto ustanovení je právě postavení ZPDS do role *lex generalis*, který umožní dalším předpisům upravit poskytování digitálních služeb odchylně.[177] Podle mého názoru však nelze vykládat toto ustanovení tak, že další předpis (*lex specialis*) může na základě tohoto ustanovení stanovit povinnost využívat některou digitální službu povinně u fyzických osob, jelikož by to bylo v přímém rozporu s § 14 odst. 1 ZPDS. Daný předpis by musel výslovně uvedené ustanovení přímo nebo nepřímo změnit. Z mého pohledu tedy jedním z limitů pro odlišnou úpravu poskytování digitální služeb je právě ono stanovení povinnosti pro fyzické osoby jí využívat.

Nabízí se však otázka, zda v důsledku toho, že DEPO nabylo účinnosti později, by nedošlo k uplatnění zásady *lex posterior derogat legi priori*? V takovém případě by se uplatnila, bez ohledu na rozpor, úprava v DEPO. Byť se ZPDS často říká digitální ústava, jedná se stejně o obecný zákon. Z mého pohledu však DEPO nemá za cíl upravit vnitřní logiku ZPDS v tom smyslu, aby byl v souladu s automatickým zřízením datových schránek. Pokud by tomu tak bylo, jistě by k novelizaci zmiňovaného ustanovení § 14 odst. 1 ZPDS došlo. Taková situace však nenastala. Uvedený rozpor je tedy velmi pravděpodobně chybou vzniklou v legislativním procesu s ohledem na to, že přezkum proveditelnosti není u pozměňovacích návrhů tolik podrobný jako v případě původních návrhů. Uplatnění této zásady je tedy přinejmenším sporné.

V současné době není zcela patrné, jaké konkrétní technické aspekty bude automatické zřizování datových schránek mít a jak budou uživatelé informování o jejím zřízení. Na základě výše uvedeného se však domnívám, že automatické zřízení datových schránek pro fyzické osoby je v rozporu s ochranným ustanovením v § 14 odst. 1 ZPDS, které garantuje nepodnikajícím fyzickým osobám svobodnou vůli při využívání digitálních služeb a digitálních

[176] Srovnání s ustanovením § 72 odst. 6 DaňŘ
[177] KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel, ZAJÍČEK, Zdeněk. § 3 [Právo na digitální službu] In: ZAJÍČEK, Zdeněk et al., op. cit. sub. 58, str. 35-36

úkonů. Je tedy v rozporu se zásadou dobrovolnosti, která je v právní úpravě eGovernmentu zásadní. Proto bude zajímavé sledovat, jakým způsobem se k celé otázce postaví judikatura.

2.8. Digitalizace v dalších vybraných právních oblastech

Na úvod je potřeba zmínit elektronizaci, respektive digitalizaci v dalších předpisech správního práva. Tím prvním je stanovení preference elektronické podoby spisové služby podle ustanovení § 63 odst. 3 zákona č. 499/2004 Sb., o archivnictví a spisové službě. Druhou je pak změna zákona č. 106/1999 Sb., o svobodném přístupu k informacím, kde došlo k zakotvení oprávnění podávat žádost elektronickou cestou, požadovat zaslání požadovaných informací na elektronickou adresu žadatele nebo zřízení informačního systému ve smyslu ZoISVS obsahující katalog otevřených dat, spravovaného Ministerstvem vnitra.

Nicméně v této podkapitole se budu především věnovat některým novinkám v oblasti právních předpisů eGovernmentu v širším významu. Tedy odvětvími, které vzdáleně s eGovernmentem souvisí, ale jako takové jsou spíše ojedinělými oblastmi správního práva s prvky toho, co nazýváme eGovernment.

2.8.1. Publikace a tvorba práva

Právo publikace a tvorby právních předpisů je ze své podstaty oblastí správního práva, byť s některými ústavněprávními aspekty. Sbírka zákonů a mezinárodních smluv je dle nové právní úpravy výslovně zřizována jako úřední list, přičemž je zachována kontinuita Ministerstva vnitra jakožto jejího vydavatele. Je zde tedy jasně zdůrazněná role ministerstva jakožto vrcholného orgánu veřejné správy na úseku publikace právních předpisů. Samotná tvorba pak je z velké části závislá no normách ústavního práva, zejména v rámci legislativního procesu. Nicméně tvorba, stejně jako publikace, je svázána konkrétními procedurami, které upravují normy správního práva.[178]

Dne 15. června 2016 byl přijat zákon č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv (dále jen „**ZoSbírce**“). Kromě sloučení dosavadní Sbírky zákonů a Sbírky mezinárodních smluv do jedné sbírky, přináší návrh právně závaznou a konsolidovanou elektronickou formu publikace

[178] Například pravidla pro tvorbu legislativy, dosud vyjádřené v Legislativních pravidlech vlády schválených usnesením vlády č. 188 ze dne 19. března 1998 ve znění pozdějších změn (dále jen „**Legislativní pravidla vlády**“), nyní nový ZoSbírce přejímá přímo do textu zákona a stanovuje tak zákonné standardy pro tvorbu právních předpisů.

právních předpisů a jak dále název předpisu naznačuje, tak i modernizaci způsobu tvorby právních předpisů. Jedním z hlavních cílů návrhu je „*zvýšení dostupnosti, přehlednosti a srozumitelnosti platného práva a usnadnění, zkvalitnění a zefektivnění jeho tvorby ve všech stadiích legislativního procesu*“[179], čímž se zákonodárce dle mého názoru, mimo výše zmíněné, snaží naplňovat obecné předpoklady zásad předvídatelnosti práva a právní jistoty.

Elektronická publikace je zásadním krokem, jelikož jak stávající právní úprava, obsažená v zákoně č. 309/1999 Sb., o Sbírce zákonů a Sbírce mezinárodních smluv, stanovuje, jediná závazná podoba publikovaných právních předpisů je ta listinná, což je z praktických důvodů problematické.[180] Byť laická i odborná veřejnost využívá řadu komerčních služeb, které poskytují elektronickou verzi platné právní úpravy, do přijetí ZoSbírce nebyla žádná z těchto služeb ani jejich obsah garantován státem. Nově bude tedy docházet k takzvanému duálnímu systému publikace. To v praxi znamená, že kromě standardní listinné podoby bude ve Sbírce zákonů a mezinárodních smluv (dále jen „**Sbírka**“) vedena též elektronická podoba dostupná způsobem umožňující dálkový přístup, přičemž obě verze mají deklarované rovné právní účinky.[181][182] Výše uvedené však narušuje fakt, že ZoSbírce stanovuje o listinné podobě řadu výjimek oproti elektronické. Jmenovitě lze zmínit například vyhlašování aktu dle § 10 odst. 1, kdy ZoSbírce výslovně stanovuje, že vyhlášením se „*rozumí zpřístupnění částky, v níž je akt obsažen, s využitím elektronického systému Sbírky*“ s dodatkem, že zaslání částky v listinné podobě nemá na vyhlášení vliv. Jinými slovy, důležité je z právního hlediska, aby existovala elektronická podoba a pokud nebude existovat ta listinná, na vyhlášení aktu to nic nemění. Pokud bych parafrázoval Orwellovu Farmu Zvířat, tak „*formy jsou si rovné, některé jsou si rovnější*“. Tím však nekritizuji úmysl zákonodárce, tedy upřednostňovat elektronickou formu nad tou listinnou, spíše naopak. Jak glosoval V. Sládeček tuto tendenci k elektronizaci „*pokrok ničím nezastavíš*“[183]. S tím lze naplno souhlasit. Zároveň upřednostňování elektronické verze úzce souvisí s klíčovou zásadu modernizací veřejné správy *digital by default* (neboli budování přednostně digitálních služeb). Co ovšem hodnotím negativně, je skoro až alibistická snaha zákonodárce prázdnými deklaracemi stavit na rovno listinnou a elektronickou formu, když

[179] Důvodová zpráva ZoSbírce, Shrnutí závěrečné zprávy RIA, kapitola 2. Cíl návrhu zákona
[180] Srov. s důvodovou zprávou ZoSbírce
[181] Správcem elektronického systému, vydavatelem Sbírky a odpovědným orgánem je Ministerstvo vnitra. Kromě toho budou ve Sbírce zpřístupněny i časové verze právních předpisů (v případě, že byly novelizovány) účinné ke konkrétnímu datu.
[182] Ustanovení § 1 odst. 2 ZoSbírce
[183] SLÁDEČEK Vladimír. Elektronická sbírka zákonů ve Slovenské republice a v České republice. In: *Zborník príspevkov z Medzinárodnej vedeckej konferece konanej v dňoch 9. – 10 mája 2019 v Trnave.* Veřejná správa, právo na spravodlivý proces a e-government. Trnava: Právnická fakulta, Trnavská univerzita v Trnave, 2019, str. 73. ISBN 978-80-568-0321-9

zároveň dává najevo, že elektronická forma čehokoliv (s čímž já plně souhlasím) je lepší, důležitější, perspektivnější a tak dále. Zde se dostávám na samý začátek této kapitoly, že takovéto jednání zákonodárce jde proti tomu, čeho chce ve výsledku dosáhnout – zajištění právní jistoty adresátů právních norem.

V souvislosti s přijetím ZoSbírce započalo Ministerstvo vnitra s přípravou dvou projektů – eSbírka a eLegislativa. „*Systém eSbírka se bude dělit na dvě části - na portál, kde se budou vyhlašovat závazná elektronická znění právních aktů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv, včetně právně závazných úplných znění, a na databázi informací o právních aktech. Ta bude sloužit k pružné práci s aktuálními či minulými úplnými zněními právních předpisů, bude též obsahovat dokumenty související s právními předpisy, jako například výkladová stanoviska jednotlivých úřadů, umožní i vyhlašování závazné listinné podoby právního předpisu v textově zcela identické podobě elektronické. Vedle závazné podoby bude právní předpis v elektronické podobě zpřístupněn i v dalších formátech umožňujících následné využití dat v komerčních i neziskových projektech. Systém bude propojen se systémy Evropské unie EUR-Lex a N-Lex.“*[184] V souvislosti s přípravou zmíněných projektů bylo zapotřebí legislativně posunout u ZoSbírce datum nabytí účinnosti. V současné době je účinnost stanovena na 1. ledna 2023 právě z důvodu technické přípravy projektů, nicméně bylo Ministerstvem vnitra avizováno další posunutí účinnosti, které musí projít řádným legislativním procesem.[185] Na realizaci elektronické Sbírky reaguje zákonodárce i v dalších oblastech, jako je například aktuální snaha o regulaci lobbingové činnosti. V této souvislosti bylo navrhováno, kromě primárního cíle tj. regulovat činnost lobbistů, aby vznikl nový institut související s publikací právních předpisů, tzv. lobbistická stopa.[186] Tato stopa by obsahovala u konkrétního právního předpisu údaje o „lobbistovi“ stejně jako údaje o každém z „lobbovaných“ a zejména údaje o změnách, ke kterým došlo v důsledku lobbování.

Projekt eLegislativa, neboli elektronický systém tvorby právních předpisů, pak souvisí s druhou velkou změnou, kterou ZoSbírce přináší. Jedná se o kompletní změnu praktického přístupu k tvorbě legislativy. Podle důvodové zprávy k ZoSbírce lze současné legislativní tvorbě vytknout 4 základní nedostatky. Prvním je problematická příprava novelizace při nepřehledné

[184] MINISTERSTVO VNITRA. Projekty. eSbírka a eLegislativa. *Ministerstvo vnitra* [online]. [cit. 2021-04-10]. Dostupné z: https://www.mvcr.cz/clanek/esbirka-a-elegislativa.aspx
[185] Ibid.
[186] Vládní návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o lobbování

podobě platného práva, tedy jaké je aktuální znění, zda není dané ustanovení novelizováno apod. Druhým je nedostatečný nástroj, který by úspěšně eliminoval legislativní chyby a nedostatky. Zbylými jsou pak nesjednocený elektronický formát legislativního dokumentu a absence povinnosti dle Jednacího řádu Poslanecké sněmovny odůvodňovat navrhované změny u projednávaného právního předpisu.[187] Výše uvedené nedostatky se snaží řešit již zmíněný systém eLegislativa, který poskytne „*editor pro tvorbu a projednání právních předpisů v úplném znění (e-Šablona), zapracovávající pravidla tvorby formy a obsahu právního předpisu, právní tezaurus a slovník CzechVoc pro přehlednost a postupné sjednocování právní terminologie. Tvorba a projednávání právních předpisů v úplném znění poskytne přehledné prostředí pro tvorbu práva, umožní reflektovat všechny aspekty jeho tvorby (návaznost na předchozí či probíhající legislativní práce, respektování odkazů a terminologických vazeb).“*[188] Kromě toho bude systém propojen s informačními systémy obou komor Parlamentu a systémem eKLEP, čímž se sníží administrativní zátěž a zajistí se jednotný systém pro legislativní proces.

2.8.2. Zdravotnictví

V širším smyslu je zdravotnické právo „*shlukem norem upravujících poskytování zdravotní péče“*[189], a to jak norem soukromoprávních, tak veřejnoprávních. Pro téma, kterému se věnuji v této kapitole, bude zásadní ta část zdravotnického práva, které se zabývá výkonem státní správy v oblasti zdravotnictví a souvisejícími regulacemi.

Před přijetím nové platné právní úpravy v oblasti elektronizace zdravotnictví vyjádřená sjednocujícím zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví, ve znění pozdějších předpisů (dále jen „**ZeZdrav**“) byla úprava elektronizace zdravotnictví spíše difúzní v rámci dílčích ustanovení norem zdravotnického práva.

Tou nejvýraznější byla dle mého názoru úprava elektronické preskripce léčivých přípravků. Historie této úpravy se v České republice váže k přijetí zákona č. 378/2007 Sb., o léčivech a o změnách souvisejících zákonů (dále jen „**ZoLéč**“) už od jeho původního znění. V původním znění byla úprava vydávání tzv. elektronických receptů nastavená takovým způsobem, že

[187] Důvodová zpráva ZoSbírce, kapitola 1.3. Obecné části
[188] Důvodová zpráva ZoSbírce, kapitola 2 Obecné částí
[189] ŠUSTEK, Petr a Tomáš HOLČAPEK. *Zdravotnické právo*. Praha: Wolters Kluwer, 2016, str. 31. ISBN 978-80-7552-321-1.

pacient si mohl sám určit, zda mu lékař vystaví lékařský předpis v elektronické nebo listinné podobě. V praxi však pacienti možnost elektronických předpisů nevyužívaly, z toho důvodu zákonodárce zakotvil zákonem č. 70/2013 Sb., kterým se měnil ZoLéč, povinnost lékařů vystavovat lékařský předpis výhradně elektronicky, neexistují-li důvody, kdy je z objektivních důvodů nutné vystavit jej v listinné podobě a dále povinnost lékaře zaslat elektronický recept do centrálního úložiště, které spravuje Státní ústav pro kontrolu léčiv (dále jen „**SÚKL**“).[190] Tato povinnost původně účinná k 1. lednu 2015 byla následně posunutá až na 1. leden 2018.[191]

Zmíněná změna úpravy elektronických receptů vytvořila hrubý základ pro systém tzv. eReceptu. Smyslem původní úpravy elektronizace receptů bylo vytvoření centrálního úložiště a umožnění zanesení údajů o konkrétní formě farmakoterapie (léčba konkrétními léčivými přípravky) toho kterého pacienta s úmyslem zabránit nežádoucím příhodám a kontraindikacím jednotlivých léčiv, které pacient užívá. Ovšem jak uvádí důvodová zpráva k zákonu č. 262/2019 Sb., kterým se mění zákon č. 378/2007 Sb., o léčivech a o změnách souvisejících, ve znění pozdějších předpisů (dále jen „**ZeRecept**“), „*Využití těchto důležitých dat* (data o farmakoterapii pacienta pozn. autora) *však současná právní úprava neumožňuje. Aktuálně má lékař přehled pouze o těch léčivých přípravcích, které sám předepsal. Farmaceut při výdeji pak má možnost zkontrolovat léčivé přípravky pouze na současně předložených receptech. Existující právní stav neumožňuje efektivní kontrolu interakcí a duplicit všech pacientem užívaných léčiv. Přestože díky elektronické preskripci jsou získávána data o léčivých přípravcích v podobě, díky které by bylo možné po technické stránce sdílet a využívat poskytovateli zdravotních služeb ve prospěch zvýšení kvality a bezpečnosti péče poskytované konkrétnímu pacientovi, současná právní úprava sdílení a využití údajů neumožňuje*.“[192] Absence takové právní úpravy řeší právě zmíněný ZeRecept.

Cílem této novely bylo postavení již pevných základů eReceptu, což je velmi zjednodušeně systém, který v zahrnuje existující centrální úložiště elektronických receptů, ale dále i například registr léčivých přípravků s omezením, lékový záznam, správu souhlasů a další součásti.[193]

---

[190] Ustanovení § 80 odst. 1 ZoLéč účinného ke dni 1. ledna 2018 dále stanovilo, že výčet objektivních podmínek, za kterých bude lékař oprávněn vydat recept v listinné podobě, bude stanoven prováděcím předpisem. Tyto podmínky stanovuje vyhláška Ministerstva zdravotnictví č. 329/2019 Sb., ve které stanovuje okruh léčivých přípravků, pro které lze recept v listinné podobě vystavit.

[191] Srovnání se zákonem č. 255/2014 Sb., kterým se mění zákon č. 70/2013 Sb., kterým se mění zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), ve znění pozdějších předpisů

[192] Důvodová zpráva ZeRecept, část A obecné části.

[193] Ustanovení § 81 odst. 1 ZoLéč

Tento systém tak umožní nepřetržitý přístup lékařů, farmaceutů nebo pacientů k údajům, které se týkají elektronických receptů jednotlivých pacientů, při současném zachování náležité ochrany osobních údajů. „*Veškeré přístupy k systému eRecept jsou logovány a je o nich veden žurnál činností tzn. je zaznamenán každý náhled a každý úkon, který přistupující subjekt provede. Veškerá komunikace probíhá zabezpečeným šifrovaným protokolem (…) K údajům v Centrálním úložišti elektronických receptů i Registru léčivých přípravků s omezením (k systému eRecept) mají přístup pouze oprávněné osoby, kterým byly přiděleny přístupové údaje ze strany SÚKL a mají komunikační certifikát poskytovatele zdravotních služeb, tedy lékaři a farmaceuti. Na základě přidělených přístupových údajů ze strany SÚKL k datům přistupují oprávnění pracovníci zdravotních pojišťoven, Ministerstva zdravotnictví a Policie ČR za účelem výkonu své působnosti. Pacient přistupuje ke všem o něm vedeným údajům prostřednictvím kvalifikovaného systému elektronické identifikace.“*[194] Vytvoření propojeného informačního systému obsahující údaje o farmakoterapii je dle mého názoru dalším důležitým krokem na půdě eGovernmentu. Jak ukazují data obsažená v důvodové zprávě k ZeRecept, před přijetím této úpravy došlo mezi lety 2007 a 2017 k více jak 3,5násobnému nárůstu počtu hospitalizovaných s diagnózou, která odpovídá „*nežádoucím účinkům při léčebném použití léků nebo biologických látek a chyb v dávkování“*[195], přičemž počet případů, kdy pacienti s touto diagnózou zemřeli, se znásobil až 10krát.[196] Řada těchto nešťastných případů vznikla právě v důsledku nedostatečných dat o léčivých přípravcích, které pacient užívá.

Jsem toho názoru, že pro lepší představu o komplexnosti sdílení dat ve zdravotnictví bylo zapotřebí nejprve rozebrat úpravu eReceptu, která v mnohém nastínila úskalí elektronizace zdravotnictví. Na jedné straně můžeme zvážit důležitost aktualizovaných údajů, které si mezi s sebou sdílí poskytovatelé zdravotních služeb, přičemž mají dokonalý přehled o pacientově zdravotním stavu a léčivých přípravcích, které užívá. Díky tomu můžou bezpochyby daleko lépe nastavit případnou vhodnou léčbu. Na druhé straně pak stojí ochrana údajů o zdravotním stavu, které podléhají speciální úpravě, jelikož se jedná o tzv. zvláštní kategorii osobních údajů.[197] Akcent na ochranu osobních údajů v oblasti zdravotnictví je o to vyšší, proto se jeví vhodné zmínit se o této problematice právě v této kapitole. ZeRecept dle mého názoru dokázal

[194] Důvodová zpráva ZeRecept, část D obecné části.
[195] Ibid.
[196] Srovnání Tabulky č. 1 a Tabulky č. 2 v Důvodové zprávě k ZeRecept, části A obecné části.
[197] Ustanovení článku 9 Nařízení Evropského parlamentu a Rady (EU) č. 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)

nalézt proporcionální cestu, která umožní vytvoření systému sdílení údajů při současném zachování vhodné ochrany osobních údajů. Tato zásada proporcionality je jednou z klíčových a jako vinoucí se červená niť prostupuje, respektive i do budoucna by měla prostupovat, právní úpravou, která, byť jen zčásti, souvisí s eGovernmentem.

V úvodu zmíněný nový ZeZdrav dále staví na vybudovaných základech sdílení dat ve zdravotnictví a má ambice posunout tuto úpravu dál. Jak jsem již zmínil a ostatně to potvrzuje i důvodová zpráva k ZeZdrav, úprava elektronizace je poměrně difúzní a nikterak koordinovaná. Vyvstala tedy potřeba vytvořit jednotnou infrastrukturou pro sdílení databáze celkového zdravotního stavu pacienta (nejen např. informace o farmakoterapii pacienta). ZeZdrav zajišťuje právní rámec pro vybudování tzv. Integrovaného datového rozhraní, což je infrastruktura spravovaná Ministerstvem zdravotnictví a provozovaná SÚKL, která se skládá z dílčích systémů a služeb, a která zajistí *„bezpečné sdílení dat a zdravotnické dokumentace a vedení autorizované komunikace mezi subjekty zapojenými do elektronického zdravotnictví*“[198] Zmíněnými součástmi Integrovaného datové rozhraní jsou A) kmenové zdravotnické registry, B) služby vytvářející důvěru, C) centrální služby elektronického zdravotnictví a D) žurnál činností.[199]

A) Kmenový zdravotnický registr je registr identifikátorů a údajů u poskytovatelů zdravotních služeb, zdravotnických pracovníků a pacientů. Tyto registry jsou současně provázány se základními registry, čímž se zajistí dostatečná provázanost s dalšími službami eGovernmentu.
B) Služby vytvářející důvěru jsou jednotlivé systémy, které zajišťují důvěryhodné metody, jakými lze například vést nebo předávat zdravotní dokumentaci nebo díky kterým může konkrétní subjekt získat přístup do toho kterého informačního systému. Konkrétně se jedná o zaručená elektronická časová razítka, zaručené elektronické pečetě, zaručené elektronické podpisy nebo resortní systémové a přístupové certifikáty.[200] Současně je v některých případech, jako je přístup do Integrovaného datového rozhraní, stanovena výslovná povinnost poskytovatele zdravotních služeb, oprávněné nebo zapisující osoby

[198] Důvodová zpráva k ZeZdrav, kapitola 3. obecné části.
[199] Ustanovení § 7 odst. 1 ZeZdrav.
[200] Ustanovení § 26 ZeZdrav.

využívat pro přístup konkrétní službu vytvářející důvěru, a to resortní systémový certifikát.[201]

C) Mezi centrální služby elektronického zdravotnictví se řadí nahlížení a zápis do kmenových registrů nebo konkrétní nastavení podmínek pro výměnné sítě, které zajišťují bezpečné předávání elektronické zdravotnické dokumentace. Dále je to systém správy souhlasů evidující souhlasy pacienta a třetích osob vyžadovaných podle právních předpisů zdravotnického práva, Portál elektronického zdravotnictví, který podobně jako Portál občana umožňuje přístup k jednotlivým službám elektronického zdravotnictví (např. přístup do Integrovaného datového rozhraní) a katalog služeb elektronického zdravotnictví, ke kterým je umožněn přístup například skrze zmíněný portál.
D) Poslední součástí je žurnál činností, ve kterém jsou zaznamenány informace o činnostech provedených v Integrovaném datovém rozhraní oprávněnými a zapisujícími osobami, přičemž je zpřístupněný k nahlížení pacientovi nebo zdravotnickému pracovníkovi.

Související změny se ZeRecept umožňují prostřednictvím legislativně technických ustanovení další propojení již existujících služeb eGovernmentu v oblasti zdravotnictví. Tento vývoj ovšem respektuje základní princip zavádění nových technologií uvážlivým způsobem, který neohrozí plynulost a bezpečnost nastavených procesů. Tedy principu, který by se dal vyjádřit jako „evoluce, nikoliv revoluce“. Novelizace například počítá s provázáním již existujícího systému eRecept, kterému zpřístupní možnost využívat služby vytvářející důvěru a kmenové registry.[202] Dále je se jedná o klíčový Národní zdravotnických informační systém (dále jen „**NZIS**“) Ústavu zdravotnických informací a statistiky ČR (dále jen „**ÚZIS**“), který vychází z úpravy zákona č. 372/2011 Sb., o zdravotnických službách a podmínkách jejich poskytování, ve znění pozdějších předpisů (dále jen „**ZoZS**“).[203] V souvislosti s NZIS byla potřeba zejména upravit tzv. identifikátory neboli údaje, které jednoznačně propojí subjekt s příslušnými údaji vedenými v registru, nově (od 1. ledna 2023) bude zrušen jedinečný resortní identifikátor pacienta vydávaný ÚZIS podle § 71c ZoZS a bude nahrazen identifikátorem podle ZeZdrav.

Elektronizace zdravotnictví, někdy nazývána jako eHealth, je dle mého názoru učebnicovým příkladem toho, jakým způsobem mohou služby eGovernmentu nejen usnadňovat komunikaci mezi veřejnou správou a jejím adresátem, ale mohou v konečném důsledku mít pozitivní vliv

[201] Srovnání s ustanovením § 26 odst. 2 písm. b) a § 26 odst. 4 ZeZdrav
[202] Část čtvrtá zákona č. 326/2021 Sb., kterým se mění některé zákony v souvislosti s přijetím ZeZdrav
[203] Ustanovení § 70 a násl. ZoZS

na kvalitu zdravotních služeb a v přeneseném důsledku i na život a zdraví. Kromě toho „eHealth“ jednoznačně potvrzuje potřebu při elektronizaci chránit osobní údaje uživatelů.

2.8.3. Stavební právo

Tendence k digitalizaci lze pozorovat i u dalších oborů správního práva. Jedním z těchto oborů je například právě stavební právo v souvislosti s přijetím nového zákona č. 283/2021 Sb., stavební zákona (dále jen „**NStavZ**“) zatím účinného od 1. července 2023[204]. Dle důvodové zprávy stojí NStavZ na jednom z pilířů, kterým je „*úplná digitalizace stavební agendy od nástrojů územního plánování, přes projektové dokumentace staveb až po elektronický spis stavebních úřadů*“[205]

Jak zmiňuje důvodová zpráva, první změnou je stanovení, oproti původní právní úpravě, jednotného standardu pro územně plánovací dokumentaci, a to výlučně v elektronické verzi ve strojově čitelném formátu.[206] Současně je jako mapový podklad nově umožněno digitalizovat státní mapové dílo (např. katastrální mapa)[207], a využívat jej pro územně plánovací činnost.[208] Další praktickou změnou je nově umožnění vedení stavebního deníku a stavební dokumentace v elektronické formě. Povinnost vést stavební deník v elektronické formě u veřejných zakázek v nadlimitním režimu vyjádřená v ustanovení § 166 odst. 5 NStavZ koresponduje s původní právní úpravou, kde byla tato povinnost zakotvena v rámci přechodných ustanovení novelou č. 403/2020 Sb., pro stavební řízení zahájené po účinnosti této novely.

Druhou velkou skupinou změn je elektronizace některých zásadních úkonů ve stavebním řízení, jako je možnost podat žádost podle stavebního řádu v NStavZ na stanoveném elektronickém formuláři nebo možnost podávat elektronickou dokumentaci pro povolení záměru. Tato novinka souvisí s třetí velkou změnou stavebního práva, a tou je vytvoření právního rámce pro standardizovaný informační systém stavební správy.[209] Toto zakotvení informačního systému koresponduje s požadavky stanovenými v ZPDS, tedy povinností orgánů veřejné správy

[204] Záměrně uvádím, že je NStavZ „zatím“ účinný od 1. července 2023. Vzhledem k nedávno proběhlým volbám do Poslanecké sněmovny a v mediálním prostoru častokrát zdůrazněným tendencím ke změně tohoto zákona, lze předpokládat, že se účinnost NStavZ, stejně jako některé jeho části, budou měnit.
[205] Důvodová zpráva NStavZ, část B, kapitola 2., obecné části
[206] Původní úprava umožňovala vedení elektronických formátů, ale nestanovila je jako výlučnou formu.
[207] Státní mapové dílo definuje v ustanovení § 3 nařízení vlády č. 430/2006 Sb., o stanovení geodetických referenčních systémů a státních mapových děl závazných na území státu a zásadách jejich používání.
[208] Ustanovení § 59 a násl. NStavZ
[209] Ustanovení § 267 a násl. NStavZ

poskytovat digitální služby, nestanoví-li právní předpis jinak.[210] V tomto případě zákonodárce oprávnění „nedigitalizovat“ nevyužil a rozhodl se pokračovat v nastoleném trendu. Součástí tohoto informačního systému je například portál stavebníka, který je, podobně jako portál občana, digitálním rozhraní, které fyzickým a právnickým osobám umožňuje činit zmíněné úkony jako je podávání žádostí a elektronických dokumentů, případně odkazování na již evidované elektronické dokumenty. Kromě toho je portál stavebníka propojen s dalšími částmi informačního systému stavební správy, tj. s geoportálem územního plánování, evidencí správních úkonů nebo elektronických dokumentací, ale i s informačními systémy jiných správních orgánu jako je Český úřad zeměměřičský a katastrální. Díky tomu má uživatel jednoduchý přístup k informacím o stavu stavebního řízení, konkrétních správních úkonech, vydaných rozhodnutí, založených elektronických dokumentech nebo o právech a povinnostech, které byly tím kterým rozhodnutím v rámci stavebního řízení založeny.[211] Do těchto evidencí má přístup ten, kdo by disponoval právem nahlížet do spisu podle § 38 a násl. SpŘ.[212]

V souvislosti s digitalizací nejen stavebního práva, ale stavebnictví jako takového, je potřeba zmínit jeden z nejnovějších nástrojů jeho modernizace. Jedná se o metodu Building Information Modeling (dále jen „**BIM**“) neboli informační modelování staveb. Dne 25. září roku 2017 přijala vláda svým usnesením č. 682 koncepci zavádění metody BIM v České republice (dále jen „**Koncepce BIM**“).[213] „*BIM si lze představit jako databázi informací, která může zahrnovat kompletní data od prvotního návrhu, přes výstavbu, správu budovy a případné změny dokončených staveb (rekonstrukce) až po její demolici, včetně ekologické likvidace stavby a uvedení prostoru do původního stavu. Tedy veškeré informace využitelné během celého životního cyklu stavby.“*[214] Součástí této databáze kromě jiného je i 3D model stavby, který je složen z evidovaných informací. Používání BIM v praxi pak přináší řadu přínosů jako je zvýšení efektivity stavebního řízení, úspora finančních nákladů a času nebo zlepšení kvality staveb.[215]

Současná právní úprava již s BIM v jistých intencích počítá. Lze zmínit například možnost zadavatele v rámci sestavení a podání nabídky na veřejnou zakázku „stavebního charakteru“

[210] Srovnání s ustanoveními § 3 odst. 1 a § 4 odst. 1 písm. d) ZPDS
[211] Důvodová zpráva NStavZ, § 267 zvláštní část.
[212] Ustanovení § 272 NStavZ
[213] Usnesení vlády České republiky ze dne 25. září 2017 č. 682
[214] MINISTERSTVO PRŮMYSLU A OBCHODU, op. cit. sub. 17, str. 5
[215] Ibid., str.6

v nadlimitním režimu uvést v zadávací dokumentaci závazný požadavek využívat zvláštní elektronické formáty jako je např. BIM.[216] Lze se domnívat, že z důvodu potenciálního zakotvení BIM do stavebních nadlimitních zakázek byla též do stavebního práva, jak je uvedeno výše, zavedena povinnost vést stavební deník v elektronické formě v případě takovýchto zakázek.

Koncepce BIM ve své kapitole uvádí 5.4 dále uvádí, že „*Stavební zákon nemusí výslovně zmiňovat existenci metody BIM, měl by jen vytvořit předpoklady pro možnost elektronického předávání dokumentace. Vzhledem k rychlému rozvoji informačních technologií je lepší řešit konkrétní technické požadavky jinou formou – např. pomocí technických norem nebo metodik vydávaných uznávanými odbornými profesními a zájmovými organizacemi*“[217]. Dále je nutné poznamenat, že řešení konkrétních technických požadavků podzákonnými normami je důležité i z dalšího zásadního důvodu, a to kvůli zachování technologické neutrality. Pokud by zákonná úprava obsahovala konkrétní technické parametry, vystavovala by se hrozícímu riziku, že nebude zákonodárce schopný včas, v důsledku dlouhého legislativního procesu, reagovat na probíhající rozvoj ICT, čímž se dříve či později stane daná úprava obsolentní. Současná právní úprava stavebního řízení neumožňuje předávání elektronické dokumentace, jejíž součástí by teoreticky BIM být mohla. Tento problém, jak bylo výše uvedeno, NStavZ řeší a lze do budoucna předpokládat, že právní rámec pro využití BIM bude dostačující.

2.8.4. Úprava pozemních komunikacích a provozu na nich

Jistou formu elektronizace lze pozorovat i v úpravě pozemních komunikací. Mám na mysli zejména novelu zákona č. 13/1997 Sb., o pozemních komunikacích (dále jen „**ZoPozKom**“), tj. zákon č. 227/2019 Sb., kterým se mění ZoPozKom s účinností od 1. ledna 2021 (dále jen „**ZeZnám**“). Tato novela odstranila stávající model hrazení tzv. časové poplatku, tedy poplatku určeného za časové období užívání pozemní komunikace v daném časovém období ve smyslu § 21 a násl. ZoPozKom. Před přijetím zmíněné novely byla zákonem stanovená pravidla prokazování úhrady tohoto časového poplatku, a to formou dvoudílného kupónu, obvykle nazývaného jako dálniční známka. Na tomto kupónu měl uživatel povinnost vyznačit údaj o registrační značce vozidla, jež mělo být pro provoz na pozemních komunikacích

[216] Ustanovení § 103 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
[217] MINISTERSTVO PRŮMYSLU A OBCHODU, op. cit. sub. 17, str. 23

užíváno.[218]Tento model byl tedy novelou vypuštěn. Navrhovatelé v důvodové zprávě k ZeZnám zmiňují, že problematických aspektů původní úpravy bylo hned několik.

Prvním byla určitě problematika samotné dostupnosti. Uživatelé byly ještě před užitím příslušné pozemní komunikace povinni navštívit některé z distribučních míst, vyplnit registrační značku a známku nalepit na čelní sklo vozidla. To ostatně v kontextu doby, kdy lze prakticky vše platit bezhotovostně a dálkově, způsobovalo uživatelům nadbytečný diskomfort a konečně též působilo dost zastarale.[219]

Druhým pak byla omezená možnost státního dozoru ve smyslu kontroly úhrady časového poplatku u uživatelů pozemní komunikace. „*Kontrolu úhrady časového poplatku lze vykonávat pouze aktivní činností dozorujících kontrolních orgánů, které musí pro její provedení dotčená vozidla zastavovat na místě, případně použít dalekohled. Kontrola je víceméně náhodná, což postupem času vedlo ke snížení odrazujícího efektu hrozby uložení sankce za porušování této povinnosti.*“[220] S tím ostatně souvisí i nemožnost plošného zamezení padělání těchto kupónů.

ZeZnám reagoval na výše uvedené nedostatky tím, že zavedl systém evidence časového zpoplatnění. Čímž neznemožnil úhradu zpoplatnění časového poplatku na místech určených Státním fondem dopravní infrastruktury (dále jen „**SFDI**“), jako tomu bylo v předchozím případě, ale pouze opustil systém fyzických „dálničních známek“ a umožnil úhradu časového poplatku i bezhotovostně na bankovní účet SFDI. Údaj o úhradě časového poplatku bude následně, ať už byla provedena hotovostně nebo bezhotovostně, zanesen do evidence vozidel v systému časového zpoplatnění u konkrétního vozidla vedle dalších údajů, jako je registrační značka vozidla, stát jeho registrace, údaj o pohonné hmotě apod.[221] Evidence vozidel v systému časového zpoplatnění je informačním systémem veřejné správy a spravuje ho SFDI, kterému mimo jiné plyne povinnost umožnit způsobem umožňující dálkový přístup zjišťovat údaje o uhrazení, případně osvobození od uhrazení časového poplatku.

„Současné technologie umožňují ztotožnit vozidlo přímo při jízdě po zpoplatněné pozemní komunikaci, a to prostřednictvím státní poznávací značky jako jednoznačného identifikátoru vozidla. Úhradu časového poplatku lze proto provádět přímo pro konkrétní vozidlo

[218] Ustanovení § 21 a násl. ZoPozKom účinné před 1. lednem 2021
[219] Důvodová zpráva ZeZnám
[220] Ibid.
[221] Ustanovení § 21a odst. 4 ZoPozKom

identifikované jeho státní poznávací značkou, přičemž tato úhrada bude zaznamenána v evidenci, která bude v této souvislosti zřízena. V provozu na zpoplatněných pozemních komunikacích pak bude možné prostřednictvím videodetekce porovnávat údaje o projíždějících vozidlech s údaji obsaženými v evidenci, kontrolovat vozidla, o kterých lze předpokládat, že nemají uhrazen časový poplatek a v případě zjištění užití zpoplatněné pozemní komunikace bez úhrady časového poplatku sankcionovat porušení zákonné povinnosti.“[222]

2.9. Právo na využívání eGovernmentu

Jak jsem již uvedl v kapitole věnované právu na digitální služby, ZPDS byl přelomovým předpisem z toho důvodu, že jako jeden z prvních v oblasti „práva eGovernmentu“ přesně vymezil katalog veřejných subjektivních práv s touto oblastí práva související a korespondující povinnosti veřejných právních subjektů. Veřejné subjektivní právo definuje D. Hendrych v právnickém slovníku jako „*oprávnění, kterým normy veřejného práva umožňují občanu, aby mohl uplatnit jako svůj právní nárok u státu nebo jiného nositele veřejné moci provedení nebo zdržení se nějakého úkonu*.“[223] Kromě zmíněného katalogu lze dohledat konkrétní veřejná subjektivní práva i v případech, kdy prostřednictvím žádosti mohou subjekty získat například údaje z té které evidence[224], mohou za splnění podmínek získat pověření k provádění akreditace nebo atestace v oblasti informačních systémů[225] nebo například mohou zažádat o zřízení datové schránky, nevztahuje-li se na ně povinné zřízení datové schránky.[226]

Právní úprava eGovernmentu má v tomto ohledu poněkud specifický charakter. Převážnou většinou obsahu dílčích předpisů je nastavení právního rámce pro existenci celé řady technologických institutů od informačních systémů po datové schránky. Právní úprava jsou však velice zjednodušeně a nadneseně „pouhá“ slova, kterým jsme se ve společenské smlouvě rozhodli svěřit velkou váhu. Tato slova nezajistí, že budou právem předpokládané informační systémy skutečně funkční a že budou splňovat funkce, za které se zákonodárce, respektive právo jako takové, zaručilo. Tyto právní normy eGovernmentu tedy nemůžou fungovat samy o

[222] Důvodová zpráva ZeZnám
[223] HENDRYCH, Dušan. [Právo veřejné subjektivní]. In: HENDRYCH, Dušan a kol, op. cit. sub. 20
[224] Srovnání § 58 a násl. ZoZR
[225] Srovnání § 6 a násl. ZoISVS
[226] Např. Datové schránky některých právnických osob, ale od roku 2023 i datové schránky fyzických podnikajících osob a fyzických osob, které použily kvalifikovaný prostředek elektronické identifikace.

sobě a nezajistí, že bude bez dalšího naplněn jejich objektivní cíl, tedy uvedení konkrétního projektu tzv. „v život“. K tomu je zapotřebí i sekundární činnost odpovědných subjektů.

Uvedené si lze demonstrovat na příkladu. ZoISVS sice vytváří právní rámec, kterým umožní existenci informačních systémů veřejné správy, ale nezajistí všechny technologické aspekty toho, že informační systémy budou splňovat svoje funkce. ZoEÚAK sám o sobě nezajistí uvedení projektu v život, tedy zajištění technické infrastruktury toho, že budou datové schránky zabezpečené a tak dále. Obdobně jako ZoPozKom také nezajistí, že budou pozemní komunikace opravené a bezpečné, pouze vytváří předpoklad toho, že něco existuje a je pak už na dalších úkonech zodpovědných osob, zda tento „předpoklad“ převedou do skutečnosti.

Pro naplnění právního rámce musí vyvíjet jednotlivé gesce státu úsilí i nad rámec práva. Tím se však nezajistí kompletní splnění povinností státu v podobě realizace institutů eGovernmentu. Kromě samotné realizace a „spuštění“ toho kterého institutu („projektu“) je na odpovědnosti státu i zajištění operability daných systémů a bezodkladného řešení případných systémových a jiných vad.

Dle práva je správcem informačních systémů a jiných systémů zajišťující funkčnost dalších nástrojů eGovernmentu vždy některý z orgánů veřejné správy. Je pak na uvážení zodpovědných osob v rámci orgánu veřejné správy, zda má dostatečné pracovní, odborné a jiné kapacity na to, zajistit funkčnost toho kterého systému nebo zda využijí spolupráci se soukromoprávními subjekty stojícími na okraji či vně veřejné správy. Jedním z takových subjektů stojící na okraji veřejné správy je např. státní podnik Národní agentura pro komunikační a informační technologie založen zakládací listinu Ministerstva vnitra dne 21. ledna 2016 (dále jen „**NAKIT**“).[227]

NAKIT zajišťuje mimo jiné komunikační a informační služby pro výkon veřejné správy. Vytváří vyžadovanou infrastrukturu a zajištuje její zabezpečení proti kybernetickým hrozbám.[228] Kromě podobných státních podniků může samozřejmě orgán veřejné správy hledat cestu formou zadávání veřejné zakázky podle příslušného právního předpisu pro realizaci projektů včetně budování infrastruktur apod. Jak jsem již zmínil, spolupráce se soukromým

[227] Statut státního podniku Národní agentura pro komunikační a informační technologie, s.p., IČO 047 67 543, zapsaného do obchodního rejstříku u Městského soudu v Praze v oddíle A, vložka 77322 ze dne 1. února 2016
[228] NÁRODNÍ AGENTURA PRO KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE. Úvodní stránka. *Národní agentura pro komunikační a informační technologie* [online]. [cit. dne 2022-05-05]. Dostupné z: https://nakit.cz

sektorem je podle zjištění Evropské komise klíčová pro budování eGovernmentu, jelikož se prokazuje, že orgány veřejné správy nemají vždy dostačující kapacitu, know-how atd.

Co se stane, pokud stát nezajistí (svépomocí nebo s pomocí soukromoprávních subjektů) realizaci projektů eGovernmentu? V rámci právní úpravy eGovernmentu zákonodárce stanovuje jasné povinnosti, které stát musí splnit, přičemž zároveň adresáti výkonu legitimně očekávají, že je splní. Tato práva by se v teorii dala nazvat souhrnným názvem jako *právo na využívání eGovernmentu*, kterému koresponduje pro stát, resp. pro jeho příslušné orgány *povinnost realizovat eGovernment.* Pokládám si však otázku, zda skupina práv zastřešená *právem na využívání eGovernmentu* vůbec existuje a zda se jedná o veřejné subjektivní právo adresátů veřejné správy odrážející objektivní povinnost státu *realizovat* své právním předpisem uložené povinnosti?

Nejprve považuji za nutné definovat si samotnou podstatu (veřejného) subjektivního práva. Jak uvádí A. Mácha, v rámci srovnání s teorií subjektivního práva podle V. Knappa a A. Gerlocha dospěl k tomu, že „*Subjektivní právo má určité složky či roviny. Obvykle se uvádějí tyto tři složky subjektivního práva:*

1) Právo (někdy označováno jako možnost) chovat se určitým způsobem v mezích zákona.

2) Právo (možnost) požadovat odpovídající chování od jiného.

3) Právo (možnost) požadovat právní ochranu“[229]

Rozlišení „soukromého“ a „veřejného“ subjektivního práva pak závisí na právních normách, ze kterých to které právo vyplývá. „*Na veřejné subjektivní právo lze hledět jako na oprávnění jednotlivce vyplývající z norem veřejného práva, právního řádu, na zákonné postupy veřejné moci vůči němu.“*[230] Pokud tedy zkoumáme existenci konkrétního subjektivního práva v předpisech upravující eGovernment, bude se, i s ohledem na klíčovou roli veřejné správy v této oblasti, jednat o potenciální subjektivní práva veřejná.

---

[229] Srovnání KNAPP, V. *Teorie práva*. Praha: C. H. Beck, 1995, str. 194, ISBN 80-7179-028-1. GERLOCH, A. *Teorie práva*. 6. vydání. Plzeň: Aleš Čeněk, 2013, str. 151, ISBN 978-80-7380-454-1 a MÁCHA, Aleš, 2017. *Veřejné užívání a vlastnické právo.* Olomouc. Disertační práce. Univerzita Palackého v Olomouci, Právnická fakulta. Vedoucí práce TOMOSZKOVÁ, Veronika

[230] KOPECKÝ, Martin, op. cit. sub. 20, str. 41

Pro zodpovězení výše uvedené otázky si uvedené znaky veřejného subjektivního práva dovolím rozebrat na praktickém příkladu, a to na zajištění realizace základních registrů státem. Hypotéza tedy zní, zda zajištění možnosti využívání základních registrů státem je jedno z veřejných subjektivních práv na využívání eGovernmentu tzv. právo na využívání základních registrů s korespondující povinností státu realizovat eGovernment, respektive realizovat základní registry?

Každý adresát může za určitých okolností a splnění určitých náležitostí žádat o výpis z některého základních registrů, může požadovat, aby veřejná správy využívala údaje zapsané v základních registrech, a dokonce může mít přístup do některých ze základních registrů (např. RÚIAN). Výše uvedené funckionality by nebyl adresát schopný vykonávat bez toho, aby byly základní registry reálně fungující informační systémy veřejné správy, jak vyžaduje ZoISVS. Jedná se však o dílčí práva na určité chování (činit jednotlivé úkony) nebo na jedno právo jako celek? Domnívám se, že veřejné subjektivní právo provést dílčí úkon (např. činit výpis ze základního registru) nelze hodnotit izolovaně. Toto právo úzce souvisí se splněním povinnosti státu realizovat právem předpokládané projekty. Pokud stát projekt nezrealizuje, nebude se moc adresát chovat určitým způsobem (tj. činit jakékoliv úkony v souvislosti se základními registry). Pokud bych přijmul opačný pohled, relativizoval bych tím legitimní očekávání, že stát bude dodržovat právo a plnit svoje povinnosti. Z tohoto důvodu jsem přesvědčen, že právo na dílčí úkon a právo legitimně očekávat realizaci projektu základních registrů jsou dvě strany stejné mince, kterou je právo na využívání základních registrů (jako jedno z práv na využívání eGovernmentu). Oprávnění činit jednotlivé úkony za využití základních registrů, tedy *právo chovat se určitým způsobem v mezích zákona* (první definiční znak subjektivního práva) je dle mého názoru splněno jako nedílná část veřejného subjektivního práva na využívání základních registrů.

Současně každý adresát veřejné správy očekává, že stát splní svou povinnost a zřídí základní registry včetně všech zákonem předpokládaných funckionalit. Adresátům těchto norem tedy náleží *právo požadovat odpovídající chování od jiného*, a to od státu. Právo na využívání základních registrů tedy splňuje i druhý definiční znak.

Dle mého názoru je tedy právo na využívání základních registrů oprávnění adresátů využívat všech právních i faktických funkcionalit základních registrů a současně požadovat určité chování ze strany státu (tj. realizace základních registrů), čímž se naplní první i druhý definiční znak (veřejného) subjektivního práva. Toto ostatně potvrzuje i M. Kopecký, který uvádí, že „*veřejné subjektivní právo, zkoumané v rámci správního práva, předpokládá, aby právní norma*

opravňovala nebo zavazovala veřejnou správu k určitému chování, a aby daná pravidla, ne třeba výlučně, ale minimálně také byla v zájmu jednotlivce, kterému takové právo svědčí.“[231]

Že jsou orgány veřejné správy zavázány k určitému chování, tedy ke splnění povinnosti realizovat konkrétní projekt eGovernmentu už plyne ze samé podstaty toho kterého předpisu. Pro vyloučení všech pochybností lze současně nalézt i závěrečná a přechodná ustanovení ZoZR, které výslovně stanovují povinnost dotčených orgánů zajistit realizaci základních registrů. ZoZR uvádí: *„Registr obyvatel se vytvoří (…), a to nejpozději do 2 let (…)“*[232]. Ostatně obdobná ustanovení lze najít i v dalších předpisech právní úpravy eGovernmentu, a to např. v ZoISVS *„Informační systém (…) musí orgány veřejné správy nejpozději do 2 let ode dne účinnosti tohoto zákona uvést do souladu s tímto zákonem nebo ukončit jejich činnost.“*[233] nebo ZPDS *„Ohlašovatelé agend zajistí digitalizaci těchto úkonů“*[234] a *„Existuje-li úkon, který není obsažen v katalogu služeb a jehož povaha to nevylučuje, příslušný orgán veřejné moci jej po uplynutí 5 let od účinnosti tohoto zákona poskytuje též jako digitální službu nebo jej umožňuje provádět též jako digitální úkon, nestanoví-li jiný zákon jinak“*[235]. Zájem jednotlivce lze pak pozorovat na výše uvedených funkcionalitách základních registrů.

Pro uzavření analýzy práva na využívání základních registrů je zapotřebí rozebrat, zda právo splňuje i třetí definiční znak subjektivního práva podle V. Knappa a A. Gerlocha. Tedy zda je takové právo uplatnitelné a zda existují *prostředky jeho právní ochrany*.

Obecně řečeno porušení veřejného subjektivního práva v závislosti na konkrétním porušení může naplňovat znaky jak nezákonného rozhodnutí (např. vydání nezákonného rozhodnutí o zamítnutí pověření k provádění akreditace[236]), nečinnosti (např. překročení lhůty pro zřízení datové schránky na základě podané žádosti[237]) nebo nezákonného zásahu, pokynu nebo donucení (např. již zmíněné nezřízení datové schránky). Ústavní soud se zabýval i otázkou, jakou povahu má zápis nebo výmaz určitého práva z informačního systému, přičemž poznamenal, že „*změna zápisu údaje o způsobu využití domu v RÚIAN podle ZoZR, představuje jednorázový zásah s trvajícími účinky a při zmeškání objektivní či subjektivní lhůty pro podání*

[231] KOPECKÝ, Martin, op. cit. sub. 20, str. 41
[232] Ustanovení § 64 odst. 1 ZoZR
[233] Ustanovení § 10 odst. 1 ZoISVS
[234] Ustanovení § 14 odst. 4 ZPDS
[235] Ustanovení § 14 odst. 5 ZPDS
[236] Ustanovení § 6 odst. 3 ZoISVS
[237] Ustanovení § 3 odst. 1 ZoEÚAK

žaloby podle § 82 a násl. SŘS nelze argumentovat tím, že důsledky tvrzeného zásahu nadále trvají.“[238] Jinými slovy, pokud by v takovém případě došlo k neoprávněné změně zapsaných údajů, jednalo by se o nezákonný zásah podle předpisů správního práva. Pro efektivní obranu je však důležité současně dodržení procesních lhůt, které právní předpisy k tomu kterému úkonu přiřazují.

Právní úprava eGovernmentu se týká výhradně norem veřejného práva, konkrétněji správního práva. Logicky je tedy nutné rozebrat prostředky obrany proti výše uvedeným porušením veřejného subjektivního práva, které normy správního práva nabízejí. Z důvodu absence správního řízení, jelikož se jedná výhradně o splnění povinnosti státu, lze vyřazovací metodou vyloučit prostředky obrany ve správním řízení jako jsou ochrana před nečinností (před nevydáním rozhodnutí), odvolací řízení, přezkumné řízení případně obnova řízení. Kde není správní řízení není ani vydání rozhodnutí, a tudíž ani obrana proti takovému rozhodnutí. Proto lze vyloučit i obranu před nezákonným rozhodnutím podle § 65 a násl. SŘS, logicky i žalobu proti nečinnosti, která navazuje na obranu před nečinností ve správním řízení. Poněkud méně zřejmé je to pak v případě obrany před nezákonným zásahem, pokynem nebo donucením.[239] „*Zásahová žaloba* (žaloba podle § 82 a násl. SŘS pozn. autora) *tak chrání proti jakýmkoli aktům či úkonům veřejné správy směřujícím proti jednotlivci, které jsou způsobilé zasáhnout sféru jeho práv a povinností a které nejsou pouhými procesními úkony technicky zajišťujícími průběh řízení.*“[240]

Zásah ve smyslu SŘS má tedy tři vlastnosti. 1) Je to projev vůle vykonavatele veřejné správy (i opomenutí učinit projev vůle), 2) směřuje proti jednotlivci a 3) je způsobilý zasáhnout sféru práv a povinností. Ačkoliv by v případě nesplnění povinnosti ve formě zajištění realizace základních registrů toto porušení povinnosti ve formě opomenutí učinit úkon veřejné správy zasáhnul sféru práv a povinností, není naměřen proti jednotlivci, ale má plošný účinek vůči všem potenciálním uživatelům základních registrů. Proto se domnívám, že se nebude jednat ani o zásah ve smyslu SŘS.

V úvahu tedy přichází poslední relevantní možnost obrany veřejného subjektivního práva, a to prostřednictvím ZoOdpŠk. Ponechávám stranou možnost odpovědnosti státu za rozhodnutí

[238] Usnesení Ústavního soudu ze dne 14. ledna 2020 sp. zn. I. ÚS 3534/19
[239] Ustanovení § 82 a násl. SŘS
[240] VOJTEK, Petr. § 13 [Nesprávný úřední postup státu]. In: VOJTEK, Petr, BIČÁK, Vít. *Odpovědnost za škodu při výkonu veřejné moci*. 4. vydání. Praha: C. H. Beck, 2017, marg. č. 27. ISBN 978-80-7400-670-8

podle § 5 písm. a) ZoOdpŠk, kde, jak jsem již uvedl výše, se nejedná o rozhodnutí ve správním, ani jiném řízení. Druhou možností odpovědnosti za škodu je u státu odpovědnost za tzv. nesprávný úřední postup.[241] Nesprávný úřední postup není přesně zákonem definovaný pojem, ZoOdpŠk stanovuje, že je to „*také porušení povinnosti učinit úkon nebo vydat rozhodnutí v zákonem stanovené lhůtě (…)*“[242] Jeho konkrétní podobu tak do jisté míry stanovuje kauzálně judikaturu či odborná literatura. *„Nesprávným je podle odborné literatury i ustálené judikatury takový úřední postup, který buď porušil normu či určitý daný pořádek postupu, přičemž nesprávným postupem lze rozumět i nečinnost příslušného orgánu, který měl jednat či rozhodnout, případně učinit jiné opatření.*“[243]

Ustanovení § 13 odst. 2 ZoOdpŠk dále stanovuje, že právo na náhradu škody má pouze ten, jemuž byla nesprávným úředním postupem způsobena škoda. „*Není významné, zda poškozený byl účastníkem řízení, v jehož rámci k nesprávnému úřednímu postupu případně došlo, nýbrž podstatné je pouze to, zda poškozenému vznikla škoda (majetková újma vyjádřitelná v penězích), která je v příčinné souvislosti s uvedeným postupem, tedy zda je nesprávný postup orgánu státu se vznikem škody ve vztahu příčiny a následku. Jinými slovy stát odpovídá za škodu (vznikla-li v příčinné souvislosti s nesprávným úředním postupem) i jiným osobám než účastníkům řízení, v jehož rámci k nesprávnému úřednímu postupu došlo*.“

Pokud by tedy skutečně stát nezajistil funkčnost základních registrů, porušil by tím svou povinnost stanovenou ZoZR, čímž by naplnil význam „nesprávného úředního postupu“ a dotčený subjekt, byla-li mu tím způsobena škoda, může uplatnit svou obranu tím, že bude po státu požadovat náhradu vzniklé škody.

Dalšími prostředky ochrany při porušování zmíněných povinností orgánů veřejné moci může být i např. úprava zákona č. 255/2012 Sb., o kontrole (dále jen „**KontrolŘ**“). „*Předmětem kontroly a jejím základním znakem, jak již vyplývá z § 2, je zjišťování plnění povinností, které vyplývají z jiných právních předpisů nebo které jí byly uloženy na základě těchto předpisů. Jedná se tedy o zjišťování skutečného skutkového stavu a jeho porovnání se stavem právním předpisem předpokládaným.*“[244] Nadřízený kontrolní orgán je současně v souladu

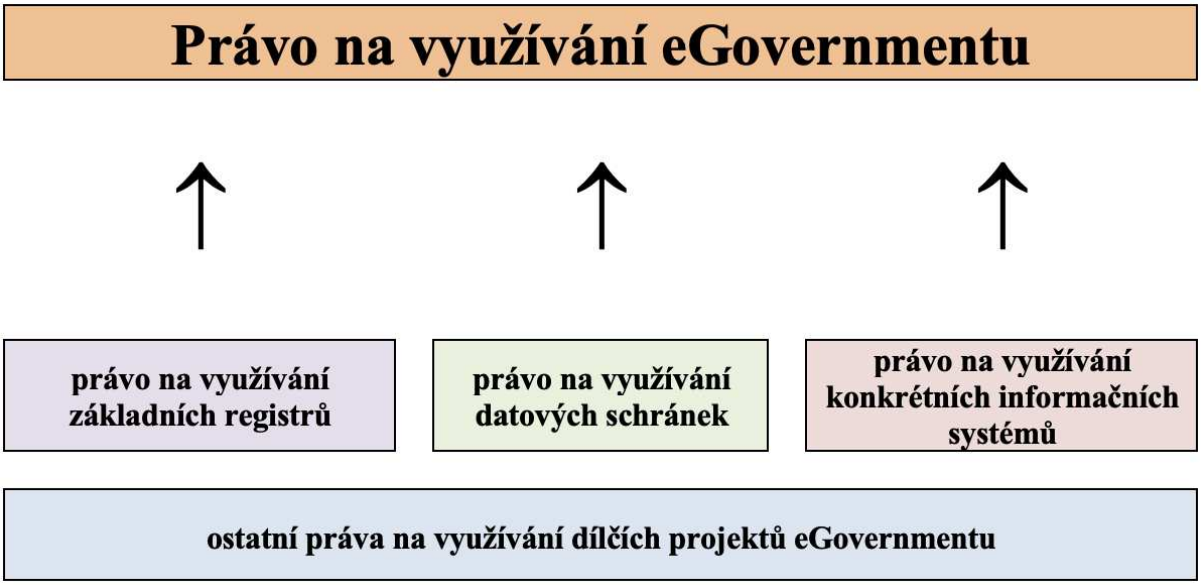
[241] Ustanovení § 5 písm. b) ZoOdpŠk
[242] Ustanovení § 13 odst. 1 ZoOdpŠk
[243] Rozsudek Nejvyššího soudu sp. zn. 25 Cdo 2120/2000 ze dne 22.srpna 2002
[244] VETEŠNÍK, Pavel. § 2 [Kontrola]. In: JEMELKA, Luboš, VETEŠNÍK, Pavel, LIBOSVÁR, Ondřej. *Zákon o kontrole.* 2. vydání. Praha: C. H. Beck, 2021, str. 30. ISBN 978-80-7400-840-5

s ustanovením § 19 KontrolŘ oprávněn ukládat opatření k odstranění nebo prevenci nedostatků. KontrolŘ ovšem upravuje situace, kdy kontrolní orgán postupuje z úřední moci, tedy ve veřejném zájmu, a nikoliv v rámci zájmu jednotlivce. KontrolŘ tedy toliko neposkytuje ochranu individuálním zájmům, o kterých jsem psal výše. Jedná se však o úpravu, která v bude pravděpodobně v praxi hojně využívána, jelikož se domnívám, že realizace zákonem předpokládaných projektů je beze všeho ve veřejném zájmu.

S výjimkou orgánů ve smyslu § 2 odst. 9 zákona č. 349/1999 Sb., o Veřejném ochránci práv (dále jen „**ZoVOP**“) může Veřejný ochránce práv osoby též ukládat opatření k nápravě, zjistí-li jednání, které je v rozporu s právem a které se týká orgánů veřejné správy. Na rozdíl od KontrolŘ, Veřejný ochránce práv chrání i individuální právní zájmy a může jednat jak na základě podnětu, tak i z vlastní iniciativy.[245] Nicméně postup podle KontrolŘ nebo postup veřejného ochránce práv nevylučuje, že nemůže existovat paralelní právní titul pro uplatnění nároku na náhradu škody vzniklou nesprávným úředním postupem apod.

S ohledem na výše uvedené je tedy zřejmé, že se naplňuje v některých případech i třetí část podstaty subjektivního práva, a to právo požadovat právní ochranu před (ne)realizací základních registrů. Domnívám se tedy, že existuje veřejné subjektivní právo adresátů veřejné správy na využívání eGovernmentu, které se skládá z řady dílčích práv, mezi kterými je i výše podrobně rozebrané právo na využívání základních registrů. Obdobně tak lze uvažovat například i o právu na využívání systému datových schránek, autorizované konverze nebo propojených informačních systémů veřejné správy. Všechna tyto práva pak zastřešuje jedno právo, právo na využívání eGovernmentu. Podstatné je, aby existence dílčího práva na využívání konkrétního projektu vždy mělo oporu v právní úpravě, která toto právo předpokládá. Vztah těchto práv lze vyjádřit následovně (viz obrázek č. 1).

[245] Ustanovení § 9 ZoVOP



Obrázek č. 1 *– Schéma vztahu práv na využívání dílčích projektů eGovernmentu a zastřešujícího práva na využívání eGovernmentu, autor textu*

Na závěr je nutné dodat, že veřejná správa odpovídá i za nesprávné nebo nezákonné jednání v oblastech, které s eGovernmentem souvisí. Velkou částí je zejména odpovědnost v souvislosti se zpracováváním osobních údajů. Praxe též ukazuje, že zákonodárce vychází v této souvislosti státu vstříc tím, že odloží účinnost konkrétního předpisu, který realizaci konkrétního projektu předpokládá. Vzorovým příkladem je opakované odkládání účinnosti

ZoSbírce, jehož účinnost se nejprve posunula z 1. ledna 2020 na 1. leden 2022 a následně na 1. leden 2023.[246]

[246] Srovnání ZoSbírce se zákonem č. 277/2019 Sb., a zákonem č. 261/2019 Sb.

3. Evropský a zahraniční přístup k právní úpravě eGovernmentu

Fenomén eGovernmentu logicky přesahuje hranice České republiky, z čehož plyne i jeho nadstátní význam. Důležitou roli sehrávají především instituce Evropské unie. Například Evropská komise sleduje prostřednictvím indexu digitální ekonomiky a společnosti neboli indexu DESI (dále jen „**DESI**“) pokrok členských států v oblasti digitalizace. Jednou ze zkoumaných kapitol v rámci DESI je právě digitalizace veřejné správy, tedy obsahově podobné významu eGovernmentu.[247] Česká Informační koncepce stanovila jako jeden z indikátorů splnění vrcholného cíle koncepce právě výslednou pozici České republiky v žebříčku dle DESI.[248] Česká republika byla na škále DESI za rok 2021 umístěna na 18. místě a oproti roku 2020 se propadla o jedno místo. Nejlepšího výsledku (15. místo) zaujímá v oblasti integrace digitálních technologií a lidského kapitálu, a naopak nejhorší je v oblasti konektivity (22. místo). V oblasti digitálních veřejných služeb, tedy zjednodušeně řečeno v úrovni eGovernmentu, je pak Česká republika na 20. místě, přičemž je o deset procentních bodů pozadu za celoevropským průměrem.[249] Kvalita digitálních veřejných služeb je hodnocena podle 5 indikátorů:

1) počet subjektů využívajících internet pro interakci s veřejnou správou („indikátor eGovernment uživatelů“),
2) množství dat, které obsahují „předvyplněné internetové formuláře“[250] služeb veřejné správy („indikátor předvyplněných formulářů“),
3) poměr služeb veřejné správy, které lze učinit prostřednictvím internetu v klíčových životních událostech jako je narození dítěte, změna trvalého pobytu apod. („indikátor digitálních veřejných služeb pro občany“),
4) poměr služeb veřejné správy určených pro podnikající právnické i fyzické osoby, které lze učinit elektronicky a které jsou určené k zahájení podnikatelské činnosti a provádění běžných podnikatelských úkonů („indikátor digitálních veřejných služeb pro podnikatele“), a

[247] EVROPSKÁ KOMISE. *Digital Economy and Society Indes (DESI) 2021.* Thematic chapters. Brusel: Evropská komise, 2021 [online]. [cit. 2021-25-11]. str. 66-77. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80563
[248] DZURILLA, Vladimír, et al, op. cit. sub. 19, str. 2
[249] EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Česko. Brusel: Evropská komise, 2021 [online]. [cit. 2021-25-11]. str. 3-5. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80581
[250] Formuláře, určené k úkonům směrem k veřejné správě, které při prokázání totožnosti automaticky vyplní data, které má příslušný orgán veřejné moci k dispozici, respektive se kterými má oprávnění disponovat.

5) indikátor složený z využívaných otevřených dat, jejich odhadovaného politického a socioekonomického dopadu při jejich využívání a charakteristika národní portálu operujícího s takovými daty („indikátor open data“).[251]

Evropská komise hraje dále důležitou roli i coby navrhovatel evropských předpisů, které tvoří významnou část právní úpravy eGovernmentu v členských státech jako je například eIDAS nebo jeho chystaná novelizace.

Kromě DESI je jedním z dalších ukazatelů pokročilosti eGovernmentu v jednotlivých evropských státech tzv. eGovernment Benchmark, který sleduje pokrok v digitalizaci veřejné správy ve všech 27 členských státech EU a v dalších 9 „přidružených státech“, mezi kterými je Island, Norsko, Švýcarsko, Velká Británie, Albánie, Černá Hora, Severní Makedonie, Srbsko a Turecko (dále jen „**Benchmark**“).[252]

Benchmark vyhodnocuje a srovnává pokroky jednotlivých států na základě dvou základních kritérií: penetrace a digitalizace. Zatímco kritérium penetrace zachycuje přijetí a využívání online služeb eGovernmentu, kritérium digitalizace monitoruje úroveň digitalizace vnitřních a vnějších procesů veřejné správy, které dále rozděluje na čtyři základní referenční dimenze:

uživatelská orientace, která je ukazatelem míry poskytovaných služeb online, přívětivosti pro mobilní zařízení, online podpory a mechanismů zpětné vazby;

transparentnost, která indikuje, v jaké míře podává veřejná správa pravdivé, srozumitelné a dohledatelné informace o způsobu a využití nabízených služeb a současně informace o zpracování osobních dat a odpovědnosti a výkonu veřejných organizací;

přeshraniční „mobilita“, která udává, do jaké míry mohou uživatelé využívat služby z jiných členských států; a

[251] EVROPSKÁ KOMISE. *Digital Economy and Society Index (DESI) 2021*. DESI methodological note. Brusel: Evropská komise, 2021 *methodological note. Evropská Komise;* [online]. [cit. 2021-25-11]. str. 8. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80560

[252] Aktuální zpráva Benchmarku je pak EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets. eGovernment benchmark 2021.* Entering a new digital government era. Brusel: Evropská komise, 2021 [online]. Dostupné z: DOI: 10.2759/485079

klíčové „nástroje“, které označují rozsah technických a organizačních předpokladů pro využívání služeb eGovernmentu jako jsou služby elektronické identifikace, digitální doručování nebo elektronická dokumentace.[253]

V oblasti digitalizace podle Benchmarku jednoznačně dominuje Malta s průměrným skóre ve výši 96 % ve všech 4 výše zmíněných referenčních dimenzích, avšak v oblasti penetrace s průměrným skóre 63 % zaostává za průměrem členských států o čtyři procentní body a celkově se umístila v třídě tzv. „postradatelných eGovernmentů“.[254] V oblasti digitalizace je na druhém místě Estonsko s průměrným skóre 92 % v oblasti digitalizace, ovšem v oblasti penetrace se umístilo na čtvrtém místě s průměrným skóre 89 % a celkově je“ s ohledem na ostatní státy na pomyslné špičce „nejlepších“ eGovernmentů.

3.1. Evropská unie

Elektronizace veřejné správy, jak jsem již zmínil, není jenom trendem právní úpravy konkrétních států. Evropská unie začíná více zasahovat do podoby elektronizace jednotlivých členských států za účelem harmonizace základní úrovně digitalizace s cílem zajistit vzájemnou interoperabilitu dílčích „eGovernmentů“. Již zmíněné eIDAS umožnilo všem členským státům poskytovat a přijímat služby elektronické identifikace a služby vytvářející důvěru za stejných podmínek ve všech členských státech. Nutno dodat, že v některých členských státech se jednalo o pouhé potvrzení právního rámce, které konkrétní státy dobrovolně přijaly. Příkladem může být existence elektronického podpisu a jiných služeb vytvářejících důvěru v České republice nebo elektronická identifikace v Estonsku před přijetím eIDAS.

3.1.1. Evropská digitální dekáda

Na začátku března roku 2021 předložila Evropská komise svou strategii v oblasti digitální transformace Evropské unie a jejích členských států. Tato strategie přijatá v rámci Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Digitální kompas 2030: Evropské pojetí digitální dekády, ze dne 9. března 2021, COM(2021), 118 final (dále jen „**Evropský kompas**“) si stanovila za cíl vstoupit do nové dekády (do roku 2030) se splněnými cíli v konkrétních „směrech“, respektive dimenzích

[253] EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Method Paper 2020-2023. eGovernment benchmark 2021*. Brusel: Evropská komise, 2021. str. 9. ISBN 978-92-76-36362-0
[254] EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets,* op. cit. sub.91 str. 71-74

pomyslného kompasu. Jedná o dimenze *digitálních dovednostní* (obyvatelstvo s digitálními dovednostmi a vysoce kvalifikovaní odborníci v oblasti digitálních technologií), *digitální infrastruktury* (bezpečné, výkonné a udržitelné digitální infrastruktury), *digitálních podniků* (digitální transformace podniků) a *digitálních veřejných služeb* (dimenze eGovernmentu).[255]

V rámci dovednostní si Evropská komise stanovila cíl mít až 20 milionů specialistů v oblasti ICT ze současných cca 8 milionů (stav k roku 2019) se zachováním rovnosti mužů a žen a docílení základních digitálních dovedností u alespoň 80 % obyvatelstva Evropské unie ve věku 16-79 let ze současných cca 58 % (stav k roku 2020).[256]

V oblasti digitální infrastruktury byl stanoven cíl pokrytí všech evropských domácnostní gigabitovou sítí a všechny osídlené oblasti pokrytí sítí 5G. Dále pak dosažení výroby špičkových a udržitelných polovodičů v poměru alespoň 20 % vůči celosvětové produkci, nasazení minimálně 10 000 klimaticky neutrálních a vysoce zabezpečených uzlů na okraji sítě a do roku 2025 získat první počítač s kvantovou akcelerací, což umožní přední postavení Evropské unie v oblasti kvantových kapacit v roce 2030.[257]

Digitální transformace podniků počítá se zapojením minimálně 75 % podniků do využívání cloudových služeb, dat velkého objemu a umělé inteligence, s dosažením alespoň základní úrovně „digitální intenzity“[258] u 90 % středních a malých podniků a zdvojnásobení počtu „jednorožců“[259].[260]

---

[255] EVROPSKÁ KOMISE. Evropská digitální dekáda: digitální cíle pro rok 2030. *Evropská komise* [online]. [cit. 2021-11-11]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_cs

[256] Příloha ke Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Digitální kompas 2030: Evropské pojetí digitální dekády, COM(2021), 118 final

[257] Ibid.

[258] „Index digitální intenzity (DII, Digital Intensity Index) je mikroekonomický index, který na úrovni podniků měří dostupnost 12 různých digitálních technologií: internet alespoň pro 50 % zaměstnanců, možnost obrátit se na specialisty v oboru ICT, rychlé širokopásmové připojení (30 Mbit/s nebo rychlejší), zařízení s mobilním internetem alespoň pro 20 % zaměstnanců, internetové stránky, internetové stránky se sofistikovanými funkcemi, sociální média, platby za reklamu na internetu, nákup pokročilých cloudových služeb, zasílání elektronických faktur, podíl elektronického obchodu na celkovém obratu vyšší než 1 % a podíl internetového prodeje spotřebitelům (B2C) na celkovém internetovém prodeji vyšší než 10 %. Hodnota indexu se tedy pohybuje v rozpětí od 0 do 12. Uvedený seznam 12 ukazatelů se každoročně reviduje a zlepšuje s cílem držet krok s nejnovějšími technologiemi a politickými prioritami.“ (Ibid., poznámka pod čarou č. 9)

[259] „Jednorožci“ se zde rozumí tyto dva typy podniků: 1) zrealizovaní „jednorožci“, tj. společnosti založené po roce 1990, které uskutečnily primární emisi akcií (IPO) nebo obchodní prodej v objemu vyšším než 1 mld. USD, a 2) nezrealizovaní „jednorožci“, tj. společnosti, které byly oceněny alespoň na 1 mld. USD při svém posledním kole soukromého rizikového financování (tím se rozumí, že toto ocenění nebylo potvrzeno v sekundární transakci). V roce 2019 bylo v USA 703 „jednorožců“ a v Číně 206 „jednorožců““ (Ibid., poznámka pod čarou č. 30)

[260] Ibid.

Hlavní a nejzásadnější oblastí pro rozvoj českého eGovernmentu je čtvrtá dimenze – digitalizace veřejných služeb. Evropský kompas cílí k absolutní digitalizaci, respektive vytvoření online alternativy klíčových veřejných služeb do roku 2030. Jen pro srovnání, pokud nedojde k posunutí účinnosti ZPDS, měl by být víceméně podobný cíl naplněn českými orgány veřejné správy do roku 2025. Druhým a třetím cílem v této oblasti je absolutní zpřístupnění elektronické zdravotnické dokumentace pro občany a dosažení alespoň 80 % všech občanů Evropské unie využívajících služby digitální identifikace (respektive elektronické identifikace pozn. autora).[261]

Pomyslným středobodem Evropského kompasu je pak institut, který Evropská komise nazývá jako „digitální občanství". Předpisy primárního i sekundárního práva Evropské unie již dnes akcentují některé digitální zásady jako je bezpečné a otevřené digitální prostředí orientované na člověka, ale i ústavní, potažmo základní práva Evropské unie na soukromí, ochranu osobních údajů a svobodu projevu nebo práva dítěte a spotřebitelská práva. Na základě článku 4 Evropského kompasu navrhuje Evropská komise stanovit ucelený soubor digitálních práv a zásad, které budou tvoři tzv. „digitální občanství".[262] Tyto digitální práva a zásady byly přijaty v rámci Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výrobu regionů o Evropském prohlášení o digitálních právech a zásadách pro digitální dekádu, ze dne 26. ledna 2022, COM(2022) 27 final (dále jen „**Evropské digitální zásady**"). Evropským digitálním zásadám se blíže věnuji v kapitole 3.1.5.

Na základě Evropského kompasu předložila Evropská komise dne 19. března 2021 návrh rozhodnutí Evropského parlamentu a Rady, kterým se zavádí politický program 2030 „Cesta k digitální dekádě", ze dne 15. září 2021, COM(2021), 574 final (dále jen „**Cesta k digitální dekádě**").

Cesta k digitální dekádě nastavuje pravidelný každoroční mechanismus spolupráce mezi Evropskou komisí a členskými státy. Tento mechanismus tvoří:

1) monitorovací systém, který vychází z dat v rámci každoročního DESI. Díky tomu bude Evropská komise schopná pozorovat pokroky a splnění dílčích cílů jednotlivými členskými státy;[263]

[261] Ibid.
[262] Ibid.
[263] Článek 5 Cesty k digitální dekádě

2) zpráva o stavu digitální dekády, kterou vypracovává Evropská komise a předkládá ji Evropskému parlamentu a Radě Evropské unie, a ve které hodnotí pokrok Evropské unie ve vztahu k cílům vzešlých z Evropského kompasu (v rámci této zprávy může Evropská komise přijmout celou řadu doporučení, které by měly členské státy přijmout);[264]
3) národní strategické plány pro digitální dekádu, které vypracovávají členské státy, a ve kterých představí konkrétní politiky, opatření a trajektorie, díky kterým naplní cíle stanovené Evropským kompasem;[265]
4) každoroční kooperace mezi Evropskou komisí a členskými státy, díky které, prostřednictvím společného dialogu, budou řešit případné nedostatky v rámci naplňování dílčích cílů Evropského kompasu s ohledem na rozdílné kapacity členských států; výsledkem této kooperace mohou být společné závazky mezi Evropskou komisí a členským státem nebo státy, případně různá opatření nebo zrealizování multinárodních projektů;[266] a
5) rámec pro multinárodní projekty, díky kterým mohou členské státy využít sdílené kapacity pro realizaci projektů, které budou řešit zjištěné nedostatky, podpoří propojení, interoperabilitu a bezpečnost jednotného digitální trhu[267].[268]

Evropská komise na svých webových stránkách mimo jiné uvádí příklad potenciálního multinárodního projektu. Může se jednat o zavedení „*sítě bezpečnostních operačních středisek založených na umělé inteligenci, která by předvídala kybernetické útoky, odhalovala je a reagovala na ně*.“[269]

3.1.2. Digitální peněženka

Na začátku července roku 2021 vydala Evropská komise prohlášení, ve kterém oznámila záměr zřídit rámec pro tzv. digitální identitu pro všechny občany, obyvatele a podniky v Evropské unii. Právní rámec bude vycházet z návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014 (tj. eIDAS pozn. autora), pokud jde o zřízení rámce pro evropskou digitální identitu, COM(2021) 281 final (dále jen „**eIDAS II**“).

[264] Článek 6 Cesty k digitální dekádě
[265] Článek 7 Cesty k digitální dekádě
[266] Článek 8 Cesty k digitální dekádě
[267] Článek 12 a násl. Cesty k digitální dekádě.
[268] EVROPSKÁ KOMISE, op. cit. sub. 93
[269] Ibid.

Původně eIDAS zakotvilo právní rámec pro využívání a poskytování služeb elektronické identifikace. V závěrečných ustanovení eIDAS, konkrétně v článku 49, je stanoveno, že „*Do 1. července 2020 přezkoumá Komise uplatňování tohoto nařízení a podá zprávu Evropskému parlamentu a Radě. Komise zejména vyhodnotí, zda je s přihlédnutím ke zkušenostem s uplatňováním tohoto nařízení a k technologickému, tržnímu a právnímu vývoji vhodné upravit oblast působnosti tohoto nařízení nebo jeho konkrétní ustanovení, včetně článku 6, čl. 7 písm. f) a článků 34, 43, 44 a 45. Ke zprávě uvedené v prvním pododstavci se případně připojí legislativní návrhy*."[270]

Na základě tohoto článku provedla Evropská komise šetření, přičemž zjistila, že *„hlavním zjištěním hodnocení s ohledem na elektronickou identitu je, že eIDAS nedosáhlo svého potenciálu. Byl oznámen pouze omezený počet elektronických identifikací, čímž bylo omezeno pokrytí oznámených systémů elektronické identifikace na přibližně 59 % obyvatelstva EU. Přijímání oznámených elektronických identifikací na úrovni členských států i na úrovni poskytovatelů služeb je mimoto omezené. Rovněž se zdá, že pouze několik služeb přístupných prostřednictvím vnitrostátní elektronické identifikace je připojeno k vnitrostátní infrastruktuře eIDAS. Hodnotící studie také zjistila, že stávající oblast působnosti a zaměření eIDAS na systémy elektronické identifikace oznámené členskými státy EU a na umožnění přístupu k on-line veřejným službám se jeví jako příliš omezené a nedostatečné. Převážná většina potřeb v oblasti elektronické identity a dálkové autentizace zůstává v soukromém sektoru, zejména v oblastech, jako jsou bankovnictví, telekomunikace a provozovatelé platforem, od nichž zákon vyžaduje, aby ověřovali totožnost svých zákazníků. Přidaná hodnota nařízení eIDAS s ohledem na elektronickou identitu je omezena vzhledem k jeho nízkému pokrytí, přijímání a používání.“*[271]

Cílem eIDAS II je kromě reakce na výše uvedené nedostatky i poskytnutí zabezpečeného a důvěryhodného řešení elektronické, respektive digitální identity a s ní spojené další cílené sdílení údajů o totožnosti určené pro konkrétní poskytnutí požadované služby a ve výsledku i motivace subjektů k využívání těchto řešení.[272] Nová digitální identita, můžeme-li jí tak nazvat, umožňuje uživateli kromě elektronické identifikace sdílet pro konkrétní službu konkrétní údaje

[270] Ustanovení čl. 49 eIDAS
[271] Důvodová zpráva eIDAS II
[272] Důvodová zpráva eIDAS II

uložené v této nové digitální identitě. [273] Jedná se o údaje o totožnosti, ale i údaje o dílčích atributech nebo kvalifikaci daného subjektu jako je řidičské oprávnění, dosažené vzdělání, nebo bankovní účty.

Kromě výše uvedeného eIDAS II zakotvuje nový zásadní institut, tzv. evropskou digitální peněženku (dále jen „**Digi Peněženka**"). Digi Peněženka je dle definice v článku 1 odst. 3 písm. i) eIDAS II „*produkt a služba, které uživateli umožňují uchovávat údaje o totožnosti, pověření a atributy spojené s jeho totožností, poskytovat je na požádání spoléhajícím se stranám a používat je pro autentizaci, on-line i offline*."[274] Jinými slovy, uživatel bude moci díky této aplikaci dostupné např. na mobilních zařízeních provést svou identifikaci (a autentizaci), stejně jako prokázání celé škály atributů a kvalifikací (např. vzdělání, lékařské předpisy nebo očkování). Kromě toho Digi Peněženka umožní větší míru ochrany soukromí jednak decentralizací, čímž se umožní uživateli komunikovat napřímo s poskytovatelem služby bez zprostředkovatele v momentu uplatňování atributů[275] a jednak rozšířením informovanosti uživatele o využívání jeho osobních údajů. „*S použitím evropské peněženky digitální identity bude uživatel moci kontrolovat množství údajů poskytnutých spoléhajícím se stranám a bude informován o atributech požadovaných k poskytování konkrétní služby."* Do Digi Peněženky bude dále integrován i například elektronický podpis, elektronické razítko nebo elektronická pečeť.[276]

Od vstupu eIDAS II v platnost budou mít členské státy povinnost vydat Digi Peněženku do 12 měsíců, kromě členských států budou moci vydávat Digi Peněženky i subjekty z pověření členského státu nebo uznány od členského státu.

Digi Peněženka svým způsobem může dosti připomínat již zmíněný Portál občana, který vznikl současně se zavedením eObčanky. Digi Peněženka by měla dle eIDAS II být daleko uživatelsky přívětivější. Lze očekávat, že její podoba bude ve formě mobilní aplikace velmi podobné jiným

[273] Je třeba rozlišovat pojmy digitální identita a elektronická identifikace. Digitální identitou se myslí identita v digitálním prostředí, tedy údaje o totožnosti, atributech a kvalifikacích jejího uživatele. Nejedná se synonymum ke slovu elektronická identifikace. Elektronická identifikace je naopak nástroj, služba nebo proces, kterým jsem blíže popsal v kapitole 2.5. Není vyloučené tvrzení, že Digi Peněženka obsahuje digitální identitu a zároveň se lze díky ní elektronicky identifikovat.
[274] Ustanovení bodu 3 písm. i) eIDAS II
[275] Legislativní finanční výkaz eIDAS II článek 1.4.3.
[276] EVROPSKÁ KOMISE. Evropská digitální identita. *Evropská komise* [online]. [cit. 2021-11-11]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_cs

digitálním peněženkám, které některé soukromé společnosti jako je Apple nebo Google již dnes nabízejí svým uživatelům.

Rozdíl mezi Digi Peněženkou a českým Portálem občana je i částečně technický a částečně v rozsahu využití údajů z Portálu občana mimo veřejnou správu. Portál občana funguje jako samostatná mobilní aplikace pouze zdánlivě, po přihlášení do mobilní aplikace Portálu občana, je uživatel stejně přesměrován na webovou stránku Portálu občana, kde je nucen využít jeden z prostředků elektronické identifikace. Sama aplikace tedy nepřináší žádné zjednodušení, pouze „nahrazuje" přihlášení se na webové stránky Portálu občana standardní cestou. V druhém případě pak Portál občana nenabízí sdílení údaje v takové míře, jakou má Digi Peněženka, respektive nová digitální identita, ambici. Díky nové úpravě digitální identity jí bude uživatel schopen využívat v rámci veřejné správy, ale i pro účely komunikace s bankou, správy daní, přihlášky na vysokou školu nebo i pro ubytování v hotelovém zařízení. Zatímco Portál občana je vyloženě určen pro komunikaci s veřejnou správou. Nabízí se pak otázka, pro které služby bude stanovena povinnost přijímat identifikaci prostřednictvím Digi Peněženky a jiných prostředků elektronické identifikace a zda je legitimní po konkrétních subjektech požadovat, aby měly dostatečné technické vybavení pro přijímání elektronické identifikace.

Povinnost přijímat Digi Peněženku budou mít dle eIDAS II orgány veřejné správy a soukromoprávní subjekty, které jsou jinak povinné vyžadovat silnou autentizaci uživatele k online identifikaci, závazky vyžadující silnou autentizaci, a to i v oblasti dopravy, energetiky, bankovnictví a finančních služeb, sociálního zabezpečení, zdravotnictví, pitné vody, poštovních služeb, digitální infrastruktury, vzdělávání nebo telekomunikací.[277] Povinnost přijímat Digi Peněženku budou mít i tzv. velmi rozsáhle online platformy ve smyslu článku 25 odst. 1 návrhu nařízení Evropského parlamentu a Rady o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES. Jedná se mimo jiné i o některé sociální sítě, které v poslední době čelí vysoké míře kritice z důvodu porušování ochrany údajů svých uživatelů.[278] Tato povinnost tedy bude dopadat primárně na subjekty, u nichž lze spravedlivě požadovat, vzhledem k jejich kapacitám, aby měly dostatečné technické vybavení a přizpůsobení svých systémů k tomu, aby službu elektronické identifikace přijímaly.

[277] Bod 16 odst. 3 eIDAS II
[278] Např. skandál společnosti Facebook ve spolupráci s Cambridge Analytica z roku 2019.

V rámci přezkumu dle článku 49 ve znění eIDAS II Evropská komise posoudí, kteří poskytovatelé on-line služeb budou povinni přijímat prostředky elektronické identifikace a Digi peněženku i nadále a kteří nikoliv.[279]Nutné je zdůraznit na závěr, že uživatelé Digi Peněženky budou moci v souladu s eIDAS II využívat tuto službu pouze na bázi dobrovolnosti.

3.1.3. Jednotná digitální brána (Single Digital Gateway)

Dalším důležitým evropským právním předpisem je Nařízení Evropského parlamentu a Rady (EU) č. 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 (dále jen „**SDGR**“).

Cílem tohoto nařízení je vytvoření tzv. jednotné digitální brány „Your Europe“ (Tvá Evropa), která umožní jejím uživatelům centralizovaný přístup k informacím, službám a některým administrativním postupům jak ve státě uživatele, tak ale i v jiném členském státě. „*Tyto postupy zahrnují situace důležité pro podnikání, práci, studium nebo stěhování z jednoho místa na druhé, např. žádost o potvrzení o pobytu, žádost o půjčky na studium a stipendia, uznávání akademických titulů, získání evropského průkazu zdravotního pojištění, registrace motorového vozidla, žádost o důchodové dávky a registrování zaměstnanců do důchodového systému a systému pojištění.“*[280] Seznam konkrétních informačních oblastí, administrativních postupů a služeb dostupných prostřednictvím jednotné digitální brány je vymezen v Příloze I až III SDGR.

Součástí SDGR je i zakotvení once only zásady na evropské úrovni. Jinými slovy, SDGR stanovuje právní rámec pro vytvoření technického systému, který zajistí uplatňování once only zásady tím, že technický systém např. umožní přenos a zpracování důkazů mezi příslušnými orgány, zajistí jejich důvěrnost a integritu nebo dostatečnou úroveň interoperability, a to napříč členskými státy.[281] Současně SDGR ukládá členským státům povinnost takový systém integrovat jako součást svých postupů „*pro účely výměny důkazů pro online postupy uvedené v příloze II tohoto nařízení* (SDGR pozn. autora) *a postupy stanovené směrnicemi 2005/36/ES,*

[279] Bod 41 eIDAS II
[280] ALA-HONKOLA, Päivikki. *Rada přijala nařízení o zřízení jednotné digitální brány: zlepší se online přístup k informacím a postupům v celé EU*. Tisková zpráva. Brusel: Rada EU, 2018 [online]. [cit. 2021-11-11]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2018/09/27/single-digital-gateway-regulation-adopted-by-council-better-online-access-to-information-and-procedures-across-the-eu/
[281] Článek 14 odst. 2 a 3 SDGR

2006/123/ES, 2014/24/EU a 2014/25/EU.“[282] Nově tedy budou moci veřejné správy jednotlivých států využívat již jednou poskytnuté informace o občanech/podnikatelích z jiných států za účelem přeshraničních úkonů a dalších procesů. Samozřejmě při současném zachování ochrany utajenosti údajů a ochrany před jejich zneužitím.[283] Ustanovení vztahující se k implementaci once only zásady nabývají účinnosti od 12. prosince 2023.[284]

3.1.4. Přístupnost webových stránek

Kromě výše uvedených strategií a dílčích předpisů, považuji za důležité zmínit další právní předpis Evropské unie, který je ve vztahu k eGovernmentu důležitý. Jedná se o směrnici Evropského parlamentu a Rady (EU) č. 2016/2102 ze dne 26. října 2016 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru (dále jen „**SměrPřWeb**“), která byla transponována do zákona č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „**ZoPřWeb**“).

SměrPřWeb stanovuje požadavek, aby členské státy zajistily, že webové stránky a mobilní aplikace subjektů veřejného sektoru splňovaly požadavky na přístupnost ve smyslu článku 4 SměrPřWeb. Jedná se o požadavek, aby byly webové stránky a mobilní aplikace založené na následujících čtyřech zásadách:

*„**vnímatelnost**, což znamená, že informace a prvky uživatelského rozhraní musí být uživatelům prezentovány tak, aby je byli uživatelé schopni vnímat;*

***ovladatelnost**, která znamená, že prvky uživatelského rozhraní a navigace musí být ovladatelné;*

***srozumitelnost**, která znamená, že informace a ovládání uživatelského rozhraní musí být srozumitelné; a*

***stabilita**, která znamená, že obsah musí být dostatečně stabilní tak, aby mohl být spolehlivě interpretován širokou škálou uživatelských aplikací, včetně pomocných technologií.“*[285]

---

[282] Článek 14 odst. 6 SDGR
[283] EVROPSKÁ KOMISE. Digital Europe Programme. *Once-Only Principle (OOP)* [online]. [cit. 2022-05-05]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Once+Only+Principle
[284] Ustanovení čl. 39 SDGR
[285] Recitál č. 37 SměrPřWeb

Výše uvedená právní úprava též vychází z technologicky neutrální regulace přístupnosti informací a služeb především tím, že není vázána na žádnou konkrétní technologii. Naopak cílem této úpravy není jen harmonizace přístupnosti webových stránek. Jedná se i o harmonizaci požadavků pro tvorbu webových stránek, která fakticky znemožňuje subjektům využívat nepřístupná řešení v oblasti komunikačního rozhraní pro uživatele takových webových stránek. V rámci přístupnosti právní úprava též stanovuje povinnost nastavení technického řešení webových stránek takovým způsobem, který umožní osobám se zdravotním postižením interagovat s webovými stránkami a využívat jejich obsah co nejvíce rovnocenným způsobem, který současný technologický pokrok umožňuje.[286]

Povinný subjekt, kterými jsou subjekty veřejné správy a další subjekty dle § 3 ZoPřWeb s výjimkou České televize a Českého rozhlasu, má současně nárok při zajišťování přístupnosti jím spravovaných webových stránek, nesplnit požadavky přístupnosti, způsobuje-li mu to nepřiměřenou zátěž. V takovém případě je však subjekt povinen v prohlášení o přístupnosti zdůvodnit nesplnění požadavků a současně nabídnout alternativní řešení. [287]

Závěrem je podstatné zdůraznit i speciální úpravu prosazování práva ve smyslu článku 9 SměrPřWeb, která stanovuje povinnost členského státu zajistit zavedení postupu prosazování práva na přístupnost webových stránek a internetových aplikací. Český zákonodárce přijal úpravu v podobě, kdy se žadatel může obracet na povinný subjekt způsobem, na jehož úpravu se užije obdobně úprava práva petičního. Jak uvádí důvodová zpráva k ZoPřWeb, jednou z možností nápravy je prostřednictvím úpravy KontrolŘ, který opravňuje kontrolní orgán k ukládání opatření k odstranění nebo prevenci nedostatků zjištěných kontrolou. „*Další možností je obrátit se na veřejného ochránce práv, který se podle § 21c odst. 1 písm. a) ZoVOP, při sledování naplňování mezinárodní smlouvy upravující práva osob se zdravotním postižením (tj. Úmluvy o právech osob se zdravotním postižením) zabývá systematicky problematikou práv osob se zdravotním postižením a za tím účelem zejména podporuje naplňování práv osob se zdravotním postižením a navrhuje opatření směřující k jejich ochraně.*“[288]

Úprava přístupnosti webových stránek dopadá logicky i na již zmíněné portály jako je např. Portál veřejné správy nebo Portál občana, které pro usnadnění komunikace mezi veřejnou

[286] Důvodová zpráva ZoPřWeb
[287] Srovnání ustanovení § 7 ZoPřWeb a čl. 5 SměrPřWeb
[288] Důvodová zpráva ZoPřWeb

správou a adresátem veřejné správy hrají v současné době klíčovou roli. I z tohoto důvodu je snaha o harmonizaci přístupnosti takových webových stránek a aplikací důležitá součást právní úpravy eGovernmentu.

3.1.5. Evropské digitální zásady

Cílem Evropských digitálních zásad je především stanovení jednotného referenčního rámce pro další činnosti v oblasti digitální transformace na území EU. Jak je uvedeno ve sdělení Komise k Evropským digitálním zásadám, měly by primárně sloužit jako referenční vodítko pro veřejné i soukromé subjekty při vývoji, zavádění a regulaci nových technologií, stejně jako pro tvorbu politik usilujících o vymezení cesty k digitálnímu světu, v jehož centru stojí člověk nikoliv technologie samotná.

Obsahem je pak 6 kapitol, které vymezují jednotlivé zastřešující zásady, kterými jsou

I. *občané jako středobod digitální transformace* jako zastřešující zásada;
II. *solidarita a inkluzivnost*;
III. *svoboda volby, zejména ověřitelnost výstupů, bezpečnost a ochrana před riziky při interakci s umělou inteligencí*;
IV. *zapojení se do digitálního veřejného prostoru bez diskriminace a cenzury*;
V. *bezpečnost, ochrana soukromí a posílení postavení dětí a jiných slabších skupin v on-line prostředí*; a
VI. *udržitelnost*.[289]

Součástí Solidarity a inkluzivnosti jsou i digitální veřejné služby. Evropské digitální zásady akcentují klíčovou zásadu pro budování eGovernmentu, a to once only zásadu, která zamezuje opakované poskytování údajů, které má veřejná správa k dispozici. V této podkapitole jsou dále rozvedeny některé cíle stanovené v Evropském kompasu jako je efektivní digitální identita a přístup ke zdravotnickým službám a související dokumentaci. Mimo tuto podkapitoly jsou součástí Solidarity a inkluzivnosti další tři, a to sice zajištění vysokorychlostní digitální konektivity, akcent na digitální vzdělávání a zajištění ochrany a bezpečných pracovních podmínek v digitálním prostředí.[290]

[289] Evropské digitální zásady
[290] Ibid.

Evropské digitální zásady nejsou přímo vymahatelné a nejedná se ani o právní předpis na rozdíl od ZPDS, který sleduje podobný záměr. Namísto vymahatelnosti je součástí systém monitoringu, který stanovuje členským státům povinnost předávat Komisi nezbytné informace potřebné pro účinné sledování vývoje navázaného na zakotvené zásady ve zmíněném dokumentu. Informace následně vyhodnotí Komise a navrhne vhodné kroky a opatření.

Kromě toho Evropské digitální zásady uvádějí, že se mají „*stát globálním kritériem pro četné nově vyvstávající společenské a etické otázky, jež digitální transformace přináší.*“[291], což je dle mého názoru poměrně ambiciózní prohlášení. Rád bych zdůraznil, že podobnou iniciativu pokládám za nesmírně důležitou s ohledem na „harmonizaci“ přístupu k digitální transformaci na půdě Evropské unie. V takovém ohledu Evropské digitální zásady dle mého názoru obstojí. Současně ovšem s mírnou dávkou zklamání pozoruji, že se Evropská unie soustředila pouze na stanovení rámce pro budování referenčního rámce na aktuální situaci. Evropské digitální zásady neobsahují téměř ani náznak jakéhokoliv výhledu do budoucnosti či prostor pro širší působnost těchto zásad než na dosud poznané technologie, které se staly součástí téměř každodenního života. Protiargumentem, a jistě relevantním, by mohl být zakotvený proces monitoringu „aktuálnosti“ Evropských digitálních zásad, kde s ohledem na technologický vývoj je Komise oprávněna předložit příslušný návrh na přezkum či úpravu některé ze zásad. To ale dle mého názoru nestačí. Není ponechán žádný prostor, který by pokrýval právní nebo etické aspekty využívání již dnes existujících technologií jako je např. „Virtuální“ nebo „Augmentovaná“ (rozšířená) realita nebo „BCI“ (brain-computer interface), tedy neurální rozhraní, které propojuje lidský mozek s výpočetní technologií. Jednoduše řečeno, domnívám se, že ať už Evropské digitální zásady nebo jakékoliv jiné zásady související s regulací digitální transformace, by se měly soustředit nejen na přítomnost, ale i na budoucnost, a ne na minulost. Zcela určitě to není snadný úkol, jelikož digitální svět je dynamicky se rozvíjející oblast, ve které jsou týdny dny a roky měsíce. I z toho důvodu je klíčové, aby si podobná iniciativa nechávala prostor pro usměrnění nadcházejícího vývoje.

3.2. Vybrané zahraniční přístupy

Vedle přístupu EU k postupné harmonizaci právních předpisů upravujících dílčí části eGovernmentu vnímám za zásadní analyzovat přístupy k elektronizaci veřejné správy

[291] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů o Evropských digitálních zásadách, COM(2022) 27 final

v některých státech, jejichž eGovernment je (respektive byl) v rámci kategorie digitálních veřejných služeb dle DESI a Benchmarku hodnocen daleko lépe než v České republice. Jedná se o Estonsko a Maltu. Za srovnání však jistě stojí i přístup Rakouské republiky a Slovenské republiky, tedy států, které mají podobné právně historické kořeny a právní kulturu jako Česká republika. *Z Rakouska jsme vznikli a Slovensko bylo naší součástí, než se od nás odtrhlo.*[292] Pro představu je dle mého názoru důležité ve stručnosti představit klíčové principy jednotlivých eGovernmentů a následně analyzovat způsob dílčí právní úpravy a porovnat jí s tuzemskou právní úpravou.

Právní komparace bude probíhat primárně ve čtyřech oblastech, které považuji za klíčové pro hrubou představu o právní úpravě eGovernmentu v některém ze zkoumaných států. Prvním měřítkem je samotná systematizace právní úpravy. V předchozích kapitolách jsem podrobně analyzoval jednotlivé právní předpisy, které tvoří právní rámec eGovernmentu v České republice. Na tomto základě lze zkonstatovat, že česká právní úprava eGovernmentu je značně difúzní a neexistuje jeden kodex, který by se dal pojmenovat jako již zmíněný „eGovernment act". Domnívám se, že pro účely komparace je jako výchozí bod zajímavé prozkoumat, zda v některých zkoumaných státech existuje kodifikovaná právní úprava eGovernmentu nebo zda je právní úprava obdobně roztříštěná jako v České republice. Sám se domnívám, že větší kodifikace právních odvětví vede k jak k lepšímu porozumění, tak k lepší vymahatelnosti práva. Cílem tedy současně je i zjištění, zda lze vůbec tak rozsáhlou oblast, jako je právní úprava eGovernmentu, kodifikovat.

Druhé a třetí měřítko pak bude srovnání právní úpravy dvou z mého pohledu důležitých nástrojů pro využívání služeb eGovernmentu. Jedná se o právní úpravu elektronické identifikace a elektronického doručování. Elektronická identifikace dnes již podléhá úpravě v eIDAS, proto se chci zaměřit na úpravu, respektive vůbec existenci takového nástroje před přijetím zmíněného nařízení. Díky elektronické identifikaci, ať už prostřednictvím čipové karty, mobilní nebo jiné aplikace se mohou uživatelé autorizovat a získat přístup k elektronickým službám, které lokální eGovernment nabízí. Lapidárně řečeno, elektronické doručování pak umožňuje uživatelům jednak komunikovat s orgány veřejné správy z pohodlí domova (i mimo něj) bez odkázání na doručovací služby ve svém státě a jednak i vyšší transparentnost při komunikaci veřejné správy s jejím adresátem. Vyšší transparentností mám na mysli zejména

[292] Konzultace k diplomové práci ze dne 17. června s JUDr. Ing. Josefem Stašou, CSc.

kompletní přehled o doručení nebo přijetí písemnosti. Součástí elektronického doručování je logicky i elektronické podání, které naopak z pohodlí domova nebo mimo něj dává uživatelům možnost v kteroukoliv denní dobu odeslat jakékoliv podání bez odkázání na otevírací dobu jednotlivých úřadů. Oba tyto nástroje považuji za minimální základ pro to, co lze nazývat v dnešní vyspělé společnosti eGovernmentem.

Čtvrté a poslední hledisko bude zaměřeno na opakovaně zmíněnou once only zásadu. Zakotvení této zásady bude v budoucnu ovlivňovat již přijaté SDGR, kterému jsem se věnoval v předchozí kapitole. Toto přímo použitelné nařízení nutí členské státy do konce roku 2023 přijmout potřebná opatření k integraci systému, který umožní uplatnění once only zásady i mezi jednotlivými členskými státy. Proto se tedy zaměřím na výslovně zakotvení této zásady v právním řádu jednotlivých států před nabytím účinnosti SDGR.

Cílem této komparace je především nastínění vývoje a pokroku mezi jednotlivými státy, porovnání způsobu úpravy eGovernmentu a v neposlední řadě i motivace pro jednotlivé státy vyrovnat rozdíly, které mezi sebou mají. Jak jsem již zmínil, eGovernment je fenomén, který již dnes překračuje hranice jednotlivých států. Z tohoto důvodu je dle mého názoru zapotřebí více harmonizovat nejen právní prostředí, ať už prostřednictvím legislativní a politické činnosti Evropské unie, tak v ideálním případě z vlastní iniciativy jednotlivých států a jejich zákonodárců.

3.2.1. Estonská republika

„*V Estonsku musí občané vyřídit osobně pouze dvě věci – svatbu a rozvod. Vše ostatní udělají během pár kliknutí na internetu.*“[293]

Od roku 2002 funguje v Estonsku využívání systému digitální identity, od roku 2007 možnost volit prostřednictvím internetu v parlamentních volbách a od roku 2010 systém elektronicky přístupné databáze zdravotního stavu uživatele včetně možnosti on-line předpisu léčiv a souvisejících výrobků.[294] V roce 2019 přijala estonská vláda strategii, ve které analyzuje

[293] BULAN, Jiří. (2022, 25. března). *Proč to v Estonsku šlo už před 20 lety, co tomu dopomohlo a co nám chybí? Z čeho se lze poučit?* Konference Institutu moderní politiky – iSTAR: Od montovny k mozkovně, Dolní Břežany, Česká republika.
[294] CASTAÑOS, Virgina, op. cit. sub. 26, str. 5

možnosti využití systému umělé inteligence v budoucnosti ve veřejném i soukromém sektoru, včetně potřeby právní regulace a zajištění zabezpečení.[295]

Není tedy žádným překvapením, že se Estonsko dlouhodobě umísťuje v čele žebříčků DESI i Benchmark. V roce 2021 DESI přisoudil Estonsku první místo v oblasti digitálních veřejných služeb a dle Benchmarku se při průměru digitalizace a penetrace umístilo na pomyslném prvním místě, tj. nejblíže ideálnímu stavu maximální digitalizace a maximální penetrace.[296]

Hlavním uzlem infrastruktury estonského eGovernmentu je národní portál (eesti.ee). Ten „*umožňuje uživatelům zkontrolovat své osobní údaje, provádět elektronicky úkony (transakce) s orgány veřejné správy, vyplňovat a podávat elektronické formuláře nebo si zřídit oficiální a státem garantovanou emailovou adresu.“*[297] Mezi zpřístupněnými transakcemi lze nalézt změnu bydliště, zřízení právnické osob, podání daňového přiznání nebo žádost o sociální příspěvky.[298]

Asi nejdůležitější součástí estonského eGovernmentu je systém pro výměnu dat zvaný „X-tee“ (dříve X-Road, čti crossroad, pozn. autora).[299, 300] X-tee[301] je také významný tím, že pracuje na základě jednoho z typů technologie distribuovaných záznamů (tzv. DLT) známého jako *blockchain*[302]. Tento systém funguje na veřejné úrovni jako interoperabilní platforma pro

---

[295] GOVERNMENT OF THE REPUBLIC OF ESTONIA. *Estonia's national artificial intelligence strategy 2019 – 2021*. Talin: Government of the Republic of Estonia. [online]. [cit. 2021-19-03]. Dostupné z: https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_27a618cb80a648c38be427194affa2f3.pdf

[296] Srovnání EVROPSKÁ KOMISE. *Digital Economy and Society Indes,* op. cit. sub. 90 a EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets,* op. cit. sub.91

[297] EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2021.* Estonia. Brusel: Evropská komise, 2021 [online]. [cit. 2022-07-03], str. 36. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Estonia_vFinal.pdf,

[298] REPUBLIC OF ESTONIA. Úvodní stránka. *Riigisportaal. Eesti.ee* [online]. [cit. 2022-07-03]. Dostupné z: https://www.eesti.ee/en

[299] Původní název X-Road je ponechán samotné technologii, kterou společně vytvořily státy: Estonsko, Finsko a Island v rámci MTÜ Nordic Institute for Interoperability Solutions (REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY. Data Exchange Layer X-tee. *Republic of Estonia Information System Authority* [online]. [cit. 2022-07-03]. Dostupné z: https://www.ria.ee/en/state-information-system/x-tee.html)

[300] X-Road jakožto *open source* (po právní i technické stránce dostupný počítačový software s otevřeným zdrojovým kódem) technologii využívají kromě Estonska státy jako Finsko, Kyrgyzstán, Faerské ostrovy, Island nebo Japonsko. (ENTERPRISE ESTONIA. Interoperabilitty services. *e-Estonia* [online]. [cit. 2022-07-03]. Dostupné z: https://e-estonia.com/solutions/interoperability-services/x-road/)

[301] X-Road je v překladu do českého jazyka křižovatka. Výraz X-tee je zkráceni estonského slova *risttee*, které též v překladu znamená křižovatka, přičemž část slova *rist* (česky *kříž*, anglicky *cross*) je nahrazeno písmenem „X“. Výraz X-tee je tedy zjednodušeně řečeno estonský překlad slova X-Road.

[302] Blockchain je decentralizovaná databáze dat, která funguje na principu na sebe řetězem navázaných tzv. bloků. V těchto blocích jsou uspořádána data včetně záznamů tzv. „otisků“, které tento blok bezprostředně napojují na předchozí blok v řetězci. Tímto jsou data v jednotlivých blocích zároveň chráněna, jelikož neoprávněnou modifikací dat v jednom bloku dojde k situaci, kdy se otisk bloku neshoduje s předchozím napojeným blokem, čímž se odhalí neoprávněný zásah do těchto dat. Zjednodušeně řečeno, aby se mohla data v jednom bloku změnit, bylo by zapotřebí změnit data ve všech předcházejících blocích, což je prakticky nemožné. (srovnání např. MINISTERSTVO FINANCÍ. *Veřejná*

výměnu dat jak mezi jeho uživateli, tak i mezi orgány veřejné správy a jejich databázemi navzájem. Každý jeho uživatel má aktuální přehled o využívání osobních údajů (včetně práv, povinností a právních skutečností) orgány veřejné moci a možnost ověření jejich autentičnosti.[303]

X-tee si lze představit jako datové prostředí, které působí jako prostředník mezi informačními systémy jednotlivých agend. Informace ze systému A tak za zákonných předpokladů „doputuje" skrze X-tee do systému B. Každý informační systém je oprávněn shromažďovat pouze základní údaje v rámci svých agend (viz dále v textu). Současně při výkonu činnosti agendy A je zapotřebí získat údaje z agendy B, které si díky X-tee za současného zajištění důvěrnosti a zabezpečení dotčené orgány mohou bez větších obtíží opatřit.[304]

Právní rámec X-tee a vesměs i celý estonský eGovernment se opírá o zákon o veřejných informacích (*Avaliku teabe seadus*, RT I 2000, 92, 567) ze dne 15. 11. 2000 (dále jen „**AvTeS**").[305] Primárním cílem AvTeS je zajištění interoperability mezi databázemi jednotlivých orgánů veřejné správy, opětovného použití veřejných informací a procesů pro přístup k informacím.[306]

Kromě výše uvedeného AvTeS též upravuje práva a povinnosti dotčených subjektů (obdobně jako český ZPDS). Například § 4 odst. 5 AvTeS upravuje právo subjektů údajů odporovat přístupu k osobním údajům v případech, kdy by byl takový přístup porušením jeho práv nebo svobod. Následující ustanovení pak upravují žádost o informace a přístup k nim. Dále pak § 9 odst. 1 AvTeS výslovně stanovuje, že „držitelé údajů"[307] mají právo k přístupu k údajům pouze v zákonných případech. Je tedy vyloučená libovůle držitelů údajů získávat a využívat údaje, ke kterým nemají mít přístup a které nemají v rámci jejich činnosti využití.[308]

---

konzultace – blockchain, virtuální měny a aktiva. Praha: Ministerstvo financi, 2018 [online]. [cit. 2021-18-03]. str. 4. Dostupné z: https://www.mfcr.cz/assets/cs/media/Konzultace_2018-11-30_Verejna-konzultace-Blockchain-virtualni-meny-a-aktiva.pdf

[303] CASTAÑOS, Virgina, op. cit. sub. 26, str. 9

[304] INFOSYSTEEMIAMET, 2016, *X-Road introduction (short video),* Youtube video. [cit. 2022-07-03]. Dostupné z: https://youtu.be/b-r6B28qVSY

[305] EVROPSKÁ KOMISE. *Digital Public Administration factsheet* 2021, op. cit. sub. 106, str. 19

[306] Ustanovení § 2 a § 3 AvTeS

[307] Ve smyslu § 5 odst. 1 AvTeS se jedná o státní a samosprávné orgány, právnické osoby veřejného práva a právnické osoby, kterým byl svěřen výkon veřejných činností

[308] Například k údajům o finančních příjmech fyzické osoby v loňském roce bude mít přístup finančně správní orgán, ale nebude ho mít orgán, který ověřuje totožnost osoby pro účely internetového hlasování apod. (pozn. autora)

AvTeS dále zakotvuje od roku 2008[309] úpravu tzv. databází státních informačních systémů, tedy dle § 43^1 odst. 1 AvTeS strukturovaných soborů dat v rámci státního informačního systému. Tyto databáze obsahují veškerá data, která veřejné orgány získaly v souvislosti se svou činností. Využívání a získávání těchto dat podléhá již výslovně zmíněné once only zásadě, zde pojmenované jako *one-request-only* princip.[310] Zřízení databází je možné čistě na základě výslovného zákonného zmocnění, přičemž AvTeS výslovně zakazuje existenci duplicitních databází, které by získávaly stejná data.[311]

Zajímavostí, oproti české právní úpravě, je opuštění konceptu základních registrů. Estonský právní řád naopak využívá instrument tzv. základních dat. Bez ohledu na to, v jaké databázi se nacházejí, základní data jsou unikátní data získána orgánem veřejné správy při výkonu své činnosti. Při zpracování (základních) dat jinými veřejnými databázemi vzniká povinnost tak činit na základě základních dat umístěných v původní databázi.[312] Označením dat jako „základní" dochází k autoritativnímu určení originálního zdroje.[313] Jinými slovy, databáze B je povinna využít základní data z databáze A. Pokud by došlo v procesu přenosu dat k nejasnostem nebo dokonce pozměnění dat, je pevně stanoveno, že základní data v databázi A jsou jediná závazná. Rozdíl oproti základním registrům je tedy v tom, že určující kritérium není konkrétní databáze, ve kterých se data nachází, nýbrž to, ve které databázi jsou data vedená jako závazná.

Ustanovení § 43^9 odst. 1 AvTeS dále vytváří právní základ pro tzv. podpůrné systémy státních informačních systémů. Ty mohou být zřízeny pouze na základě nařízení Estonské vlády. Již jsem zmínil v úvodu této kapitoly, že se právě X-tee opírá o tuto právní úpravu. Ustanovení § 43^9 odst. 1 bod 5) AvTeS stanovuje oprávnění vládním nařízením zřídit systém výměny dat. Toto vládní nařízení bylo přijato jako nařízení estonské vlády č. 105 ze dne 23. září 2016 o systému výměny dat (*Infosüsteemide andmevahetuskiht*).

[309] Původní úprava databází v zákoně o databázích byla v důsledku novely č. RT I 2007, 12, 66 zrušena. Obsah původního předpisu byl konsolidován v rámci AvTeS.
[310] Ustanovení § 43^1 odst. 3 AvTeS
[311] Ustanovení § 43^3 odst. 1 a 2 AvTeS
[312] Ustanovení § 43^6 AvTeS
[313] EVROPSKÁ KOMISE. *Digital Public Administration factsheet* 2021, op. cit. sub. 106, str. 19

Závěrem analýzy AvTeS lze zmínit i ustanovení 6. části, které zajišťují záruky základních zásad spojených s ochranou osobních údajů včetně sdílení údajů na základě souhlasu uživatele a správní dozor dotčených orgánů v oblasti sdílení veřejných informací.[314]

Podobně jako český právní řád, i estonský umožňuje oboustrannou elektronickou komunikaci s orgány nejen veřejné správy. Za zmínku stojí výslovné zakotvení jak elektronického podání, tak elektronického doručování ve správním řízení, které upravuje estonský zákon o správním řízení (*Haldusmenetluse seadus,* RT I 2001, 58, 354) ze dne 6. června 2001 (dále jen „**HalS**“).[315] Držitel estonského občanského průkazu má právo na zřízení oficiální emailové adresy (@eesti.ee) poskytovanou Estonskou republikou. Tato adresa funguje jako oboustranný kanál pro přijímání a doručování oficiálních písemností.[316]

Konkrétní podmínky komunikace orgánů veřejné správy s osobami prostřednictvím oficiální emailové adresy dále upravuje nařízení estonské vlády č. 88 ze dne 25. května 2017 o zásadách řízení služeb a správy (*Määrus teenuste korraldamise ja teabehalduse alused)*. Toto nařízení mimo jiné upravuje technické aspekty oznamování o doručení písemnosti nebo oznámení o aktivaci emailové schránky. Zajímavé je, že na rozdíl od české úpravy datových schránek, HalS výslovně nestanovuje povinnost dotčených orgánů komunikovat elektronicky. Naopak blanketové ustanovení § 25 odst. 3 HalS ponechává na úvaze zákonodárce v konkrétních případech stanovit konkrétní formu doručení. V ostatních případech pak postačí dle dispozitivního ustanovení jakákoliv zvolená forma doručení. Kromě elektronické se jedná o doručení poštou nebo správním orgánem.[317]

Již jsem zmínil, že Estonsko využívá formu elektronické identifikace už od roku 2002, tedy o více jak 14 let před přijetím eIDAS. *„V roce 1992, po tom, co Estonsko vyhlásilo nezávislost na Sovětském svazu, začala Rada pro občanství a migraci (Kodakondsus- ja Migratsiooniamet) vydávat pasy. První generace pasů měla platnost 10 let, a bylo tedy zapotřebí je v roce 2002 obnovit. Estonská vláda se rozhodla využít tuto situaci jako příležitost a přijít s novým druhem dokladu totožnosti ve formě národní identifikační karty (ID karty). Hlavní účel představení ID karty byl zprostředkování estonským občanům prostředku k digitálním podpisům ve smyslu*

[314] Ustanovení §§ 44 a násl. AvTeS
[315] Srovnání ustanovení § 14 a § 27 HalS
[316] REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY. *@eesti.ee e-mail addresses are becoming more and more popular*. Talinn: Riigi Infosüsteemi Amet, 2020 [online]. [cit. 2022-07-03]. Dostupné z: https://www.id.ee/en/article/eesti-ee-e-mail-addresses-are-becoming-more-and-more-popular/
[317] Ustanovení § 25 HalS

zákona o digitální podpisech [estonský zákon (Digitaalallkirja seadus) RT I 2000, 26, 150 o digitálních podpisech ze dne 8. března 2000, pozn. autora][318]*, jehož zpracování probíhalo od roku 1997 do března 2000.*[319]

Původní verze ID karty byla klasická karta s identifikačními údaji a strojově čitelným čipem, díky kterému se každý uživatel mohl identifikovat elektronicky skrze čtečku karet (obdobně jako eObčanka, ovšem o 16 let dříve, pozn. autora).[320] Tato verze není už v dnešním světě natolik převratným instrumentem, jelikož vývoj identifikačních prostředků (nejen) v Estonku tímto neskončil. Pomíjím technologický vývoj zabezpečení strojově čitelných karet. V souvislosti se dvěma novelami z roku 2009 a 2010 u zákona o dokladech totožnosti (*Isikut tõendavate dokumentide seadus,* RT I 1999, 25, 356) ze dne 15. února 1999 (dále jen „**ITDS**“) došlo k dalšímu vývoji.

První novelou byl do ITDS zakotven právní rámec i pro tzv. digitální ID[321], což je prostředek pouze elektronické identifikace. Lze jej využít obdobně jako ID kartu pro elektronickou identifikaci, elektronický podpis, elektronické hlasování nebo využívání služeb estonského eGovernmentu, ale nikoliv jako prostředek fyzické identifikace.[322] Hlavní výhodou sekundárního prostředku elektronické identifikace je především hledisko minimalizace rizika ztráty jednoho z průkazů a tím znemožnění elektronické identifikace po dobu absence „řádné“ ID karty.

Na konci roku 2010 s účinností od 1. února 2011 byla do ITDS vtělena úprava umožňující digitální ID ve formě mobil ID. Úprava tedy počítala s tím, že se držitelé digitální ID budou moci elektronicky identifikovat a činit elektronické podpisy skrze své mobilní telefony.[323]

---

[318] S přijetím eIDAS došlo k nahrazení tohoto zákona novým estonským zákonem o elektronické identifikaci a službách vytvářejících důvěru, který eIDAS transponoval do estonského právního řádu.
[319] PARSOVS, Arnis, 2021. *Estonian Electronic Identitty Card and its Security Challenges.* Tartu, Estonsko. Dizertační práce. Institute of Computer Science, Faculty of Science and Technology, University of Tartu, Estonia. Vedoucí práce UNRUH, Dominique. str. 17
[320] Ibid., str. 45
[321] Ustanovení § 20^1 až 20^3 ITDS
[322] REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY. *Digital documents: ID-card, digital ID, residence permit card and e-Resident digital ID*. Talinn: Riigi Infosüsteemi Amet, 2020 [online]. [cit. 2022-07-03]. Dostupné z: https://www.id.ee/en/article/digital-documents-id-card-digital-id-residence-permit-card-and-e-resident-digi-id/
[323] Ustanovení 20^4 ITDS

Mobilní ID je pak zajištěno skrze speciální SIM kartu, kterou zpřístupní svým klientům mobilní operátoři.[324]

Od roku 2018 je též možné nejen v Estonsku, ale i v dalších pobaltských státech využívat soukromou mobilní aplikaci Smart-ID, která umožňuje uživatelům se jak elektronicky identifikovat, tak i zároveň činit i kvalifikované elektronické podpisy v souladu s eIDAS.[325]

3.2.2. Maltská republika

Maltský právní systém je oproti kontinentální právní úpravě poměrně odlišný v důsledku historického vývoje tohoto ostrova. Kořeny místní právní úpravy lze nalézt obdobně jako téměř ve zbytku Evropy v římském právu. Tato kontinuita byla ovšem narušena francouzskou invazí v 18. století. Proti této invazi na straně Malty stála tehdejší Velká Británie. Po porážce Francie se Malta stala součástí britského impéria až do roku 1964, což výrazně ovlivnilo její právní systém. Současně panuje shoda na tom, že Maltský právní systém je smíšený systém, který v sobě skloubí prvky common law, ale i kontinentálního evropského práva.[326] Z tohoto důvodu může být poněkud zavádějící komparace právní úpravy eGovernmentu s ostatními evropskými státy. Přesto se domnívám, že zajímavé zmínit několik klíčových prvků a právních předpisů, které tvoří páteř maltského eGovernmentu.

Tento středomořský ostrov poněkud vyčnívá mezi ostatními skandinávskými nebo pobaltskými státy, které jsou současnými lídry v digitalizaci státní správy. Dle DESI se v roce 2021 umístila Malta na 4. místě v oblasti digitálních veřejných služeb, podle Benchmarku se dokonce jedná o nejvíce digitalizovaný stát. Malta však dosahuje vysokého skóre v digitalizaci, ale lehce podprůměrného výsledku v penetraci. [327]

„Veškeré maltské digitální veřejné služby jsou dostupné prostřednictvím portálu „Servizz.gov", který je jednotné kontaktní místo jak pro občany, tak pro podnikající osoby."[328] Jedná se o tzv. „*one stop shop*", tedy jednotné místo, portál, ze kterého má veřejnost přístup k celé řadě veřejně

[324] ENTERPRISE ESTONIA. e-Identity. *e-Estonia* [online]. [cit. 2022-07-03]. Dostupné z: https://e-estonia.com/solutions/e-identity/mobile-id/
[325] Ibid.
[326] GRIMA, Noel. *The basics of the Maltese legal system.* St.Julians: The Malta Independent, 2015 [online]. [cit. 2022-10-04]. Dostupné z: https://www.independent.com.mt/articles/2015-04-13/books/The-basics-of-the-Maltese-legal-system-6736133706
[327] EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets,* op. cit. sub. 92, str. 71-74
[328] EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Malta. Brusel: Evropská komise, 2021 [online]. [cit. 2022-11-04]. str. 15. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80497

dostupných informací vždy v rámci daného sektoru, tj. zdravotnictví, zemědělství, průmysl apod. Současně lze tam, kde to je možné (např. žádost o sociální dávky, nebo podání daňového přiznání), mohou uživatelé přímo uskutečnit ten který úkon. Maltský portál dále nabízí možnosti žádosti o informace, sjednání schůzky s příslušným úředníkem nebo přímého zapojení občanů do zlepšování místního eGovernmentu skrze umožnění podávat podněty ke zlepšení.

Prameny právní úpravy Malty se dělí na dvě základní kategorie: I) primární předpisy (*Primary Legislation*) přijaté maltským parlamentem a II) podpůrné předpisy (*Subsidiary Legislation*) přijaté dalšími orgány jako jsou ministerstva, správní orgány a další veřejné orgány.[329] Úprava eGovernmentu Malty není koncentrovaná a je roztříštěná do desítek různých primárních i podpůrných právních předpisů.

V této oblasti lze pak zmínit několik klíčových předpisů. Prvním je zákon o opakovaném použití informací veřejného sektoru z roku 2015, ve znění pozdějších předpisů [Cap. 546] (*Re-Use of Public Sector Information Act*) (dále jen „**ReUseAct**"). ReUseAct vznikl původně jako implementace evropské směrnice[330], která stanovila pravidla pro veřejné orgány pro využívání dostupných informací. V důsledku dvou pozdějších novelizací se však stal ReUseAct poměrně zásadním předpisem pro fungování eGovernmentu. První novela byl zákona č. XI z roku 2020, který kromě zavedení odvolacích postupů[331] a nových pravomocí regulačního orgánu[332], především rozšířil definici opětovného použití a zřízení registrů, které umožní zavedení once only zásady.[333] Druhou novelou č. 35 z roku 2021 pak došlo k implementaci evropské směrnice o open datech[334]. V rovině podpůrných předpisů je pak důležité zmínit nařízení o organizačních strukturách pro sdílení dat a jejich opětovné použití [S.L. 546.01] (*Organisational Structures for Data Sharing and Re-Use* Regulations), který mimo jiné opravňuje Malta Information

[329] EVROPSKÁ KOMISE. National Legislation. Malta. *European e-Justice* [online]. [cit. 2022-05-05]. Dostupné z: https://e-justice.europa.eu/6/EN/national_legislation?MALTA&member=1
[330] Směrnice 2013/37/EU Evropského parlamentu a Rady, kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru
[331] Ustanovení čl. 24B a 24C ReUseAct
[332] Ustanovení čl. 24A ReUseAct
[333] Ustanovení čl. 25 písm. e) ReUseAct
[334] Směrnice 2019/1024 Evropského parlamentu a Rady o open datech a opakovaném použití informací veřejného sektoru

Technology Agency tzv. MITA k tomu, aby byla autoritou zodpovědnou za implementaci ustanovení ReUseAct.[335]

Vedle Estonska je Malta jedním z prvních států, který v určité formě umožnil elektronickou identifikaci a autentizaci. První zmínka o Maltské elektronické identifikaci je z března roku 2004, kdy byla tato služba zpuštěna za účelem umožnit občanům přístup k některým elektronickým službám vyžadujícím identifikaci.[336] Na základě podpůrného předpisu o zřízení Identity Malta Agency (dále jen „**IMA**“) [S.L. 595.07] (*IMA Establishment Order*) byla zřízena IMA, která zodpovídá za výkon veřejné správy v oblasti identifikace občanů a z pohledu eGovernmentu zejména v oblasti elektronické identifikace. Následující rok v lednu spustila IMA projekt eID karet, tedy karet obsahující elektronický čip, díky kterému se budou moci subjekty identifikovat přes čtečku karet a využít služby maltského eGovernmentu.[337]

Přestože Benchmark udělil Maltě maximální možné skóre v oblasti „digitální pošty“,[338] Maltský eGovernment nenabízí jednotnou službu elektronického doručování jako jsou české datové schránky. Tento Benchmark indikátor ovšem sleduje toliko možnost komunikovat s příslušnými orgány elektronicky (tj. emailem, faxem apod.), nikoliv poskytování služby jako takové.[339] Úprava možnosti podávat návrhy elektronicky je pak doslova roztříštěná mezi několik předpisů upravující dílčí oblast elektronické komunikace. Lze zmínit hned několik podpůrných předpisů, ve který se pojednává o úpravě podávání návrhů před soud.

V rámci civilního procesu je pro podání v rámci tzv. „malých nároků“[340] úprava obsažena v podpůrném předpisu o pravidlech (podání pomocí elektronických prostředků) pro jednání před tribunálem malých nároků [S.L. 380.04] [*Small Claims Tribunal (Filing of Acts by Electronic Means) Rules*]. Pro podání k soudu v ostatních případech je úprava obsažena

---

[335] Ustanovení článku 16 odst. 1 nařízení o organizačních strukturách pro sdílení dat a jejich opětovné použití [S.L. 546.01] (Organisational Structures for Data Sharing and Re-Use Regulations)

[336] GÁSPÁR, Pál, JAKSA, Anna Renata, RESTALL, Brian, XUEREB, Marisa. *The Development of eService in an Enlarged EU: eGovernment and eHealth in Malta*. Luxemburg: Office for Official Publications of the European Communities, 2008. str. 42. ISSN 1018-5593,

[337] EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2014.* Malta. Brusel: Evropská komise, 2021 [online]. [cit. 2022-07-03], str. 4. Dostupné z https://joinup.ec.europa.eu/sites/default/files/document/2014-06/eGov%20in%20MT%20-%20March%202014%20-%20v.16.0_0.pdf

[338] EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets,* op. cit. sub. 92, str. 71

[339] EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Background report. eGovernment benchmark 2021.* Entering a new digital government era. Brusel: Evropská komise, 2021 [online]. str. 29. Dostupné z: DOI: 10.2759/798973

[340] Malým nárokem (*small claim*) se myslí ve smyslu čl. 3 odst. 2 zákona o tribunálu malých nároků [Cap. 380] (*Small Claims Tribunal Act*) nárok, který nepřevyšuje € 5 000

v nařízení o občanském řízení (úprava rejstříků, archivů a funkcí předsedy soudu (Gozo) a dalších soudních úředníků) [S.L. 12.21] [*Civil Procedure (Regulation of Registries, Archives and Functions of Director Courts (Gozo) and other Court Executive Officers) Regulations*]. Příloha posledního zmíněného předpisu výslovně určuje, ke kterým soudům a jaké úkony je možné činit elektronicky.[341]

Pro obdobu správního soudnictví je pak elektronické podání upraveno podpůrným předpisem o podávání návrhů elektronickými prostředky před tribunálem správního přezkumu [S.L. 490.05] (*Filings of Acts before the Administrative Review Tribunal by Electronic Means Regulations*). V rámci obdoby správního řízení umožňuje maltský právní řád komunikovat s příslušnými orgány jak písemně, tak elektronicky a mezi těmito formami nerozlišuje.[342] Co se týče doručování písemností do rukou občanů, tak v tomto případě nemá Malta nástroj a ani neumožňuje přijímat např. soudní písemnosti skrze elektronický prostředek.[343]

3.2.3. Rakouská republika

Rakousko se jako jediný stát střední Evropy vedle skandinávských a pobaltských států a některých států Beneluxu pravidelně umísťuje mezi špičkami evropských eGovernmentů. Za rok 2021 v rámci DESI umístilo celkově na 9. místě v oblasti „Digital public services" a dle Benchmarku je Rakousko s digitalizací se skóre 84 % a penetrací se skóre 81 % mezi tzv. „plodnými" eGovernmenty.[344]

Hlavním středobodem rakouského eGovernmentu jsou portál pro občany (oesterreich.gv.at) a portál pro podnikatele (usp.gv.at). Prostřednictvím portálu pro občany mají (nejen) tuzemští občané přístup k celé řadě informací souvisejících s interakcí s orgány veřejné správy v nejčastějších životních situacích. Současně mohou uživatelé rovnou vyřídit celou řadu úkonů

---

[341] Příloha nařízení o občanském řízení (úprava rejstříků, archivů a funkcí předsedy soudu (Gozo) a dalších soudních úředníků) [S.L. 12.21] [*Civil Procedure (Regulation of Registries, Archives and Functions of Director Courts (Gozo) and other Court Executive Officers) Regulations*]

[342] Podkapitola 3.1. písm. b), Směrnice č. 4-1, o standardech bezchybnosti služeb poskytovaných veřejnou správou veřejnosti a veřejným zaměstnancům, vydané dne 6. dubna 2017 státním tajemníkem na základě zákona o veřejné správě (*Standards for Service of Excellence Offered by the Public Administration to the Public and to Public Employees*).

[343] EVROPSKÁ KOMISE. Service of documents: official transmission of legal documents. Malta. *European e-Justice* [online]. [cit. 2022-05-05]. Dostupné z: https://e-justice.europa.eu/371/EN/service_of_documents_official_transmission_of_legal_documents?MALTA&member=1

[344] Srovnání EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Rakousko. Brusel: Evropská komise, 2021 [online]. [cit. 2021-25-11]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80575 a EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets,* op. cit. sub. 92, str. 6-8

jako je změna bydliště, nahlášení krádeže, žádost o vydání rodného listu, výpisu z rejstříku trestů nebo o voličský průkaz.[345]

Druhým významným portálem je portál pro podnikatele. Zde můžou například začínající podnikatelé založit jednočlennou obchodní korporaci, případně získat obdobu živnostenského oprávnění, změnit adresu svého sídla nebo přímo vystavit elektronickou fakturu federální vládě.

Mezi dalšími službami, které rakouský portál pro občana nabízí lze zmínit přístup do tzv. E-Tresoru, který je zabezpečené úložiště pro elektronický podepsané dokumenty, smlouvy, faktury apod. a přístup do elektronické schránky (Mein Postkorb) obdobné přístupu do datové schránky skrze český portál občana. Zajímavou součástí je odkaz na portál JustizOnline, kde má uživatel přímý přístup k informacím ohledně probíhajícího řízení, jehož je účastníkem, dále přístup do veřejných rejstříku nebo odkaz na formuláře, skrze které lze činit některé procesní úkony od klasického podání, exekuční návrh po uznání zahraničního rozhodnutí o osvojení.[346]

Obdobou českých základních registrů a ISVS je rakouský systém elektronického spisu tzv. ELAK (*Der elektronische Akt im Bund*), který nahradil papírový spis ve všech ústředních úřadech spolkové vlády. Hlavní myšlenkou ELAK je urychlená a zabezpečená výměna souborů mezi orgánem veřejné správy a občanem nebo orgány veřejné správy navzájem.[347] Bezpečnost dat je zajištěna prostřednictvím bezvýznamových identifikátorů fungujícím na obdobném principu jako AIFO a ZIFO. Namísto AIFO zná rakouský právní řád tzv. specifický sektorový identifikátor (*Bereichsspezifisches Personenkennzeichen*) a namísto ZIFO tzv. zdrojové číslo (*Stammzahl*).[348]

Nástroj rakouského eGovernmentu pro využívání služeb je tzv. Karta občana (*Bürgerkarte*). Jedná se o rakouský prostředek užívaný k elektronické identifikaci za použití fyzické karty a čtečky karet, podobně jako je to u eObčanky, ale i ke kvalifikovaném elektronickému podpisu ve smyslu článku 3 odst. 12 eIDAS. Na konci roku 2009 došlo k implementaci modelu aplikace v mobilním telefonu, jakožto prostředku elektronické identifikace a kvalifikovaného

---

[345] Srovnání ÖSTERREICHS REGIERUNG. Österreichs digitales Amt. *Oesterreich.gv.at* [online]. [cit. 2022-10-03]. Dostupné z: https://www.oesterreich.gv.at/public.html a ÖSTERREICHS REGIERUNG. Das digitale Unternehmensservice. *Unternehmensservice Portal* [online]. [cit. 2022-10-03]. Dostupné z: https://www.usp.gv.at

[346] Ibid.

[347] EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2019.* Austria. Brusel: Evropská komise, 2021 [online]. [cit. 2022-07-03], str. 26. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Austria_2019_3.pdf

[348] Ustanovení § 6 až 9 E-GovG

elektronického podpisu zároveň (*Handy – Signatur*). Rozdíl oproti kartě občana byl v tom, že nebylo nadále nutné vlastnit fyzickou čtečku karet, ale každý uživatel Handy Signatur se mohl pomocí aplikace v mobilními telefonu elektronicky identifikovat a zároveň připojit svůj kvalifikovaný elektronický podpis. V případě, že právní předpisy stanoví povinnost identifikovat se při využívání služeb eGovernmentu, má uživatel možnost využít jeden z výše uvedených prostředků.[349]

Jádro právního rámce rakouského eGovernmentu je zákon BGBl. Č. 10/2004, o předpisech pro usnadnění elektronické komunikace s orgány veřejné moci (zákon o eGovernmentu – E-GovG), ve znění pozdějších předpisů [*Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz)*] (dále jen „**E-GovG**“). Mezi další rakouské spolkové předpisy klíčové pro rakouský eGovernment lze zařadit zákon BGBl. č. 51/1991, všeobecný správní řád (*Allgemeines Verwaltungsverfahrensgesetz*) (dále jen „**AVG**“), zákon BGBl. č. 1982/200, o doručování písemností [Bundesgesetz über die Zustellung behördlicher Dokumente (Zustellgesetz – ZustG)] (dále jen „**ZustG**“), a zákon BGBl. č. 50/2016, o elektronickém podpisu a službách vytvářejících důvěru v elektronických transakcích [Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)] (dále jen „**SVG**“), který implementuje eIDAS.[350]

E-GovG jako klíčový předpis především definuje základní pojmy a pravidla fungování rakouského eGovernmentu. Pravděpodobně nejzásadnější novela tohoto předpisu, od jeho přijetí v roce 2004, byla v souvislosti s takzvaným „deregulačním zákonem“ BGBl. č. 40/2017.[351] Ten zakotvil do E-GovG nová ustanovení § 1a, které stanovilo právo na elektronickou komunikaci pro každého, a § 1b stanovující pro podnikající osoby podle § 3 BGBl. č. 193/1999, zákona o spolkové statistické činnosti (*Bundesgesetzes über die*

[349] Srovnání FEDERAL MINISTRY REPUBLIC OF AUSTRIA DIGITAL AND ECONOMIC AFFAIRS. Mobile Phone Signature. *Bundesministerium Digitalisierung und Wirtschaftsstandort* [online]. [cit. 2022-11-05]. Dostupné z: https://www.bmdw.gv.at/en/Topics/Digitalisation/For-citizens/Mobile-Phone-Signature.html a EVROPSKÁ KOMISE, op. cit. sub. 115, str. 27

[350] HÖCHTL, Bettina, LAMPOLTSHAMMER, Thomas J. Rechtliche Rahmenbedingungen und technische Umsetzung von E-Government in Österreich. In: STEMBER, J. et al. *Handbuch E-Government*. Wiesbaden: Springer Gabler, 2018 [online]. str. 2. Dostupné z: https://doi.org/10.1007/978-3-658-21596-5_10-1

[351] Zákon BGBl. I Nr. 40/2017, kterým se mění E-GovG a některé další zákony (deregulační zákon) [*mit dem das E-Government-Gesetz und anderen Gesetze geändert werden (Deregulierungsgesetz 2017)*]

Bundesstatistik), povinnost k registraci k elektronické komunikaci s výjimkou těch, kteří nejsou registrování k platbě DPH z důvodu nedostatečného obratu.

Rakousko je také státem, který implementoval jistou verzi elektronické identifikace ještě před přijetím eIDAS, a to od účinnosti E-GovG v roce 2004. Prvním takovým prostředkem je Bürgerkarte se strojově čitelným čipem, která v souladu s § 4 odst. 1 a 2 E-GovG v původním znění umožňovala jak prokázání totožnosti elektronicky, tak elektronický podpis. Kolem roku 2012 byla následně představa i tzv. virtuální identita, která současně umožňovala učinit elektronický podpis, a to prostřednictvím Handy-Signatur.[352]

Elektronické doručování a elektronickou komunikaci dále upravuje ZustG, na který E-GovG odkazuje. Hlavním východiskem pro elektronické doručování je již zmíněná registrace do tzv. Adresáře účastníků elektronické komunikace (*Teilnehmerverzeichnis*) za použití Bürgerkarte nebo Handy - Signatur ve smyslu § 2 odst. 10 E-GovG. Adresář účastníků obsahuje zejména identifikační údaje uživatelů, kteří se dobrovolně přihlásili k elektronickému doručování a uživatelů, kteří jsou přihlášeni ex lege jako např. advokáti, notáři, finanční a úvěrové instituce, pojišťovny a další subjekty ve smyslu § 89c odst. 5 spolkového zákona RGBl. č. 217/1896 o organizaci soudů (*Gerichtsorganisationsgesetz*) a již výše uvedené podnikající osoby. Údaje jsou v souladu s § 28b odst. 2 ZustG průběžné aktualizovány automaticky, jsou-li dostupné z evidencí vedených správními orgány. V ostatních případech má účastník povinnost oznámit jakoukoliv změnu vedených údajů. Subjekty, které nemají zákonnou povinnost komunikovat elektronicky se mohou obdobně z Adresáře účastníků odhlásit ve smyslu § 28b odst. 6 ZustG.

Zajímavým konceptem v oblasti elektronické komunikace se státem je oprávnění soukromých doručovacích služeb doručovat oficiální dokumenty (vyjma právních předpisů) jménem orgánu veřejné moci. A to za předpokladu, že jsou právně spolehlivé s ohledem na ochranu osobních údajů, splňují technické, organizační a další požadavky ve smyslu § 29 odst. 1 ZustG a především získali povolení (akreditaci) Spolkového ministerstva digitalizace a ekonomických záležitostí.[353] Oproti tomu české datové schránky provozované Ministerstvem vnitra jsou jediný instrument pro oficiální elektronické doručování. Český právní řád tak nemá obdobný model akreditace pro elektronické doručování jako je tomu například u elektronické

[352] FUTUREZONE. *Handy-Signatur im Test: Mühsam zum Ziel*. Vídeň: Future Zone, 2012 [online]. Dostupné z: https://futurezone.at/digital-life/handy-signatur-im-test-muehsam-zum-ziel/24.588.429e
[353] Ustanovení § 29 odst. 3 ZustG

identifikace, kterou může poskytovat vícero subjektů soukromých i veřejných v souladu s eIDAS.

Doručovací orgán nebo akreditovaná doručovací služba má povinnost před odesláním oficiálního dokumentu zjistit z Adresáře účastníků, zda je zde adresát registrován. Pakliže ano, písemnost mu musí být zaslána elektronicky. ZustG předpokládá dvě základní varianty elektronického doručení. Doručení s potvrzením o doručení (*Zustellnachweis*) a doručení bez potvrzení. Doručení s potvrzením o doručení nastává automaticky následující pracovní den po obdržení elektronické notifikace na adresu uvedenou v Adresáři účastníků v případě, že nesplňuje podmínky pro udělení výjimky z této zásady.[354] Přístup k dokumentu má adresát následně po své identifikaci a autentizaci jedním z dostupných prostředků, kterým potvrdí přijetí příslušného dokumentu.[355]

Rakouská právní úprava již od roku 2016 v souvislosti s přijetím SVG zakotvila do E-GovG once only zásadu, která garantuje subjektu údajů právo opakovaně neposkytovat údaje orgánům veřejné moci, pakliže je má k dispozici a jsou zjistitelné se souhlasem subjektu nebo na základě zákonného zmocnění.[356] Konkrétně původní znění ustanovení § 17 odst. 2 E-GovG v překladu zní: „*Mají-li přesnost údajů obsažených v elektronickém registru veřejného zadavatele posoudit orgány veřejné moci, provedou v souladu s technickými možnostmi, existuje-li souhlas subjektu údajů s určením údajů nebo zákonné zmocnění k úřednímu určení údajů, určení údajů samy prostřednictvím dálkového přenosu údajů, je-li to nezbytné.“*[357] Jedná se o významný posun oproti původnímu textu E-GovG, který znemožňuje orgánům veřejné moci libovolně nevyužívat dostupné údaje na základě vlastního uvážení a jednoznačně stanovuje povinnost tyto informace zjišťovat.

Lze shrnout, že rakouská právní úprava je tedy o poznání mnohem koncentrovanější než tuzemská. Základ celého právního rámce tvoří převážně jeden klíčový předpis, dalo by se říci kodex, E-GovG, který kromě základních pojmů a pravidel, poskytuje právní rámec pro elektronickou identifikaci, ochranu osobních údajů a elektronickou komunikaci. Součástí jsou i též principiální ustanovení, které garantují právo elektronické komunikace a jednoznačné

[354] Ustanovení § 35 odst. 6 ZustG
[355] HÖCHTL, Bettina, LAMPOLTSHAMMER, Thomas J. Rechtliche Rahmenbedingungen und technische Umsetzung von E-Government in Österreich. In: STEMBER, J. et al., op. cit. sub.116, str. 17
[356] EVROPSKÁ KOMISE, op. cit. sub. 115, str. 16
[357] Novela E-GovG, spolkový zákon BGBl. č. 32/2018 mimo jiné upřesnila, že se jedná o „osobní“ údaje ve větě první a subjekt „veřejného zadavatele“ (*Auftraggebers*) byl nahrazen „zodpovědnou osobou“ (*Verantwortlichen*)

zakotvení once only zásady. Úprava obecného správního řízení v AVG vytváří právní rámec elektronické komunikace s orgány veřejné správy, kdy výslovně umožňuje činit úkony vůči veřejné správě elektronicky s odkazem na E-GovG.[358] ZustG pak dále upravuje podrobněji způsob elektronického doručování (mimo klasické doručování oficiálních dokumentů).

Zajímavostí na závěr této kapitoly jsou i snahy do rakouského právního řádu, ale především do fungování veřejné moci včetně veřejné správy, integrovat inovativní ICT. V půlce roku 2019 představila rakouská vláda strategii pro využití umělé inteligenci v celé škále veřejných sektorů, mezi kterými lze nalézt stavebnictví, energetiku nebo zemědělství. Tato strategie například výslovně zmiňuje snahu o zapojení umělé inteligence do projektování staveb pomocí BIM, kterému jsem se již věnoval v kapitole 2.8.3.[359] Současně je jedním ze společných cílů vytvoření ekosystému, ve kterém dojde k zapojení umělé inteligence i do samotné veřejné správy a tímto způsobem k její modernizaci.[360] Druhou novinkou byla iniciativa rakouského města Scheibbs ve spolupráci s Federálním centrem výpočetní technologie (*Bundesrechenzentrum*), kdy v rámci projektu elektronické participace dostali občané zmíněného města možnost pomocí virtuální reality prozkoumat, respektive navštívit, několik různých modelů renovace mostu přes řeku Erlauf a následně za pomocí zabezpečeného modelu elektronického hlasování pomocí protokolu blockchain hlasovat o preferované variantě.[361]

3.2.4. Slovenská republika

V rámci srovnání vybraných států v této diplomové práci je Slovenská republika jediným státem, který je dle DESI i Benchmarku hodnocen hůře než Česká republika. Podle DESI je celkově na 22. místě, přičemž nejhoršího výsledku dosahuje právě v oblasti digitálních veřejných služeb, kde je celkově na 23. místě. Naopak nejlepší výsledek je 19. místo v oblasti lidského kapitálu a konektivity.[362] Dle Benchmarku je poměr penetrace (68%) a digitalizace

[358] Např. ustanovení § 18 odst. 3 a 4 AVG
[359] MINISTERSTVO PRŮMYSLU A OBCHODU, op. cit. sub. 17, str. 16
[360] FEDERAL MINISTRY REPUBLIC OF AUSTRIA DIGITAL AND ECONOMIC AFFAIRS. Strategy of the Austrian Federal Government for Artificial Intelligence "AIM AT 2030". *Bundesministerium Digitalisierung und Wirtschaftsstandort* [online]. [cit. 2022-11-05]. Dostupné z: https://www.bmdw.gv.at/en/Topics/Digitalisation/Strategy/Artificial-Intelligence.html
[361] BUNDESRECHENZENTRUM. *Building bridges: e-participation combined with virtual reality.* Vídeň: Bundesrechenzentrum, 2020 [online]. [cit. 2022-11-05]. Dostupné z: https://www.brz.gv.at/en/how_we_operate/e-participation-combined-with-virtual-reality-.html
[362] EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Slovensko. Brusel: Evropská komise, 2021 [online]. [cit. 2022-19-06]. str. 4. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80581

(61%), víceméně vyrovnaný, avšak celkově se slovenský eGovernment pohybuje na hranici tzv. „nevyužitých eGovernmentů“ a „nekonsolidovaných eGovernmentů“.[363]

Obdobou slovenského *one stop shopu* pro slovenský eGovernment je ústredný portál verejnej správy slovensko.sk,[364] který je v souladu s SDGR.[365] Skrze něj mají jak občané, tak „podnikatelé“ přístup k celé řadě sektorových služeb. Zde mohou například ohlásit živnost, přihlásit se k trvalému pobytu, zažádat o vydání občanského průkazu nebo o výpis z různých rejstříků a evidencí.[366] Ústredný portál verejnej správy je též tzv. přístupovým místem (*prístupové miesto*) ve smyslu § 5 odst. 1 slovenského zákona č. 305/2013 Zb., o elektronické podobě výkonu působnosti orgánů veřejné moci a o změně a doplnění některých zákonů (zákon o e-Governmentu) [*o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)*] (dále jen „**SZeGOV**“). Ustanovení § 4 odst.2 SZeGOV definuje přístupové místo jako „*komunikační rozhraní, jejichž prostřednictvím lze provádět elektronickou komunikaci, která je určena k zajištění kontaktu mezi orgánem veřejné moci a osobami, o jejichž právech, právem chráněných zájmech a povinnostech orgány veřejné moci při výkonu veřejné moci elektronicky jednají nebo ve vztahu ke kterým veřejnou moc vykonávají.*“ Kromě Ústredného portálu jsou přístupovým místem též specializované portály pro konkrétní agendy, integrovaná obslužná místa (v podstatě obdoba kontaktních míst veřejné správy ve smyslu Zákona o EÚAK, tj. Czech POINTů) a ústřední kontaktní centrum, které poskytuje informace o výkonu a činnosti orgánů veřejné správy a posuzuje, zda nejsou v rozporu se zvláštními předpisy.[367]

Asi nejmarkantnější rozdílností oproti české právní úpravě je téměř absolutní konsolidovanost slovenské úpravy eGovernmentu do jednoho právního předpisu, a sice do SZeGOV. Tento zákon, kromě již zmíněných přístupových míst, upravuje též elektronickou identifikaci a autentizaci[368], elektronické schránky a elektronické doručování[369], vládní cloud[370], elektronické

[363] EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets,* op. cit. sub. 92, str. 98
[364] https://www.slovensko.sk/sk/titulna-stranka
[365]EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2021*. Slovakia. Brusel: Evropská komise, 2021 [online]. str. 10. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Slovakia_vFinal.pdf
[366] NÁRODNÁ AGENTÚRA PRO SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY. Úvodní stránka. *Slovensko.sk, ústredný portál verejnej správy* [online]. [cit. 2022-19-06]. Dostupné z: https://www.slovensko.sk/sk/clanok/_vybrane-e-sluzby
[367] Ustanovení § 5 odst. 1-5 SZeGOV
[368] Ustanovení § 19–23a SZeGOV
[369] Ustanovení § 11–16 a § 24–34 SZeGOV
[370] Ustanovení § 10a SZeGOV

konverze[371], ale i informační systémy (nazvané jako společné moduly a agendové systémy)[372] a referenční registry[373].

Elektronická identifikace má na Slovensku svou historii od nabytí účinnosti SZeGOV (od konce roku 2013) v podobě občanského průkazu se strojově čitelným čipem. Slovenští občané tak mají možnost se identifikovat a autentizovat přes hardware čtečku těchto karet a počítačový software, který umožňuje tuto kartu „přečíst".[374] Kromě toho SZeGOV předpokládá mezi dalšími prostředky elektronické identifikace tzv. autentizační certifikát, tedy elektronický dokument vydaný pro účely identifikace a autentizace při automatizovaném přístupu k informačnímu systému nebo elektronické komunikaci elektronickou schránkou.[375] Současně se slovenská právní úprava odvolává i na další prostředky, a to ty, které splňují požadavky kladené eIDAS.

Úprava elektronického doručování a odesílání je v mnoha ohledech téměř totožná s českou právní úpravou. Slovenský eGovernment poskytuje službu tzv. elektronické schránky, která je velmi podobná české datové schránce. Elektronická schránka je též zřizována bezplatně a pro konkrétní právní postavení (tj. fyzická nebo fyzická podnikající osoba atd.) je možné mít zřízenou pouze jednu elektronickou schránku.[376] Slovenskou elektronickou schránku ovšem zřizuje orgán veřejné moci automaticky všem právnických, podnikajícím fyzickým a fyzickým osobám, které dovršily 18. let.[377] To je zásadní rozdílnost oproti české právní úpravě, kde došlo až v důsledku DEPO za daných podmínek k (byť v některých ohledech pochybnému) mechanismu automatického zřizování datových schránek. Rozdílem také je, že samotným zřízením fyzické a fyzické podnikající osobě automaticky nevznikají práva využívat doručování do té které elektronické schránky a povinnosti toto doručování strpět.

Aby bylo do elektronické schránky doručováno, počítá slovenská právní úprava s institutem tzv. aktivace elektronické schránky ve smyslu § 13 odst. 1 SZeGOV. Pokud není elektronická schránka aktivována, orgán veřejné moci do ní nedoručuje.[378] Obdobně lze logicky

[371] Ustanovení § 35-39 SZeGOV
[372] Ustanovení § 4 odst. 1 a
[373] Ustanovení § 49-55 SZeGOV
[374] NÁRODNÁ AGENTÚRA PRO SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY. Vybrané e-služby. *Slovensko.sk, ústredný portál verejnej správy* [online]. [cit. 2022-19-06]. Dostupné z: https://www.slovensko.sk/sk/clanok/_vybrane-e-sluzby
[375] Srovnání ustanovení § a §22a odst. 1 SZeGOV
[376] Ustanovení § 12 SZeGOV
[377] Ustanovení § 11 odst. 1 a § 12 odst. 4 SZeGOV
[378] Ustanovení § 13 odst. 1 písm. b) SZeGOV

elektronickou schránku i deaktivovat u fyzických a fyzických podnikajících osob na jejich žádost.[379] Přístup do elektronické schránky je pak vykonáván buďto za pomocí občanského průkazu s čipem nebo prostřednictvím autentizačního certifikátu.[380]Okamžik doručení do elektronické schránky je řešen v souladu s § 32 odst. 2 až 4 SZeGOV fikcí, a to buď okamžikem, kdy došlo k potvrzení elektronické doručenky nebo uplynutím 15 denní lhůty, doručuje-li se do vlastních rukou. V ostatních případech se uplatní fikce doručení dnem doručení do elektronické schránky.

Druhým významným předpisem je slovenský zákon č. 95/2019 Zb., o informačních technologiích ve veřejné správě a o změně a doplnění některých zákonů [*o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov*] (dále jen „**SZoIT**"). „*Tato právní úprava nahradila předchozí zákon č. 275/2006 Sb. a zavedla systémovou změnu v řízení IT ve veřejné správě tím, že upravuje celý životní cyklus správy IT. Rozšířil také rozsah povinností veřejných institucí odpovědných za řízení IT, pokud jde o plánování, zadávání veřejných zakázek, implementaci, monitorování a hodnocení IT.*

Kromě toho SZoIT také usnadnil snižování nákladů při pořizování IT tím, že stanovil výhodnější licenční podmínky pro pořizování unikátních softwarových řešení. Nový zákon rovněž odráží změny, které přináší technologický vývoj a globální trendy, jež je třeba zohlednit, aby bylo možné naplnit očekávání občanů. V neposlední řadě zákon také zavádí kontrolní mechanismus, který má zajistit plnění povinností a nabídnout zpětnou vazbu o průběhu řízení IT. "[381]

SZoIT je tedy poměrně ojedinělým předpisem v oblasti právní úpravy eGovernmentu obecně. Jako jediný řeší praktické aspekty včetně prevence tzv. vendor lock-in[382], které se správou eGovernmentu přirozeně souvisí. V ostatních členských státech je tato úprava řešena spíše obecnými normami.

Posledním předpisem, který v souvislosti se slovenským eGovernmentem zmíním je novela slovenského zákona č. 71/1967 Zb., o správním řízení (správní řád) [*o správnom konaní (správny poriadok)*] (dále jen „**SlovSpŘ**"), zákon č. 177/2018 Zb., o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o

[379] Ustanovení § 14 odst. 2 písm. e) bod 1. SZeGOV
[380] Ustanovení § 13 odst. 4 SZeGOV
[381] EVROPSKÁ KOMISE, op. cit. sub. 120, str. 19
[382] Jedná se o situaci, kdy je v důsledku špatně nastavených právních vztahů s prvotním dodavatelem případná změna dodavatele přílišně nákladná.

zmene a doplnení niektorých zákonov (zákon proti byrokracii). Tento zákon je podobně jako DEPO souhrnem dílčích novel celé řady předpisů. Za zmínku stojí zejména novelizace SlovSpŘ, která zakotvuje do slovenského právního řádu once only zásadu. „*Údaje z informačních systémů veřejné správy a výpisy z nich, kromě údajů a výpisů z rejstříku trestů, se považují za všeobecně známé skutečnosti a jsou použitelné pro právní účely. Tyto údaje nemusí účastník řízení a zúčastněná osoba správnímu orgánu prokazovat doklady. Doklady vydané správním orgánem a obsah vlastních evidencí správního orgánu se považují za skutečnosti známé správnímu orgánu z úřední činnosti, které nemusí účastník řízení a zúčastněná osoba správnímu orgánu dokládat*.“[383]

Jak je však z výše uvedeného patrné, převážná většina právní úpravy eGovernmentu je vtělena do jednoho předpisu, na který přirozeně navazují další změny, které však přímo eGovernment jako takový neupravují. Slovenský případ též může indikovat, že koncentrace právní úpravy nutně nesouvisí s kvalitou eGovernmentu jako takového.

3.2.5. Shrnutí

V rámci podkapitoly 3.2 jsem komparoval zahraniční úpravy eGovernmentu ve vybraných státech na základě čtyř základních kritérií, a to 1) jakým způsobem je právní úprava systematizována, 2) zda existovala metoda elektronické identifikace před přijetím eIDAS, 3) jestli právní řád umožňuje doručování oficiálních dokumentů a písemností elektronickými prostředky, a 4) zda a kde je zakotvena once only zásada.

V rámci právní úpravy lze pozorovat zásadní rozdíly ve způsobu úpravy právního rámce pro eGovernment v jednotlivých státech. Jak v České republice, tak i na Maltě se jedná o značnou roztříštěnost této úpravy oproti zbylým dvou sledovaným státům. Právní řády České republiky, ani Malty neobsahují jeden konkrétní kodex, který by fungoval jako základ právního rámce, na který by navazovaly dílčí právní předpisy. Opakem je pak Estonsko, Rakousko a Slovensko, kde je úprava převážně koncertovaná v AvTeS (Estonsko), v E-GovG (Rakousko) a v SZeGOV (Slovensko). Tyto předpisy neupravují kompletně každý dílčí institut toho, co lze nazývat eGovernmentem (snad s výjimkou Slovenska), neboť ze samé podstaty se jedná o velmi široké pole. Přesto lze dle mého názoru zmíněné předpisy považovat za určitou formu koncentrace, neboť přinejmenším upravují základní instituty a zásady místního eGovernmentu a fungují jako

[383]Ustanovení § 32 odst. 2 SlovSpŘ

lex generalis. Na tyto kodexy pak navazují další předpisy jako *lex specialis*, které upravují spíše dílčí oblasti jako je doručování v Rakousku nebo elektronická identifikace v Estonsku.

Již jsem zmínil elektronickou identifikaci v Estonsku, bohužel v této oblasti byla Česká republika jediným státem, který nenastavil právní rámec takovým způsobem, aby bylo možné reálně využívat služby elektronické identifikace, nejen při kontaktu s veřejnou správou, před přijetím eIDAS.

Naopak v oblasti doručování všechny státy, kromě Malty, k dnešnímu datu výslovně umožňují jak podávání, tak zejména doručování elektronických dokumentů jejich adresátům. Pro takovou službu současně vytvořily nebo přijaly nástroj, který umožňuje adresátům doručit elektronický dokument a současně ověřit, že k doručení došlo. Ověření o doručení pak má další význam zejména s ohledem na určení počátku běhu lhůt a podobně.

Klíčovou once only zásadu výslovně zakotvilo všech pět zkoumaných států různými způsoby ve svém právním řádu. Zatímco Estonsko a Rakousko je přijalo do svých kodexů, Česká republika, Malta a Slovensko je zakotvily do ustanovení jednoho z dílčích předpisů. Toto ustanovení je obecně uplatnitelné při jakékoliv formě využívání služeb eGovernmentu.

Pro lepší přehlednost níže přikládám tabulku srovnání jednotlivých prvků právní úpravy eGovernmentu ve zkoumaných státech (viz Tabulka č. 1).

	ČR	**Estonsko**	**Malta**	**Rakousko**	**Slovensko**
Právní úprava eGov.	Difúzní	Koncentrovaná (AvTeS + navazující)	Difúzní	Koncentrovaná (E-GovG + navazující)	Koncentrovaná (SZeGOV)
e-Identifikace (před eIDAS)	NE	ANO	ANO	ANO	ANO
e-Doručování písemností	ANO (Datová schránka)	ANO (např. email @eesti.ee)	NE (pouze podání)	ANO (Mein Postkorb a akreditované služby)	ANO (Elektronická schránka)
Once only zásada	ANO (§ 7 až 9 ZPDS)	ANO (§43[1] AvTeS)	ANO (Článek 25 písm. e) ReUseAct)	ANO (§ 17 odst. 2 E-GovG)	ANO (§ 32 odst. 2 SlovSpŘ)

Tabulka č. 1 *- Tabulka srovnání jednotlivých prvků právní úpravy eGovernmentu ve zkoumaných státech, autor textu*

4. Právo eGovernmentu

Český eGovernment ve své podstatě první kroky zaznamenal v okamžiku přijetí ZoISVS, byl to okamžik, který postavil základy budoucímu rozvoji, na který další právní úprava a s ní související projekty navazovaly. Po dlouhé období se právní úprava eGovernmentu věnovala pouze vytváření právního rámce pro konkrétní projekty. Tyto projekty vznikaly na základě společenské poptávky a politické vůle zákonodárce reformovat praktickou stránku veřejné správy a zapojovat jí do procesu digitalizace. Současně lze podobný trend k digitalizaci pozorovat i v dalších členských státech Evropské unie, ale co je důležitější, i v rámci politiky Evropské unie jako takové.[384] Vytváření eGovernmentu je tedy minimálně celoevropský trend, který jde logicky ruku v ruce i s proměnou práva jako takového. O existenci právní úpravy eGovernmentu není pochyb, pokládám si však otázku, zda lze vymezit specifické právní odvětví[385] právo eGovernmentu?

A. Gerloch definuje právní odvětví jako „*část práva, resp. systému práva, která se vyznačuje relativní autonomií v daném systému na základě rozlišujících znaků či kritérií. Právo dělíme na odvětví zejména podle tří kritérií: předmětu, způsobu a účelu právní regulace.“*[386]

Na základě této definice pak lze rozlišit dva kumulativní znaky:

1) část práva je relativně autonomní, a
2) její relativní autonomii tvoří konkrétní znaky či konkrétní kritéria.

Jaké tedy jsou konkrétní znaky či konkrétní kritéria právní úpravy eGovernmentu?

Právní úprava eGovernmentu se více či méně opírá o normy správního práva, které upravují povinnost státu budovat eGovernmentu, jsou nepřímou novelizací procesních norem správního práva, tj. SpŘ, ukládají orgánům veřejné moci, primárně orgánům veřejné správy, konkrétní povinnosti (např. povinnost využívat údaje z elektronických evidencí), stejně jako práva a

[384] Např. Evropský Kompas a Cesta k digitální dekádě

[385] Používám zjednodušeně pojem odvětví, byť samozřejmě problematika v teoreticko-právní rovině je poměrně složitější. Jak uvádí A. Gerloch „*Kritérium předmětu právní regulace spočívá v rozdílech v charakteristice společenských vztahů upravovaných právními normami. V zásadě z tohoto kritéria vychází dělení práva na ústavní, občanské, obchodní, pracovní, rodinné, správní, trestní, finanční právo a event. další P. Podle způsobu právní regulace se v kontinentálním typu právní kultury vydělují dvě velká P.: právo soukromé a právo veřejné. Vztah účelu a prostředku je u základu rozdělení práva na právo hmotné a na právo procesní.“* (cit. GERLOCH, Aleš. [Právní odvětví] In: HENDRYCH, Dušan. op. cit. sub. 20). Při zpracování této problematiky budu tedy z výše uvedené definice vycházet.

[386] Ibid.

povinnosti adresátům výkonu veřejné správy (např. právo na zřízení datové schránky a odpovídající povinnost strpět právní fikci doručení do datové schránky).

Ve správním právu se rozlišuje obecná a zvláštní část. Obecná část upravuje v zásadě pojmy, zásady, instituty a úpravu, která je společná pro veškerou veřejnou správu.[387] Zvláštní část obsahuje hmotněprávní úpravu v jednotlivých oborech činnosti veřejné správy v tzv. správních odvětvích (např. stavební právo).[388] Jak jsem již uvedl v kapitole 1, eGovernment je činnost, při které dochází k zapojování ICT do činnosti veřejné správy a digitalizaci veřejné správy. Není to dle mého názoru pouze jednostranný vztah, kdy je veřejná správa pasivní a zjednodušeně řečeno čeká na to, co jí bude závazným předpisem stanoveno za povinnost.

Na prvním místě samozřejmě stojí zákonodárce, který přijme konkrétní právní úpravu, která stanovuje veřejné správě konkrétní povinnosti. Nicméně pro realizaci takových povinností musí sama veřejná správa provádět určitou činnost, jelikož samotná právní úprava netvoří eGovernment. Co tvoří eGovernment je právě realizace právem předpokládaných projektů, tedy činnost veřejné správy, při které dochází k právem předpokládanému zapojení ICT ve veřejné správě. Součástí této činnosti je logicky i správa jednotlivých systémů na bázi ICT a plnění dalších souvisejících povinností. To jsou dle mého názoru konkrétní znaky takové právní úpravy. Konkrétní kritéria jsou pak dle mého názoru následující:

- **předmětem** takové právní úpravy je
  a) úprava právního rámce pro zapojování ICT do veřejné správy a digitalizaci veřejné správy a odpovídající povinnosti orgánů veřejné správy toto zapojování realizovat;
  b) úprava práv a povinností adresátů jako jsou jednotlivá práva na využívání eGovernmentu (blíže rozebrané v kapitole 2.9) nebo práva a povinnosti spojená s dílčími nástroji, službami a procesy v souvislosti s eGovernmentem; a
  c) dozorčí a kontrolní činnosti a správně právní odpovědnost v oblasti právní úpravy eGovernmentu;
- **způsobem** jsou závazné normy práva veřejného, a
- **účelem** je

[387] HENDRYCH, Dušan. *Správní právo: obecná část*. 9. vydání. V Praze: C.H. Beck, 2016. Academia iuris (C.H. Beck). str. 12. ISBN 978-80-7400-624-1.
[388] Ibid.

a) v hmotném právu úprava činnosti orgánů veřejné správy, stanovení konkrétních požadavků pro výkon veřejné správy v oblasti eGovernmentu a související práva a povinnosti; a
b) v procesním právu v širším smyslu úprava organizace a působnosti konkrétních orgánů veřejné správy v oblasti eGovernmentu, v užším specifika postupů při výkonu veřejné správy v této oblasti.

Domnívám se tedy, že lze pozorovat tendence k vytváření a zlepšování právního odvětví, které má výše uvedené znaky či kritéria. Jeho relativní autonomie pak v zásadě vychází z norem správního práva, proto bude zřejmě figurovat jako správní odvětví správního práva, tedy jako součást zvláštní části správního práva.

Na základě výše uvedeného se domnívám, že lze vyjádřit, že toto objevující se právo eGovernmentu je správním odvětvím, které je souborem právních norem, které upravuje zavádění a využívání informačních a komunikačních technologií v rámci činnosti veřejné správy, digitalizaci veřejné správy a související práva a povinnosti adresátů veřejné správy a povinnosti orgánů veřejné správy.

Právo eGovernmentu však není izolované a prostupuje i do jiných odvětví či oblastí práva. Lze zmínit například úpravu digitalizace ve stavebním právu, zdravotnickém právu nebo právu publikace právních předpisů. V případě úpravy datových schránek lze pozorovat přesah i do občanského práva procesního. Za zmínku stojí i úprava služeb vytvářejících důvěru pro elektronické transakce, která nepřímo zasahuje do soukromého práva, zejména pak do úpravy právního jednání.

Vymezení nového právního odvětví není bezvýznamové. Cílem je především definování pevných základů jak pro právní vědu, tak i pro samo zákonodárství. Právo eGovernmentu zcela jistě obsahuje celou řadu zajímavých právních otázek, které můžou být předmětem výzkumu. Ve vztahu k zákonodárství může definované odvětví práva na základě definovaných zásad fungovat jako korektiv pro další legislativní vývoj takového odvětví. Zásady práva eGovernmentu v zásadě vychází ze základních zásad činnosti správních orgánů nebo obecně platných zásad jako je ochrana osobních údajů apod. Nicméně i přesto se domnívám, že lze vyjádřit určité zásady určené především pro budoucí normotvorbu v oblasti práva eGovernmentu jako jsou například:

- *Zásada technologicky neutrální normotvorby*.[389] Již jsem zmínil, že vazba právní úpravy na konkrétní technologii může vzhledem k dynamickému rozvoji tohoto odvětví být naprosto kontraproduktivní.
- *Zásada once only*.[390] Tato již v ZPDS ukotvená zásada zaručuje, že jednou sdílené údaje vůči veřejné správě nebude veřejná správa opakovaně vyžadovat po jejím adresátovi, pokud má k takovým údajům přístup. Smyslem této zásady je cílení na zákonodárství v právu eGovernmentu v tom smyslu, aby zákonodárce úmyslně nastavoval právní úpravu takovým způsobem, která sdílení údajů za stanovených podmínek umožní, nikoliv znemožní. Tato zásada úzce souvisí se zásadou interoperability eGovernmentu, tedy zajištění schopnosti dílčích systémů vzájemně si vyměňovat informace.
- *Zásada dobrovolnosti* (právo ne povinnost).[391] Digitalizace je bezpochyby trend současné doby, stále ovšem existuje ve společnosti řada lidí, kteří ať už z důvodu digitální negramotnosti nebo z absence vůle nemají zájem na využívání eGovernmentu. Je zásadní, aby právní úprava nenutila fyzické osoby využívat eGovernment proti jejich vůli, a namísto toho je spíše motivovala. Nicméně dobrovolnost by se i do budoucna měla týkat výhradně fyzických nepodnikajících osob. Jak jsem již uvedl, na zapojení podnikatelů do eGovernmentu je veřejný zájem zejména s ohledem na efektivnější vymáhání povinností a zvýšení transparentnosti.
- *Zásada primární digitalizace* („digital by default“)[392], která zakotvuje prioritu, v případě vytváření právního rámce, vytvářet cestu pro digitalizaci konkrétní služby, je-li to s ohledem na podstatu té dané služby vhodné a možné.

Právo eGovernmentu je s ohledem na současný vývoj inovativních technologií dynamicky vznikajícím oborem. Zřejmě však bude docházet primárně k technologickým vylepšením, které nebudou v ideálním případě vyžadovat právní úpravu. Domnívám se, že právo eGovernmentu má i konkrétní systematiku, nikoliv pouze podle právní síly norem, jak je obvyklé, ale podle jejich významu s ohledem na fungování eGovernmentu jako takového.

---

[389] Tuto zásadu jsem nově definoval v kapitole 1.2.1, ovšem původně vychází ze zásady *technologické neutrality*, o které je výše uvedeno viz. HARAŠTA, Jakub, op. cit. sub. 27 nebo DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. § 13 [Právo na technologickou neutralitu] ZAJÍČEK, Zdeněk et al., op. cit. sub. 58, str. 138

[390] Tuto zásadu zmiňuje např. DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. § 7 [Právo na využívání údajů] In: Ibid., str. 92 nebo SDGR

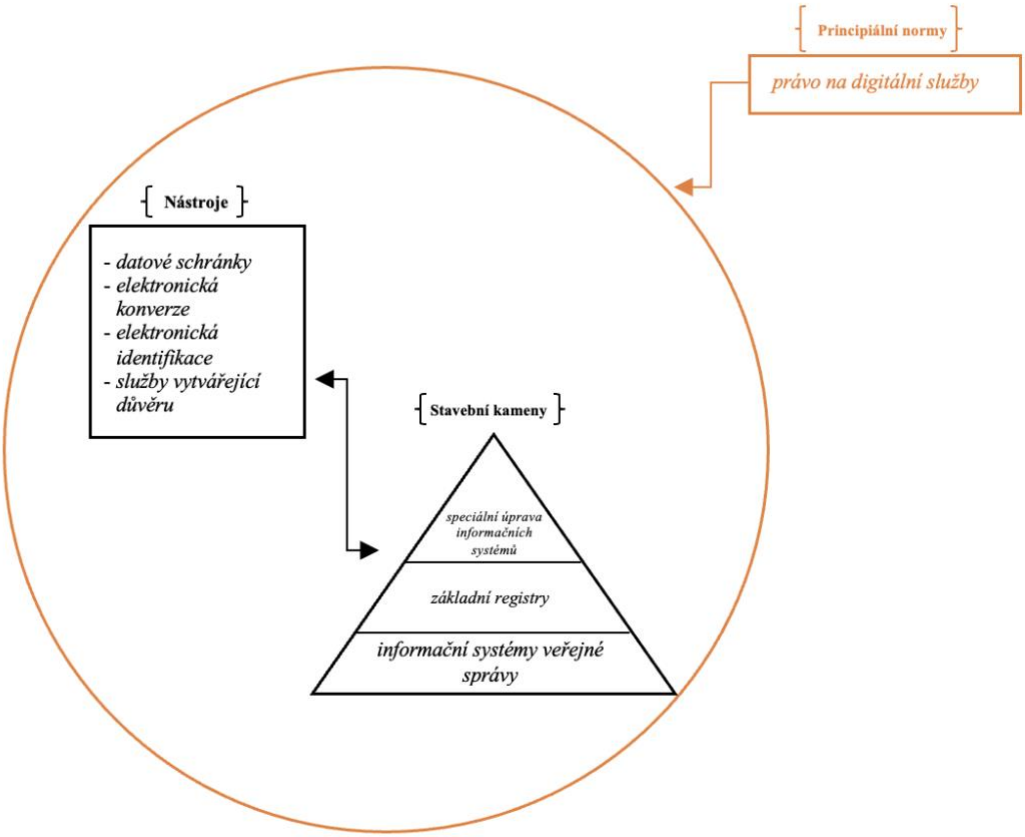
[391] Je odrazem např. § 14 odst. 1 ZPDS nebo koncepcí eIDAS II

[392] Uvádí jí např. DZURILLA, Vladimír, et al, op. cit. sub. 19, str. 6

Právní předpisy práva eGovernmentu v České republice nejsou obsaženy v žádném kodexu, naopak je právní úprava difúzní. Nutné je zdůraznit, že právo eGovernmentu v širším smyslu obsahuje i normy ústavního, správního nebo i soukromého práva. V užším smyslu lze funkční systematiku norem práva eGovernmentu v České republice rozdělit na následující kategorie.

- *Principiální normy eGovernmentu,* kam lze v současné době zařadit pouze ZPDS;
- normy upravující *základní stavební kameny eGovernmentu*, kam lze zařadit normy upravující informační systémy veřejné správy (ZoISVS), základní registry (ZoZR) a speciální úpravu informačních systémů veřejné správy vyjádřenou v dalších normách práva eGovernmentu (např. ZoEÚAK, ZeRecept, ZeZnám, NStavZ atd.); a
- normy upravující *nástroje eGovernmentu*, kam lze zařadit normy upravující datové schránky a elektronické konverze (ZoEÚAK), normy upravující elektronickou identifikaci (eIDAS a ZoEI) nebo normy upravující služby vytvářející důvěru pro elektronické transakce (eIDAS a ZoSVD).

Graficky lze vztah těchto norem vyjádřit následovně (viz obrázek č. 2)



Obrázek č. 2 - *Schéma funkční systematiky práva eGovernmentu, autor textu*

Principiální normy tvoří obecná pravidla, která jsou závazná jak pro právní úpravu nástrojů eGovernmentu, tak pro právní úpravu stavebních kamenů eGovernmentu.

Stavební kameny jsou záměrně znázorněny v pyramidě, jelikož jsou na sebe navazující. Informační systémy veřejné správy tvoří základní stavební kámen úpravy, na kterou navazuje úprava základních registrů jakožto speciálních informačních systémů veřejné správy zřízených jako centrální databáze klíčových údajů. Na ně následně navazuje speciální úprava informačních systémů v dílčích předpisech. Jak ZoZR, tak i speciální úprava v dílčích předpisech mají vztah vůči ZoISVS jako *lex specialis*.

Obousměrná šipka znázorňuje vztah mezi nástroji a základními kameny. Nástroje nejsou ve vzájemném vztahu nadřazenosti a podřazenosti a umožňují všem subjektům komunikovat s orgány veřejné správy, získávat údaje z informačních systémů či naopak takové údaje závazně veřejné správě poskytovat. Naopak informační systémy veřejné správy umožňují existenci dílčích nástrojů, jelikož právní úprava společně s každým právním nástrojem eGovernmentu vytváří příslušný informační systém, ve kterém jsou evidovány údaje o uživatelích toho kterého nástroje.

Toto schéma se výslovně vztahuje pouze na právní úpravu eGovernmentu v České republice, která je subjektem této diplomové práce. V rámci komparace v předchozí kapitole jsem zkoumal právní úpravu eGovernmentu i v ostatních státech a na tomto základě lze do budoucna vytvářet obdobná schémata, která budou v některých aspektech více či méně podobná. Ovšem zkoumání úpravy v dalších státech nebylo tak komplexní jako v případě České republiky, jelikož to téma ani rozsah této práce nedovoluje. Z tohoto důvodu nelze na zkoumaném základě takto stanovit schéma pro právní úpravy i jiných států. Obecně však lze říct, že každý právní řád obsahuje v rámci práva eGovernmentu jak úpravu stavebních kamenů, tj. úpravu informačních systémů, databází, zajištění interoperability a podobně, tak nástrojů, díky kterým mohou subjekty využívat nabízené služby eGovernmentu. Může se jednat o elektronické doručování, elektronickou identifikaci, elektronické podpisy, elektronické peněženky a další. Třetí část, tj. principiální normy pak mohou být upraveny přímo v některém z kodexů nebo dílčím předpise nebo i ve speciálním předpise jako je ZPDS.

Závěr

V první kapitole této práce jsem nabídnul několik relevantních definic eGovernmentu jako takového a vysvětlení rozdílů mezi některými často zaměňovanými pojmy. Na tomto základě jsem vymezil hlavní části „páteře eGovernmentu“, a to sice průběžně aktualizované databáze údajů relevantních v rámci veřejné správy, propojené komunikační sítí a nástroje, díky kterým může probíhat obousměrná komunikace mezi veřejnou správou a jejím adresátem. V závěru první kapitoly jsem poskytnul krátké zamyšlení nad potřebností digitalizace veřejné správy, respektive nad potřebností digitalizace a poukázal jsem na některá úskalí, která digitalizace přináší.

Druhá kapitola této práce je obsahově nejrozsáhlejší. V této kapitole nabízím detailní analýzu klíčových předpisů, které tvoří právní rámec eGovernmentu v České republice a vysvětlení fungování jeho jednotlivých institutů a instrumentů. Jedná se o právní úpravu základních registrů, informačních systémů veřejné správy, služeb vytvářejících důvěru pro elektronické transakce, datové schránky nebo elektronickou identifikaci.

Svou pozornost jsem dále zaměřil na problematiku elektronické identifikace pomocí datové schránky a fikce doručení v souvislosti s datovou schránkou. Zejména pak na nedávné novelizace, díky kterým bude fikce doručení platit i při komunikaci soukromoprávních subjektů a zároveň bude docházet i k automatickému zřizování datových schránek pro všechny uživatele elektronické identifikace. Poslední zmíněná změna přijatá v rámci DEPO pak vzbuzuje řadu otázek, zejména v tom smyslu, zda je takové plošné zřizování datových schránek nutné, či zda je vůbec v souladu se stěžejní zásadou dobrovolnosti vyjádřenou mimo jiné v ZPDS. Osobně se domnívám, že by takový zásah měl by být dostatečně odůvodněn (což se nestalo) a zcela jistě by měl být v souladu s dalšími předpisy práva eGovernmentu (což se domnívám, že také není). Je též důležité, aby stát dostatečně a včas informoval všechny dotčené subjekty o této povinnosti.

Dále jsem v druhé kapitole rozebral nejnovější legislativní změny, vycházející částečně z textu práce SVOČ. Jedná se o DEPO, právní úpravu služeb elektronické identifikace, zejména pak nejnovější bankovní identity, ale i o úpravu práva na digitální služby. Jak bankovní identita, tak právo na digitální služby přinášejí v právní úpravě eGovernmentu v České republice poměrně razantní změny, jejichž vývoj bude zajímavé sledovat v budoucnosti.

Kromě předpisů vysloveně spojených s eGovernmentem v užším smyslu jsem se dále zabýval i digitalizací v dalších oborech správního práva jako je stavební právo, zdravotnictví, provozu na pozemních komunikacích nebo publikace právních předpisů. V některých odvětvích jako je např. publikace právních předpisů lze pozorovat jistou formu rozpolcenosti nebo nerozhodnosti zákonodárce, kdy na jednu stranu vytváří dojem vzájemné zaměnitelnosti „papírové“ a „elektronické“ publikace právních případech a současně dává jasně najevo svou preferenci vůči elektronické.

Na závěr druhé kapitoly jsem zkoumal a potvrdil existenci nově definovaného veřejného subjektivního práva na využívání eGovernmentu, které je dle mého názoru uplatnitelné i vymahatelné a kterému odpovídá povinnost státu realizovat eGovernment. Toto právo se skládá z dílčích práv na využívání konkrétních projektů eGovernmentu a dílčích povinností realizovat konkrétní projekty eGovernmentu, jako jsou například datové schránky, základní registry nebo jednotlivé informační systémy.

Třetí kapitolu jsem rozdělil na dvě hlavní části. V první části jsem se věnoval právním předpisům a současnému přístupu Evropské unie k digitalizaci v rámci evropského prostoru. Za zmínku stojí především přijetí SDGR, které do budoucna zajistí uplatnění once only zásady v celém evropském prostoru a chystající se eIDAS II, které umožní všem evropským občanům se identifikovat, autentizovat a prokázat některý ze svých atributů jako je např. vzdělání, lékařské předpisy nebo očkování prostřednictvím Digi peněženky v mobilním telefonu.

V druhé části jsem pak komparoval právní úpravu eGovernmentu ve čtyřech evropských státech s Českou republikou. Jednalo se o státy, jejichž eGovernmenty jsou dlouhodobě velmi pozitivně hodnoceny DESI a Benchmarkem na rozdíl od České republiky (Estonsko a Malta, lze sem ostatně řadit i Rakousko). Nebo o státy, jejichž právně historické kořeny jsou blízké České republice (Rakousko a Slovensko).

Právní úpravu jsem pak porovnával na základě čtyř ukazatelů: 1) roztříštěnost/koncentrace právní úpravy; 2) právní úprava elektronické identifikace před přijetím eIDAS; 3) úprava doručování a přijímání elektronických písemností; a 4) zakotvení once only zásady v právním řádu. V druhém a čtvrtém ukazateli lze najít shody mezi jednotlivými státy. Naopak jednotlivé právní úpravy se liší v prvním ukazateli, kde jednoznačně roztříštěnou právní úpravu mají Česká republika a Malta.

U třetího ukazatele pak poněkud vyčnívá Malta, která je sice pozitivně hodnocena v oblasti digitální pošty, zároveň ale nemá zřízený nástroj a odpovídající právní úpravu, která by

umožňovala obousměrnou elektronickou komunikaci s veřejnou správou. Pozitivní hodnocení pak lze pravděpodobně přisoudit tomu, že DESI i Benchmark hodnotí digitální poštu v tom směru, zda lze komunikovat s veřejnou správou jakýmkoliv elektronickým prostředkem, tedy i emailem, což Malta umožňuje. Malta naopak nedisponuje obdobným nástrojem jako jsou např. datové schránky, které by umožňovaly nejen komunikaci, ale i transparentnost při přijímání a odesílání takových písemností.

Závěrem této komparace tedy není jednoznačné určení, že koncentrovaná právní úprava přispívá lepšímu eGovernmentu. Malta má roztříštěnou úpravou, zatímco Slovensko koncentrovanou. Oba státy však stojí na opačných krajích žebříčku kvality, vývoje a dostupnosti eGovernmentu. Ukazuje se však, že koncentrovaného přístup lze dosáhnout. Koncentrovanost právní úpravy pak dle mého názoru pravděpodobně napomáhá lepšímu právnímu porozumění a větší právní jistotě. Jedná se však o mou domněnku, nikoliv o podložené tvrzení.

Ve čtvrté a poslední kapitole jsem se na základě získaných znalostí v předchozích kapitolách zabýval potvrzením, případně vyvrácením v úvodu stanovené hypotézy, a to sice: „*Právo eGovernmentu je specifické právní odvětví, které je tvořeno konkrétními právními předpisy a stojí na konkrétních právních zásadách jak pro jeho tvorbu, tak i aplikaci. Součástí práva eGovernmentu jsou i specifická práva a povinnosti všech zúčastněných subjektů.*“

Ve svém výzkumu jsem dospěl k tomu, že lze pozorovat tendence k vytváření a vylepšování takového právního odvětví, které je velmi pravděpodobně součástí zvláštní části správního práva. Předmětem tohoto správně právního odvětví je jednak právní úprava rámce pro zapojování ICT do veřejné správy a digitalizaci veřejné správy a jednak úprava práv a povinností adresátů i orgánů veřejné správy jako jsou jednotlivá práva na využívání eGovernmentu a povinnosti státu realizovat eGovernment nebo práva a povinnosti spojená s dílčími nástroji, službami a procesy v souvislosti s eGovernmentem. Kromě obecných zásad správního práva lze pozorovat čtyři hlavní zásady, které jsou součástí tohoto právního odvětví a které slouží především pro jeho tvorbu a aplikaci. Jedná se zásadu technologicky neutrální normotvorby, zásadu once only, zásadu dobrovolnosti a zásadu primární digitalizace. Konečně jsem pak z toho základu vytvořil funkční systematiku jednotlivých norem (nikoliv podle právní síly), které jsou součástí práva eGovernmentu. Jedná se o normy upravující základní stavební kameny eGovernmentu a normy upravující nástroje eGovernmentu, které mají mezi sebou kooperační vztah a principiální normy eGovernmentu, která regulují obě předchozí kategorie norem jako celek.

Pevně věřím, že výše uvedená zjištění poslouží do budoucnosti jako podklad pro další výzkum práva eGovernmentu jako nově se objevujícího právního odvětví. Současně si přeji, aby posloužily i pro budoucí zákonodárství v České republice, které nastaví právní rámec eGovernmentu takovým způsobem, díky kterému se český eGovernmentu bude v budoucnosti pohybovat v rámci DESbo Benchmarku v horní polovině úspěšných eGovernmentů.

Seznam použitých zdrojů

Seznam použité literatury

1. EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Method Paper 2020-2023. eGovernment benchmark 2021*. Brusel: Evropská komise, 2021. ISBN 978-92-76-36362-0
2. FELIX, Ondřej, KAUCKÝ, Jiří, KOLÁŘ, Jindřich, et al. *Jak se (z)rodil eGON: reforma a elektronizace veřejné správy*. Praha: CEVRO Institut, 2015. ISBN 978-80-87125-28-1
3. GERLOCH, Aleš. *Teorie práva*. 6. vydání. Plzeň: Aleš Čeněk, 2013. ISBN 978-80-7380-454-1
4. HARAŠTA, Jakub, 2017. *Princip technologické neutrality v kybernetické bezpečnosti*. Brno. Disertační práce. Masarykova univerzita v Brně. Právnická fakulta. Vedoucí práce POLČÁK, Radim.
5. HENDRYCH, Dušan. *Právnický slovník*. 3.vydání. V Praze: C.H. Beck, 2009. Beckovy odborné slovníky. ISBN 978-80-7400-059-1
6. HENDRYCH, Dušan. *Správní právo: obecná část*. 9. vydání. V Praze: C.H. Beck, 2016. Academia iuris (C.H. Beck). ISBN 978-80-7400-624-1.
7. JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. *Správní řád*. 6. vydání. Praha: C. H. Beck, 2019. ISBN 978-80-7400-751-4
8. JEMELKA, Luboš, VETEŠNÍK, Pavel, LIBOSVÁR, Ondřej. *Zákon o kontrole.* 2. vydání. Praha: C. H. Beck, 2021. ISBN 978-80-7400-840-5
9. KNAPP, Viktor. *Teorie práva*. Praha: C. H. Beck, 1995. ISBN 80-7179-028-1
10. KOOPS, Bert-Jaap, Miriam LIPS, Corien PRINS a Maurice SCHELLEKENS et al. *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. The Hague: T.M.C. Asser Press, 2006. ISBN: 978-90-6704-216-1
11. KOPECKÝ, Martin. *Správní právo: obecná část*. V Praze: C.H. Beck, 2019. Beckovy právnické učebnice. ISBN 978-80-7400-727-9
12. KÜHN, Zdeněk. *Soudní řád správní: komentář*. Praha: Wolters Kluwer, 2019. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-479-1

13. MATES, Pavel. *E-government v české veřejné správě*. Praha: Právní rozhledy, 2005, č. 8. ISSN: 1210-6410

14. MATES, Pavel a Vladimír SMEJKAL. *E-government v českém právu*. Praha: Linde, 2006. ISBN 80-7201-614-8

15. MÁCHA, Aleš, 2017. *Veřejné užívání a vlastnické právo.* Olomouc. Disertační práce. Univerzita Palackého v Olomouci, Právnická fakulta. Vedoucí práce TOMOSZKOVÁ, Veronika

16. NEŠPOR, Jan, 2021. *Aktuální legislativní změny a budoucnost eGovernmentu v České republice*. Praha. Práce v rámci Studentské vědecké odborné činnosti (SVOČ). Univerzita Karlova, Právnická fakulta. Vedoucí práce STAŠA, Josef.

17. PARSOVS, Arnis, 2021. *Estonian Electronic Identitty Card and its Security Challenges*. Tartu, Estonsko. Dizertační práce. Institute of Computer Science, Faculty of Science and Technology, University of Tartu, Estonia. Vedoucí práce UNRUH, Dominique.

18. PETERKA, Jiří, Podaný, Jan. *Problematika podání k soudu prostřednictvím datové schránky*. Praha: Bulletin advokacie. spojené 1. a 2. vydání z roku 2013. ISSN 1210-6348

19. POTĚŠIL, Lukáš, HEJČ, David, RIGEL, Filip, MAREK, David. Správní řád. 2. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-804-7

20. ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení.* V Praze: C.H. Beck, 2012. Beckova edice ekonomie. ISBN 978-80-7400-261-8

21. ŠUSTEK, Petr a Tomáš HOLČAPEK. *Zdravotnické právo*. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-321-1.

22. VOJTEK, Petr, BIČÁK, Vít. *Odpovědnost za škodu při výkonu veřejné moci*. 4. vydání. Praha, C. H. Beck, 2017. ISBN 978-80-7400-670-8

23. VYŠKOVSKÝ, Pavel, 2014. *e-Government*. Praha. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce KORBEL, František.

24. ZAJÍČEK, Zdeněk a kol. *Zákon o právu na digitální služby: komentář*. Praze, C.H. Beck, 2021. Beckovy komentáře. ISBN 978-80-7400-822-1

25. *Zborník priíspevkov z Medzinárodnej vedeckej konference konanej v dňoch 9. – 10 mája 2019 v Trnave.* Veřejná správa, právo na spravodlivý proces a e-government. Trnava: Právnická fakulta, Trnavská univerzita v Trnave, 2019. ISBN 978-80-568-0321-9

Seznam použitých internetových zdrojů

1. ALA-HONKOLA, Päivikki. *Rada přijala nařízení o zřízení jednotné digitální brány: zlepší se online přístup k informacím a postupům v celé EU*. Tisková zpráva. Brusel: Rada EU, 2018 [online]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2018/09/27/single-digital-gateway-regulation-adopted-by-council-better-online-access-to-information-and-procedures-across-the-eu/
2. BERRYHILL, Jamie, BOURGERY, Théo, HANSON, Angela. Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. *OECD Working Papers on Public Governance* [online studie]. 2018, č. 28. ISSN: 19934351. Dostupné z: https://www.oecd-ilibrary.org/governance/blockchains-unchained_3c32c429-en
3. BLAŽEK, Tomáš, JIRÁSEK, Jan, MOLEK, Pavel, POSPÍŠIL, Petr, SOCHOROVÁ, Vendula, ŠEBEK, Petr. *Soudní řád správní – online komentář*. 3. vydání. V Praze: C. H. Beck, 2016 [online]. Dostupné z: https://www-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembrgzpw62zsl4zs443cl4zdambsl4ytkma
4. BOLIVAR, Manuel Pedro Rodriguez, et al. *Digital Government and Achievieng e_Public Participation: Emerging Research and Opportunities.* [online]. Hershey: IGI Global, 2020. ISBN: 978-1-7998-1529-7. Dostupné z: DOI:10.4018/978-1-7998-1526-6.ch005
5. CASTAÑOS, Virgina. *Case Study Report: e-Estonia.* [online]. Brusel: Evropská komise, 2018. Dostupné z: https://jiip.eu/mop/wp/wp-content/uploads/2018/10/EE_e-Estonia_Castanos.pdf
6. DZURILLA, Vladimír, et al. Digitální Česko. Vládní program digitalizace České republiky 2018+. Informační koncepce. Koncepce budování eGovernmentu v ČR 2018+ a jeho IT podpory podle zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. Praha: Úřad vlády České republiky, 2020. Dostupné z: https://www.digitalnicesko.cz/informacni-koncepce-cr/
7. E-ESTONIA. *Interoperabilitty services* [online]. Dostupné z: https://e-estonia.com/solutions/interoperability-services/x-road/
8. ESTONIAN ARTIFICIAL INTELLIGENCE DEPLOYMENT. *Estonia's national artificial intelligence strategy 2019 – 2021* [online]. Dostupné z: https://f98cc689-5814-

47ec-86b3-
db505a7c3978.filesusr.com/ugd/7df26f_27a618cb80a648c38be427194affa2f3.pdf

9. EVROPSKÁ KOMISE. *Case Study Report: e-Estonia* [online]. Dostupné z: https://jiip.eu/mop/wp/wp-content/uploads/2018/10/EE_e-Estonia_Castanos.pdf
10. EUROPEAN UNION AGENCY FOR CYBERSECURITY. *Cloud Computing Risk Assessment* [online]. Dostupné z: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
11. EVROPSKÁ KOMISE. *Digital Economy and Society Index (DESI) 2021*. DESI methodological note. Brusel: Evropská komise, 2021 *methodological note. Evropská Komise;* [online]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80560
12. EVROPSKÁ KOMISE. *Digital Economy and Society Indes (DESI) 2021.* Thematic chapters. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80563
13. EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2014.* Malta. Brusel: Evropská komise, 2021 [online]. Dostupné z https://joinup.ec.europa.eu/sites/default/files/document/2014-06/eGov%20in%20MT%20-%20March%202014%20-%20v.16.0_0.pdf
14. EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2021.* Austria. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Austria_2019_3.pdf
15. EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2021.* Estonia. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Estonia_vFinal.pdf,
16. EVROPSKÁ KOMISE. *Digital Public Administration factsheet 2021.* Slovakia. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2021_Slovakia_vFinal.pdf

17. EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Česko. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80581

18. EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Malta. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80497

19. EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Rakousko. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80575

20. EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021*. Slovakia. Brusel: Evropská komise, 2021 [online]. Dostupné z: https://ec.europa.eu/newsroom/dae/redirection/document/80581

21. VROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Background report. eGovernment benchmark 2021.* Entering a new digital government era. Brusel: Evropská komise, 2021 [online]. Dostupné z: DOI: 10.2759/798973

22. EVROPSKÁ KOMISE. GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOLOGIE. *Country Factsheets*. *eGovernment benchmark 2021*. Entering a new digital government era. Brusel: Evropská komise, 2021 [online]. Dostupné z: DOI: 10.2759/485079

23. FINANCIAL ACTION TASK FORCE. *FATF Guidance on digital identity In brief* [online]. Paříž: Financial Action Task Force, 2020. Dostupné z: https://www.fatf-gafi.org/media/fatf/documents/reports/Digital-ID-in-brief.pdf

24. GÁSPÁR, Pál, JAKSA, Anna Renata, RESTALL, Brian, XUEREB, Marisa. *The Development of eService in an Enlarged EU: eGovernment and eHealth in Malta*. Luxemburg: Office for Official Publications of the European Communities, 2008. ISSN 1018-5593

25. GOVERNMENT OF THE REPUBLIC OF ESTONIA. *Estonia's national artificial intelligence strategy 2019 – 2021*. Talin: Government of the Republic of Estonia. [online]. Dostupné z: https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_27a618cb80a648c38be427194affa2f3.pdf

26. GRIMA, Noel. *The basics of the Maltese legal system*. St.Julians: The Malta Independent, 2015 [online]. Dostupné z: https://www.independent.com.mt/articles/2015-04-13/books/The-basics-of-the-Maltese-legal-system-6736133706

27. HÖCHTL, Bettina, LAMPOLTSHAMMER, Thomas J. Rechtliche Rahmenbedingungen und technische Umsetzung von E-Government in Österreich. In: STEMBER, J. et al. *Handbuch E-Government*. Wiesbaden: Springer Gabler, 2018 [online]. Dostupné z: https://doi.org/10.1007/978-3-658-21596-5_10-1

28. KORBEL, František, KOVÁŘ, Dalibor, AMLER, Petr. *Interpretace elektronického podpisu a související identifikace v soukromém právu* [online]. Praha: Právní prostor, 2020. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/interpretace-elektronickeho-podpisu-souvisejici-identifikace-v-soukromem-pravu

29. MEDIAN. *Digitální gramotnost. Zpráva o stavu a výuce digitální gramotnosti a komparace se zahraničím.* Praha: Median, 2017. Dostupné z: https://www.mpsv.cz/documents/20142/225517/Digitalni_gramotnost__-_Zprava_o_stavu_a_vyuce_digitalni_gramotnosti_a_komparace_se_zahranicim.pdf/f633dd0f-e5df-c19f-7cfa-38291b31ceb4

30. MINISTERSTVO FINANCÍ. *Veřejná konzultace – blockchain, virtuální měny a aktiva* [online]. 30. 11. 2018. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613e-rozdil-mezi-pojmy-blockchain-a-dlt/

31. MINISTERSTVO VNITRA. *Koncepce budování eGovernmentu v ČR 2018+ a jeho IT podpory podle zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů* [online]. Praha: Ministerstvo vnitra. Dostupné z: https://www.digitalnicesko.cz/informacni-koncepce-cr/

32. MINISTERSTVO PRŮMYSLU A OBCHODU. *Koncepce zavádění metody BIM v České republice* [online]. Praha: Ministerstvo průmyslu a obchodu, 2017. Dostupné z: https://www.koncepcebim.cz/uploads/inq/files/Koncepce%20zaváděn%C3%AD%20metody%20BIM%20v%20ČR.pdf

33. VON BUTTLAR, Julia, BRAGELMANN, Tom. A Wonderful Step Towards Fully Dematerialized Securities: Germany Is Utterly Serious About Carrying Out Its Blockchain trategy With Europe. *The FinReg Blog. Global Financial Markets Center. Duke University School of Law* [online blog]. Dostupné z:

https://sites.law.duke.edu/thefinregblog/2021/01/05/a-wonderful-step-toward-fully-dematerialized-securities-germany-is-utterly-serious-about-carrying-out-its-blockchain-strategy-within-europe/?fbclid=IwAR2xdmiKh6VhbkvnjlYThJ4-yFYToV6ti5nYylTVFaZ4oWG3DJ6pe1HsAD8

34. PALVIA, Shailendra C. Jain, SHARMA, Sushil S. *E-Government and E-Governance: Definitions/Domain Frameworkd and Status around the World.* Karkala: Computer Society Of India, 2007. Dostupné z: http://governance40.com/wp-content/uploads/2019/06/E-Government_and_E-Governance_Definition.pdf

35. PETERKA, Jiří. Bankovní identita: 1,6 milionu aktivovaných identit, (snad) jen jedna SONIA a první ceník jejích služeb. *Lupa.cz*. *Server o českém internetu* [online]. Dostupné z: https://www.lupa.cz/clanky/bankovni-identita-1-6-milionu-aktivovanych-identit-snad-jen-jedna-sonia-a-prvni-cenik-jejich-sluzeb/

36. SAEBØ, Øystein et al. *The Shape of Eparticipation: Characterizing an Emerging Research Area* [online]. Amsterdam: Elsevier, 2007. Dostupné z: DOI:10.1016/j.giq.2007.04.007

37. SPENCER, Matthew. *What`s the difference between „electronic“ and „digital“?* Quora.com [online]. Dostupné z: https://www.quora.com/Whats-the-difference-between-electronic-and-digital

38. UNIVERSITY OF CAMBRIDGE. Význam slova „Digital“ v Cambridge English Dictionary. *Cambridge Dictionary*. *English Dictionary, Translations & Thesaurus* [online]. Copyright © Cambridge University Press. Dostupné z: https://dictionary.cambridge.org/dictionary/english/digital

39. VITNEROVÁ, Marika. *Tisková zpráva. První eObčanky se začnou vydávat od července* [online]. Praha: Ministerstvo vnitra. Dostupné z: https://www.mvcr.cz/clanek/prvni-eobcanky-se-zacnou-vydavat-od-cervence.aspx

40. ZAJÍČEK, Zdeněk a kol. *Zákon o právu na digitální služby: komentář*. V Praze: C.H. Beck, 2021. Beckovy komentáře. ISBN 978-80-7400-822-1

41. ZVIRAN, Moshe, ERLICH, Zippy. *Identification and Authentication: Technology and Implementation Issues* [online]. Tallahassee: Association for Information Systems, 2006. ISSN: 1529-3181. Dostupné z: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=2969&context=cais

Seznam použitých právních předpisů

Česká republika

1. Nařízení vlády č. 430/2006 Sb., o stanovení geodetických referenčních systémů a státních mapových děl závazných na území státu a zásadách jejich používání.
2. Vládní návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o lobbování
3. Vyhláška Ministerstva zdravotnictví č. 329/2019 Sb., o předepisování léčivých přípravků při poskytování zdravotních služeb
4. Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů
5. Zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů
6. Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů
7. Zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů, ve znění pozdějších předpisů
8. Zákon č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a některé další zákony
9. Zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů
10. Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
11. Zákon č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů
12. Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
13. Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
14. Zákon č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů

15. Zákon č. 187/2006 Sb., o nemocenském pojištění ve znění účinném k 1. březnu 2017
16. Zákon č. 195/2017 Sb., kterým se mění zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a další související zákony
17. Zákon č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv, ve znění pozdějších předpisů
18. Zákon č. 227/2019 Sb., kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů
19. Zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů
20. Zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů
21. Zákon č. 250/2017 Sb., o elektronické identifikace, ve znění pozdějších předpisů
22. Zákon č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci, ve znění pozdějších předpisů
23. Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů
24. Zákon č. 255/2012 Sb., o kontrole, ve znění pozdějších předpisů
25. Zákon č. 255/2014 Sb., kterým se mění zákon č. 70/2013 Sb., kterým se mění zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), ve znění pozdějších předpisů
26. Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, ve znění pozdějších předpisů
27. Zákon č. 262/2019 Sb., kterým se mění Zákon o léčivech, ve znění pozdějších předpisů
28. Zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů
29. Zákon č. 269/2007 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a další související zákony
30. Zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů
31. Zákon č. 283/2021 Sb., (nový) stavební zákon, ve znění pozdějších předpisů

32. Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
33. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
34. Zákon č. 325/2021 Sb., o elektronizaci zdravotnictví, ve znění pozdějších předpisů
35. Zákon č. 326/2021 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona č. 325/2021 Sb., o elektronizaci zdravotnictví
36. Zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů
37. Zákon č. 349/1999 Sb., o Veřejném ochránci práv, ve znění pozdějších předpisů
38. Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů, ve znění pozdějších předpisů
39. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně dalších zákonů, ve znění pozdějších předpisů
40. Zákon č. 372/2011 Sb., o zdravotnických službách a podmínkách jejich poskytování, ve znění pozdějších předpisů
41. Zákon č. 378/2007 Sb., o léčivech a o změnách souvisejících, ve znění pozdějších předpisů
42. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
43. Zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů
44. Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
45. Zákon č. 517/2002 Sb., kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé
46. Zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů

Estonská republika

1. Zákon o veřejných informacích (*Avaliku teabe seadus*, RT I 2000, 92, 567)
2. Zákon o správním řízení (*Haldusmenetluse seadus,* RT I 2001, 58, 354)
3. Zákon o dokladech totožnosti (*Isikut tõendavate dokumentide seadus,* RT I 1999, 25, 356)

Maltská republika

1. Nařízení o občanském řízení (úprava rejstříků, archivů a funkcí předsedy soudu (Gozo) a dalších soudních úředníků) [S.L. 12.21] [*Civil Procedure (Regulation of Registries, Archives and Functions of Director Courts (Gozo) and other Court Executive Officers) Regulations*].
2. Nařízení o organizačních strukturách pro sdílení dat a jejich opětovné použití [S.L. 546.01] (*Organisational Structures for Data Sharing and Re-Use* Regulations)
3. Podpůrný předpis o podávání návrhů elektronickými prostředky před tribunálem správního přezkumu [S.L. 490.05] (*Filings of Acts before the Administrative Review Tribunal by Electronic Means Regulations*).
4. Podpůrný předpis o pravidlech (podání pomocí elektronických prostředků) pro jednání před tribunálem malých nároků [S.L. 380.04] [*Small Claims Tribunal (Filing of Acts by Electronic Means) Rules*]
5. Podpůrný předpis o zřízení Identity Malta Agency [S.L. 595.07] (*IMA Establishment Order*)
6. Směrnice č. 4-1, o standardech bezchybnosti služeb poskytovaných veřejnou správou veřejnosti a veřejným zaměstnancům, vydané dne 6. dubna 2017 státním tajemníkem na základě zákona o veřejné správě (*Standards for Service of Excellence Offered by the Public Administration to the Public and to Public Employees*).
7. Zákon o opakovaném použití informací veřejného sektoru z roku 2015 ve znění pozdějších předpisů [Cap. 546] (*Re-Use of Public Sector Information Act*)

Rakouská republika

1. Zákon BGBl. Č. 10/2004, o předpisech pro usnadnění elektronické komunikace s orgány veřejné moci (zákon o E-Governmentu – E-GovG) ve znění pozdějších předpisů [*Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz)*]
2. Zákon BGBl. č. 32/2018, adaptační zákon, kterým se mění zákony o ochraně osobních údajů a ochraně věcí (*Materien-Datenschutz-Anpassungsgesetz*)
3. Zákon BGBl. I Nr. 40/2017, kterým se mění E-GovG a některé další zákony (deregulační zákon) [*mit dem das E-Government-Gesetz und anderen Gesetze geändert werden (Deregulierungsgesetz 2017*)]

4. Zákon BGBl. č. 50/2016, o elektronickém podpisu a službách vytvářejících důvěru v elektronických transakcích [Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)]
5. Zákon BGBl. č. 51/1991, všeobecný správní řád (*Allgemeines Verwaltungsverfahrensgesetz*)
6. zákon BGBl. č. 1982/200, o doručování písemností [Bundesgesetz über die Zustellung behördlicher Dokumente (Zustellgesetz – ZustG)]

Slovenská republika

1. Zákon č. 71/1967 Zb., o správnom konaní (správny poriadok)
2. Zákon č. 95/2019 Zb., o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
3. Zákon č. 177/2018 Zb., o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii)
4. Zákon č. 305/2013 Zb., o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

Evropská unie

1. Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 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)
2. Nařízení Evropského parlamentu a Rady (EU) č. 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
3. 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
4. Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, COM(2021) 281 final

5. Směrnice 2013/37/EU Evropského parlamentu a Rady, kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru
6. Směrnice Evropského parlamentu a Rady (EU) č. 2016/2102 ze dne 26. října 2016 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru
7. Směrnice 2019/1024 Evropského parlamentu a Rady o open datech a opakovaném použití informací veřejného sektoru

Seznam použité judikatury

1. Nález Ústavního soudu spisová značka Pl. ÚS 77/06 ze dne 15. února 2007
2. Nález Ústavního soudu spisová značka Pl. ÚS 21/14 ze dne 30. června 2015
3. Rozsudek Městského soudu v Praze č.j. 8 A 9/2015-29 ze dne 29. dubna 2015
4. Rozsudek Nejvyššího soudu č.j. 25 Cdo 2120/2000 ze dne 22. srpna 2002
5. Rozsudek Nejvyššího soudu č.j. 8 Tdo 517/2014 ze dne 7. května 2014
6. Rozsudek Nejvyššího správního soudu č.j. 1 Afs 148/2008-73 ze dne 6. března 2009
7. Rozsudek Nejvyššího správního soudu č.j. 3 As 26/2016-45 ze dne 30. listopadu 2016
8. Rozsudek Nejvyššího správního soudu č.j. 4 Afs 264/2018-85 ze dne 26. května 2022
9. Rozsudek Nejvyššího správního soudu č.j. 5 As 112/2018-53 ze dne 22. ledna 2021
10. Rozsudek Nejvyššího správního soudu č.j. 6 As 22/2018-32 ze dne 30. ledna 2019
11. Rozsudek Nejvyššího správního soudu č.j. 8 As 89/2011–31 ze dne 17. února 2012
12. Usnesení Nejvyššího soudu sp. zn. 8 Tdo 266/2017 ze dne 15. srpna 2018
13. Usnesení Nejvyššího soudu sp. zn. 21 Cdo 3489/2012 ze dne 6. listopadu 2013
14. Usnesení Ústavního soudu sp. zn. I. ÚS 3534/19 ze dne 14. ledna 2020
15. Usnesení Ústavního soudu sp. zn. II. ÚS 2385/18 ze dne 31. srpna 2018
16. Usnesení Ústavního soudu sp. zn. III. ÚS 1513/11 ze dne 21. července 2011
17. Usnesení Ústavního soudu sp. zn. IV. ÚS 3891/18 ze dne 26. února 2019

Seznam ostatních zdrojů

1. BANKID. Jak bankovní identitu získat? *BankID* [online]. Dostupné z: https://www.bankid.cz

2. BULAN, Jiří. (2022, 25. března). *Proč to v Estonsku šlo už před 20 lety, co tomu dopomohlo a co nám chybí? Z čeho se lze poučit?* Konference Institutu moderní politiky – iSTAR: Od montovny k mozkovně, Dolní Břežany, Česká republika.

3. BUNDESRECHENZENTRUM. *Building bridges: e-participation combined with virtual reality.* Vídeň: Bundesrechenzentrum, 2020 [online]. Dostupné z: https://www.brz.gv.at/en/how_we_operate/e-participation-combined-with-virtual-reality-.html

4. Důvodová zpráva k návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, COM(2021) 281 final

5. Důvodová zpráva k zákonu č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů

6. Důvodová zpráva k zákonu č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

7. Důvodová zpráva k zákonu č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů

8. Důvodová zpráva k zákonu č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů

9. Důvodová zpráva k zákonu č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv, ve znění pozdějších předpisů

10. Důvodová zpráva k zákonu č. 227/2019 Sb., kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů

11. Důvodová zpráva k zákonu č. 250/2017 Sb., o elektronické identifikace

12. Důvodová zpráva k zákonu č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci

13. Důvodová zpráva k zákonu č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci

14. Důvodová zpráva k zákonu č. 262/2019 Sb., kterým se mění zákon č. 378/2007 Sb., o léčivech a o změnách souvisejících

15. Důvodová zpráva k zákonu č. 269/2007 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a další související zákony

16. Důvodová zpráva k zákonu č. 283/2021 Sb., (nový) stavební zákon, ve znění pozdějších předpisů

17. Důvodová zpráva k zákonu č. 325/2021 Sb., o elektronizaci zdravotnictví ve znění pozdějších

18. Důvodová zpráva k zákonu č. 365/2000 Sb., o informačních systémech veřejné správy a o změně dalších zákonů

19. ENTERPRISE ESTONIA. e-Identity. *e-Estonia* [online]. Dostupné z: https://e-estonia.com/solutions/e-identity/mobile-id/

20. ENTERPRISE ESTONIA. Interoperabilitty services. *e-Estonia* [online]. Dostupné z: https://e-estonia.com/solutions/interoperability-services/x-road/

21. EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. *Cloud Computing Risk Assessment*. Hérakleion: European Network and Information Security Agency, 2009 [online]. Dostupné z: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment)

22. EVROPSKÁ KOMISE. Digital Europe Programme. *Once-Only Principle (OOP)* [online]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Once+Only+Principle

23. EVROPSKÁ KOMISE. Evropská digitální dekáda: digitální cíle pro rok 2030. *Evropská komise* [online]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_cs

24. EVROPSKÁ KOMISE. Evropská digitální identita. *Evropská komise* [online]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_cs

25. EVROPSKÁ KOMISE. National Legislation. Malta. *European e-Justice* [online]. Dostupné z: https://e-justice.europa.eu/6/EN/national_legislation?MALTA&member=1

26. EVROPSKÁ KOMISE. Service of documents: official transmission of legal documents. Malta. *European e-Justice* [online]. Dostupné z: https://e-justice.europa.eu/371/EN/service_of_documents_official_transmission_of_legal_documents?MALTA&member=1

27. FEDERAL MINISTRY REPUBLIC OF AUSTRIA DIGITAL AND ECONOMIC AFFAIRS. Mobile Phone Signature. *Bundesministerium Digitalisierung und Wirtschaftsstandort* [online]. Dostupné z: https://www.bmdw.gv.at/en/Topics/Digitalisation/For-citizens/Mobile-Phone-Signature.html

28. FEDERAL MINISTRY REPUBLIC OF AUSTRIA DIGITAL AND ECONOMIC AFFAIRS. Strategy of the Austrian Federal Government for Artificial Intelligence "AIM AT 2030". *Bundesministerium Digitalisierung und Wirtschaftsstandort* [online]. Dostupné z: https://www.bmdw.gv.at/en/Topics/Digitalisation/Strategy/Artificial-Intelligence.html

29. FUTUREZONE. *Handy-Signatur im Test: Mühsam zum Ziel*. Vídeň: Future Zone, 2012 [online]. Dostupné z: https://futurezone.at/digital-life/handy-signatur-im-test-muehsam-zum-ziel/24.588.429e

30. INFOSYSTEEMIAMET, 2016, *X-Road introduction (short video),* Youtube video. Dostupné z: https://youtu.be/b-r6B28qVSY

31. Legislativní pravidla vlády schválená usnesením vlády č. 188 ze dne 19. března 1998 ve znění pozdějších změn

32. MINISTERSTVO FINANCÍ. *Veřejná konzultace – blockchain, virtuální měny a aktiva.* Praha: Ministerstvo financi, 2018 [online]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Konzultace_2018-11-30_Verejna-konzultace-Blockchain-virtualni-meny-a-aktiva.pdf

33. MINISTERSTVO VNITRA. *Agenda odboru hlavního architekta eGovernmentu*. [online]. Praha: Ministerstvo vnitra. Dostupné z: https://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu-agenda-odboru-hlavniho-architekta-egovernmentu.aspx

34. MINISTERSTVO VNITRA. Projekty. eSbírka a eLegislativa. *Ministerstvo vnitra* [online]. Dostupné z: https://www.mvcr.cz/clanek/esbirka-a-elegislativa.aspx

35. MINISTERSTVO VNITRA. Základní registry a Správa základních registrů. *Ministerstvo vnitra* [online]. Dostupné z: https://www.mvcr.cz/clanek/zakladni-registry-a-sprava-zakladnich-registru.aspx

36. MINISTERSTVO VNITRA. Zřízení datové schránky. *Portál veřejné správy* [online]. Dostupné z: https://portal.gov.cz/sluzby-vs/zrizeni-datove-schranky-S5692

37. NÁRODNÁ AGENTÚRA PRO SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY. Úvodní stránka. *Slovensko.sk, ústredný portál verejnej správy* [online]. Dostupné z: https://www.slovensko.sk/sk/clanok/_vybrane-e-sluzby

38. NÁRODNÁ AGENTÚRA PRO SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY. Vybrané e-služby. *Slovensko.sk, ústredný portál verejnej správy* [online]. Dostupné z: https://www.slovensko.sk/sk/clanok/_vybrane-e-sluzby

39. NÁRODNÍ AGENTURA PRO KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE. Podrobnější popis projektů. *Národní agentura pro komunikační a informační technologie* [online]. Dostupné z: https://nakit.cz/projekty-popis/

40. NÁRODNÍ AGENTURA PRO KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE. Úvodní stránka. *Národní agentura pro komunikační a informační technologie* [online]. Dostupné z: https://nakit.cz

41. Návrh rozhodnutí Evropského parlamentu a Rady, kterým se zavádí politický program 2030 „Cesta k digitální dekádě“, ze dne 15. září 2021, COM(2021), 574 final

42. ÖSTERREICHS REGIERUNG. Österreichs digitales Amt. *Oesterreich.gv.at* [online]. Dostupné z: https://www.oesterreich.gv.at/public.html

43. ÖSTERREICHS REGIERUNG. Das digitale Unternehmensservice. *Unternehmensservice Portal* [online]. Dostupné z: https://www.usp.gv.at

44. Příloha ke Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Digitální kompas 2030: Evropské pojetí digitální dekády, COM(2021), 118 final

45. REPUBLIC OF ESTONIA. Úvodní stránka. *Riigisportaal. Eesti.ee* [online]. Dostupné z: https://www.eesti.ee/en

46. REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY. Data Exchange Layer X-tee. *Republic of Estonia Information System Authority* [online]. Dostupné z: https://www.ria.ee/en/state-information-system/x-tee.html

47. REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY. *Digital documents: ID-card, digital ID, residence permit card and e-Resident digital ID*. Talinn: Riigi Infosüsteemi Amet, 2020 [online]. Dostupné z: https://www.id.ee/en/article/digital-documents-id-card-digital-id-residence-permit-card-and-e-resident-digi-id/

48. REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY. *@eesti.ee e-mail addresses are becoming more and more popular*. Talinn: Riigi Infosüsteemi Amet, 2020 [online]. Dostupné z: https://www.id.ee/en/article/eesti-ee-e-mail-addresses-are-becoming-more-and-more-popular/

49. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Digitální kompas 2030: Evropské pojetí digitální dekády, ze dne 9. března 2021, COM(2021), 118 final

50. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výrobu regionů o Evropském prohlášení o digitálních právech a zásadách pro digitální dekádu, ze dne 26. ledna 2022, COM(2022) 27 final

51. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výrobu regionů o Evropském rámci interoperability – Strategie provádění, ze dne 23. března 2017, COM(2017) 134 final

52. SPRÁVA ZÁKLADNÍCH REGISTRŮ. Dokumenty k problematice ROS. Seznam osob a editorů ROS. *Správa základních registrů* [online]. Dostupné z: https://www.szrcr.cz/images/dokumenty/ROS/seznam_osob_a_editoru_ros.xlsx

53. SPRÁVA ZÁKLADNÍCH REGISTRŮ. Editační agendové systémy. *Správa základních registrů* [online]. Dostupné z: https://www.szrcr.cz/cs/registr-obyvatel/editacni-agendove-systemy

54. SPRÁVA ZÁKLADNÍCH REGISTRŮ. Portál národního bodu pro identifikaci a autentizaci. *Identita občana* [online]. Dostupné z: https://www.eidentita.cz/Home

55. SPRÁVA ZÁKLADNÍCH REGISTRŮ. Registr osob. *Správa základních registrů* [online]. Dostupné z: https://www.szrcr.cz/cs/registr-osob

56. SPRÁVA ZÁKLADNÍCH REGISTRŮ. Registr územní identifikace, adres a nemovitostí. *Správa základních registrů* [online]. Dostupné z: https://www.szrcr.cz/cs/registr-uzemni-identifikace-adres-a-nemovitosti

57. SPRÁVA ZÁKLADNÍCH REGISTRŮ. Rozcestník vygenerovaných agend. *Registr práv a povinností – agendové informační systémy* [online]. Dostupný z: https://rpp-ais.egon.gov.cz/gen/agendy-detail/

58. SPRÁVA ZÁKLADNÍCH REGISTRŮ. Úvodní stránka. *Správa základních registrů* [online]. Dostupné z: https://www.szrcr.cz/cs/

59. Statut státního podniku Národní agentura pro komunikační a informační technologie, s.p., IČO 047 67 543, zapsaného do obchodního rejstříku u Městského soudu v Praze v oddíle A, vložka 77322 ze dne 1. února 2016

60. Stenozáznam z 10. schůze Senátu Parlamentu České republiky 13. funkčního období ze dne 29. dubna 2021

61. Stenozáznam z 87. schůze Poslanecké sněmovny Parlamentu České republiky 8. volební období ze dne 5. března 2021

62. Usnesení Vlády ČR ze dne 25. září 2017 č. 682, o Koncepci zavádění metody BIM (Building Information Modelling) v České republice

63. Usnesení Vlády ČR ze dne 8. října 2014 č. 815, o strategii rozvoje infrastruktury pro prostorové informace v České republice do roku 2020

64. Usnesení č. 133 Výboru pro veřejnou správu a regionální rozvoj ze dne 5. září 2019

65. VLÁDA ČESKÉ REPUBLIKY. Usnesení ze dne 8. října 2014 č. 815, o strategii rozvoje infrastruktury pro prostorové informace v České republice do roku 2020

Seznam obrázků a tabulek

Abstrakt

Právní úprava eGovernmentu v České republice

Diplomová práce se zabývá právní úpravou českého eGovernmentu, tedy úpravou vybraných služeb veřejné správy poskytovaných s využitím informačních a komunikačních technologií a úpravou digitalizace veřejné správy. Kromě české právní úpravy je pozornost zaměřena také na právní úpravu vybraných evropských států a „nadnárodní“ přístup Evropské unie k digitalizaci.

Cílem práce je stručně představit fenomén eGovernmentu a analyzovat právní předpisy, které tvoří právní rámec eGovernmentu v České republice a v zahraničí. Na tomto základě zkoumám hypotézu potvrzující existenci práva eGovernmentu jako specifického právního odvětví.

Za pomocí metody doktrinální a kvalitativní analýzy zkoumám v druhé kapitole jednotlivé právní předpisy související s eGovernmentem v České republice a ve třetí kapitole i ve vybraných evropských státech a Evropské unii. Ve téže kapitole jednotlivé právní úpravy následně právně komparuji na základě předem definovaných kritérií. Získané informace posléze ve čtvrté kapitole syntetizuji do jednotného celku, který z mého pohledu potvrzuje uvedenou hypotézu a za pomoci modelování vytvářím konkrétní funkční systematiku nově definovaného odvětví správního práva.

Potvrzením hypotézy o existenci práva eGovernmentu spolu se souvisejícími právy a povinnostmi tato práce umožní další vědecké zkoumání práva eGovernmentu a souvisejících aspektů. V ideálním případě práce poslouží i pro budoucí zákonodárství, které bude z uvedených zjištění vycházet.

Klíčová slova: eGovernment, veřejná správa, právo eGovernmentu

Abstract

Legal Regulation of eGovernment in the Czech Republic

The diploma thesis deals with the legal regulation of the Czech eGovernment, i.e. with the regulation of the selected public administration services provided while using information and communication technologies and with the regulation of digitalization of public administration. In addition to the Czech legal regulation, the focus is also on the legal regulation in selected European countries and the "supranational" approach of the European Union towards digitalization.

The thesis aims to introduce the phenomenon of eGovernment briefly and to analyse the legal regulations that form the legal framework of eGovernment in the Czech Republic and abroad. On this basis, I examine the hypothesis confirming the existence of eGovernment law as a specific branch of law.

Using the method of doctrinal and qualitative analysis, I examine individual eGovernment-related legislation in the Czech Republic in Chapter two and in the selected European countries and the European Union in Chapter three. In the same chapter, I then compare the individual legal regulations based on predefined criteria. The obtained information is then synthesized in Chapter fourth into a unified whole, which from my point of view, confirms the hypothesis. With the help of the modelling method, I created specific functional systematics of the newly defined legal branch of administrative law.

By confirming the hypothesis of the existence of eGovernment law along with the associated rights and obligations, this thesis will enable further scholarly investigation of eGovernment law and related aspects. Ideally, the thesis will also serve to inform future legislation based on these findings.

Key words: eGovernment, public administration, eGovernment law