

UNIVERZITA KARLOVA
Právnická fakulta

Richard Vogel

Veřejná správa a eGovernment

Diplomová práce

Vedoucí diplomové práce: prof. JUDr. Richard Pomahač, CSc.

Katedra: Katedra správního práva

Datum vypracování práce (uzavření rukopisu): 27. 06. 2022

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 198 253 znaků včetně mezer.

Richard Vogel, diplomant

V Praze dne 27. 6. 2022

Obsah

Úvod.....	1
1 Veřejná správa a eGovernment.....	3
1.1 Vymezení eGovernmentu.....	3
1.2 Vztah k souvisejícím obecným pojmům.....	5
1.3 Vztah k souvisejícím dílčím pojmům.....	6
1.4 Dělení a fáze eGovernmentu.....	7
1.4.1 Layneův a Leeův čtyřfázový model budování eGovernmentu.....	7
1.4.2 Teorie generací eGovernmentu.....	9
1.4.3 Veřejná správa vycházející z dat.....	11
1.5 Vztah veřejné správy a eGovernmentu.....	11
2 EGovernment v ČR.....	13
2.1 Indexy a benchmarky relevantní pro eGovernment v ČR.....	13
2.1.1 Index digitální ekonomiky a společnosti (DESI, 2021).....	13
2.1.2 E-Government Development Index (2020).....	14
2.1.3 EGovernment benchmark (2021).....	15
2.1.4 Benchmark veřejné správy (2021).....	15
2.2 Funkční rozdělení podle vrstev.....	17
2.3 Institucionální zajištění.....	20
3 Úvod do právního rámce eGovernmentu v ČR.....	22
3.1 Právní principy eGovernmentu.....	22
3.1.1 Principy obsažené v Akční plánu EU.....	22
3.1.2 Další principy dovozené z tuzemského právního řádu.....	25
3.1.3 Vztah právních principů a norem eGovernmentu.....	26
3.2 Ústavní pořádek.....	27
4 Právní předpisy eGovernmentu.....	29
4.1 Právní úprava základních registrů.....	31
4.2 Právní úprava informačních systémů veřejné správy.....	33
4.3 Právní úprava datových schránek.....	35
4.3.1 Změna u datových schránek pro fyzické osoby.....	37
4.4 Právní úprava elektronické identifikace.....	39
4.4.1 Prostředky pro elektronickou identifikaci.....	40
4.4.2 Přihlašování se k portálům veřejné správy.....	43

4.4.3	Budoucí vývoj elektronické identity	47
4.5	Právní úprava elektronických podpisů a dalších elektronických institutů	49
4.5.1	Různé podoby elektronického podpisu a dalších elektronických institutů	49
4.5.2	Účinky elektronických podpisů.....	51
4.5.3	Kvalifikovaná forma elektronického podání	52
4.5.4	Nekvalifikovaná forma elektronického podání	56
4.6	Právní úprava spisové služby	56
4.7	Zákon o právu na digitální služby (ZPDS).....	58
4.7.1	Obecně o dvou nejvýznamnějších zákonech pro eGovernment posledních let .	58
4.7.2	Specifika legislativního procesu ZPDS.....	58
4.7.3	Další eGovernment zákon, proč?	59
4.7.4	Právo na digitální služby	62
4.7.5	Právo na technologickou neutralitu.....	64
4.7.6	Právo činit digitální úkon	65
4.7.7	Digitální úkon jako volba	66
4.7.8	Katalog služeb	67
4.7.9	Další práva související s digitálními úkony	73
4.7.10	Právo na sdílení vedených údajů.....	74
4.7.11	Další práva související s vedenými údaji	76
4.7.12	Vymahatelnost digitálních práv	77
4.8	DEPO zákon	81
4.8.1	Specifika legislativního procesu.....	81
4.8.2	Obsah zákona	82
4.8.3	Změny promítající ZPDS	82
4.8.4	Změny eGovernmentu.....	82
	Závěr.....	83
	Seznam použitých zdrojů	86
	Seznam grafů a obrázků	96
	Abstrakt	97
	Abstract	98

Úvod

Hlavním cílem této diplomové práce je rozbor a kritické zhodnocení nové právní úpravy související s poskytováním digitálních služeb veřejnou správou a její zasazení do kontextu současné právní úpravy eGovernmentu v České republice.

Vedlejším cílem je zodpovězení následujících otázek: Umožňuje stávající právní úprava existenci a následný rozvoj eGovernmentu? Je nově přijatá právní úprava digitálních služeb přelomová? Jaký je vztah nové úpravy digitálních služeb ke stávajícím institutům eGovernmentu? Byly naplněny veškeré ambice tvůrců zákona o právu na digitální služby vkládané do jeho přijetí? Které problémy týkající se poskytování digitálních služeb nová úprava neřeší? Lze očekávat snadnou vymahatelnost digitálních práv přiznaných občanům?

Jsem přesvědčen, že naplnění hlavního cíle diplomové práce a zodpovězení uvedených otázek bude přínosem pro současné právní poznání tuzemského eGovernmentu a veřejné správy.

Tato diplomová práce je členěna do čtyř kapitol.

V první kapitole je eGovernment představen jako globální fenomén. Součástí této kapitoly je i úvaha nad problematikou definování samotného eGovernmentu, představení některých teoretických přístupů k jeho budování a zařazení eGovernmentu jako jednoho z významných trendů modernizace veřejné správy.

Druhá kapitola je věnována současnému stavu eGovernmentu v České republice. S pomocí mezinárodních indexů a benchmarků je poukázáno na slabé stránky tuzemského eGovernmentu a prostřednictvím Architektonické vize je objasněna vzájemná provázanost jeho základních složek. Pozornost je věnována také probíhající transformaci institucí veřejné správy zajišťujících provoz tuzemského eGovernmentu.

Další kapitoly jsou již dedikovány právní úpravě eGovernmentu v České republice. Ve třetí kapitole jsou vyzdvihnuty základní právní principy eGovernmentu a relevantní ústavní principy. V úvodu čtvrté kapitoly je provedena horizontální systemizace relevantních zákonných předpisů. Následují právní rozборы jednotlivých zákonů eGovernmentu, přičemž hlavní pozornost je soustředěna na právní instituty mající zásadní význam pro poskytování digitálních služeb veřejnou správou. V souvislosti s těmito právními instituty je věnován prostor také aktuální problematice přihlašování se do portálů veřejné správy, automatickému zřizování datových schránek některým fyzickým osobám nebo kvalifikovaným a nekvalifikovaným formám elektronického podání.

Nejpodrobnější pojednání se týká zákona o právu na digitální služby. Nejprve je zodpovězena otázka nezbytnosti dalšího eGovernment zákona. Dále jsou do kontextu stávající úpravy zasazena a rozebrána jednotlivá nově přiznaná digitální práva jako například právo na digitální služby, právo činit digitální úkon nebo právo na sdílení vedených údajů. Samostatná pozornost je věnována katalogu služeb a vymahatelnosti digitálních práv.

K teoretickému pojednání o eGovernmentu je využita česká odborná literatura z počátku druhého desetiletí tohoto století společně se zahraničními odbornými články a dalšími publikacemi reflektujícími relevantní témata. Právní rozbor zákonů eGovernmentu bude vycházet mimo platného znění právních předpisů také z recentní judikatury, komentářové literatury a dalších odborných právních textů.

1 Veřejná správa a eGovernment

1.1 Vymezení eGovernmentu

eGovernment je klíčovým pojmem této práce, jeho význam nelze zcela jednoznačně vymezit. Na rozdíl od některých jiných technických pojmů jej pozitivní právo neuznává ani jako legislativní zkratku. V souvislosti s objektivním právem se lze s tímto pojmem setkat především v teoreticko-právní literatuře a v oblasti koncepčních dokumentů veřejné správy. Přestože jde již delší dobu o běžně užívaný pojem, není mezi odborníky na přesném vymezení shoda. Za příčinu dosavadního neúspěchu při dosažení jednotného definování eGovernmentu považují někteří odborníci vágnost celého konceptu eGovernmentu, který je dán jeho neohrazeností, komplexností a složitým politickým a institucionálním prostředím spjatým s procesem budování a rozvoje eGovernmentu¹.

Než přistoupím ke komparaci některých z definic eGovernmentu, považuji za nezbytné zavést některé z nejčastějších pojmů, které jsou typické pro většinu odborných textů o eGovernmentu. Jde především o pojem informační a komunikační technologie (ICT) a související běžně používaná termíny digitalizace či elektronizace.

Pojem ICT zahrnuje „*veškeré informační technologie používané pro komunikaci a práci s informacemi*“². Za konkrétní informační technologie jsou považovány: hardwarové vybavení (například počítače a servery), softwarové vybavení (například počítačové programy a různá přístupová rozhraní) a komunikační vybavení, které umožňuje hardwarovému a softwarovému vybavení navzájem komunikovat.

Adjektivum digitální označuje v širokém pojetí vše, co se vztahuje k ICT. V úzkém pojetí může uvedené adjektivum nabývat význam podle některé ze čtyř různých činností, jež popisuje:

- digitizace (přeměna analogových dat na elektronicky dále zpracovatelná data);
- digitalizace (využívání digitálních dat k získání informací);
- elektronizace (operativní změna procesů s pomocí využívání ICT);
- digitální transformace (strategický přechod na digitální model fungování)³.

¹ YILDIZ, Mete. E-government research: Reviewing the literature, limitations, and ways forward. In: *Government Information Quarterly* [online]. Elsevier, 2007, 24(3), 647 [cit. 20.6.2022]. ISSN: 0740-624X. Dostupné prostřednictvím Science Direct. DOI: [10.1016/j.giq.2007.01.002](https://doi.org/10.1016/j.giq.2007.01.002).

² BEZPALEC, Pavel. *Management ICT systémů: Nové trendy v elektronických komunikacích* [online]. ČVUT, 2015, s. 1 [cit. 20.6.2022]. Dostupné z: <https://entk.publi.cz/book/242-management-ict-systemu>.

³ VAŠEK, Jan. *Jak se vyznat v digitální terminologii* [online]. 2020 [cit. 20.6.2022]. Dostupné z: <https://kem.vscht.cz/digitalni-nakup-scm/archiv-2021/jak-se-vyznat-v-digitalni-terminologii>.

Typické pro výše uvedené činnosti je, že se prolínají.

Mezi zásadní českou literaturu eGovernmentu patří monografie E-government v České republice: právní a technologické aspekty⁴. V ní autoři provádějí komparaci zahraničních a tuzemských pokusů o definici eGovernmentu. Hlavním rozdílem mezi jednotlivými definicemi je jejich šíře. Příkladem slouží definice Richarda Heekse vymezující eGovernment jednoduše jako „*použití informačních technologií ve veřejném sektoru*“⁵. Tato definice je příliš široká, a protože není popisná, tak jen málo vypovídá o skutečných specifikách eGovernmentu.

S popisnějšími definicemi se setkáváme v evropských a českých koncepčních dokumentech. Podle EU se eGovernmentem rozumí: „*využívání informačních a komunikačních technologií ve veřejné správě v kombinaci s organizačními změnami a novými dovednostmi s cílem zlepšit veřejné služby a demokratické procesy a posílit podporu veřejných politik*“⁶. V rámci českého koncepčního přístupu se lze setkat i s vymezením popisujícím ideálně dosažený stav eGovernmentu jako: „*moderní digitální veřejnou správu, využívající k výkonu svých působností digitální infrastrukturu, realizující sadu ICT služeb, které jsou sdílené, vzájemně sladěné, důvěryhodné, propojené, přístupné, bezpečné, dostupné a efektivní*“⁷. V souladu s tím používá Odbor Hlavního architekta eGovernmentu Ministerstva vnitra vlastní definici eGovernmentu: „*Digitální veřejná správa, která předpokládá používání digitálních technologií jakožto integrované části strategií modernizace vlád k vytvoření veřejné hodnoty*“⁸.

Při porovnání znění jednotlivých definic z předchozího odstavce lze shrnout, že podstatou koncepčních definic eGovernmentu jsou dva více či méně explicitně vyjádřené kumulativní charakteristické znaky. Prvním z nich je využívání ICT, druhým pak oblast veřejné správy. Tyto znaky zároveň doplňují další znaky popisného charakteru. Například, že jde o poskytování veřejné služby s určitými vlastnostmi.

⁴ MATES, Pavel, SMEJKAL, Vladimír. *E-government v České republice: právní a technologické aspekty*. 2. podstatně přeprac. a rozš. vyd. ed. Praha: Leges, 2012, s. 38. ISBN: 978-80-87576-36-6.

⁵ HEEKS, Richard. *Implementing and Managing eGovernment* [online]. SAGE, 2006, s. 1 [cit. 20.6.2022]. ISBN: 978-14-46220-19-1. Dostupné prostřednictvím SAGE Publishing. DOI: [10.4135/9781446220191](https://doi.org/10.4135/9781446220191).

⁶ EVROPSKÁ KOMISE. *Communication from the Commission...: The Role of eGovernment for Europe's Future* [online]. 2003 [cit. 20.6.2022]. CELEX: 52003DC0567. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52003DC0567>.

⁷ DZURILLA, Vladimír, TÝM OHA MV. *Informační koncepce České republiky* [online]. Ministerstvo vnitra: 2020, s. 2. Poslední změna: 29.5.2020 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/soubor/informacni-koncepce-cr-2020.aspx>.

⁸ ŠEDIVEC, Tomáš. Slovník pojmů eGovernmentu. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 4.5.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/slovník_egov.

Domnívám se, že koncepční definice umožňují vytvořit si jasnější představu o významu pojmu eGovernmentu než výše zmíněná Heeksova definice. Nicméně za problematické shledávám, že se obě koncepční definice omezují pouze na veřejnou správu a zcela pomíjejí ostatní složky veřejné moci. V důsledku toho by byly nesprávně vyčleněny některé oblasti eGovernmentu. Příkladem v oblasti moci soudní je eJustice a v moci zákonodárné eSbírka a eLegistativa. Vzhledem k tomu, že se v uvedených oblastech taktéž uplatňují obecné principy eGovernmentu, měla by ideální definice obsahovat místo znaku „*ve veřejné správě*“ znak „*v rámci veřejné moci*“⁹. Nicméně tato práce je věnovaná v první řadě eGovernmentu ve veřejné správě, a proto i přes výše uvedené důvody není nezbytné pojetí eGovernmentu na ostatní složky moci rozšiřovat.

1.2 Vztah k souvisejícím obecným pojmům

Podle amerického autora Miriama Lipse je eGovernment pojmem již překonaným. A proto Lips prosazuje jeho nahrazení komplexnějším pojmem digitální vláda (anglicky Digital Government), který definuje jako: „*zavádění, uplatnění a používání digitálních technologií a dat ve veřejné správě a jejich vnějších vztazích působících navenek (vůči občanům, podnikům, občanské společnosti nebo vůči mezinárodním organizacím) včetně možných důsledků pro demokracii, způsob vládnutí a řízení*“¹⁰.

Pojem digitální vláda je natolik široký, že obsáhne nejen eGovernment ale i eDemokracii.

Přičemž eDemokracie představuje „*využití ICT k zapojení občanů, podpoře demokratických rozhodovacích procesů a posílení zastupitelské demokracie*“¹¹. Stejně jako v případě eGovernmentu jde o zavádění ICT do oblastí souvisejících s výkonem veřejné moci. Přes společné znaky s eGovernmentem, jde o relativně samostatný trend v oblasti modernizace veřejné správy.

S pojmem eDemokracie souvisí i pojem eParticipace, který je také nutné odlišit od eGovernmentu. Dle Davida Špačka se eParticipací rozumí „*specifický soubor nástrojů,*

⁹ K obdobnému závěru dochází i autorka komentáře ke slovenskému zákonu o eGovernmentu: GREGUŠOVÁ, Daniela. *Zákon o e-Governmente: komentár*. Bratislava: Eurokódex, 2018, s. 4-5. ISBN: 978-80-8155-080-5.

¹⁰ LIPS, Miriam. *Digital Government: Managing Public Sector Reform in the Digital Era* [online]. Routledge, 2020, s. 9 [cit. 20.6.2022]. ISBN: 978-13-15622-40-8. Dostupné z: <https://1lib.cz/book/17584618/07b207>.

¹¹ MACINTOSH, Ann. Characterizing E-Participation in PolicyMaking. In: *Proceedings of the 37th Annual Hawaii International Conference on System Sciences* [online]. IEEE, 2004, s. 2 [cit. 20.6.2022]. ISBN: 0-7695-2056-1. Dostupné prostřednictvím IEEE Xplore. DOI: [10.1109/HICSS.2004.1265029](https://doi.org/10.1109/HICSS.2004.1265029).

keré mají posílit zapojování potenciálně dotčených subjektů či veřejnosti obecně do rozhodovacích procesů veřejných záležitostech.¹² V České republice (ČR) nové možnosti eParticipace nepředstavují ucelenou reformní snahu¹³. Oblasti eParticipace a eDemokracie jsou relativně oddělitelné od eGovernmentu, a proto se jimi nebudu v této práci zabývat. Ze stejného důvodu upřednostním pojem eGovernment před označením digitální vláda.

Dalším důvodem, proč se chystám pracovat právě s pojmem eGovernment, a ne s jiným souvisejícím pojmem, je zjištění bibliometrického výzkumu¹⁴, podle kterého se v ČR jedná o nejrozšířenější pojem popisující spojení ICT a veřejné správy. Ostatní pojmy jako například eGovernance, Smart Government či Smart Governance se oproti eGovernmentu v českých odborných zdrojích vyskytují jen sporadicky.

V zahraničních zdrojích se lze setkat kromě pojmu eGovernment zejména s pojmem eGovernance. Odlišení od eGovernmentu nemusí být vždy zjevné. Přesto lze vysledovat zásadní odlišnosti, které spočívají v tom, že kromě výkonu veřejné správy eGovernance popisuje i řízení veřejné správy a participaci občanů.

Významným pojmem překrývajícím se s eGovernmentem na místní úrovni je pojem Smart Government, který označuje chytré řízení města. Tento pojem se prosadil v posledních letech jako součást konceptu Smart City, který představuje strategický přístup k řízení za účelného propojení klíčových oblastí života města s pomocí moderních technologií v souladu s principem udržitelnosti¹⁵.

1.3 Vztah k souvisejícím dílčím pojmům

V souvislosti s velmi rychlým rozšířením mobilních technologií ve společnosti je ve spojitosti s eGovernmentem používán i dílčí pojem mGovernment. Tato oblast v rámci eGovernmentu se soustředí na otázky přístupnosti a odstranění překážek při používání

¹² ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Praha: C.H. Beck, 2012, s. 3. ISBN: 978-80-7400-261-8.

¹³ ŠPAČEK, David. Public Administration Reform in Czechia after 2000: Ambitious Strategies and Modest Results? In: *NISPAcee Journal of Public Administration and Policy* [online]. Sciendo, 2018, 11(1), 178 [cit. 20.6.2022]. ISSN: 1337-9038. DOI: [10.2478/nispa-2018-0007](https://doi.org/10.2478/nispa-2018-0007)

¹⁴ STELLNER, František, VOKOUN, Marek, SOBĚHART, Radek. Smart government, smart administration a eGovernment v České republice. In: *Mladá Věda* [online]. Presov: 2021, 9(4), 63-77 [cit. 20.6.2022]. ISSN: 1339-9318. Dostupné z: <https://proquest.com/docview/2617199270>.

¹⁵ ÚŘAD VLÁDY ČR. *Akční plán pro Společnost 4.0* [online]. 2017, s. 39 [cit. 20.6.2022]. Dostupné z: <https://databaze-strategie.cz/cz/urad-vlady/strategie/akcni-plan-pro-spolecnost-4-0-2017?typ=download>.

mobilních technologií¹⁶. Jinými slovy jde o přístup ke zkoumání eGovernmentu, který se zaměřuje na jednotlivé aspekty využití mobilních technologií ve veřejné správě.

V některých situacích se eGovernment dělí podle elektronizace jednotlivých oblastí kompetencí orgánů veřejné moci. Lze se setkat s pojmem elektronické vzdělávání (anglicky eEducation), elektronická kultura (anglicky eCulture), elektronické zdravotnictví (anglicky eHealth), elektronické zadávání veřejných zakázek (anglicky eProcurement) nebo elektronická justice (eJustice)¹⁷. Každá oblast má svá specifika a zpravidla kopíruje horizontální rozdělení působnosti v rámci organizace veřejné správy.

1.4 Dělení a fáze eGovernmentu

EGovernment lze členit podle směru a stran komunikace. Běžnými směry komunikace jsou:

- veřejná správa občanům (anglicky Government-to-Citizens, G2C);
- veřejná správa podnikatelům (anglicky Government-to-Bussines, G2B).

Souhrnu těchto směrů komunikace odpovídá pojem front-office. Naproti tomu pojem back-office označuje směr komunikace uvnitř orgánů veřejné správy nebo mezi nimi (anglicky Government to Government, G2G). Takto pojatý back-office bývá v rámci eGovernmentu odlišován pod samostatným označením eSpráva (anglicky eAdministration)¹⁸.

1.4.1 Layneův a Leeův čtyřfázový model budování eGovernmentu.

Tento čtyřfázový model budování eGovernmentu byl vypracován již na počátku tisíciletí. Nicméně díky své obecnosti zůstal relevantní dodnes¹⁹. Zásadní zjištění, které provází tento model, spočívá v přímé úměře mezi nárůstem dosažené integrace eGovernmentu, což je pozitivní a žádaný výsledek, a nárůstem organizační a technologické komplexity, což je negativní a nežádoucí výsledek. Časová posloupnost jednotlivých fází není nezbytná. V praxi se jednotlivé fáze vzájemně prolínají.

¹⁶ ŠPAČEK, pozn. 12, s. 3.

¹⁷ MINISTERSTVO VNITRA. *Strategický rámec rozvoje veřejné správy ČR pro období 2014-2020* [online]. Polygrafie Úřadu vlády ČR, 2017, s. 45 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/soubor/strategicky-ramec-rozvoje-verejne-spravy-v-cr-pro-obdobi-2014-2020.aspx>.

¹⁸ YILDIZ, pozn. 1, s. 652.

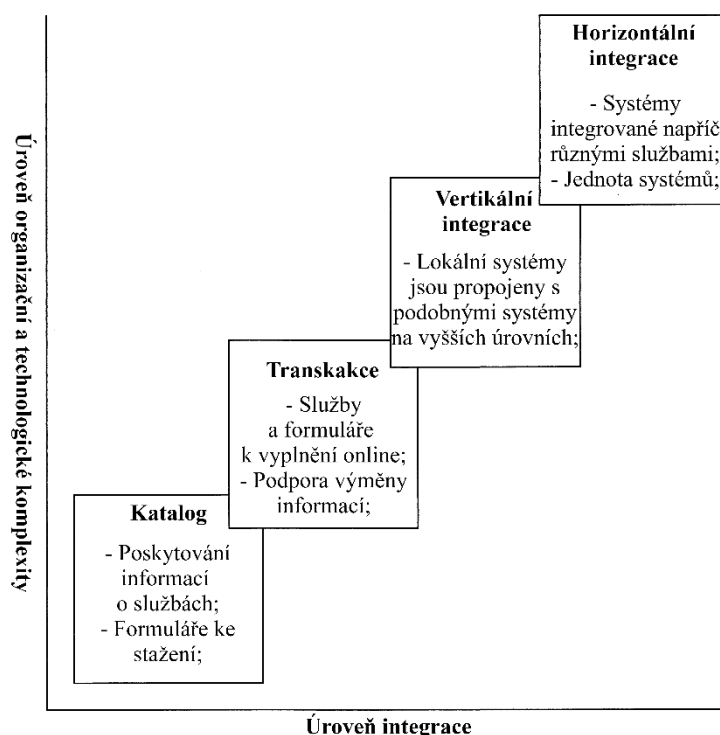
¹⁹ CHARALABIDIS, Yannis, LOUKIS, Euripidis, ALEXOPOULOS Charalampos, LACHANA Zoi. The Three Generations of Electronic Government. In: *Electronic Government* [online]. Springer, 2019, s. 12 [cit. 20.6.2022]. ISBN 978-3-030-27325-5. DOI: [10.1007/978-3-030-27325-5_1](https://doi.org/10.1007/978-3-030-27325-5_1).

V první fázi eGovernment představuje pouhý roztržitý katalog nedigitálních služeb veřejné správy. Největším přínosem je samotná dostupnost informací na Internetu. Ve druhé fázi je již možné vyřídit záležitosti elektronicky, což má vést ke zvýšení efektivity jednotlivých činností a snížení výdajů na straně veřejné správy i občanů. Tato transakční fáze podporuje dvoustranou komunikaci mezi občanem a veřejnou správou.

Následující dvě fáze se zaměřují na transformaci procesů veřejné správy směrem k integrovanému celku. Cílem je překonání roztržitosti informačních systémů včetně jejich databází a transakčních portálů. Transformací by tedy měly projít vnitřní i vnější činnosti veřejné správy. Vertikální integrace předpokládá, že informační systémy na lokální, národní i nadnárodní úrovni jsou integrovány a umožňují veřejné správě komunikovat a poskytovat služby na jednom místě. Například centralizované transakční portály budou čerpat údaje z decentralizovaných evidencí.

Plného potenciálu ICT může veřejná správa dosáhnout pouze kompletní integrací, která zahrnuje kromě vertikální integrace též integraci horizontální. V této čtvrté fázi jde o překonání překážek mezi jednotlivými agendami veřejné správy odstraněním překážek sdílení dat uvnitř

veřejné správy a poskytováním všech digitálních služeb navenek na jednom místě bez ohledu na působnost jednotlivých orgánů²⁰.



Graf č. 1: Layneův a Leeův čtyřfázový model budování eGovernmentu²¹.

1.4.2 Teorie generací eGovernmentu

Další teoretický přístup k budování eGovernmentu nabízí teorie generací. Ve vývoji ICT v posledních letech někteří odborníci identifikovali generačně-revoluční změny, které spojují s prosazením se pokročilejších internetových technologií. Tyto technologické změny, které se označují zpravidla jako Web 1.0 až 3.0, mají podle nich potenciál revolučně proměnit eGovernment pomocí zavádění nových ICT nebo nových způsobů využití stávajících technologií. Podle zmíněných změn rozlišují eGovernment na jednotlivé generace.

eGovernment 1.0 představuje jednosměrnou komunikaci s veřejnou správou, která se začala rozšiřovat od devadesátých let minulého století²². Cílem je poskytování efektivnějších a hospodárnějších veřejných služeb. Zároveň se předpokládá i změna procesů uvnitř i navenek veřejné správy směrem k horizontální i vertikální integraci. Lze tedy říci, že tato generace

²⁰ LAYNE, Karen, LEE, Jungwoo. Developing fully functional E-government: A four stage model. In: *Government information quarterly* [online]. Elsevier, 2001, 18(2), 122-136 [cit. 20.6.2022]. ISSN: 0740-624X. Dostupné prostřednictvím Science Direct. DOI: [10.1016/S0740-624X\(01\)00066-1](https://doi.org/10.1016/S0740-624X(01)00066-1).

²¹ Tamtéž, s. 124 [přeloženo].

²² CHARALABIDIS, pozn. 19, s. 12.

eGovernmentu zahrnuje všechny čtyři fáze Layneova a Leeova modelu budování eGovernmentu.

Naproti tomu eGovernment 2.0 je spojován s postupným technologickým vývojem Internetu v prvním desetiletí tohoto tisíciletí²³. Podstatou Web 2.0. jsou nové technologické možnosti umožňující spolupráci pomocí internetových nástrojů, kterými jsou například sociální sítě, Wikipedie nebo GitHub. Tyto nástroje obecně umožňují vyšší úroveň spolupráce, větší otevřenost a transparentnost. V rámci eGovernmentu by se tato revolučně-technická změna měla projevit ve spolupráci občana s veřejnou správou. Veřejná správa může například provozovat internetovou platformu, kde se občané budou moci zapojit do rozhodování veřejné správy. EGovernment 2.0 je na rozdíl od předchozí generace více interaktivní a jeho pozornost je zaměřena více na eParticipaci než na poskytování digitálních služeb.

EGovernment 3.0 je obtížnější k uchopení, kvůli neujasněnosti podstaty fungování Webu 3.0. Diskuse o třetí generaci Internetu probíhají přibližně od druhé poloviny první dekadý tohoto století a stále je nelze považovat za ukončené. Často zmiňovaný je posun k sémantickému webu, což znamená zpřístupnění všech informací na Internetu tak, aby byly zpracovatelné nejen lidmi, ale i počítačovými programy²⁴. V posledních letech je aktuální téma decentralizace Internetu pomocí blockchainu, který umožní přenos informací bez centralizovaných poskytovatelů služeb²⁵.

EGovernment 3.0 podle jedné z definic znamená využití nových revolučních ICT, jako jsou například big data, internet věcí a umělá inteligence v kombinaci s dosud zavedenými ICT. Tato kombinace technologií by měla veřejné správě umožnit rozhodování založené na datech a důkazech (anglicky data-driven and evidence-based decision) a přenést část činností na občany (tzv. crowdsourcing)²⁶. Tato generace popisuje vize budoucího vývoje eGovernmentu spíše než soudobá řešení.

²³ KUSIAK-WINTER, Renata. Kierunki i etapy rozwoju e-administracji publicznej. In: *Ewolucja elektronicznej administracji publicznej* [online]. E-Wydawnictwo, 2021, s. 18 [cit. 20.6.2022]. ISBN 978-83-66601-43-7. DOI: [10.34616/23.21.008](https://doi.org/10.34616/23.21.008).

²⁴ HENDLER, Jim. Web 3.0 Emerging. In: *Computer* [online]. IEEE, 2009, 42(1), s. 111 [cit. 20.6.2022]. ISSN: 1558-0814. Dostupné prostřednictvím IEEE Xplore. DOI: [10.1109/MC.2009.30](https://doi.org/10.1109/MC.2009.30).

²⁵ RAGNEDDA, Massimo. DESTEFANIS, Giuseppe. Blockchain. A disruptive technologies. In: *Blockchain and Web 3.0* [online]. Taylor & Francis, 2019, s. 3 [cit. 20.6.2022]. ISBN: 978-04-29029-53-0. DOI: [10.4324/9780429029530-1](https://doi.org/10.4324/9780429029530-1).

²⁶ CHARALABIDIS, pozn. 19, s. 10.

1.4.3 Veřejná správa vycházející z dat

Tento koncept představuje ideální finální fázi eGovernmentu, která spočívá v dokonalém sdílení a využívání anonymizovaných a souhrnných dat napříč veřejnou správou i navenek²⁷. Podstata přínosu tohoto přístupu spočívá v tom, že veřejná správa získá více informací o občanech a jejich potřebách, na základě kterých bude občanům schopna poskytovat cílenější a efektivnější služby. Přínosem pro veřejnou správu je, že disponuje komplexními informacemi o tom, zda poskytování konkrétní služby naplňuje záměry právní regulace. Tento koncept však vzbuzuje vážné etické otázky, jak a zda by měla veřejná správa nebo veřejnost disponovat tak komplexními daty.

1.5 Vztah veřejné správy a eGovernmentu

eGovernment lze chápat jako jeden z trendů modernizace veřejné správy posledních let.

Rozvoj ICT má potenciál přetvořit veřejnou správu zevnitř i navenek. ICT umožňují nové možnosti vertikální i horizontální integrace veřejné správy. Mohou zrychlit rozhodovací procesy a zesílit účinky naplňování politik a zvýšit tak kvalitu poskytovaných služeb. Zároveň není v současné době plně technologií a dat dobře představitelné, že by veřejná správa bez ICT byla schopna efektivně fungovat²⁸.

Z tohoto důvodu musí být veřejná správa schopna se rozvoji ICT vhodným způsobem přizpůsobit. Přizpůsobení se spočívá v přijímání modernizačních opatření, která umožní kvalitně a efektivně zajistit tradiční funkce a úkoly veřejné správy a zároveň zajistí růst ekonomické konkurenceschopnosti a uspokojování potřeb současné společnosti. V důsledku přijatých opatření se mění výkon a organizace veřejné správy.

Produktem přizpůsobení se veřejné správy rozvoji ICT je právě eGovernment. Ten byl vytvořen při respektování specifík veřejné správy, mezi která patří její monopolní postavení, více stupňovitost a závislost na legislativě. David Špaček v této souvislosti připomíná, že veřejná správa je předmětem politického rozhodování a politické kontroly²⁹.

Typ přijatých opatření s cílem modernizovat veřejnou správu se časem proměnil. Velké systémové reformy veřejné správy jsou v evropských zemích minulostí, protože jejich příprava a realizace byla zpravidla tak časově náročná, že v okamžiku realizace takových reforem si již

²⁷ LIPS, pozn 10, s. 95-96.

²⁸ HUSTEDT, Thurid, RANDMA-LIIV, Tiina, SAVI, Riin. Public Administration and Disciplines. In: *European Perspectives for Public Administration* [online]. Leuven, 2020, s. 140-141 [cit. 20.6.2022]. ISBN: 978-94-6166-307-8. Dostupné prostřednictvím JSTOR. DOI: doi.org/10.2307/j.ctvv417th.11.

²⁹ ŠPAČEK, pozn. 12, s. 21.

dynamika společenského vývoje žádá další reformu veřejné správy. V současné Evropě se proto přijímají spíše konkrétní modernizační kroky, které při zachování kontinuity vývoje veřejné správy lépe akcentují dynamiku společenského vývoje³⁰.

Veřejná správa a ICT vychází z různých logik, a proto je nezbytné najít způsoby, jak ICT ve veřejné správě uplatnit. Veřejnou správu i přes nalezení správných způsobů uplatnění ICT nelze plně digitalizovat ze dne na den. Činnost veřejné správy je limitována množstvím právních omezení a faktickými možnostmi spočívajícími ve finančních a personálních nedostatcích. Veřejná správa je složitý konstrukt, který se v průběhu času vyvíjel. Proto bývají postupné i institucionální změny. To pomáhá pochopit, proč je digitalizace správy veřejného sektoru zpravidla evolučním procesem³¹.

³⁰ PAVLÍK, Marek, ŠIMKA, Karel, POSTRÁNECKÝ, Josef, POMAHAČ, Richard. *Moderní veřejná správa: zvyšování kvality veřejné správy, dobrá praxe a trendy*. Praha: Wolters Kluwer, 2020. s. 131. ISBN: 978-80-7598-048-9.

³¹ KITSING, Meelis. Scenarios as Thought Experiments for Governance. In: *European Perspectives for Public Administration* [online]. Leuven, 2020, s. 120 [cit. 20.6.2022]. ISBN: 978-94-6166-307-8. Dostupné prostřednictvím JSTOR. DOI: [10.2307/j.ctvv417th.10](https://doi.org/10.2307/j.ctvv417th.10).

2 EGovernment v ČR

2.1 Indexy a benchmarky relevantní pro eGovernment v ČR

Digitalizace je celosvětový trend posledních desetiletí. ČR není ve své snaze být „jednou z předních zemí v praktickém využívání moderních služeb eGovernmentu“³² osamocena. Ze srovnání s ostatními zeměmi lze získat poznatky, kde český eGovernment zaostává a kde naopak již dosahuje dostatečných kvalit.

Různé mezinárodní organizace provádějí mezinárodní srovnání eGovernmentu. Řada z nich je založena pouze na omezeném počtu ukazatelů, a proto nereflexuje zcela komplexitu eGovernmentu. Současně nejsou schopny zachytit vnitřní reorganizaci veřejné správy nebo její národní specifika³³. Postihnout celý fenomén digitalizace není možné v rámci jednoho měření. Každé měření se věnuje proto určité oblasti a volí rozdílné metriky a postupy.

Na mezinárodní úrovni se problematikou eGovernmentu zabývá několik mezinárodních organizací. V této kapitole budu vycházet především z dat těchto mezinárodních organizací, které do svých dlouhodobých výzkumů zahrnují i ČR.

2.1.1 Index digitální ekonomiky a společnosti (DESI, 2021)³⁴

Evropská komise od roku 2014 každoročně měří pokrok jednotlivých členských států v digitální transformaci. V roce 2021 byl upraven způsob výpočtu, aby odpovídal koncepci Digitální dekády EU a přijatému Nástroji pro oživení a odolnost³⁵, který je v ČR znám jako Národní plán obnovy. Index se zabývá čtyřmi oblastmi digitální ekonomiky a společnosti: lidským kapitálem, konektivitou, integrací digitálních technologií a digitálními veřejnými službami.

Nadprůměrné výsledky ve srovnání s ostatními státy dosahuje ČR jen v oblasti rozšiřování digitálních technologií v soukromém sektoru. Příčinou je úspěšné zavádění technologických inovací podniky a rozvinutý tuzemský elektronický obchod (anglicky eCommerce). Naopak v poskytování digitálních veřejných služeb ČR za průměrem EU zaostává. ČR se sice meziročně ve sledovaných parametrech zlepšuje, přesto její současné

³² DZURILLA, pozn. 7, s. 2.

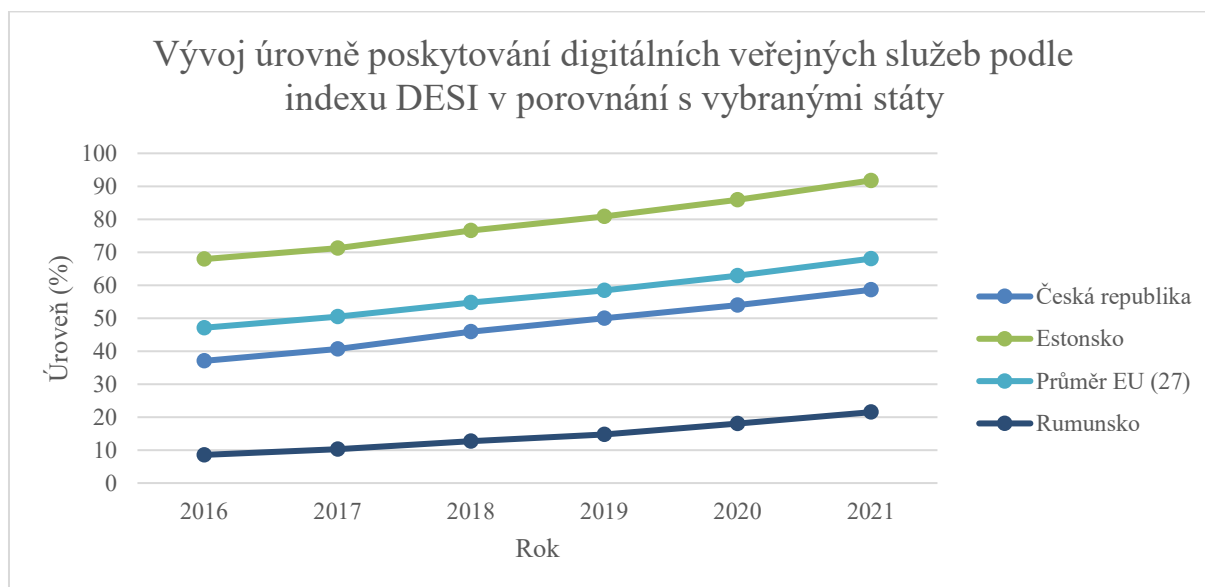
³³ MÁCHOVÁ, Renáta, LNĚNIČKA, Martin. Reframing E-Government Development Indices with Respect to New Trends in ICT. In: *Review of economic perspectives* [online]. De Gruyter, 2015. 15(4), 385-386 [cit. 20.6.2022]. ISSN: 1804-1663. DOI: [10.1515/revecp-2015-0027](https://doi.org/10.1515/revecp-2015-0027).

³⁴ EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021: Česko* [online]. Evropská komise, 2021 [cit. 20.6.2022]. Dostupné z: <https://ec.europa.eu/newsroom/dae/redirection/document/80581>.

³⁵ Nařízení Evropského parlamentu a Rady (EU) č. 2021/241 ze dne 12. února 2021, kterým se zřizuje Nástroj pro oživení a odolnost.

postavení odpovídá průměru EU zhruba před dvěma roky. Pokud bude ČR pokračovat v digitalizaci veřejných služeb dosavadní rychlostí, dosáhne současných hodnot Estonska, nejdříve v první polovině příští dekády.

Výkon ČR v žebříčku DESI má význam pro vyhodnocování plnění některých cílů Informační koncepce ČR³⁶.



Graf č. 2: Vývoj úrovně poskytování digitálních veřejných služeb podle indexu DESI v porovnání s vybranými státy³⁷.

Více než 60 % uživatelů internetu v ČR využije alespoň jednou ročně některou z elektronických služeb veřejné správy. Výrazné nedostatky má ČR v poskytování předvyplněných formulářů a digitálních veřejných služeb pro podniky.

2.1.2 E-Government Development Index (2020)

Celosvětové srovnání poskytuje pravidelný výzkum OSN E-Government Development Index (EGDI). ČR v roce 2020 zaujímala 39. místo v žebříčku 193 zemí³⁸. ČR se tak řadí mezi první čtvrtinu států s nejrozvinutějším eGovernmentem, což kontrastuje s evropským

³⁶ DZURILLA, pozn. 7, s. 2.

³⁷ Vlastní tvorba na základě dat indexu DESI:

EVROPSKÁ KOMISE. DESI by components [tabulky] In: *Data Visualisation Tool* [online]. 2021 [cit. 20.6.2022]. Dostupné z: <https://digital-agenda-data.eu/charts/desi-components>.

³⁸ OSN. E-government survey 2020: *Digital Government in the Decade of Action for Sustainable Development*. [online]. OSN, 2020, s. 8 [cit. 20.6.2022]. ISBN: 978-92-1-005145-3. Dostupné z: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>.

srovnáním pomocí DESI, kde se ČR v posledních letech umísťuje pravidelně mezi třetí a čtvrtou čtvrtinou zemí.

2.1.3 EGovernment benchmark (2021)

Benchmark je označení pro systematický proces porovnávání a měření. A právě taková porovnávání a měření zajišťuje ve tříletých intervalech Evropská komise. EGovernment benchmark zkoumá způsob, jakým státy v Evropě poskytují digitální služby veřejnosti. Hlavní metodou je mystery shopping. Výzkumníci ručně testují veřejné digitální služby, v několika zkoumaných oblastech pohledem uživatele a jeho typizovaných životních situací³⁹. Touto specifickou metodou se tento benchmark od indexů zmíněných výše.

ČR měla v roce 2021 podprůměrné umístění v celkovém i ve většině dílčích hodnocení. ČR mírně ztrácí na průměr EU například v oblasti rozšíření jednotného přihlašování k digitálním službám. V souvislosti s tím je negativně hodnocena opětovná potřeba přihlašování se při přechodu na mezi jednotlivými portály veřejné správy, byť zpravidla s totožnými přihlašovacími údaji. V ČR také existuje jen malé množství digitálních služeb, které by byly proaktivní. Takové služby nevyžadují po občanech aktivní jednání jako například podání žádosti.

Silnou stránkou českého eGovernmentu je rozšířená komunikace prostřednictvím datových schránek a informování o poskytovaných službách, i když jsou ve 28 % ze všech zkoumaných případů stále poskytovány jen nedigitálně⁴⁰.

2.1.4 Benchmark veřejné správy (2021)⁴¹

V České republice se v rámci platformy Digitální Česko jednou za tři roky provádí a vyhodnocuje Benchmark veřejné správy (Benchmark VS). Jeho cílem je zjistit a vyhodnotit stav řízení ICT v orgánech veřejné správy a také jejich připravenost na digitální transformaci. Na základě anonymních dotazníků, které vyplňují zástupci ministerstev a dalších ústředních správních úřadů, je sestavena souhrnná zpráva. Tato souhrnná zpráva nabízí srovnání mezi jednotlivými dotazovanými a identifikuje konkrétní problémy v řízení ICT a digitalizaci

³⁹ EVROPSKÁ KOMISE. *EGovernment benchmark: Method Paper 2020-2023* [online]. Publications Office of the EU, 2021, s. 16 [cit. 20.6.2022]. ISBN 978-92-76-36362-0. DOI: [10.2759/640293](https://doi.org/10.2759/640293).

⁴⁰ EVROPSKÁ KOMISE. *EGovernment benchmark 2021: Source Data* [tabulky]. Evropská komise: 2021 [cit. 20.6.2022]. Dostupné z: <https://ec.europa.eu/newsroom/dae/redirection/document/80571>.

⁴¹ DZURILLA, Vladimír, TÝM OHA MV. *ICT benchmark veřejné správy 2021* [online]. Archi.gov.cz, 2022. Poslední změna: 21.1.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/media/dokumenty:benchmark_2021_dc_final.pdf.

veřejné správy. Překonání těchto problémů by mělo vést ke zlepšení poskytování digitálních služeb.

Přestože předmětem této práce nejsou otázky řízení ve veřejné správě, pro širší kontext stavu českého eGovernmentu a zejména procesu jeho budování a udržování uvádím některá relevantní zjištění z oblasti řízení ICT:

- U 35 % dotazovaných subjektů došlo mezi lety 2018 a 2021 ke zhoršení celkové úrovně řízení IT. U zbývajících 65% došlo naopak ke zlepšení;
- Většina subjektů nepoužívá žádný standardní řídicí rámec řízení ICT;
- Více než 40 % subjektů nemá jasně definovány cíle ani neprovádí kontinuální sběr dat a jejich vyhodnocování;

Z oblasti personální:

- Subjekty mají problém s obsazením pozic klíčových ICT zaměstnanců;
- ICT pozice jsou oproti soukromému sektoru podfinancovány v řádu vyšších desítek procent;
- Udržovat a rozvíjet vlastními silami své klíčové platformy zvládne jen 15 % dotazovaných subjektů;

A konečně také zmíním oblast zadávání veřejných IT zakázek, ve které přetrvává nízká schopnost vysoutěžit a následně provozovat vysoutěžená ICT řešení. Dále je zaznamenána setrvalá tendence upřednostňovat nejnižší pořizovací cenu, která může vést v budoucnu k vyšším nákladům na provoz⁴².

Například Ministerstvo práce a sociálních věcí se již od roku 2011 snaží neúspěšně zbavit dosavadní závislosti na původním externím dodavateli informačního systému zajišťujícího výplatu dávek. Přestože nové informační systémy měly být nejprve uvedeny do provozu nejpozději do roku 2016, později do roku 2018, nestalo se tak nakonec dodnes. Tyto průtahy dle zjištění Nejvyššího kontrolního úřadu⁴³ představují nehospodárné výdaje pro státní rozpočet. Navíc průtahy těchto zakázek doprovází opakovaná procesní pochybení při jejich soutěžení a trvající nedostatek IT odborníků na ministerstvu, což v důsledku vede opět k závislosti na externích dodavatelích informačních systémů.

⁴² DZURILLA, pozn. 41.

⁴³ NKÚ. *Kontrolní závěr z kontrolní akce č. 17/22: Realizace projektů v oblasti ICT u MPSV* [online]. 2018 [cit. 20.6.2022]. Dostupné z: <https://nku.cz/assets/kon-zavery/k17022.pdf>

2.2 Funkční rozdělení podle vrstev

Často se při popisu funkčního uspořádání eGovernmentu vzpomíná eGON, což bylo společné označení čtyř klíčových projektů realizovaných v České republice mezi lety 2006 a 2012. EGON se schematicky znázorňuje jako oranžový panáček, jehož části těla reprezentují provázanost zmíněných projektů. Mozek znázorňoval základní registry, srdce datové schránky a elektronické doručování, oběhový systém komunikační infrastrukturu a prsty Czech POINT⁴⁴. Provázanost jednotlivých částí těla má především vyjadřovat nezbytnost vzájemného doplňování se jednotlivých částí eGovernmentu. Data bez vhodného způsobu vzájemné komunikace jsou k ničemu, stejně jako mozek bez srdce.



Obrázek č. 1: Panáček eGON spolu s tehdejším ministrem vnitra Ivanem Langerem a jeho náměstkem Zdeňkem Zajíčkem⁴⁵.

Éra těchto projektů se označuje jako první etapa budování tuzemského eGovernmentu. Podle Romana Vrby bylo druhou etapou další rozvíjení a stabilizace eGovernmentu a na prahu

⁴⁴ MINISTERSTVO VNITRA. eGON. In: *Mvcr.cz* [online]. Ministerstvo vnitra, [cca 2008, cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/clanek/egon-66.aspx>.

⁴⁵ MINISTERSTVO VNITRA. *eGON News* [online]. Ministerstvo vnitra, 2008, 3, s. 1 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/soubor/egon-news-3-pdf.aspx>.

třetí etapy se ČR nachází právě teď a to v souvislosti s nárůstem počtu uživatelů elektronické identity a datových schránek⁴⁶.

Při popisu jednotlivých složek současného eGovernmentu si s panáčkem eGON již nevystačím. S reálnějším funkčním znázorněním pracuje v rámci své činnosti Odbor Hlavního architekta eGovernmentu na Ministerstvu vnitra.

V Architektonické vizi⁴⁷, která je součástí Národního architektonického plánu, je rozpracována podoba tuzemského eGovernmentu jako propojeného a rozvrstveného celku. Tato vize zahrnuje stávající a do roku 2024 zamýšlené součásti eGovernmentu. Podstatou vrstvení je vytvoření komplexního řešení eGovernmentu, kde změna v jedné z vrstev ovlivní fungování jiné vrstvy jen minimálně, nejlépe však vůbec.

Uvedené znázornění má význam především pro praktické modelování architektury eGovernmentu. Já jej považuji za užitečné i pro úvodní vysvětlení vzájemných vazeb jednotlivých částí tuzemského eGovernmentu.

Na základě Architektonické vize je možné eGovernment rozdělit na čtyři vrstvy podle svých funkcí: byznys vrstva, aplikační vrstva, komunikační vrstva a technologická vrstva.

Byznys vrstva představuje vrstvu výkonu veřejné správy. Prostřednictvím této vrstvy se realizuje vše, co veřejná správa při výkonu svých pravomocí digitálně činí. Jedná se o souhrn všech digitálních procesů, funkcí a činností. Patří mezi ně činnosti ve vztahu k veřejnosti (G2C, G2B) jako například poskytování výpisu z informačních systémů, přijímání podání s pomocí datových schránek nebo identifikace a autentizace osob. Všechny tyto činnosti jsou regulovány veřejnoprávními normami. V dalších kapitolách se těmito normami budu zabývat.

Realizace služeb pro veřejnost je možná pomocí kontaktních míst veřejné správy. Těmi se rozumí „*místa a prostředky, kterými klienti veřejné správy mohou realizovat služby veřejné správy, bez ohledu na věcnou a místní příslušnost služby a služebního úřadu*“⁴⁸. Dle způsobu poskytování se dělí na čtyři kategorie podle toho, zda jsou poskytovány s pomocí

⁴⁶ VRBA, Roman. Zpráva o stavu eGovernmentu pro rok 2022. In: *ISSS 2022* [zvuková nahrávka]. 2022, 53.-60. minuta [cit. 20.6.2022]. Dostupné z: <https://issc.cz/archiv/2022/download/audio/zprava-o-stavu-egovernmentu-pro-rok-2022.mp3>.

PETERKA, Jiří. ISSS 2022: Blíží se zemětřesení v eGovernmentu a tsunami datových schránek. In: *Lupa.cz* [online]. Internet Info, 2022 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://lupa.cz/clanky/issc-2022-blizi-se-zemetreseni-v-egovernmentu-a-tsunami-datovych-schranek/>

⁴⁷ ŠEDIVÉC, Tomáš, RADA, Michal. Architektonická vize eGovernmentu ČR. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2018. Poslední změna: 31.5.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap_dokument:architektonicka_vize_e_governmentu_cr.

⁴⁸ ŠEDIVÉC, Tomáš. Univerzální kontaktní místo. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 4.5.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap:univerzalni_kontaktni_misto.

specializovaného personálu nebo samoobslužného portálu a podle toho, zda jsou poskytovány osobně nebo samoobslužně prostřednictvím digitálních kanálů:

- Samoobslužné univerzální;
- Samoobslužné specializované;
- Asistované univerzální;
- Asistované specializované.

Kromě výše uvedených činnosti spadají do byznys vrstvy i činnosti uvnitř samotných orgánů veřejné správy nebo mezi nimi navzájem (G2G).

Aplikační vrstva zahrnuje informační systémy veřejné správy, provozní informační systémy a další aplikační části, které veřejná správa provozuje nebo využívá. Často jsou využívány údaje ze základních registrů anebo z jiných datových zdrojů pomocí rozhraní, která se taktéž řadí do této vrstvy.

Z hlediska práva jsou v této vrstvě nejvýznamnější podmínky, za kterých lze takový informační systém, rozhraní nebo jinou součást aplikační vrstvy provozovat či využívat.

Technologická vrstva představuje vrstvu „zabývající se technologiemi, které svými funkcionalitami a službami podporují aplikace, systémy a obecně prvky z aplikační architektury“⁴⁹. Tato vrstva zahrnuje jak hardwarové vybavení jako například servery, datová úložiště a koncová zařízení, tak také nezbytný software.

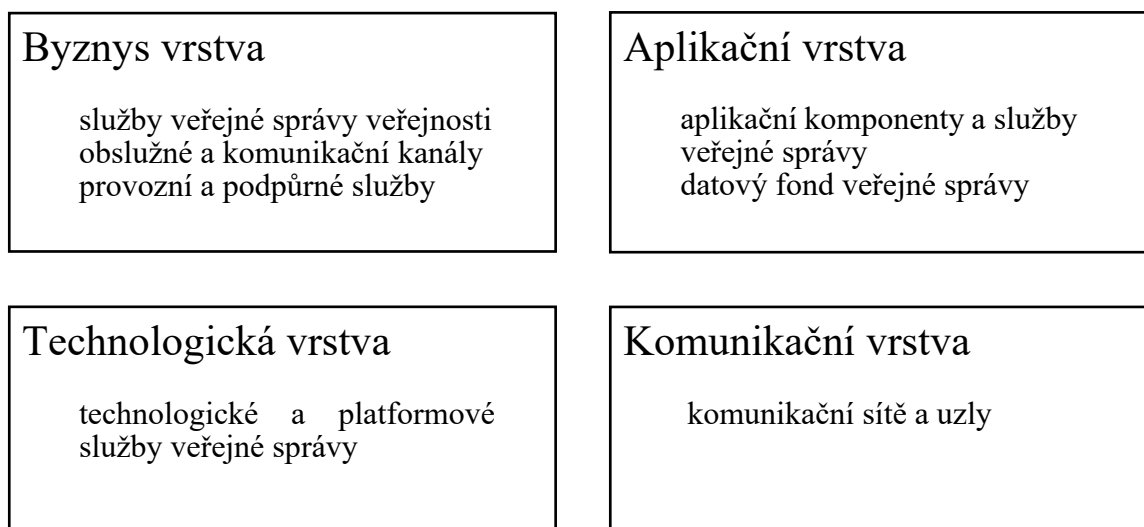
Klíčové právní otázky spočívají v kybernetické bezpečnosti a v podmínkách provozu technologií.

Komunikační vrstva zahrnuje výhradně fyzická datová centra a komunikační cesty, s jejichž pomocí je umožněno vnější a vnitřní propojení. Komunikační cesty zahrnují komunikační sítě a komunikační uzly. Jako komunikační síť se využívá internet nebo privátní síť zvaná Komunikační infrastruktura veřejné správy (KIVS). Komunikačním uzlem je Centrální místo služeb (CMS). KIVS/CMS tvoří funkční celek, který umožňuje především zabezpečený a regulovaný přístup k aplikačním službám jednotlivých informačních systémů veřejné správy⁵⁰.

⁴⁹ ŠEDIVEC, pozn 47, s. 1.

⁵⁰ ŠEDIVEC, Tomáš, RADA, Michal. Komunikační infrastruktura veřejné správy. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 1.6.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap:komunikacni_infrastruktura_veřejne_spravy.

Tato vrstva je právními předpisy eGovernmentu regulována především v oblasti zabezpečení, podmínek provozu a využívání KIVS/CMS.



Graf č. 3: Schématické znázornění vrstev architektury tuzemského eGovernmentu⁵¹.

2.3 Institucionální zajištění

Historicky měla ČR samostatný ústřední orgán, jehož hlavním úkolem byla koordinace rozvoje eGovernmentu, pouze v období 2003 až 2007. Po zániku Ministerstva informatiky byla podstata jeho působnosti přenesena změnou kompetenčního zákona na Ministerstvo vnitra. Dnes na tomto ministerstvu působí v rámci Sekce informačních a komunikačních technologií tři odbory: Odbor eGovernmentu, Odbor hlavního architekta eGovernmentu a Odbor koordinace informačních a komunikačních technologií a eGovernment cloudu⁵².

Ministerstvo vnitra má kompetenčním zákonem přiřazenu působnost v oblasti informačních systémů státní správy a elektronické identifikace⁵³. Další působnost vychází ze zvláštních zákonů. Ministerstvo vnitra například zřizuje a spravuje datové schránky⁵⁴, zajišťuje a spravuje některé základní registry⁵⁵ nebo vykonává činnost v oblasti akreditace a atestace informačních systémů veřejné správy.

⁵¹ Zpracováno volně podle ŠEDIVÉC, pozn 47.

⁵² MINISTERSTVO VNITRA. Organizační struktura. In: *Mvcr.cz* [online]. Ministerstvo vnitra, [cca 2022, cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/clanek/organizacni-struktura-362751.aspx>.

⁵³ § 12 odst. 1 písm. o) a n) zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky (kompetenční zákon), ve znění pozdějších předpisů.

⁵⁴ § 2 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (zákon o datových schránkách), ve znění pozdějších předpisů.

⁵⁵ § 20 odst. 1 a § 49 odst. 1 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Velký význam pro rozvoj tuzemského eGovernmentu mají také státní podniky: Národní agentura pro komunikační a informační technologie (NAKIT) a Státní pokladna Centra sdílených služeb (SPCSS).

Na stávající podobě koordinace digitalizace veřejné správy bývá kritizován přetrvávající resortismus a slabá pozice Odboru hlavního architekta eGovernmentu. Za účelem překonání těchto problémů se strany nynější vládnoucí koalice dohodly na transformaci koordinace a řízení digitalizace⁵⁶. Podstatou jsou přesuny kompetencí, lidských zdrojů a závazků. Transformace si vyžádá současně i legislativní změny.

Zásadní bude přeměna Správy základních registrů, ze které má vzniknout nový ústřední správní úřad Národní digitální agentura (NDA). Název dosud není jistý. V prezentaci ředitele odboru Hlavního architekta eGovernmentu na konferenci ISSS 2022 se hovořilo o vznikajícím úřadu jako o Digitální a informační agentuře (DIA)⁵⁷. Každopádně podstatné jsou kompetence, které má NDA získat. Kromě kompetencí přecházejících ze zanikající Správy základních registrů, má NDA nabýt i kompetence, které vykonávají všechny zmíněné odbory Ministerstva vnitra vyjma Odboru hlavního architekta eGovernmentu.

Odbor hlavního architekta eGovernmentu by se měl stát součástí nové sekce při Úřadu vlády. Ta bude mít na starosti především strategické řízení eGovernmentu včetně přípravy Informační koncepce ČR. Další nově vzniklé odbory na Úřadu vlády se budou zabývat evropskou digitální legislativou a koordinací digitalizace. Sekce by měla být podřízena místopředsedovi vlády pro digitalizaci.

NDA by měla řídit i nový státní podnik Národní datové centrum, který bude zajišťovat infrastrukturu. A také by se agentura měla stát připomínkovým místem v oblasti digitální legislativy.

Usnesením vlády č. 289 ze dne 6. dubna 2022⁵⁸ byl výše představený záměr transformace schválen. K naplnění většiny změn by mělo dojít k 1. ledna 2023.

⁵⁶ VLÁDA ČR. Příloha č. 1 usnesení vlády ze dne 6. dubna 2022 č. 289: Projektový záměr „Transformace koordinace a řízení digitalizace [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://apps.odok.cz/attachment/-/down/NANACDEH9J99>.

⁵⁷ KUCHAR, Petr. Koordinace eGovernmentu z pohledu HAeG [prezentace]. In: ISSS 2022 [online]. 2022 [cit. 20.6.2022]. Dostupné z: https://iss.s.cz/archiv/2022/download/prezentace/mvcr_kuchar.pdf.

⁵⁸ Usnesení vlády ČR č. 289/2022 k realizaci projektu Transformace koordinace a řízení digitalizace.

3 Úvod do právního rámce eGovernmentu v ČR

Současný právní rámec eGovernmentu je v České republice tvořen souhrnem především zákonných a podzákonných právních norem. Význam mají i normy Evropské unie.

3.1 Právní principy eGovernmentu

Právní principy jsou abstraktní regulativní právní ideje, které jsou součástí právního řádu. Právní principy se na rozdíl od právních norem neuplatňují absolutně⁵⁹. Tato odlišnost znamená, že v případě střetu dvou principů je nezbytné jednotlivé principy poměřit a uplatnit je tak, aby byly oba dodrženy v co nejširší možné míře. Právní principy mohou být buď deskriptivní povahy, pokud popisují, co je, anebo normativní, pokud popisují, co má být. Normativní právní principy zpravidla vycházejí z hlubšího hodnotového ukotvení⁶⁰.

Systematická práce s právními principy eGovernmentu je českými autory zpravidla opomíjena. Podle mého názoru by jí měla být věnována větší pozornost, protože by to přispělo k větší systematickosti studia a zkoumání pozitivního práva upravujícího eGovernment. Analyzování právní úpravy eGovernmentu jen s popisem historického vývoje bez formulování základních právních principů zbytečně ochuzuje právní poznání o eGovernmentu.

Během desítek let budování a rozvoje eGovernmentu se etablovalo několik principů. Tyto principy jsou explicitně vyjádřeny ve strategických dokumentech a částečně i v teoreticko-právní literatuře⁶¹. Realizovány jsou při stanovování a dosahování cílů v Informační koncepci ČR a v souvislosti s digitálně přívětivou legislativou, které se budou ještě věnovat. Implicitně jsou principy eGovernmentu vyjádřeny v právním řádu.

Jedna část principů uplatňujících se v České republice byla formulovaná v Akčním plánu EU pro eGovernment na období 2016-2020⁶², a druhou část představují další principy eGovernmentu, které jsou dovozené z tuzemského právního řádu.

3.1.1 Principy obsažené v Akčním plánu EU

Princip preference elektronizace (také standardně digitalizované, anglicky Digital-by-default) znamená, že veřejná správa nahradí výchozí formu poskytování veřejných služeb

⁵⁹ GERLOCH, Aleš. *Teorie práva*. 8. aktualizované vydání ed. Plzeň: Aleš Čeněk, 2021, s. 24. ISBN: 978-80-7380-838-9.

⁶⁰ Tamtéž, s. 31-32.

⁶¹ Například TULÁČEK, Michal. *Elektronizace správy daní*. Praha: Leges, 2020. ISBN: 978-80-7502-434-3.

⁶² EVROPSKÁ KOMISE. Sdělení Komise...: Akční plán EU pro eGovernment na období 2016-2020 [online]. 2016 [cit. 20.6.2022]. CELEX: 52016DC0179. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52016DC0179>.

spočívající v osobní a papírové interakci digitálními způsoby prostřednictvím elektronické komunikace ať už prostřednictvím transakčních portálů nebo třeba datových schránek. Mimo služeb poskytuje veřejná správa primárně elektronickým způsobem i data, aby je veřejnost mohla využít pro svůj rozvoj⁶³.

S tímto principem jsou neodmyslitelně spojeny některé otázky:

- jak jeho realizace dopadne na skupinu občanů, kteří elektronické způsoby komunikace nemohou nebo nechtějí využívat (anglicky Digital divide);
- jak těmto skupinám občanů veřejné služby nadále poskytovat.

Většinou nezbyvá než udržovat vedle elektronických způsobů komunikace i původní neelektronické způsoby.

Princip elektronizace jako volby doplňuje princip preference elektronizace v tom smyslu, že by nikomu neměla být odebrána možnost rozhodnout se, zda chce nebo nechce komunikovat s veřejnou správou elektronicky.

Nástroje a služby eGovernmentu jsou občany mnohdy preferovány samy od sebe. Například kvůli rychlejšímu nebo pohodlnějšímu vyřízení věci. V některých případech ale veřejná správa vytváří tlak, aby občané využívali elektronické způsoby komunikace. Důvodem může být snazší a hospodárnější sdílení informací nebo zpracování dat uvnitř orgánu veřejné správy. Tento tlak na elektronizaci řeší zákonodárce tím, že stanoví použití určitého typu komunikace buď jako možnost či zvýhodněnou možnost, anebo jako povinnost s hrozbou sankce⁶⁴.

V případě zvýhodněné možnosti dochází k prosazování elektronizace veřejné správy, při kterém jsou občanům poskytovány výhody motivující k využívání elektronických způsobů komunikace. Takovou výhodu může představovat například pozdější datum podání, nižší správní poplatek nebo poskytnutí dodatečných funkcionalit. O vynuucování elektronizace veřejné správy, se hovoří v případech, kdy je stanovena povinnost využít elektronických způsobů komunikace pod hrozbou sankce⁶⁵. Tak tomu je u tzv. elektropokuty v daňovém řádu⁶⁶. V oblasti správy daní je proto podle Michala Tuláčka přítomný i princip vynuucování

⁶³ LIPS, pozn. 10, s. 93-94.

⁶⁴ PAVLÍK, pozn. 30, s. 150.

⁶⁵ TULÁČEK, pozn. 61, s. 57.

⁶⁶ § 247a odst. 2 zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů.

elektronizovaného institutu⁶⁷. Tento zvláštní princip je protikladem k principu elektronizace jako volby.

Princip pouze jednou (anglicky Only once) představuje povinnost orgánů veřejné správy nevyžadovat od občanů a podniků stejné informace opakovaně i v případech, pokud informace byla sdělena jinému orgánu veřejné správy⁶⁸. Na rozdíl od Tuláčka⁶⁹ považují princip sdílení informací mezi orgány veřejné moci za součást principu pouze jednou. Sdílení informací mezi orgány veřejné moci totiž představuje jen způsob naplnění principu pouze jednou. Těžko by se princip pouze jednou realizoval bez vzájemného sdílení údajů uvnitř veřejné správy.

Princip otevřenosti a transparentnosti (anglicky Openness and Transparency) znamená mimo jiné povinnost orgánů veřejné správy při své činnosti sdílet navenek informace a data, umožnit k nim přístup občanům a umožnit jim opravit údaje, které o nich veřejná správa eviduje⁷⁰.

Princip začlenění a dostupnosti (anglicky Inclusiveness and Accessibility) zavazuje veřejnou správu poskytovat služby tak, aby byly přístupné i skupině lidí, kteří ICT nemohou nebo nechtějí využívat. Za tímto účelem musí veřejná správa odstranit překážky, které mají například osoby se zdravotním postižením při procházení internetových stránek veřejné správy. Tento konkrétní problém řeší směrnice EU o přístupnosti⁷¹.

Princip důvěryhodnosti a bezpečnosti (anglicky Security & Privacy by design) zavazuje orgány veřejné moci ke dbání na bezpečnost ICT, ochranu osobních údajů a ochranu soukromí občanů. S tím souvisí požadavek, aby orgány veřejné správy zpracovávaly jen nezbytné osobní údaje v co nejmenším možném rozsahu⁷².

Poslední dva evropské principy zohledňují specifika EU. *Princip preference přeshraničního přístupu* (anglicky Cross border interoperability) představuje povinnost orgánů veřejné správy umožnit přístup k digitálním službám i z ostatních členských států EU. Tento princip upravuje poskytování služeb navenek. Jak veřejné správy členských států koordinují

⁶⁷ TULÁČEK, pozn. 61, s. 176.

⁶⁸ ŠEDIVÉC, Tomáš, RADA, Michal. Informační koncepce ČR. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019, bod Architektonický princip EU P2: Zásada „pouze jednou“. Poslední změna: 21.7.2021 [cit. 20.6.2022]. Dostupné z: <https://archi.gov.cz/ikcr>.

⁶⁹ TULÁČEK, pozn. 61, s. 169.

⁷⁰ ŠEDIVÉC, pozn. 68, bod Architektonický princip EU P4: Otevřenost a transparentnost.

⁷¹ Směrnice Evropského parlamentu a Rady (EU) 2016/2102 ze dne 26. října 2016 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru, CELEX: 32016L2102.

⁷² EVROPSKÁ KOMISE, pozn. 62, kapitola 2.

a integrují informační systémy a činnosti uvnitř řeší *princip vzájemné propojitelnosti* (anglicky Interoperability by design). Podstatou je povinnost orgánů veřejné správy zajistit na různých úrovních vzájemnou součinnost různých systémů bez ohledu na vykonávanou agendu. Důsledkem by mělo být především bezproblémové poskytování digitálních služeb na vnitřním trhu⁷³.

3.1.2 Další principy dovozené z tuzemského právního řádu

Princip technologické neutrality (anglicky Technological neutrality) vyžaduje, aby poskytování digitálních služeb veřejnou správou nebylo závislé na konkrétní technologii. Uplatní se i při tvorbě nové legislativy, kdy je vhodné zavádět právní instituty na základě technicky neutrálních pojmů. Příkladem může být sousloví doručení „*prostřednictvím veřejné datové sítě*“⁷⁴ ve správněprocesních předpisech, které je vhodnější než sousloví doručení přes internet nebo e-mailem, protože oba pojmy jsou svázány s konkrétními technickými protokoly TCP/IP a mohou být v budoucnu nahrazeny zcela jinou technologií.

Princip rovnocennosti elektronického úkonu představuje rovnost mezi veřejnoprávními úkony činěnými elektronicky a úkony činěnými v listinné podobě⁷⁵.

Zákaz přírážky za elektronizovaný úkon orgánu veřejné moci je právním principem úzce souvisejícím s principem preference elektronizace. Tuláček tento princip dovozuje z absence zvláštních správních poplatků za elektronické úkony⁷⁶. Navíc jsou v praxi elektronické úkony spíše zvýhodňovány jako například podání elektronického platebního rozkazu⁷⁷.

Většina z výše uvedených principů je promítnuta v Zásadách pro tvorbu digitálně přívětivé legislativy, což je metodický materiál z roku 2017 určený předkladatelům právních norem k provedení analýzy posouzení dopadů informačních technologií (anglicky Information Technology Impact Analysis, ITIA). Od ledna roku 2020 musejí předkladatelé jakýchkoliv návrhů právních předpisů, které jsou předkládány vládě, obsahovat zhodnocení souladu

⁷³ ŠEDIVÉC, pozn. 68, bod Principy eGovernmentu EU.

⁷⁴ § 19 odst. 1 zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

§ 42 odst. 1 zákon č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů.

⁷⁵ Obsažen v článku 25 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 (nařízení eIDAS), CELEX: 32014R0910.

⁷⁶ TULÁČEK, pozn. 61, s. 175.

⁷⁷ Položka 2 sazebníku poplatků, přílohy k zákonu č. 549/1991 Sb., o soudních poplatcích, ve znění pozdějších předpisů.

navrhované právní úpravy s principy digitálně přívětivé legislativy⁷⁸. Návrhy posuzuje Výbor pro digitálně přívětivou legislativu Rady vlády pro informační společnost⁷⁹. Cílem je vynucení prosazení principů eGovernmentu v nově přijaté legislativě napříč odvětvími veřejné správy.

3.1.3 Vztah právních principů a norem eGovernmentu

Právní předpisy eGovernmentu jsou součástí veřejného práva. Z tohoto důvodu je veškerá činnost orgánů veřejné moci při výkonu působnosti v oblasti eGovernmentu vázána ústavním principem enumerativnosti veřejnoprávních pretenzí. Podstata tohoto principu spočívá v možnosti orgánů veřejné moci moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon⁸⁰.

Oblast právní úpravy eGovernmentu je podmnožinou správního práva, a proto na něj dopadají obecné principy správního práva, z nichž některé jsou explicitně vyjádřeny v základních principech činnosti orgánů veřejné správy v ustanoveních § 2 až § 8 správního řádu. Jde zejména o princip subsidiarity předepisující minimalizaci zásahů veřejné správy do právních poměrů dotčených osob⁸¹, o princip legality vycházející z výše uvedeného ústavního principu enumerativnosti veřejnoprávních pretenzí, o princip spolupráce ve veřejné správě a o princip dobré správy⁸². Aplikace těchto principů, které se vztahují na veškerou činnost správních orgánů, přesahuje správní řád ve dvou případech. V prvním případě se tyto v zákoně explicitně vyjádřené principy při výkonu veřejné správy použijí i v případech, kdy zvláštní zákon stanoví, že se správní řád nepoužije⁸³. A ve druhém případě správní věda dovozuje část těchto zásad jako deklaratorní vyjádření obecných zásad právních⁸⁴, které jsou v některých případech vyjádřeny i v ústavním pořádku jako například výše uvedená zásada legality.

⁷⁸ REKONSTRUKCE STÁTU: *Nedigitální Česko* [online]. 2021, s. 8 [cit. 20.6.2022]. Dostupné z: https://rekonstrukcestatu.cz/download/3nQoIlg/nedigitalni_cesko.pdf.

⁷⁹ Čl. 2 odst. 2 písm. k) a l) přílohy Usnesení vlády ČR č. 961/2014 o zřízení Rady vlády pro informační společnost (statut Rady vlády pro informační společnost).

⁸⁰ Čl. 2 odst. 3 ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů.

Čl. 2 odst. 2 usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky (Listina), ve znění pozdějších předpisů.

⁸¹ § 2 odst. 2 správního řádu.

⁸² § 8 odst. 1 a 2 správního řádu.

⁸³ § 177 odst. 1 správního řádu.

Výjimkou je daňový řád, který obsahuje úpravu odpovídající těmto principům.

⁸⁴ JEMELKA, Luboš, PONĎĚLÍČKOVÁ, Klára, BOHADLO, David. *Správní řád*. 6. vydání. Praha: C.H. Beck, 2019, s. 21. ISBN 978-80-7400-751-4.

Z toho lze usoudit, že základní principy podle správního řádu mají ve vztahu k principům eGovernmentu subsidiární povahu. To znamená, že v případě konfliktu nevylučují jeden druhý, ale je nezbytné principy poměřit a uplatnit tak, aby byly oba, pokud možno, zachovány.

3.2 Ústavní pořádek

Jak bylo uvedeno výše, právní úprava eGovernment je součástí veřejného práva, a proto jej výrazně ovlivňuje v ústavním pořádku zakotvený princip enumerativnosti veřejnoprávních pretenzí. V důsledku tohoto principu musí být eGovernment vždy upraven v zákoně nebo v právním předpisu vydaném na základě zákona nebo v jeho mezích.

Mimo tohoto principu mají pro eGovernment význam i některá práva zaručená v Listině základních práv a svobod (Listina). Pro veřejnou správu v demokratickém právním státě není únosné, aby občanům a priori neumožnila dozvědět se, co a jak dělá, protože by tím odepírala nezbytnou kontrolu veřejné moci ze strany veřejnosti⁸⁵. Proto je v Listině přiznáno právo na informace⁸⁶. Tomu odpovídá povinnost orgánů veřejné moci umožnit jeho realizaci⁸⁷. Pro právo na informace je typické, že jej provádějící zákon⁸⁸ ani jeho výklad nemůže omezit nad rámec Listiny, která připouští jen omezení v demokratické společnosti nezbytná z taxativních důvodů⁸⁹. Pro naplnění práva na informace přinesl rozvoj eGovernmentu především nové komunikační kanály poskytování a zveřejňování informací.

Dalším právem v Listině, na které je vhodné v souvislosti s eGovernmentem upozornit, je právo na ochranu soukromí. Ústavní soud jej vykládá ve smyslu práva „*fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob*“⁹⁰.

⁸⁵ MIKULE, Vladimír, KOPECKÝ, Martin. Právo na přístup k informacím. In: HENDRYCH, Dušan aj. *Správní právo: Obecná část*. 9. vydání. Praha: C. H. Beck, 2016, s. 455, marg. č. 844. ISBN: 978-80-7400-624-1.

⁸⁶ Čl. 17 odst. 1 Listiny.

⁸⁷ Nález Ústavního soudu ze dne 16. 6. 2015, sp. zn. I. ÚS 3930/14, bod 17.

⁸⁸ Zejména zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů, a zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸⁹ Čl. 17 odst. 4 Listiny.

⁹⁰ Nález Ústavního soudu ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99.

Obecně každý zásah do základních práv a svobod musí být ústavně konformní. Pro posouzení ústavní konformity zásahu vypracoval Ústavní soud v rámci své soudní činnosti více kritériální judiciální testy. Nerozšířenější z nich jsou test proporcionality a test racionality.

4 Právní předpisy eGovernmentu

Vzhledem k množství zákonů, které mají pro eGovernment větší či menší význam, považují za vhodné zákony alespoň zhruba horizontálně systematizovat. Zákony, které se týkají eGovernmentu, lze podle jejich obsahu dělit na několik různých skupin⁹¹: agendové zákony, zákony eGovernmentu a správně procesní předpisy.



Graf č. 4: Pyramida zákonných předpisů relevantních pro eGovernment⁹²

Agendové zákony obsahují hmotněprávní i procesně právní normy, které se vztahují ke konkrétním činnostem veřejné správy. Jedná se o nejrozsáhlejší skupinu zákonů právního rámce eGovernmentu. Toto pojmenování vychází z dikce zákona o základních registrech, kde se agendou rozumí „*ucelená oblast působení orgánu veřejné moci*“, respektive ucelená oblast působení podnikajících fyzických osob či právnických osob, které mimo výkon veřejné moci využívají údaje z registrů⁹³. Tyto agendy jsou registrovány v Registru práv a povinností. V červnu 2022 bylo zaregistrováno více než 470 agend napříč veřejnou správou⁹⁴. Jde například o agendu evidence obyvatel, správních poplatků, stavebního řádu nebo občanských průkazů.

Toto vymezení pojmu agendy je vhodné především pro vedení Registru práv a povinností. Pro systematiku zákonných předpisů eGovernmentu postačí vymezení

⁹¹ OPEN-SOURCE ALIANCE. Veřejná část workshopu k nové e-government legislativě. In: *Youtube* [online]. 20. 7. 2021 [cit. 31. 3. 2022], 3. minuta 40. sekunda. Dostupné z: <https://youtu.be/yTHr2ZSvf10?t=220>. ŠEDIVEC, Tomáš, RADA, Michal. Klíčové zákony týkající se eGovernmentu. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 30.4.2021 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap:komunikacni_infrastruktura_veřejne_spravy.

⁹² OPEN-SOURCE ALIANCE, pozn. 91.

⁹³ § 2 písm d) a e) zákona o základních registrech.

⁹⁴ MINISTERSTVO VNITRA. *Rozcestník vygenerovaných agend* [online]. 2022 [cit. 8.6.2022]. Dostupné z: <https://rpp-ais.egon.gov.cz/gen/agendy-detail/>.

agendy jako ucelené oblasti působení veřejné správy, které vychází ze zákonných předpisů, bez ohledu na to, zda je taková činnost někde registrována.

Zákony eGovernmentu představují právní úpravu specifických způsobů vykonávání veřejné správy prostřednictvím ICT. Předmětem úpravy jsou zejména právní instituty specifické pro eGovernment, jakými jsou například elektronické podpisy, informační systémy veřejné správy nebo datové schránky. Zákony eGovernmentu je možné dále systematizovat do podskupin podle typu právních institutů, které primárně upravují⁹⁵.

První a nejobecnější podskupina zahrnuje zákony významné pro klíčové informační systémy eGovernmentu. Patří mezi ně zákon o základních registrech, zákon o informačních systémech veřejné správy (ZISVS) a zákon o kybernetické bezpečnosti.

Druhou podskupinu zastupují dva zákony významné pro zdroje identit, kterými jsou zákon o službách vytvářejících důvěru pro elektronické transakce (ZSVDET) a zákon o elektronické identifikaci.

Třetí podskupina zahrnuje ostatní klíčové eGovernment zákony, jako jsou zákon o právu na digitální služby (ZPDS), zákon o elektronických úkonech a autorizované konverzi dokumentů (zákon o datových schránkách), zákon o archivnictví a spisové službě, zákon o svobodném přístupu k informacím nebo zákon o přístupnosti.

Působnost, kterou veřejná správa vykonává na základě výše uvedených předpisů, lze podřadit i pod mnou vymezený pojem agenda. I v Registru práv a povinností jsou evidovány činnosti typické pro eGovernment jako například agenda informačního systému datových schránek, kontaktních míst veřejné správy nebo správy základních registrů. Tyto agendy se od agend upravených v agendových zákonech liší tím, že obsahují činnosti důležité pro samotnou elektronizaci. Jinými slovy eGovernment zákony upravují obecné nástroje eGovernmentu, s jejichž pomocí jsou agendy vykonávány.

Správně procesní předpisy upravují ty nejobecnější způsoby, jakými orgány veřejné správy vykonávají veřejnou správu. Nejvýznamnější pro veřejnou správu je správní řád upravující správní řízení a základní principy činnosti orgánů veřejné správy. Pro správu daní má obdobně významné postavení daňový řád.

⁹⁵ OPEN-SOURCE ALIANCE. *Legislativa* [online]. 2021 [cit. 20.6.2022]. Dostupné z: <https://openczeg.cz/legislativa/>.

Dále se v textu budu zabývat právní úpravou jednotlivých zákonů eGovernmentu vyjma trojice specifických zákonů: zákonu o kybernetické bezpečnosti, zákonu o svobodném přístupu k informacím a zákonu o přístupnosti.

4.1 Právní úprava základních registrů

Komplexní právní úprava obsažená v zákoně o základních registrech byla přijata s cílem nahradit dosavadní roztržitěné evidence a umožnit efektivní sdílení a využívání základních údajů, které veřejná správa v souvislosti s výkonem veřejné moci shromažďuje⁹⁶. Základní registry slouží jako „základní datový zdroj údajů o subjektech a objektech práva a o výkonu veřejné správy“⁹⁷. Převážná část zákonné úpravy se věnuje požadavkům a procesu registrace a spravování a využívání údajů vedených v jednotlivých zákonem označených základních registrech:

- Registr obyvatel, který obsahuje údaje o fyzických osobách;
- Registr osob, který obsahuje údaje o právnických osobách a dalších entitách;
- Registr územní identifikace, který obsahuje údaje adres a nemovitostí;
- Registr práv a povinností, který obsahuje zejména údaje o agendách⁹⁸.

Společně tyto registry tvoří informační systém základních registrů. Každý základní registr má přiřazeného editora, jímž je orgán veřejné moci s oprávněním referenční údaje do základního registru zapisovat a měnit⁹⁹.

V Registru práv a povinností se evidují referenční údaje o agendách veřejné správy včetně výčtu a popisů činností, úkonů vykonávaných v rámci agendy, výslovného označení ustanovení, z něhož vyplývá pravomoc orgánu veřejné moci k určité agendě atd¹⁰⁰. Informační systémy veřejné správy, které orgány veřejné správy používají při výkonu agendy se označují jako agendové informační systémy a jejich vazba na základní registry je taktéž předmětem této zákonné úpravy. Předpokladem registrace agendy je její ohlášení Ministerstvu vnitra.

Druhá část úpravy je v zákoně věnovaná obecným a společným ustanovením pro všechny základní registry. Pro bezproblémové sdílení a využívání údajů je důležité

⁹⁶ MATES, pozn. 4, s. 90.

⁹⁷ ŠEDIVÉC, Tomáš, RADA, Michal. Základní registry. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 30.4.2021 [cit. 28.2.2022]. Dostupné z: https://archi.gov.cz/nap:zakladni_registry.

⁹⁸ § 3, § 18, § 26 a § 32 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ZISVS), ve znění pozdějších předpisů.

⁹⁹ § 4 zákona o základních registrech.

¹⁰⁰ § 50 a § 51 odst. 6 zákona o základních registrech.

postavení referenčních údajů, což jsou právě ty údaje v základním registru, které zákon formálně za referenční označí¹⁰¹. Pro referenčních údaje se uplatní vyvratitelná domněnka správnosti. Každý „referenční údaj je považován za správný, pokud není prokázán opak nebo pokud nevznikne oprávněná pochybnost o správnosti referenčního údaje“¹⁰². Výslovně je upravena vyvratitelná domněnka dobré víry toho, kdo vychází z referenčního údaje. Ten je v dobré víře, pokud není prokázáno, že musel o jeho nesprávnosti vědět¹⁰³.

Pro naplnění zásady eGovernmentu pouze jednou je orgán veřejné moci povinen při výkonu své činnosti využít referenční údaje ze základních registrů a zároveň nesmí vyžadovat jejich poskytnutí od subjektů, kterých se údaje týkají. Výjimkou z této povinnosti jsou případy, kdy referenční údaj není v žádném z registrů evidován nebo je sice v registru evidován, ale je označen za nesprávný nebo existuje oprávněná pochybnost o jeho správnosti¹⁰⁴.

Úprava základních registrů umožňuje fyzickým osobám získat přehled o využívání jejich údajů z registru osob. Osoba, o které jsou tyto údaje vedeny, může při nesouladu referenčních údajů, které jsou o ní vedeny, se skutečným stavem, podat žádost o změnu údajů v registru obyvatel. Následně „editor zapíše referenční údaj do základního registru nebo provede jeho změnu bez zbytečného odkladu“¹⁰⁵. Ministerstvo vnitra tento postup označuje za proces reklamace správnosti údaje¹⁰⁶. Jedná se o změnu údajů v registru, informační úkon, který stejně jako například registrační úkony řadí správně právní teorie mezi neregulativní úkony. Tedy mezi „úkony, jejichž prostřednictvím vykonavatelé veřejné správy plní úkoly veřejné správy, které přímo nezasahují do něčích práv“¹⁰⁷. Z hlediska zásad eGovernmentu jde o realizaci principu otevřenosti a transparentnosti.

¹⁰¹ § 2 písm. a) a § 3 zákona o základních registrech.

¹⁰² § 4 odst. 4 zákona o základních registrech.

¹⁰³ § 4 odst. 6 zákona o základních registrech.

¹⁰⁴ § 5 zákona o základních registrech.

¹⁰⁵ § 14 odst. 6 a 4 odst. 3 zákona o základních registrech.

¹⁰⁶ ŠEDIVÉC, Tomáš. Referenční údaje. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019, bod Proces reklamace správnosti údaje. Poslední změna: 30.4.2021 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap:referencni_udaje.

¹⁰⁷ STAŠA, Josef. Oddíl 1. Charakteristika. In: HENDRYCH, pozn. 85, s. 191, marg. č. 338.

4.2 Právní úprava informačních systémů veřejné správy

Informačním systémem se obecně rozumí konkrétní organizovaný způsob uspořádání a předávání informací včetně jeho vnitřních a vnějších vztahů¹⁰⁸. Historicky měla být problematika informačních systémů komplexně upravena již v roce 1992, avšak původní poslanecký návrh byl zúžen jen na oblast ochrany osobních údajů při používání informačních systémů¹⁰⁹. Cílem úpravy bylo překonat dosavadní přílišnou volnost v přístupu jednotlivých ministerstev a dalších orgánů veřejné správy, které si pořizovali informační systémy, a vytvořit předpoklad pro rozvoj navzájem propojených informačních systémů¹¹⁰. Nakonec byl zákon informační systémy veřejné správy (ZISVS) přijat na počátku tisíciletí. Předmětem zákona jsou zejména právní vztahy související s „*vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy*“¹¹¹ (ISVS).

Základní otázkou kladenou od samotného přijetí tohoto zákona je, na které informační systémy se regulace vztahuje. V prvním případě se regulace vztahuje na informační systémy, které zákon za ISVS formálně označí. Dalšími jsou informační systémy, které nejsou z působnosti zákona vyjmuty, a zároveň naplňují materiální znaky obsažené v rozsáhlé a popisné definici ve vymežovacím ustanovení § 2 písm. a) a b) ZISVS. Zjednodušeně se podle této definice jedná o každý funkční celek nebo jeho část, který zabezpečuje cílevědomou a systematickou práci s informacemi spočívající zejména v získávání a poskytování informací pro účely výkonu veřejné správy nebo plnění jiných veřejných funkcí¹¹². Z toho vyplývá, že úprava zákona dopadá i na řadu subjektů, které sice zpracovávají informace pro účely výkonu veřejné správy, ale v organizačním smyslu veřejné správy se za veřejnou správu zpravidla nepovažují. Rozhodující proto je funkční pojetí veřejné správy. Tedy otázka, zda konkrétní vykonávaná činnost je veřejnoprávní, nebo není.

Jak bylo řečeno výše, za informační systémy veřejné správy nelze považovat ty informační systémy, které jsou vyňaty z působnosti tohoto zákona jako je například skupina informačních systémů spravovaná zpravodajskými službami a dalšími bezpečnostními úřady nebo provozními systémy, při jejichž provozu nedochází k výkonu vrchnostenské moci¹¹³. Další skupinou informačních systémů, které pod tento zákon nespádají, jsou

¹⁰⁸ MATES, pozn. 4, s. 48.

¹⁰⁹ TULÁČEK, pozn. 61, s. 90-91.

¹¹⁰ MATES, pozn. 4, s. 48-49.

¹¹¹ § 1 odst. 1 ZISVS.

¹¹² § 2 písm. a) a b) ZISVS.

¹¹³ § 1 odst. 2 až 5 ZISVS.

informační systémy vedené podle právních předpisů EU. Například celní informační systém nebo informační systémy podle směrnice DAC¹¹⁴. Zvláštní zákony obsahují spoustu další výjimek například v oblasti krizového řízení či praní špinavých peněz¹¹⁵.

Důvodem nezbytnosti předcházejícího vymezení je právní institut atestací, kterému se musí podrobit všechny ISVS. Atestace vynucují shodu informačních systémů s požadavky zákona. Průběh atestací a zejména konkrétní požadavky upravují vyhlášky ministerstva¹¹⁶. Typově jde o různé požadavky na řízení kvality a bezpečnosti či soulad s Informační koncepcí ČR. V případě, kdy informační systém tyto požadavky nespĺňuje, není mu umožněno komunikovat s dalšími ISVS. Jedná se tak o faktickou sankci, která nutí správce informačního systému zjednat nápravu, aby mohl s pomocí tohoto systému vykonávat svou agendu, ke které potřebuje informace z jiných systémů, zejména z informačního systému základních registrů. Jiné nedostatky při postupu orgánů veřejné správy podle tohoto zákona kontroluje Ministerstvo vnitra, které může uložit opatření k nápravě¹¹⁷.

Co se týče povahy ostatních informací evidovaných v ISVS, tak u těch se na rozdíl od referenčních údajů v základních registrech neuplatní domněnka správnosti. Nelze tedy presumovat, že jsou evidovány správně. Orgán veřejné správy musí s těmito informacemi nakládat stejně jako s každou jinou informací, kterou při své činnosti získá¹¹⁸.

Další zásadní pravidlo spočívá v realizaci principu rovnocennosti elektronického úkonu. Zákon jednak spojuje s úkonem účinky podpisu osoby, která činí úkon prostřednictvím ISVS¹¹⁹, v případě její úspěšné autentifikace a autorizace. A jednak může mít za splnění určitých podmínek výstup z ISVS povahu veřejné listiny.

Mezi další zásadní instituty eGovernmentu, které upravuje tento zákon patří komunikační infrastruktura veřejné správy a centrální místo služeb, a některých kontaktních míst veřejné správy. Samoobslužným univerzálním kontaktním místem je Portál občana, který je transakční částí Portálu veřejné správy. Asistovaným univerzálním kontaktním místem je síť

¹¹⁴ TULÁČEK, pozn. 61, s. 92.

¹¹⁵ MATES, pozn. 4, s. 52-53.

¹¹⁶ Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy.

Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy.

¹¹⁷ § 5c odst. 1 a 2, § 4 odst. 2 písm. a) ZISVS.

¹¹⁸ A contrario § 4 odst. 4 a 6 ZISVS.

Rozsudek Městského soudu v Praze ze dne 16.1.2013, čj. 10 A 320/2011-50, s. 5.

¹¹⁹ § 8 ZISVS.

Czech POINT. Tato síť představuje v podstatě síť elektronických podatelen, kde je možné získat některé výpisy z ISVS, provést konverzi dokumentů podle zákona o datových schránkách anebo učinit podání vůči veřejné správě jako například ohlášení živnosti.

Samoobslužná specializovaná kontaktní místa jsou upravena prostřednictvím obecné úpravy ZISVS. Transakční části těchto systémů se označují jako portály a jejich prostřednictvím jsou občanům poskytovány služby nebo jejich prostřednictvím občané činní úkony. Příkladem je Portál farmáře, AIS MPO nebo AIS SFŽP ČR.

Poslední kategorie asistovaných specializovaných kontaktních míst není upravena ZISVS. Podstatou je totiž fyzický kontakt občana s úředníky na přepážce orgánu veřejné moci, na kterých odbavuje služby a úkony odborný personál zpravidla znalý poskytované agendy¹²⁰.

Pro úplnost uvádím, že pro ISVS má význam také zákon o kybernetické bezpečnosti. Ten stanovuje přísnější požadavky na kybernetickou bezpečnost pro informační a komunikační systémy kritické informační infrastruktury, významné informační systémy a informační systémy základní služby.

Na základě zmocnění podle § 5a odst. 1 ZISVS je vypracována současná Informační koncepce ČR. Jedná se o základní strategický dokument eGovernmentu. Upravuje tři základní oblasti: rozvoj eGovernmentu, řízení ICT a rozvoj ISVS. V oblasti rozvoje informačních systémů veřejné správy stanovuje cíle a principy vytváření, pořizování, správy a provozování těchto informačních systémů. Povinným subjektům je uložena povinnost uvést do souladu s touto koncepcí své vlastní informační systémy a koncepce. Období koncepce je pětileté.

4.3 Právní úprava datových schránek

Zákon o elektronických úkonech a autorizované konverzi dokumentů (zákon o datových schránkách) býval svého času neformálně označován jako zákon o eGovernmentu¹²¹. Tento název se sice neujal, nicméně dokresluje význam institutů, které upravuje. Nejvýznamnější z nich jsou datové schránky, které byly zavedeny jako řešení nedostatků běžně dostupných forem elektronické komunikace. Mezi tyto nedostatky patřily: nedostatečná zabezpečení komunikace a nemožnost státu věrohodně ověřit odesílatele, příjemce ani stav a čas doručení.

Alternativní řešení těchto problémů sice již o několik let dříve nabídl tehdejší zákon o elektronickém podpisu, avšak takto upravený elektronický podpis se celoplošně neprosadil

¹²⁰ ŠEDIVÉC, pozn. 47, bod Asistovaná specializovaná kontaktní místa.

¹²¹ Zmínka například:

MINISTERSTVO VNITRA. Snižování regulatorní zátěže občanů a veřejné správy. In: *Mvcr.cz* [online]. 2017 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/clanek/snizovani-regulatorni-zateze-obcanu-a-verejne-spravy.aspx>.

a uskutečňování elektronického podání s jeho pomocí bylo v praxi značně problematické¹²². Oproti tomu datové schránky jsou všeobecně považovány za spolehlivý nástroj pro doručování. Datové schránky se zpravidla přirovnávají k doporučeným dopisům, neboť taktéž představují právem regulovaný způsob doručování, kdy je možné se s vysokou mírou jistoty spolehnout, že zpráva je v určitý časový okamžik odeslána a v určitý časový okamžik doručena.

Pro uchopení právní úpravy datové schránky je nezbytné vyrovnat se s několika základními pojmy. Legislativně je datová schránka definována jednoznačně 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*“¹²³.

Oproti tomu nejednoznačný byl zpočátku přístup soudů k pojmu datová zpráva. Potíž je v tom, že datová zpráva v širším slova smyslu označuje v podstatě obálku, elektronický nosič, přiložených elektronických dokumentů. Takto přiložené dokumenty, které obsahují samotný obsah v povoleném datovém formátu¹²⁴, některé tuzemské soudy považovaly za nepodepsané s tím, že podepsána je jen obálka. Proti této formalistické interpretaci se ohradil Nejvyšší soud ve významném stanovisku Plsn 1/2015, podle kterého v souladu se zákonem mají úkony obsažené v příloze datové zprávy stejné účinky jako každý jiný úkon učiněný písemně a podepsaný¹²⁵.

Obálka obsahuje kvalifikované časové razítko k prokázání času, kdy došlo k jednotlivým událostem jako například odeslání nebo doručení, a obsahuje informace o adresátovi a příjemci, díky čemuž je zajištěna jednoznačná identifikace komunikujících osob¹²⁶. S pomocí takového systému stát garantuje odesílání a doručování datových zpráv. S úkonem doručeným datovou zprávou zákon spojuje právní účinky podpisu¹²⁷. Což dohromady tvoří základ důvěryhodného elektronického způsobu komunikace s orgány veřejné správy.

¹²² MATES, pozn. 4, s. 163.

¹²³ §2 odst. 1. zákona o datových schránkách.

¹²⁴ Povolné formáty stanovuje:

Příloha č. 1 vyhlášky č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

¹²⁵ Stanovisko Nejvyššího soudu ze dne 05.01.2017, sp. zn. Plsn 1/2015.

§ 18 odst. 2 zák. č. 300/2008 Sb.

¹²⁶ Usnesení Krajského soudu v Brně ze dne 12. 6. 2012, č. j. 47 Co 71/2010-249.

¹²⁷ § 18 odst. 1 a 2 zákona o datových schránkách.

Velkým tlakem na prosazování principu preference digitalizace v rámci komunikace orgánů veřejné správy a občanů je postupné rozšiřování povinností datovou schránku mít a využívat ji. Ze zákona je datová schránka zřízena automaticky pro orgány veřejné moci, právnické osoby vedené v obchodním rejstříku a některé podnikající fyzické osoby. Ostatní osoby včetně fyzických si ji dle aktuálně účinného znění zákona mohou zřídit pouze na vlastní žádost.

V některých případech je komunikace s pomocí datové schránky povinná a v jiných případech zůstává nadále dobrovolná. Povinná je zásadně v případě komunikace mezi orgány veřejné moci navzájem (G2G) a v případě orgánu veřejné moci vůči osobě, která má zřízenou a zpřístupněnou svou datovou schránku. Tato povinnost orgánů veřejné moci se v oblasti doručování uplatní bez ohledu na zvláštní procesní ustanovení v jiných zákonech upravující doručování¹²⁸. Zvláštní právní předpisy si však mohou stanovit vlastní pořadí doručování. Datové zprávy mají mezi ostatními přípustnými způsoby doručování v procesních předpisech zpravidla prioritní postavení.

Dobrovolná je komunikace prostřednictvím datových schránek v ostatních případech, kdy zákon nestanoví jinak, přičemž zpráva je adresována buď orgánu veřejné moci nebo ostatním osobám¹²⁹. Osoby, které mají zřízenou datovou schránku, mohou jejím prostřednictvím provádět úkony vůči orgánům veřejné moci umožňuje-li to povaha takového úkonu.

Podání vůči orgánu veřejné moci prostřednictvím datové schránky je učiněno okamžikem dodání datové zprávy do schránky orgánu veřejné moci¹³⁰. Zásadní je, že takovému podání jsou přiznány stejné účinky, jako kdyby byl učiněn písemně a podepsaný.

4.3.1 Změna u datových schránek pro fyzické osoby

Novela zákona o datových schránkách přináší automatické zřizování datových schránek i pro některé fyzické osoby¹³¹. Dosud si fyzické osoby mohly zřídit datovou schránku pouze dobrovolně na žádost. Tato kontroverzní změna zatím nevstoupila v účinnost. Podle odhadu České pošty bude v jejím důsledku zřízena datová schránka zhruba milionu fyzických osob¹³². K automatickému zřízení datové schránky bude stačit, aby se fyzická osoba jednou

¹²⁸ § 17 odst. 1 zákona o datových schránkách.

¹²⁹ § 18 a 18a zákona o datových schránkách.

¹³⁰ Usnesení Nejvyššího správního soudu ze dne 15. 7. 2010, č. j. 9 Afs 28/2010-79.

¹³¹ Čl. CXLII zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (DEPO zákon).

¹³² BAREŠOVÁ, Andrea. Miliarda! [prezentace]. In: *ISSS 2022* [online]. 2022 [cit. 20.6.2022]. Dostupné z: https://issz.cz/archiv/2022/download/prezentace/ceska-posta_baresova.pdf.

autentizovala s využitím prostředku elektronické identifikace. Zřízená datová schránky tak bude navíc od počátku zpřístupněna. O zneprístupnění může fyzická osoba po jejím zpřístupnění požádat¹³³.

Během projednávání v Senátu se tato změna setkala s kritikou. Zaznělo i varování ohledně povinností vyplývajících z takovéhoho zřízení datových schránek¹³⁴. Důsledkem takto zřízených datových schránek je totiž například povinnost podávat daňová přiznání podle § 72 odst. 6 daňového řádu. Ta musí podat elektronicky všechny osoby se zřízenou a zpřístupněnou datovou schránkou ze zákona. Podle názoru Jiřího Peterky se nejedná o zřízení datové schránky ani na žádost ani ze zákona, nýbrž o zřízení *sui generis*¹³⁵. Pokud bych přisvědčil jeho názoru, měla by se na takto zřízené datové schránky vztahovat jen obecná úprava datových schránek a nikoliv povinnosti, které jsou stanoveny pro držitele datových schránek ze zákona. Já však s Peterkovým názorem nesouzním a to s následujícími argumenty.

O datovou schránku na žádost se skutečně nejedná, protože jejímu zřízení nepředchází podání žádosti, jejímž důsledkem by byl postup Ministerstva vnitra podle části čtvrté správního řádu¹³⁶.

Avšak odlišností od ostatních datových schránek jako možnost fyzické osoby zneprístupnit datovou schránku a povinnost upozornit fyzickou osobu na skutečnost, že po prvním použití elektronického prostředku identifikace jí bude zřízena datová schránka¹³⁷, nejsou relevantní pro samotné zřízení datové schránky. Zákonná konstrukce, kdy *ex lege* vzniká Ministerstvu vnitra povinnost při určité právní skutečnosti bezodkladně zřídit datovou schránku určité osobě, je stejná i u osob, které datovou schránku mají nebo budou mít podle nové právní úpravy zřízeny ze zákona, tedy bez ohledu na to, zda je právní skutečností první použití prostředku elektronické identity, zápis právnické osoby v registru osob, nebo zapsání do evidence či rejstříku v případě fyzických podnikajících osob. Výklad, že nejde o datové schránky ze zákona by byl v rozporu s textem zákona.

¹³³ § 11 odst. 5 zákona od datových schránek ve znění účinném od 1. ledna 2023.

¹³⁴ GOLÁŇ Tomáš. In: SENÁT. Stenozáznam z 2. dne 10. schůze [online]. 2021 [cit. 20.6.2022]. Dostupné z: <https://senat.cz/xqw/webdav/pssenat/original/99360/83399/91229>.

¹³⁵ PETERKA, Jiří. Zprávy z Depa (2): Automatické zřízení datové schránky pro informačně gramotné. In: *Lupa.cz* [online]. Internet Info, 2021 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://www.lupa.cz/clanky/zpravy-z-depa-2-automaticke-zrizeni-datove-schranky-pro-informacne-gramotne/>.

¹³⁶ Obranou proti nevyhovění žádosti je správní zásahová žaloba.

Rozsudek Nejvyššího správního soudu ze dne 17. 10. 2013, č. j. 6 Ans 1/2013-66.

¹³⁷ § 15 odst. 3 písm. a) zákona od datových schránek ve znění účinném od 1. ledna 2023.

Důsledkem přijaté změny tak bude nerovnost v povinnostech fyzických osob, které si zřídily, nebo si zřídí datovou schránku dobrovolně a těch, kterým bude zřízena ze zákona při prvním využití jednoho z prostředků elektronické identity.

Senát, vědom si těchto možných dopadů, prosadil posunutí počátku účinnosti na 1. ledna 2023. Ani půl roku před počátkem účinnosti však nebyl Poslanecké sněmovně předložen návrh úpravy této změny ani návrh jejího dalšího odložení. Lze proto očekávat, že tato kontroverzní změna začátkem příštího roku nabude účinnosti. V jejím důsledku pak strmě naroste počet fyzických osob, které budou držiteli datových schránek.

4.4 Právní úprava elektronické identifikace

V některých případech veřejná správa poskytuje své služby neadresovaným způsobem. Takové služby mohou spočívat například ve zpřístupnění informací široké veřejnosti prostřednictvím internetových stránek. V tomto případě ale není zřetelné, že by taková činnost orgánů veřejné správy měla vrchnostenskou povahu nebo, že by zasahovala do konkrétních práv a povinností a vyvolávala konkrétní právní následky. V důsledku toho chybí objektivní potřeba ztotožnit osoby, které si takovou informaci zobrazí. V jiných případech je ale nezbytné, aby byla určitá služba poskytnuta adresně a veřejná správa ztotožnila každou osobu, pokud činí úkon nebo je jí poskytována nějaká služba. Důvodem proč veřejná správa vyžaduje ověření totožnosti, je zejména potřeba s dostatečnou mírou jistoty určit, které konkrétní osoby se týkají právní následky.

V rámci nedigitalní veřejné správy dochází k fyzickému ztotožnění osoby zpravidla pomocí předložení identifikačních dokladů, za které se obvykle považuje občanský průkaz nebo cestovní pas. Takový fyzický doklad (identifikační prostředek), obsahuje jedinečný souhrn informací o určité fyzické osobě, s jehož pomocí je možné určit totožnost dané osoby s dostatečnou mírou jistoty. Zajistit ztotožnění osoby je nezbytné i v případech, kdy jsou veřejné služby poskytovány nebo úkony činěny digitálně. Na první pohled viditelný rozdíl mezi tradiční fyzickou identifikací a identifikací elektronickou spočívá v tom, že identifikační prostředek nemusí být svázán s hmotnou kartičkou, ale může být uchovávan v nehmotné podobě. Navíc ale však musí být zajištěn proces, který umožňuje ověřit elektronickou identitu určité osoby jinak než pohledem na hmotnou kartičku.

Pro správné pochopení, jak elektronickou identifikaci chápe právní řád, je nutné rozlišovat mezi třemi pojmy informační bezpečnosti: identifikace, autentizace a autorizace. Identifikace označuje určení konkrétní fyzické osoby. Je to schopnost odlišit jednotlivou osobu od masy ostatních osob. Autentizace představuje ověření, že jde skutečně o tu osobu, za kterou

se fyzická osoba vydává. Při autorizaci se ověřuje, jestli autentizovaná osoba je oprávněna přistupovat k nějaké službě¹³⁸.

Jádro regulace elektronické identifikace obsahuje nařízení eIDAS, podle kterého se za elektronickou identifikaci považuje „*postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu*“¹³⁹. Na základě porovnání s výše uvedenými pojmy informační bezpečnosti je zřejmé, že nařízení reguluje oblast identifikace a autentizace osob. Naopak oblast autorizace, což je krok, který zpravidla následuje po autentizaci, není v rámci úpravy elektronické identifikace řešena. Prakticky orgán veřejné správy zjistí s pomocí elektronické identifikace, která konkrétní osoba úkon činí. A následně sám ověří, jestli je tato osoba skutečně oprávněna takový úkon učinit. Orgán veřejné správy si musí sám zodpovědět otázku, zda je autentizovaná osoba oprávněná například žádat o vdovský důchod.

4.4.1 Prostředky pro elektronickou identifikaci

Hmotný nebo nehmotný nástroj, který slouží k elektronické identifikaci osoby, se podle nařízení eIDAS nazývá prostředkem pro elektronickou identifikaci. Teoreticky jím může být cokoli, co obsahuje identifikační údaje o konkrétní osobě. Typickými příklady je kombinace přihlašovacího jména a hesla, elektronická vrstva občanského průkazu obsahující biometrické údaje nebo USB token. Podstatné je, že právní úprava v nařízení eIDAS dopadá z množiny všech používaných prostředků elektronické identifikace výhradně na ty prostředky, které jsou součástí kvalifikovaných systémů elektronické identifikace. Tyto kvalifikované systémy představují fundament, na základě kterého se prostředky elektronické identifikace v souladu s pravidly jednotlivých členských států EU vydávají a jsou spravovány. Následně členský stát může takový kvalifikovaný systém oznámit Evropské komisi, která ověří naplnění podmínek způsobilosti podle nařízení a prováděcího rozhodnutí Evropské komise¹⁴⁰. V případě, že kvalifikovaný systém těmto podmínkám vyhovuje a kladně se vyjádří i ostatní státy

¹³⁸ MICROSOFT. Authentication vs. authorization. In: *Microsoft technical documentation* [online]. Microsoft: 2022. Poslední změna: 6.2.2022 [cit. 20.6.2022]. Dostupné z: <https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-vs-authorization>.

¹³⁹ Čl. 3 odst. 1 nařízení eIDAS

¹⁴⁰ Zejména prováděcí nařízení Komise (EU) 2015/806 ze dne 22. května 2015, kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru, CELEX: 32015R0806.

Evropské unie, uvede jej Komise na seznam notifikovaných systémů elektronické identifikace, který je publikován v Úředním věstníku Evropské unie¹⁴¹.

Význam zápisu kvalifikovaného systému do tohoto seznamu spočívá v tom, že po uplynutí jednoho roku od zápisu, jsou ostatní členské státy povinny uznávat oznámené elektronické identifikační prostředky. Za ČR je na tomto seznamu veden Vnitrostátní systém identifikace ČR, jehož jediným identifikačním prostředkem je Český elektronický průkaz totožnosti (eObčanka). Pokud se tedy chce občan ČR přihlásit například do slovenského Ústředního portálu veřejné správy¹⁴², tak je eObčanka v tuto chvíli jediným českým elektronickým prostředkem identifikace, který slovenský portál pro přihlášení akceptuje. V září roku 2021 ČR ohlásila Evropské komisi záměr oznámit další systém elektronické identifikace. Ten by měl zahrnovat dva existující identifikační prostředky Mobilní klíč eGovernmentu a MojeID.

Výše uvedené tři prostředky elektronické identifikace, které stát notifikoval nebo bude notifikovat, nejsou jediné, které může český občan využít pro přihlášení se k digitálním službám veřejné správy. Mezi další prostředky patří: NIA ID, bankovní identita nebo čipová karta společnosti První certifikační autorita. Protože se nejedná o oznámené kvalifikované systémy, je v současné době možné tyto prostředky využít pouze pro přístup k tuzemským službám, neboť ostatní členské státy nejsou povinny je s pomocí mezinárodní brány přijímat. Poslední dostupnou možností pro elektronickou identifikaci k tuzemským digitálním službám je právě mezinárodní brána umožňující akceptovat notifikované prostředky identifikace ostatních členských států EU.

Kvalifikovaní správci systémů elektronické identifikace zajišťují fungování jednotlivých systémů a poskytují jednotlivé prostředky elektronické identifikace. NIA ID, eObčanka a mobilní klíč eGovernmentu zajišťuje stát. Ostatní prostředky poskytují soukromé subjekty.

Prostředky elektronické identifikace se dělí na prostředky s nízkou, značnou, nebo vysokou úrovní záruky. Nízká úroveň záruky má jen omezenou spolehlivost ověření totožnosti určité osoby, kdy vydání prostředku zpravidla nepředchází fyzického ověření osoby. Naopak

¹⁴¹ EVROPSKÁ KOMISE. *Systémy elektronické identifikace oznámené podle čl. 9 odst. 1 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu ze dne 27. dubna 2014* [online]. 2014 [cit. 20.6.2022]. CELEX:52022XC0218(06). Dostupné z: [https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52022XC0218\(06\)](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52022XC0218(06)).

Interaktivní seznam notifikovaných prostředků je dostupný z: <https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Czech+Republic>.

¹⁴² Dostupné z: <https://slovensko.sk/>.

je tomu u značné záruky, kde je standardem úvodní fyzické ověření společně s následným několika faktorovým ověřováním například pomocí přihlašovacích údajů a SMS nebo otisku prstu. Vysokou úroveň záruky poskytují zvláštní státem zaručená řešení, například eObčanka, k jejíž funkci je potřeba speciální hardwarové vybavení nebo MojeID, které vyžaduje speciálně zabezpečený token¹⁴³.

Společně jsou všechny jmenované prostředky elektronické identifikace evidovány v informačním systému Národního bodu pro identifikaci a autentizaci (Národní bod, NIA). Národní bod zprostředkovává elektronickou identifikaci mezi kvalifikovanými správci (anglicky identity providers) a kvalifikovanými poskytovateli služeb (anglicky service providers)¹⁴⁴. Přístupovat k Národnímu bodu mohou pouze orgány vykonávající veřejnou moc.

Ustanovení § 2 zákona o elektronické identifikaci stanovuje obecnou povinnost umožnit prokázání totožnosti výhradně prostřednictvím kvalifikovaného systému elektronické identifikace, pokud vyžaduje prokázání totožnosti právní předpis nebo výkon působnosti. Vzhledem k tomu, že zákon blíže neohraničuje výkon působnosti, na který se toto ustanovení vztahuje, je nezbytné jej vztáhnout na výkon působnosti celé výkonné moci¹⁴⁵. Příkladem právního předpisu, který vyžaduje prokázání totožnosti mimo výkon veřejné moci je AML zákon¹⁴⁶.

Konkrétní orgán veřejné správy nebo jakýkoliv jiný subjekt práva, který má povinnost umožnit prokázání totožnosti tímto způsobem, je označen zákonem za kvalifikovaného poskytovatel služeb. Zákon takovému poskytovateli služeb ukládá povinnost vyrozumět správce Národního bodu, kterým je Správa základních registrů¹⁴⁷. Po vyrozumění je poskytovatel služeb zařazen na seznam, který publikuje správce na webu¹⁴⁸.

¹⁴³ KORBEL, František, KOVÁŘ, Dalibor, POTOČNÁK, Štefan, AMLER, Pavel. Elektronická identita při elektronickém (hmotně)právním jednání. In: *Právní rozhledy* [online]. 2019, 18 [cit. 20.6.2022]. ISSN: 1805-2797. Dostupné z: <https://beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhfxa4s7ge4f6427gyzdm>.

¹⁴⁴ § 20 zákona č. 250/2017 Sb. o elektronické identifikaci.

¹⁴⁵ Korb. pozn. 143, poznámka pod čarou č. 32.

¹⁴⁶ § 7 zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

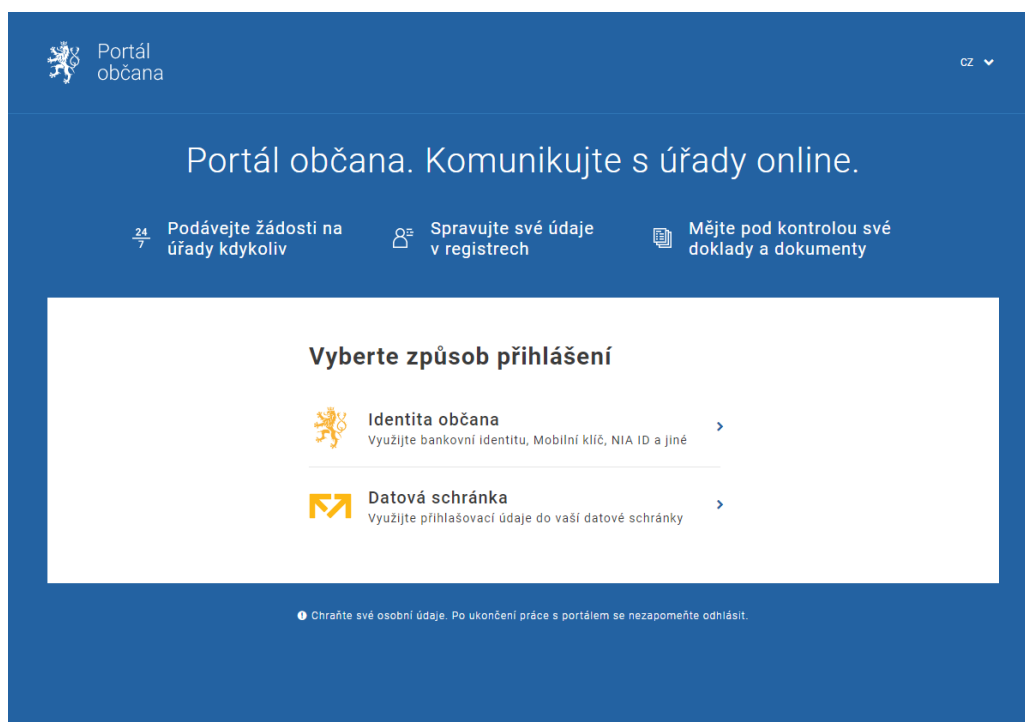
¹⁴⁷ § 18 zákona o elektronické identifikaci.

¹⁴⁸ Dostupné z: <https://info.identitaobcana.cz/sep/>.

4.4.2 Přihlašování se k portálům veřejné správy

Pro samotnou elektronickou identifikaci pomocí Národního bodu se používá uživatelsky přívětivější název Identita občana. Identitu občana využívají, jak univerzální tak i specializovaná samoobslužná kontaktní místa veřejné správy.

Nyní se zaměřím na rozdílnou praxi jednotlivých portálů orgánů veřejné správy. Některé z portálů akceptují přístup výhradně prostřednictvím Národního bodu. Příkladem takového přístupu je portál Registru živnostenského podnikání¹⁴⁹. Naproti tomu pro přihlášení k Portálu občana, ePortálu ČSSZ nebo Portálu MPSV lze kromě Národního bodu využít i přihlášení zprostředkované pomocí informačního systému datových schránek. Tento způsob zahrnuje pět různých metod přihlášení. Specifickými jsou možnosti přihlášení s pomocí SMS nebo pomocí speciálního přihlašovacího certifikátu. Dostupná je i možnost přihlásit se prostřednictvím Identity občana, které je tak k dispozici duplicitně.



Obrázek č. 2: Přihlašovací stránka Portálu občana¹⁵⁰.

U některých jiných veřejně přístupných portálů veřejné správy jsou možnosti přihlašování ještě různorodější. Například Centrální registr životního prostředí nebo Online

¹⁴⁹ Dostupné z: <https://rzp.cz/epo/cs/>.

¹⁵⁰ MINISTERSTVO VNITRA. *Portál občana: Přihlášení* [online]. 2022, verze 1.7.7 [zjednodušeno]. [cit. 20.6.2022]. Dostupné z: <https://obcan.portal.gov.cz/prihlaseni>.

finanční úřad, který je součástí daňového portálu, umožňují i přihlašování pomocí svých vlastních elektronických prostředků identifikace, které tyto orgány samy vydávají. V případě posledně zmíněného Online finančního úřadu je specifické, že možnosti přihlašování jsou taxativně vyjmenovány přímo v daňovém řádu¹⁵¹. Konkrétně se jedná o přístup se zaručenou identitou, identitu ověřenou způsobem, kterým se lze přihlásit do datové schránky, a přístup prostřednictvím přístupových údajů přidělených na žádost. Tento explicitní legislativní přístup je výjimečný.

Využívání přihlašování pomocí informačního systému datových schránek a jiných elektronických prostředků identifikace, které nejsou součástí Národního bodu, je upraveno mimo zákon o elektronické identifikaci a nařízení eIDAS. Z pohledu informačních systémů veřejné správy lze tento způsob přihlašování označit za přístup se zaručenou identitou, kterým se podle § 2 písm. u) ZISVS rozumí: „*přístup do informačního systému veřejné správy nebo elektronické aplikace s využitím prostředku pro elektronickou identifikaci, při jehož vydání nebo v souvislosti s ním anebo v souvislosti s umožněním jeho využití byla totožnost osoby ověřena (...) orgánem (...) veřejné moci (...) nebo který byl vydán v rámci kvalifikovaného systému elektronické identifikace*“¹⁵².

Toto ustanovení bylo do ZISVS začleněno v roce 2017 v rámci novely zákona o občanských průkazech, která již reflektovala přijetí nařízení eIDAS. Důvodová zpráva k této novele uvádí, že toto ustanovení by mělo „*sehrát roli určité obecné platformy pro problematiku tohoto druhu přístupu a odlehčit zvláštní právní předpisy od zbytných, ryze technicistních ustanovení o jednotlivých typech prostředků pro elektronickou identifikaci*“¹⁵³.

Význam tohoto ustanovení spočívá v tom, že osoba přistupující s takto zaručenou identitou je oprávněna vstoupit do informačního systému veřejné správy a získat z něj výpisy a jiné výstupy podle § 9 ZISVS¹⁵⁴. Tomuto oprávnění odpovídá povinnost orgánů veřejné moci zaručenou identitu vyžadovat. Z toho vyplývá, že ZISVS připouští ve vztahu k informačním systémům veřejné správy, jak přístup pomocí kvalifikovaných prostředků obsažených v Národním bodu, tak i pomocí jiných nekvalifikovaných prostředků, které splňují požadavek na ověření totožnosti držitele tohoto prostředku orgánem veřejné moci.

¹⁵¹ § 69a daňového řádu.

¹⁵² § 2 písm. u) ZISVS.

¹⁵³ VLÁDA ČR. Sněmovní tisk 928/0: Návrh zákona, kterým se mění zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a další související zákony včetně důvodové zprávy. In: *Psp.cz* [online] 2016, s. 23 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/orig2.sqw?idd=116235>.

¹⁵⁴ § 9 odst. 4 a 5 ZISVS.

Nicméně takovéto pojetí není v souladu s výše zmíněnou povinností obsaženou v § 2 zákona o elektronické identifikaci, která vyžaduje výhradně přístup pomocí kvalifikovaných prostředků obsažených v Národním bodu a vylučuje používání ostatních nekvalifikovaných prostředků. Vzhledem k tomu, že obě úpravy dopadají na překrývající se oblast činnosti veřejné správy, je nutné určit, která norma se uplatní přednostně pomocí interpretačních pravidel. Obě normy mají právní sílu zákona, přičemž je bez významu, že jedna z norem adaptuje evropské nařízení, neboť tato norma není zároveň zakotvena v tomto nařízení, ale je ryze tuzemská. Nelze tak aplikovat pravidlo *lex superior derogat legi inferiori*.

Směr mé úvahy bude proto směřovat na určení, která norma je podle míry abstraktnosti formulace hypotézy speciální a která obecná. Ustanovení § 2 zákona o elektronické identifikaci dopadá na všechny situace, kdy právní předpis nebo výkon působnosti vyžaduje prokázání totožnosti pomocí elektronické identifikace. Toto pravidlo je zjevně konstituováno jako obecné. S tímto tvrzením souhlasí i důvodová zpráva¹⁵⁵. Je proto přípustné, aby toto pravidlo bylo modifikováno nebo i zcela nahrazeno speciální normou.

Oproti tomu vymezení přístupu se zaručenou identitou v ZISVS je omezeno pouze na oblast ISVS včetně portálů a dalších elektronických aplikací, které jsou jejich součástí. Přístup se zaručenou identitou tedy představuje výchozí a obecné využití elektronické identifikací ale pouze ve vztahu k informačním systémům. Z toho vyplývá, že ustanovení ZISVS, která spojují s přístupem se zaručenou identitou povinnost veřejné moci vyžadovat určitou množinu prostředků elektronické identifikace, jsou speciální vůči ustanovení § 2 zákona o elektronické identifikaci. Uplatní se proto interpretační pravidlo *lex specialis derogat legi generali*.

Z toho usuzuji, že prostřednictvím přístupu se zaručenou identitou je možné se přihlašovat napříč celou veřejnou správou i s pomocí nekvalifikovaných prostředků elektronické komunikace, které splňují požadavky ZISVS. Taková autentifikace umožní především získávat z informačních systémů veřejné správy výpisy a jiné výstupy podle § 9 ZISVS. S takovým výkladem se lze setkat na portálech, kde je dostupné zároveň přihlášení pomocí Národního bodu i informačního systému datových schránek jako například zmíněný Portál občana nebo ePortál ČSSZ. Jiného názoru jsou však autoři komentáře k zákonu

¹⁵⁵ VLÁDA ČR. Sněmovní tisk 1069/0: Návrh zákona o elektronické identifikaci včetně důvodové zprávy. In: *Psp.cz* [online]. 2008 s. 27 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=7&ct=1069>.

o poskytování digitálních služeb¹⁵⁶. Podle nich přihlašování s pomocí takovýchto nekvalifikovaných prostředků není obecně možné, neboť mu chybí právní základ. Proti tomuto závěru však stojí má výše uvedená argumentace.

Pojetí přístupu se zaručenou identitou není možné vykládat tak, že by se uživatelé mohli domoci přístupu pomocí nekvalifikovaného prostředku namísto kvalifikovaného, pokud takovou možnost informační systém veřejné správy nenabízí. V ZISVS je stanoveno totiž pouze oprávnění správce informačního systému vyžadovat přihlášení k určitým činnostem s pomocí některého identifikačního prostředku podřízeného pod přístup se zaručenou identitou. Pokud zákonodárce chtěl na zákonné úrovni skutečně prosadit kvalifikované prostředky sdružené v Národním bodu jako jediný způsob přihlašování se do portálů veřejné správy, měl by přeformulovat definici přístupu se zaručenou identitou v ZISVS.

Nevhodně zpracovaný je podle mého názoru i dříve zmíněný taxativní výčet v daňovém řádu, který vedle sebe staví přihlášení s využitím přístupu se zaručenou identitou a přihlášení prostřednictvím datové schránky, neboť přihlášení s pomocí datové je obsaženo již v přístupu se zaručenou identitou. Ze stejného důvodu nesouhlasím s interpretací komentáře k daňovému řádu, který přístupem se zaručenou identitou rozumí pouze kvalifikované systémy Národního bodu a přehlíží tím, že tento pojem nevychází ze zákona o elektronické identifikaci, ale ze ZISVS.

V této souvislosti je významné z hlediska schopnosti vyvolat další právní důsledky ustanovení § 8 ZISVS. Toto ustanovení spojuje fikci podpisu s úkonem, „*jehož náležitostí má být podpis toho, kdo jej činí, prostřednictvím informačního systému veřejné správy (...)*“¹⁵⁷. Aby se mohla fikce uplatnit, musí informační systém umožnit: prokázání totožnosti toho, kdo úkon činí, s využitím elektronické identifikace; autorizaci úkonu tím, kdo úkon činí; zpětné prokázání projevu vůle toho, kdo úkon činí. V tomto případě zákonodárce použil pojmu elektronické identifikace namísto přístupu se zaručenou identitou. Z toho usuzuji, že aby měl úkon učiněný prostřednictvím informačního systému veřejné správy účinky podpisu, je nezbytné osobu, která úkon činí, autentizovat pomocí Národního bodu. Zákon tedy nepřipouští možnost obecně činit podepsané úkony jen s pomocí přístupu se zaručenou identitou.

¹⁵⁶ KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel. § 12 Právo na elektronickou identifikaci a autentizaci. In: ZAJÍČEK, Zdeněk, KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel, DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. *Zákon o právu na digitální služby: komentář*. Praha: C.H. Beck, 2021, s. 136, marg. č. 26. ISBN: 978-80-7400-822-1.

¹⁵⁷ § 8 ZISVS.

Na příkladu přihlašování se k portálům veřejné správy jsem upozornil na rozdílnou praxi v oblasti elektronického ztotožňování osob. Na zákonné úrovni jsou stanoveny různé požadavky na autentifikaci uživatelů. Rozdílná terminologie adaptačního zákona nařízení eIDAS a ZISVS převážně tuzemského původu dopadá na podobnou množinu činností veřejné správy. Vykládat terminologii a související povinnosti v rámci zákonů eGovernmentu je zapotřebí systematicky a ve vzájemných souvislostech. Nehledě na to, lze v tomto případě říct, že tato právní úprava je příliš komplikovaná, což ztěžuje určení, které povinnosti má který orgán veřejné moci dodržovat.

Národní bod v současné době umožňuje využít stejné identifikační prostředky na značném množství portálů veřejné správy. Navíc i samotné identifikační prostředky se s rozšířením o bankovní identitu staly všeobecně dostupnější. Tuto kombinaci považuji za největší přínos probrané právní úpravy. Některé nedostatky nařízení eIDAS jako je například nízký počet vzájemně uznávaných prostředků musí vyřešit EU.

4.4.3 Budoucí vývoj elektronické identity

Při hodnocení nařízení eIDAS¹⁵⁸, které bylo vypracováno po pěti letech od vstupu nařízení v platnost, bylo konstatováno nenaplnění původního cíle vytvořit celoevropsky rozšířené interoperabilní řešení elektronické identity. Rozšíření zabránil nízký počet oznámených systémů elektronické identifikace, který je na úrovni EU vzájemně uznáván. Spolu s rozšířením zaostává i míra využívání oznámených systémů. Hodnocení v neposlední řadě kritizuje příliš úzké zaměření na oblast poskytování veřejných služeb a zároveň, že úprava neumožňuje nahrazení stávajících papírových identifikačních dokumentů občanů EU.

Aktuálně je na začátku unijního legislativního procesu návrh novelizace nařízení eIDAS, který má mimo jiné zřídit rámec pro evropskou digitální identitu¹⁵⁹. Návrh zapracoval zjištění výše uvedeného hodnocení, a kromě několika zásadních změn, zavádí nový právní institut, kterým by měla být evropská peněženka digitální identity. Tento právní institut bude součástí kvalifikovaného systému elektronické identifikace vydaného s vysokou úrovní záruky.

¹⁵⁸ EVROPSKÁ KOMISE. *Zpráva Komise Evropskému parlamentu a Radě o hodnocení nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS) ze dne 3. června 2021* [online]. 2021 [cit. 20.6.2022]. CELEX: 52021DC0290. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021DC0290>.

¹⁵⁹ EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu ze dne 3. 6. 2021* [online]. 2021 [cit. 20.6.2022]. CELEX: 52021PC0281. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52021PC0281>.

Sloužit bude k autentizaci pro poskytování veřejných i soukromých služeb pomocí osobních identifikačních údajů a dalších informací. Také by mělo být umožněno uvedenou peněženkou podepisovat dokumenty kvalifikovaným elektronickým podpisem.

Návrh evropské peněženky digitální identity představuje značnou decentralizaci osobních identifikačních údajů. Předpokládá se, že identifikační údaje a související atributy by měly být uloženy v mobilní aplikaci¹⁶⁰. Takový přístup k autentizaci je značně odlišný od toho, jak funguje v současné době Národní bod. Ten totiž ověřuje totožnost uživatele podle centrálně evidovaných údajů v základním registru. V tomto považuji navrhanou úpravu za přelomovou. V případě přijetí tohoto návrhu, bude třeba řešit, zda je Národní bod nadále udržitelný v takto centralizované podobě.

Za žádoucí považuji, že každý členský stát bude povinen evropskou peněženkou digitální identity vydat a alespoň jeden kvalifikovaný elektronický prostředek ohlásit. Protože současný princip dobrovolnosti při oznamování kvalifikovaných systémů elektronické identifikace k dostatečnému rozšíření nevedl. Návrh současně ponechává obrysy stávajícího řízení, ve kterém jednotlivé členské státy oznamují Komisi kvalifikované systémy elektronické identifikace. Nejde tedy o zcela přelomový návrh ve všech ohledech, a proto lze očekávat, že částečná kontinuita se stávající právní úpravou bude zachována.

Právní regulace elektronické identity, která překoná mezinárodní i vnitrostátní roztržitost různých způsobů identifikace a autorizace, je živým tématem nejen v orgánech Evropské unie, ale i například v Komisi OSN pro mezinárodní obchodní právo (UNCITRAL), která již několik desítek let zdokonaluje svůj univerzální modelový zákon o elektronické identitě a prostředcích¹⁶¹. Ten však na rozdíl od stávající evropské právní úpravy předpokládá působnost pouze v oblasti poskytování služeb soukromého sektoru.

Celkově lze předpokládat, že budoucí vývoj právní úpravy bude i u nás směřovat k právní regulaci umožňující skutečně široké rozšíření elektronické identifikace mezi obyvateli a vzájemnou interoperabilitu mezi různými státem regulovanými prostředky elektronické identifikace. Očekávám také větší zapojení soukromého sektoru především na straně

¹⁶⁰ MÜHLFEIT, František. Místo plastové kartičky datový záznam. EU chystá jednotnou peněženkou digitálních identit. In: *E15.cz* [online]. CNC, 2021 [cit. 20.6.2022]. Dostupné z: <https://e15.cz/domaci/misto-plastove-karticky-datovy-zaznam-eu-chysta-jednotnou-penezenku-digitalnich-identit-1385271>.

¹⁶¹ UNCITRAL. *Draft Model Law on the Use and Cross border Recognition of Identity Management and Trust Services: advance copy* [online]. UN, 2022 [cit. 20.6.2022]. Dostupné z: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/acn9-1112-e.pdf>.

poskytovatelů služeb, protože i ti mohou využít výhod důvěryhodného elektronického ověření totožnosti osob.

4.5 Právní úprava elektronických podpisů a dalších elektronických institutů

Stephen Medson, zahraniční autor věnující se problematice elektronických podpisů, rozlišuje dva pojmy: digitální a elektronický podpis¹⁶². Pojmem digitální podpis označuje technologický prostředek prokázání pravosti a zachování integrity dat. Využívá zásadně kombinaci asymetrické kryptografie a kontrolního součtu podepsaných dat. Umožňuje, aby uživatel se soukromým klíčem data podepsal a jiný uživatel s veřejným klíčem pravost a integritu podepsaných dat ověřil.

Elektronický podpis je na rozdíl od digitálního podpisu podle Medsona právní institut, zahrnující vše, čím podepisující osoba v elektronické podobě projevuje svou vůli způsobit právní následky. Teoreticky je tedy elektronický podpis pojímán velmi široce. Z jedné strany lze pod něj podřadit sofistikované digitální podpisy nabízející nejvyšší záruky a z druhé strany i pouhé uvedení vlastního jména na konci emailu. Další formy mohou spočívat ve vyplnění jména v elektronickém formuláři, připojení obrázku znázorňující vlastnoruční podpis nebo biodynamický podpis zachycený na speciální podložce a převedený do elektronické podoby¹⁶³. V zásadě je jen na zákonodárci, které formě přizná právní účinky.

Elektronický podpis plní mnohem více funkcí než elektronická identifikace. V závislosti na zvolené formě a míře záruky, kterou poskytuje, umožňuje ověřit pravost podpisu nebo celého podepsaného dokumentu, identifikovat podepisujícího, předcházet pozdější modifikaci dokumentu a v případě sporu může být použit i jako důkazní prostředek¹⁶⁴.

4.5.1 Různé podoby elektronického podpisu a dalších elektronických institutů

Evropská právní úprava elektronických podpisů, která předcházela nařízení eIDAS, byla kritizována, protože v praxi neumožnila vytvořit jednotný evropský prostor vzájemně kompatibilních elektronických podpisů. Podmínky byly stanoveny směrnicí pouze jako minimální požadavky, a proto existovaly značné rozdíly mezi jednotlivými národními

¹⁶² MASON, Stephen. *Electronic Signatures in Law* [online]. 4th edition. Institute of Advanced Legal Studies, 2016, s. 199-200 [cit. 20.6.2022]. ISBN: 978-1-911507-01-7. Dostupné z: <https://humanities-digital-library.org/index.php/hdl/catalog/view/electronic-signatures/1/86-1>.

¹⁶³ Podrobněji KMENT, Vojtěch. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? [online]. In: bulletin-advokacie.cz. 2016 [cit. 20.6.2022]. ISSN: 1805-8280. Dostupné z: <http://www.bulletin-advokacie.cz/nahradi-elektronicky-podpis-prosty-ten-tradicni-vlastnorucni>.

¹⁶⁴ Tamtéž.

úpravami, což znemožňovalo efektivní přeshraniční využívání elektronických podpisů¹⁶⁵. Udržování stávajících překážek a vytváření nových překážek v oblasti elektronické komunikace bylo v rozporu s myšlenkami vnitřního trhu Evropské unie. Proto byla potřeba v souladu s § 114 odst. 1 Smlouvy o fungování Evropské unie právní úpravu jednotlivých členských států harmonizovat přímo prostřednictvím závazného nařízení.

Nařízení eIDAS upravuje zejména „*právní rámec pro elektronické podpisy, elektronické pečeti, elektronická časová razítka (a) elektronické dokumenty (...)*“¹⁶⁶. V souvislosti s těmito elektronickými instituty reguluje služby vytvářející důvěru. Takovou službou se rozumí zpravidla úplatná elektronická služba prostřednictvím, které se vytvářejí nebo uchovávají výše uvedené elektronické instituty nebo se ověřuje jejich shoda či platnost.

V nařízení je definován prostý elektronický podpis jako: „*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*“. Jedná se o velmi širokou definici. V zásadě je to zbytková kategorie, do které spadá vše, co nespĺňuje požadavky zaručeného nebo kvalifikovaného podpisu. Nařízení stanovuje, že prostému elektronickému podpisu musí být přiznány právní účinky, i když nespĺňuje předpoklady kvalifikovaného elektronického podpisu¹⁶⁷, což je naprosto klíčové ustanovení na základě, kterého se lze domoci účinků prostých elektronických podpisů.

Za zaručený elektronický podpis nařízení označuje elektronický podpis, který umožňuje jednoznačnou identifikaci a spojení s podepisující osobou a vyhovuje požadavkům nařízení na jeho vytváření a uchování. Pokud je takto zaručený elektronický podpis založen na kvalifikovaném certifikátu, tvoří samostatný druh elektronického podpisu.

Kvalifikovanému elektronickému podpisu přiznává nařízení právní účinky rovnocenné vlastnoručnímu podpisu¹⁶⁸. Tato podoba elektronického podpisu představuje nejvyšší míru záruky a je založen na principech asymetrické kryptografie. Vytváří jej fyzická osoba prostřednictvím privátního klíče, který je zpravidla uložen v zabezpečeném zařízení, jakým je například šifrovaný USB token. Ověření totožnosti podepisující osoby, a především platnosti podpisu se realizuje s pomocí veřejného klíče, který byl spolu s kvalifikovaným certifikátem

¹⁶⁵ SEALED, TIME.LEX, SIEMENS. *Study on Cross-Border Interoperability of eSignatures* [online]. Publication office of the EU, 2010, s. 13-15 [cit. 20.6.2022]. Dostupné z: <https://op.europa.eu/en/publication-detail/-/publication/280dc30e-6adb-4b83-af38-fe6083bffeaf>.

¹⁶⁶ Čl. 1 písm. c) nařízení eIDAS.

¹⁶⁷ Čl. 25 odst. 1 nařízení eIDAS.

¹⁶⁸ Čl. 25 odst. 2 nařízení eIDAS.

vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Kvalifikovaný elektronický podpis odpovídá tomu, co Medson označil za digitální i elektronický podpis.

Elektronické podpisy, nehledě na druh či poskytovanou záruku, jsou vždy svázány s konkrétní fyzickou osobou. Pro právnické osoby jsou určeny elektronické pečeti. Tento institut nelze chápat jen jako obdobu elektronického podpisu fyzických osob, protože rozdíly, zejména co se týče právních účinků, jsou až příliš zásadní. Příčinnou, proč se elektronické podpisy nevydávají i právnickým osobám, je nemožnost samotné právnické osoby projevit svou vlastní vůli. V tuzemském právním řádu musí být při právním jednání vždy zastoupená fyzickou osobou. Elektronické pečeti se dělí obdobně jako elektronické podpisy na čtyři druhy. Nejvyšší úroveň záruky je přiznána kvalifikované elektronické pečetě. U té se na rozdíl od kvalifikovaného podpisu neuplatní fikce vlastnoručního podpisu, ale pouhá vyvratitelná domněnka integrity a správnosti původu dat¹⁶⁹. Tedy především, fakt že pečeť skutečně patří konkrétní právnické osobě a že data, se kterými je pečeť spojena, nebyla dodatečně upravována.

Podstatou elektronických časových razítek je hodnověrné přiřazení datumu a času k určitým elektronickým datům. Vzhledem k tomu, že pečeti i časová razítka jsou velmi specifickými instituty, soustředím se dále pouze na elektronické podpisy.

4.5.2 Účinky elektronických podpisů

Tuzemský adaptační zákon o službách vytvářejících důvěru pro elektronické transakce (ZSVDET) upravuje dílčí otázky týkající se těchto služeb. Mimo úpravy povinností státu a kvalifikovaných poskytovatelů služeb upravuje tento zákon především elektronické podepisování a pečetění elektronických dokumentů. Elektronickým dokumentem se rozumí „*jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka*“¹⁷⁰.

K podepsání elektronického dokumentu lze v zásadě použít jakýkoliv elektronický podpis včetně prostého elektronického podpisu. Avšak v případě, že úkon činí osoba při výkonu své působnosti, tedy při výkonu veřejné moci, musí tato osoba v souladu s § 5 ZSVDET podepsat elektronický dokument kvalifikovaným elektronickým podpisem¹⁷¹. Stejná povinnost

¹⁶⁹ Čl. 35 odst. 2 nařízení eIDAS.

¹⁷⁰ Čl. 3 odst. 35 nařízení eIDAS.

¹⁷¹ § 5 písm. b) zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (ZSVDET).

platí i pro veškeré úkony tzv. veřejnoprávních podepisujících¹⁷². Jde svým charakterem o obecnou povinnost těch, kteří mají ve veřejném právu významné postavení.

Naopak osobám činícím úkon vůči veřejnoprávnímu podepisujícímu nebo osobě, která vykonává veřejnou moc, postačí použít uznávaný elektronický podpis. Nejedná se o další druh elektronického podpisu, nýbrž o tuzemskou legislativní zkratku, která zahrnuje kvalifikovaný elektronický podpis nebo elektronický podpis založený na kvalifikovaném certifikátu. Tento požadavek je obsažen v § 6 ZSVDET a dopadá především na občany a podniky. Charakterem jde opět o obecný standart a zvláštní normy jej mohou zpřísnit nebo zmírnit.

4.5.3 Kvalifikovaná forma elektronického podání

Podání je „úkonem směřujícím vůči správnímu orgánu“¹⁷³. Správní řád taxativně vymezuje tři kvalifikované formy podání: písemně, ústně do protokolu a v elektronické podobě¹⁷⁴. Jednou z obligatorních náležitostí podání je podpis osoby, která jej činí (podatele)¹⁷⁵. Z toho vyplývá, že i podání v elektronické podobě musí být podepsáno. A protože podání v elektronické podobě nelze z jeho povahy podepsat vlastnoručně, je nutné jej podepsat elektronicky.

Správní řád neurčuje konkrétní elektronické instituty s pomocí, kterých má být podání elektronicky podepsáno. Lukáš Potěšil považuje absenci výčtu konkrétních přípustných institutů za evidentní nedostatek právní úpravy¹⁷⁶. Já se domnívám, že je to naopak vhodný přístup, neboť procesní předpisy by měly být, co se týče elektronických institutů, co nejvíce neutrální. Obligatorní náležitosti podání jsou pro klasickou i elektronickou podobu upraveny ve správním řádu stejně. Odlišnosti elektronické podoby obecně upravují zákony eGovernmentu, a proto není nutné ve správním řádu, a stejně tak v ostatních procesních předpisech, uvádět opakovaně výčet konkrétních přípustných institutů, s pomocí kterých se lze elektronicky podepsat. Postačí proto, že procesní předpis explicitně vyžaduje podpis.

V probrané právní úpravě zákonů eGovernmentu jsem již uvedl dva právní instituty, jejichž použití má účinky podpisu. Prvním je doručení datové zprávy do datové schránky

¹⁷² § 5 písm. a) ZSVDET za veřejnoprávního podepisujícího označuje: „stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem nebo jejich orgán anebo jiná jejich součást“.

¹⁷³ § 37 odst. 1 správního řádu.

¹⁷⁴ § 37 odst. 4 věta první správního řádu.

¹⁷⁵ § 37 odst. 2 věta poslední správního řádu.

¹⁷⁶ POTĚŠIL, Lukáš. § 37 [Podání]. In: POTĚŠIL, Lukáš, HEJČ, David, RIGEL, Filip, MAREK, David. *Správní řád*. 2. vydání. Praha: C.H. Beck, 2020, s. 232, marg. č. 30. ISBN: 978-80-7400-804-7.

správním orgánu podle § 18 zákona o datových schránkách. A druhým je doručení elektronického dokumentu opatřeného uznávaným elektronickým podpisem podle § 6 odst. 1 ZSVDET. Tyto instituty jsou, co se týče účinků podání, rovnocenné.

Základním požadavkem na uznávaný elektronický podpis je, aby byl platný, přičemž rozhodujícím okamžikem, ke kterému se platnost ověřuje, je čas doručení¹⁷⁷. Čas doručení má zásadní význam pro běh lhůt. Zvolení času doručení jako rozhodujícího časového okamžiku se může jevit jako logické a jednoznačné, avšak nebylo tomu tak vždy. Znejistění přinesl náleží Ústavního soudu z roku 2014¹⁷⁸, který označil podání doručené více než dvacet minut po půlnoci, kdy vypršela lhůta, za včasné doručené. Rozhodl tak na základě předložené kopie emailové zprávy s hlavičkou obsahující čas odeslání více než dvacet minut před půlnocí. Za předpokladu, že jsou oba časové údaje pravdivé, trvalo doručení přes čtyřicet minut, což je neobvyklá prodleva, protože email běžně servery odbaví během několika sekund či minut.

Ústavní soud se bez dalšího dovolal staršího nálezu z roku 2011¹⁷⁹, ve kterém judikoval, že při realizaci práva účastníka činit úkon není „*spravedlivé, aby nedostatek ve fungování elektronického systému doručování šel k tíži stěžovatelů*“¹⁸⁰, protože účastník řízení nemůže ovlivnit, že v procesu doručování dojde k prodlevě, která by mu znemožnila uplatnit svá procesní práva. Účastníku potom stačí „*odeslání takové e-mailové zprávy věrohodným způsobem prokázat, nevyplývá-li již ze samotné přijaté zprávy datum a čas jejího odeslání*“¹⁸¹.

Osobně za největší potíže tohoto přístupu považují, že spoléhání se na čas odeslání, značně oslabuje právní jistotu, protože mohou nastat situace, kdy prodleva nebude jen čtyřicet minut, ale třeba několik dnů či týdnů. Zvláště nežádoucí situace by pak mohla nastat, pokud by podatel vědomě využíval nespolehlivé servery pro odchozí emailovou poštu za účelem pozdržení doručení a následně by rozporoval odmítnutí takového podání.

Právě princip právní jistoty byl jedním z argumentů, proč Ústavní soud změnil právní názor a přehodnotil svůj přístup k problematice včasnosti doručení podání pomocí emailu. Dále bylo původnímu překonanému názoru Ústavního soudu vyčteno relativizování tvrdosti běhu procesních lhůt. A nebrání do úvahy roli poskytovatelů emailových služeb, kteří na rozdíl od doručování prostřednictvím držitele poštovní licence nemají zákonnou povinnost doručit

¹⁷⁷ Usnesení Nejvyššího soudu ze dne 12. 9. 2018, č. j. 3 Tdo 1003/2018-37.

¹⁷⁸ Nález Ústavního soudu ze dne 20. 5. 2014, sp. zn. II. US 2560/13.

¹⁷⁹ Nález Ústavního soudu ze dne 29. 3. 2011, sp. zn. II. ÚS 1911/11.

¹⁸⁰ Tamtéž.

¹⁸¹ Tamtéž.

email v dohledné době. Navíc čas doručení jsou si orgány veřejné moci samy schopny ověřit prostřednictvím vlastních údajů, zatímco u času odeslání by se musela provádět složitá dokazování¹⁸².

Plénium Ústavního soudu přijalo v roce 2021 stanovisko se dvěma výroky:

- „*Včasnost elektronického podání učiněného prostřednictvím e-mailu je třeba posuzovat podle okamžiku, kdy podání dojde soudu, nikoliv podle okamžiku, kdy je podatelem odesláno*“;
- „*Za okamžik, kdy je podání řádně učiněno, se považuje okamžik, kdy se e-mailová zpráva dostane do dispozice soudu; pro posouzení včasnosti podání není relevantní, kdy se s ním soud fakticky seznámil*“¹⁸³.

Těmito výroky Ústavní soud otázku včasnosti elektronického podání prostřednictvím emailu v podstatě vyřešil. Za zásadní považují, že vymezil okamžik, kdy je podání řádně učiněno. Dispozice soudu znamená, že email je doručen v emailové schránce soudu. Od tohoto momentu se teoreticky může personál soudu seznámit s obsahem podání. Pro úplnost stanovisko v odůvodnění uvádí ještě výjimku, kdyby se mohl podatel dovolat včasného odeslání emailového podání, pro případ, že pozdní doručení způsobí prodleva na straně e-mailového serveru státu.

Povinnost ověřovat platnost elektronického podpisu nevyplývá jen z ustanovení o náležitostech podání v procesních předpisech. Soudy jako veřejnoprávní původci podle zákona o archivnictví a spisové službě mají povinnost ověřit platnost uznávaného elektronického podpisu u všech elektronických dokumentů, které přijaly¹⁸⁴. K této povinnosti se váže i povinnost zaslat odesílateli elektronického dokumentu na jeho emailovou adresu potvrzení o doručení včetně výsledku ověření platnosti uznávaného elektronického podpisu¹⁸⁵. Měl jsem pochybnosti ohledně vymahatelnosti této povinnosti, neboť jsem se nedomníval, že by absence tohoto potvrzení mohla výrazněji zasáhnout do procesních práv podatele. Přece jen nejde o povinnost stanovenou procesním předpisem ale jiným zákonem. Nejvyšší správní

¹⁸² Obdobně také:

Rozsudek Nejvyššího správního soudu ze dne 16. 7. 2015, č. j. 9 As 261/2014-44.

Rozsudek Nejvyššího správního soudu ze dne 23. 3. 2016, č. j. 6 As 276/2015-31.

¹⁸³ Stanovisko pléna Ústavního soudu ze dne 7. 9. 2021, sp. zn. Pl. ÚS-st. 53/21.

¹⁸⁴ § 3 odst. 1 písm. a) zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a § 4 odst. 5 písm. a) vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

¹⁸⁵ § 4 odst. 8 vyhlášky o podrobnostech výkonu spisové služby.

soud však judikoval, že absence tohoto potvrzení zasahuje do Listinou zaručeného práva na soudní ochranu a je proto nepřijatelné¹⁸⁶.

Co se týče správního řízení, domnívám se, že analogie je do určité míry namístě. Nicméně je třeba respektovat, že správní a soudní řízení je velmi odlišné. Nemůže být řeč o právu na soudní ochranu podle Listiny, přesto porušením povinnosti správního orgánu zaslat potvrzení o doručení dochází k zásahu do práv toho, kdo podání činí. Porušení normy zákona o archivnictví a spisové službě při správním řízení bude zároveň porušením základního principu správního řízení, kterým je princip legality. Rozhodnutí, které by bylo vydáno v rozporu s tímto principem, nemůže obstát. Podatel by se měl bránit pomocí opravných prostředků, popřípadě iniciovat soudní přezkum.

Zajímavou otázkou, se kterou se tuzemská judikatura také vyrovnala, se týkala podepisování příloh. Předmětem úvahy bylo, zda musí být uznávaným elektronickým podpisem opatřena i příloha emailu, která obsahuje samotný text podání. V tomto případě mám za to, že vyžadování několikanásobného podepisování by bylo zbytečně formalistické a nelze pro něj najít opodstatnění. Pokud podepíše podatel uznávaným elektronickým podpisem email, lze jej se zákonem požadovanou jistotou identifikovat. Navíc kontrolní součet, který je součástí uznávaného elektronického podpisu, zahrnuje do svého výpočtu i přílohy. To znamená, že je možné ověřit i integritu celé zprávy včetně příloh. Podle nálezu ústavního soudu¹⁸⁷ podpis samotného emailu uznávaným elektronickým podpisem poskytuje dostačené záruky. Tyto záruky v některých ohledech, jako například záruka integrity dat, dokonce převyšují míru jistoty, které poskytuje listinné podání s vlastnoručním podpisem. Ani u vlastnoručního podpisu si nelze být stoprocentně jistý, že osoba, která připojila svůj podpis, je skutečně autorem předmětného podání, a přesto žádný z těchto nedostatků není překážkou, kvůli které by mělo být podání odmítnuto a soud by byl oprávněn podateli odeprít právo na soudní ochranu.

S přehnaným formalismem v oblasti elektronických podpisů se lze setkat i při jiných správních úkonech než jsou podání. Například Nejvyšší správní soud se zabýval otázkou, zda je vadou rozhodnutí umístění elektronického podpisu na jiné než poslední straně¹⁸⁸. Takový požadavek je opět přehnaně formalistický. Dle mého názoru opět nedává smysl s ohledem na to, že uznávaný elektronický podpis bez ohledu na umístění v elektronickém dokumentu zaručuje

¹⁸⁶ Nález Ústavního soudu ze dne 28. 6. 2021, sp. zn. II. ÚS 671/21.

¹⁸⁷ Nález Ústavního soudu ze dne 27. 8. 2013, sp. zn. II. ÚS 3042/12.

¹⁸⁸ Rozsudek Nejvyššího správního soudu ze dne 31. 1. 2018, č.j. 5 As 295/2016-45.

integritu celého dokumentu i identitu podepisujícího. Není proto překvapivé, že Nejvyšší správní soud tomuto požadavku nevyhověl.

4.5.4 Nekvalifikovaná forma elektronického podání

Správní řád a obdobně i jiné procesní předpisy, připouští i nekvalifikovanou formu elektronického podání. Jedná se o specifická elektronická podání, při kterých nejsou naplněny požadavky fikce účinku podpisu. S touto nekvalifikovanou formou podání je spojeno včasné doručení podání pouze za předpokladu, že podatel splní v určité lhůtě povinnost doručit potvrzení podání kvalifikovaným způsobem. Jsou dva typické případy nekvalifikovaných elektronických podání, se kterými se lze běžně setkat v judikatuře tuzemských soudů. Jde o podání emailem bez uznávaného elektronického podpisu a podání cizí datovou schránkou.

Pro podání emailem bez uznávaného elektronického podpisu se uplatní vše, co bylo řečeno o včasnosti doručení emailu s uznávaným elektronickým podpisem. Za obdobný případ nekvalifikovaného podání je podle Nejvyššího správního soudu nutné považovat i situaci, kdy podatel sice podepíše podání uznávaným elektronickým podpisem, ale doručí jej na jinou emailovou adresu, než je adresa elektronické podatelny správního orgánu¹⁸⁹. Jedná se o přístup, který se prosadil v judikatuře již před více než deseti lety¹⁹⁰.

Zvláštnost podání pomocí cizích datových schránek spočívá v tom, že účinky fikce podpisu se nepřiznávají datové zprávě, která je odeslána z datové schránky jiné osoby. Podatel je vždy osobou, která podání činí materiálně. Z toho pohledu se mi jeví jako adekvátní, že podání se nepřičítá automaticky osobě, prostřednictvím jejíž datové schránky bylo doručeno. Jde o promítnutí pravidla, že podání se posuzuje podle skutečného obsahu¹⁹¹. V takovém případě nelze identifikovat podatele pomocí informačního systému datových stránek, protože údaje o odesílateli svědčí o osobě, která je držitelem datové schránky. A proto musí být podání pomocí cizích datových schránek i podle judikatury Nejvyššího správního soudu opatřeno uznávaným elektronickým podpisem podatele¹⁹².

4.6 Právní úprava spisové služby

Velký význam pro každodenní činnost veřejné správy má zákon o archivnictví a spisové službě. Tento zákon byl již zmíněn v souvislosti s povinnostmi

¹⁸⁹ Rozsudek Nejvyššího správního soudu ze dne 16. 5. 2019, č.j. 1 As 106/2018-45.

¹⁹⁰ Rozsudek Nejvyššího správního soudu ze dne 16. 12. 2010, č. j. 1 Ans 5/2010-172.

¹⁹¹ § 37 odst. 1 správního řádu.

¹⁹² Usnesení Nejvyššího soudu ze dne 27.10.2020, sp. zn. 27 Cdo 143/2020.

veřejnoprávních původců v oblasti uznávaných elektronických podpisů. V oblasti výkonu spisové služby, ke kterému jsou povinni veřejnoprávní a další určení původci¹⁹³, zákon reaguje na rozšíření elektronických forem komunikace. Veřejnoprávní původci jsou zpravidla povinni spisovou službu vést v elektronické podobě¹⁹⁴. Podrobnosti vedení spisové služby stanovuje vyhláška o podrobnostech výkonu a Národní standard pro elektronické systémy spisové služby oznamovaný Ministerstvem vnitra¹⁹⁵.

V roce 2019 byly představeny výsledky analýzy spisové služby¹⁹⁶. Zjištěný stav vedení spisové služby byl hodnocen jako dlouhodobě neudržitelný. V oblasti využívání elektronických nástrojů bylo shledáno několik zásadních nedostatků. Mezi nejzásadnější patří špatné zpracování a odesílání elektronických dokumentů. Konkrétně se tyto nedostatky projevují chybějícími elektronickými podpisy a časovými razítky nebo nevyhovujícím způsobem konverze dokumentů. Tato analýza také potvrzuje neuspokojivou praxi v přijímání elektronických dokumentů včetně neplnění povinnosti potvrzení jejich přijetí. Z výsledků analýzy usuzují, že státní úřady ne vždy plní všechny své povinnosti v oblasti elektronizace spisové služby, přičemž ne vždy jde o nové povinnosti, na které by se měly úřady adaptovat pod časovým tlakem. Některé nedodržované povinnosti jsou součástí právní úpravy již více než deset let.

Nedostatky ve vedení spisové služby snižují schopnost orgánů veřejné správy zabezpečit hladký a efektivní oběh papírových i elektronických dokumentů. Projevující se nedostatky mohou vést, jak připomíná Akční plán rozvoje spisové služby Úřadu vlády ČR, k horšímu právnímu postavení orgánů veřejné správy při výkonu své působnosti¹⁹⁷. V důsledku může být ohrožena zejména formální bezvadnost vydaných rozhodnutí nebo správnost úředních postupů.

¹⁹³ Výchet veřejnoprávních původců je obsažen v § 63 odst. 1 zákona o archivnictví a spisové službě.

¹⁹⁴ SKALICKÁ, Martina. Řízení ve věcech služby v digitalizované spisové službě [online]. In: *Epravo.cz*. 2021 [cit. 20.6.2022]. ISSN 1213-189X. Dostupné z: <https://epravo.cz/top/clanky/rizeni-ve-vecech-sluzby-v-digitalizovane-spisove-sluzbe-112403.html>.

¹⁹⁵ MINISTERSTVO VNITRA. Národní standard pro elektronické systémy spisové služby [online]. 2021 [cit. 20.6.2022]. In: *Mvcr.cz*, 2022. Dostupné z: <https://mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx>.

¹⁹⁶ ÚLOVEC, Jiří. Informace o současném stavu elektronických systémů spisové služby a informačních systémů pro správu [prezentace]. In: *ISSS 2019* [online]. 2019 [cit. 20.6.2022]. Dostupné z: https://issc.cz/archiv/2019/download/prezentace/mvcr_ulovec.pdf.

¹⁹⁷ ÚŘAD VLÁDY ČR. *Akční plán rozvoje spisové služby Úřadu vlády České republiky* [online]. 2019, s. 3 [cit. 20.6.2022]. Dostupné z: <https://vlada.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha-c--2---Akni-plan-rozvoje-spisove-sluzby.pdf>.

4.7 Zákon o právu na digitální služby (ZPDS)

4.7.1 Obecně o dvou nejvýznamnějších zákonech pro eGovernment posledních let

Během minulých dvou let byly přijaty dva zákony, kterým je přisuzován potenciál vyřešit problematické aspekty českého eGovernmentu. Nejprve byl přijat zákon o právu na digitální služby (ZPDS) a rok po něm změnový zákon, kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (DEPO).

Těmto dvěma zákonům jsem se rozhodl věnovat poslední část této práce. Oba zákony považuji za rozsáhlé. Jeden ambicemi a druhý počtem paragrafů. Moje snaha bude směřovat k vysvětlení podstaty vybraných institutů eGovernmentu, které tyto zákony mění nebo nově vytvářejí. Tyto právní instituty uvedu do kontextu stávající úpravy a případně upozorním na problematické aspekty nové právní úpravy. Jelikož je velká část změn v DEPO velmi specifická, soustředím se na novou obecnou právní úpravu v ZPDS.

Přestože původní myšlenky vedoucí ke vzniku obou zákonů vznikly v zásadě nezávisle na sobě, v jejich konečné podobě je možné oba zákony považovat za navzájem se doplňující. Konečnou podobu obou zákonů značně ovlivnil jejich rozdílný osud v legislativním procesu.

4.7.2 Specifika legislativního procesu ZPDS

Návrh ZPDS byl v březnu 2019 předložen poslanci napříč všemi devíti tehdejšími poslaneckými kluby, avšak původní iniciativa není přisuzována poslancům, ale ICT unii, což je sdružení zástupců technologických firem a vysokých škol, ve spolupráci se zaměstnavatelskými a podnikatelskými svazy a dalšími sdruženími¹⁹⁸.

K návrhu přijala druhá vláda Andreje Babiše souhlasné stanovisko¹⁹⁹, avšak podrobila jej zároveň značné kritice. Kritika směřovala na nadbytečnost dalšího zákona vedle stávajících eGovernment zákonů, nerealizovatelnost proklamativních ustanovení a nezbytnost přijetí navazujícího změnového zákona, který navrhovatelé sami nepředložili. Další výtky se týkaly absence podrobných analýz a poměření nákladů a potenciálních přínosů navrženého řešení, což u poslaneckého návrhu není překvapivé.

¹⁹⁸ ICT UNIE. Informace o stavu přípravy projednávání návrhu zákona o právech na digitální služby. In: *Ictu.cz* [online]. 2018 [cit. 20.6.2022]. Dostupné z: [http://www.ictu.cz/aktualne/detail-aktuality/?tx_ttnews\[tt_news\]=104](http://www.ictu.cz/aktualne/detail-aktuality/?tx_ttnews[tt_news]=104).

¹⁹⁹ VLÁDA ČR. Sněmovní tisk 447/1: Stanovisko vlády k návrhu zákona o právu na digitální služby. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=447>.

Původní znění návrhu²⁰⁰ bylo z pohledu stávajících zákonů eGovernmentu rozporu plné. Návrh zaváděl zbytečné pojmy. V průběhu legislativního procesu například navrhovaný pojem autoritativní údaj nahradilo popisnější spojení údaj vedený v agendových informačních systémech a pojem speciální uživatelské rozhraní byl zcela vypuštěn.

Významný zásah do původního znění zákona měl velký pozměňovací návrh²⁰¹ Výboru pro veřejnou správu a regionální rozvoj Poslanecké sněmovny, který připravilo Ministerstvo vnitra. Ten například z úpravy zcela odstranil povinnost poskytovat digitální služby územními samosprávami v samostatné působnosti. Mimo dílčích změn v samotném zákoně se také značně rozšířilo množství změnových ustanovení.

ZPDS byl na konci roku 2019 přijat oběma komorami parlamentu a podepsán prezidentem. Vyhlášen byl pod číslem 12/2020 Sb. a nabyl účinnosti 1. února 2020. Avšak řada zásadních ustanovení měla nebo stále má odloženou účinnost. Většina ustanovení nabyla účinnosti do 1. února 2022. Některá práva související s elektronickými podpisy nebo elektronickou identifikací však nabývají účinnost až 1. července 2022. Se zákazem poskytování rodných čísel jako součást identifikačních údajů zákon počítá dokonce až od počátku roku 2025. Důvodem odložené účinnosti je zřejmě snaha poskytnout veřejné správě dostatek času na přípravu potřebných administrativních a technologických změn, které nová legislativa vyžaduje.

4.7.3 Další eGovernment zákon, proč?

Legislativním cílem ZPDS bylo vytvořit nový ani ne dvacetiparagrafový zákon, který bude obecným předpisem eGovernmentu pro poskytování digitálních služeb. Otázka, zda je zapotřebí nový zákon a zda nestačí jen upravit stávající zákony eGovernmentu provází ZPDS od počátku.

Podle Zdeňka Zajíčka, člena ICT unie, který se podílel na tvorbě návrhu, bylo myšlenkou vzniku samostatného zákona: „*ukázat (lidem), že pokud jsou IT gramotní, nebojí se technologií, denně je používají, tak mají úplně stejná práva vůči státu a mají na digitální*

²⁰⁰ KOŘANOVÁ, Barbora aj. Sněmovní tisk 447/0: Návrh zákona o právu na digitální služby včetně důvodové zprávy. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=447>.

²⁰¹ VÝBOR PRO VEŘEJNOU SPRÁVU A REGIONÁLNÍ ROZVOJ. Sněmovní tisk 447/0: Usnesení VSR ze dne 5. září 2019. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=447&ct1=4>.

komunikaci nárok“²⁰². Přičemž připouští, že si sami tvůrci byli vědomi, že pro odblokování stagnace rozvoje českého eGovernmentu je potřeba změnit více než 50 stávajících právních předpisů. V průběhu diskuse o návrhu tohoto zákona bylo argumentů pro potřebnost samostatného zákona uvedeno samozřejmě více. Já se však pozastavím právě nad citovaný zdůvodněním Zdeňka Zajíčka, neboť mě navedlo k otázce, zda bylo možné identifikovat obecné právo na digitální komunikaci občana vůči veřejné správě již ve stávajících zákonech. Výslovně vyjádřené právo na digitální komunikaci vůči veřejné správě náš právní řád skutečně nikdy neznal. Zato znal povinnosti orgánů veřejné moci přijímat datové zprávy a elektronické dokumenty s uznávaným elektronickým podpisem. Umožňoval také elektronicky se identifikovat a provádět úkony vůči orgánu veřejné moci v informačních systémech veřejné správy a získávat z něj výpisy. I hlavní procesní předpis veřejné správy, správní řád, přiznával právo činit elektronická podání a ukládal povinnost doručovat elektronicky, je-li to možné. Souhrn těchto práv, ať už přímo vyjádřených nebo odpovídajících povinnosti orgánů veřejné správy, považuji za jednotlivá dílčí práva na digitální komunikaci občana vůči veřejné správě.

Důvody, proč při tvorbě dřívějších zákonů eGovernmentu nebyla akcentovaná potřeba zobecnovat tato dílčí práva, shledávám v základním principu fungování tuzemské veřejné správy, kterým je zásada enumerativnosti veřejnoprávních pretenzí. Ta vyžaduje, aby si orgány veřejné moci byly při své činnosti vždy vědomy na základě, jakého právního zmocnění vykonávají svou pravomoc. Proto dřívější zákony eGovernmentu namísto přiznávání práv osobám komunikujícím s veřejnou správou, stanovovaly a priori povinnosti orgánům veřejné správy. Místo stanovování obecných práv v novém zákoně, bylo možné stejného výsledku dosáhnout rozšířením a popřípadě zobecněním dosavadních povinností. Přestože pro ostatní veřejnoprávní předpisy obecně je typické spíše stanovování povinností orgánům veřejné správy zvolené legislativní vyjádření je zcela přípustné.

Právě kvůli specifickému legislativnímu vyjádření a snad i kvůli své obecnosti bývá zákon přezdíván jako digitální ústava. To je však velmi zavádějící. Práva obsažená v ZPDS nejenže nemají ústavní sílu, ale nejsou ani nezadatelná či nezrušitelná jako základní lidská práva. Na rozdíl třeba od práva na přístup k internetu, u kterého alespoň probíhá diskuse, zda

²⁰² ZAJÍČEK Zdeněk. Zdeněk Zajíček (ICT Unie): Digitální ústava absolutně mění pohled na to, jak má stát fungovat. In: SLÍŽEK, David. *Lupa.cz* [online]. Internet Info, 2018 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://lupa.cz/clanky/zdenek-zajicek-ict-unie-digitalni-ustava-absolutne-meni-pohled-na-to-jak-ma-stat-fungovat/>.

by mělo být státy uznáno jako samostatné lidské právo²⁰³. Otázka, zda vůbec stát umožní občanům komunikovat s veřejnou správou elektronicky, je pouze politická nikoliv lidskoprávní. A jako taková je řešena v zákonných a podzákonných předpisech.

Přijetí nového zákona nemění nic na tom, že zásadní význam pro realizaci konkrétních práv v ZPDS mají stále zákony eGovernmentu a konkrétní agendové zákony. Právě agendové zákony mohou výrazně zasáhnout do způsobů realizace těchto práv, anebo je z postavení *lex specialis* dokonce popřít.

Na základě výše uvedeného se domnívám, že samostatný zákon nebyl zapotřebí a že ustanovení přiznávající práva by mohla být součástí jiných předpisů eGovernmentu. Jak by to mohlo vypadat, lze ukázat na příkladu zákona o základních registrech. Do nabytí účinnosti změnových ustanovení v ZPDS se působnost zákona vztahovala pouze na základní registry a v nich obsažené údaje, nyní ale reguluje i sdílení údajů mezi agendovými a soukromoprávními informačními systémy. V ZPDS obsažený zákaz orgánu veřejné moci vyžadovat jemu přístupné údaje ze základního registru nebo agendového informačního systému, by mohl být systematicky zařazen namísto do ZPDS přímo do zákona o základních registrech.

Obdobně by bylo možné zařadit práva související s elektronickými podpisy a elektronickou identifikací do prováděcích zákonů eIDAS. Zákonu o datových schránkách, bylo již dávno přezdíváno zákon o eGovernmentu²⁰⁴. A proto si myslím, že by nebylo na překážku, pokud by obsahoval navíc obecnou část týkající se digitálních služeb a digitálních úkonů, jak je tomu v ZPDS.

Koncept nového zákona, který tvůrci zvolili, je zajisté přípustný a legitimní. Mým úmyslem však bylo poukázat na jeho netradičnost. Domnívám se, že tento koncept odráží frustraci tvůrců zákona nad stavem tuzemského eGovernmentu, který na jedné straně stanovuje orgánům veřejné moci spoustu povinností, ale na straně druhé není jednoduché se domoci nápravy, pokud je orgány veřejné moci neplní. V budoucnu bude možné zhodnotit, zda prosazení tohoto konceptu přispěje k dalšímu rozvoji digitalizace veřejné správy a zda se nově zakotvená obecná práva prosadí v praxi.

²⁰³ FIALOVÁ, Eva. Právo na přístup k internetu. In: *Pravniprostor.cz* [online]. ATLAS, 2019 [cit. 20.6.2022]. ISSN: 2336-4114. Dostupné z: <https://pravniprostor.cz/clanky/pravo-it/pravo-na-pristup-k-internetu>.

²⁰⁴ Například: REDAKCE EURO.CZ, NĚMEC, Jan. Upravený zákon jde do vlády. In: *Pravniprostor.cz* [online]. Internet Info, 2007 [cit. 20.6.2022]. ISSN 1212-9437. Dostupné z: <https://euro.cz/byznys/upraveny-zakon-jde-do-vlady-887462>.

4.7.4 Právo na digitální služby

Základem nové právní úpravy je zakotvení obecného práva na digitální komunikaci s orgány veřejné moci. Za tímto účelem zákon vymezuje výslovné právo na digitální služby a právo na digitální úkon. Nejprve rozeberu první z těchto dvou zásadních práv. Aby bylo možné vysvětlit obsah tohoto práva, je zapotřebí definovat subjekty a pojem digitální služby. Legislativní vymezení tohoto pojmu i oprávněného subjektu je obsaženo v § 2 ZPDS.

První odstavec nazývá osobu oprávněnou z práva na digitální služby uživatelem služeb. Může jím být pouze fyzická, nebo právnická osoba, která při poskytování digitální služby nemá postavení orgánu veřejné moci. Je bez významu, zda osoba podniká, nebo ne. Z vymezení osoby oprávněné vyplývá, že jí nemůže být orgán veřejné moci. Takový orgán může mít pouze postavení povinného. Z toho vyplývá, že ve vztazích mezi orgány veřejné moci navzájem, se toto právo neuplatní.

Digitální služba je pojmem, který tuzemský právní řád a eGovernment znal již před přijetím ZPDS, avšak ve zcela jiném významu a kontextu. V důsledku transpozice směrnice EU 2016/1148 byl tento pojem zahrnut do zákona o kybernetické bezpečnosti. Digitální služba v tomto smyslu představuje jakoukoliv soukromoprávní službu poskytnutou na žádost, na dálku, elektronicky a zpravidla za úplatu²⁰⁵. Zmíněný zákon podrobuje zvláštní regulaci pouze tři druhy služeb provozovaných na internetu: on-line tržiště, internetové vyhledávače a cloudy. Soukromoprávních digitálních služeb se bude týkat i připravované nařízení o digitálních službách²⁰⁶.

V případě, že orgány veřejné moci nebudou v rámci výkonu veřejné moci poskytovat výše zmíněné služby soukromoprávní povahy, nemělo by docházet k překrytí s pojmem digitální služba podle ZPDS, protože ten reguluje digitální služby veřejnoprávní povahy.

ZPDS digitální službu vymezuje jako „*úkon vykonávaný orgánem veřejné moci vůči uživateli služby v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě*“²⁰⁷. Jinými slovy jde o elektronický úkon, který je orgánu veřejné moci svěřen do jeho působnosti

²⁰⁵ Podrobnému rozboru obsahu a původu pojmu digitální služba v pojetí zákona o kybernetické bezpečnosti se věnuje: KOLOUCH, Jan, BAŠTA, Pavel, KROPÁČOVÁ, Andrea, KUNC, Martin. Digitální služba. In: *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

²⁰⁶ EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES ze dne 15.12.2020* [online]. 2020 [cit. 20.6.2022]. CELEX: 52020PC0825. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0825>.

²⁰⁷ § 2 odst. 2 věta první zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů (ZPDS).

a který je formálně veden ve zvláštní evidenci podle tohoto zákona. Za digitální službu se považuje také „úkon vykonávaný vůči uživateli služby kontaktním místem veřejné správy v rámci agendy“²⁰⁸.

§ 3 odst. 1 ZPDS stručně přiznává všem uživatelům služby právo využívat digitální službu a zároveň orgánu veřejné služby ukládá povinnost poskytovat digitální službu. Uložení obecné povinnosti poskytovat digitální službu má být podle autorů komentáře k tomuto zákonu jasným příkazem všem orgánům veřejné moci, aby neodmítali poskytování digitálních služeb²⁰⁹.

Povinnost poskytovat digitální službu je formulována zdánlivě bez omezení. Avšak řadu různých omezení obsahují další ustanovení ZPDS, ostatní zákony eGovernmentu i agendové zákony. Podle druhu omezení rozlišují:

- omezení regulující způsob poskytnutí digitální služby;
- omezení vztahující se na některé z orgánů veřejné moci;
- omezení týkající se konkrétních digitálních služeb.

Způsoby poskytování digitálních služeb reguluje především samotný ZPDS a další eGovernment zákony. ZPDS například v § 13 omezuje způsob poskytování digitálních služeb požadavky na technologickou neutralitu a na výstupy v otevřeném formátu. Jednotlivé způsoby poskytování se řídí příslušným eGovernment zákony například zákonem o datových schránkách.

Pro některé orgány veřejné moci ZPDS výslovně vylučuje povinnost poskytovat digitální služby, nebo pro ně stanovuje jiný režim. Podle § 14 odst. 2 ZPDS jsou takovými orgány Národní bezpečnostní úřad při provádění bezpečnostního řízení a tři tuzemské zpravodajské služby bez ohledu na prováděnou činnost. Taktéž podle § 14 odst. 3 ZPDS povinnost poskytovat digitální služby se nevztahuje na obce a kraje při výkonu jejich samostatné působnosti. Tyto územní samosprávy jsou ale oprávněny digitální služby poskytovat dobrovolně za stejných podmínek jako jiné orgány veřejné moci. Při výkonu svěřené působnosti na ně povinnost poskytovat digitální služby ale dopadá v plném rozsahu.

Vzhledem k tomu, že ZPDS obsahuje jen obecnou úpravu poskytování digitálních služeb, mohou být různá omezení stanovena pro konkrétní službu v agendových zákonech, které mají povahu *lex specialis*. Taková omezení obsahuje například zákon o svobodném

²⁰⁸ § 2 odst. 2 věta druhá ZPDS.

²⁰⁹ KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel, ZAJÍČEK, Zdeněk. § 3 Právo na digitální službu. In: ZAJÍČEK. pozn. 156, s. 33-34.

přístupu k informacím a zákon o právu na informace o životním prostředí. Oba zákony upravují specifické podmínky a proces poskytování informací včetně náležitostí žádostí a lhůt pro jejich vyřízení.

4.7.5 Právo na technologickou neutralitu

S právem poskytovat digitální služby úzce souvisí ustanovení § 13 odst. 1 ZPDS, které upravuje povinnost orgánů veřejné moci poskytovat digitální služby technologicky neutrálním způsobem. Zákon tím míní nezávislosti na konkrétní platformě či technologii. V rozporu s tímto ustanovením bude, pokud digitální služby nepůjde využít například s pomocí některého z operačních systémů nebo internetového prohlížeče. Zákaz vyjádřený v § 13 odst. 1 ZPDS platí i pro vyžadování konkrétního hardwaru.

V současné době se lze při komunikaci se státní správou setkat s vyloženě odstrašujícími případy technologické závislosti. Takovým případem je sedm let starý Portál Národního elektronického nástroje, který slouží pro administraci a zadávání veřejných zakázek. Front-end autorizované části portálu vyžaduje po uživateli zastaralé rozšíření MS Silverlight²¹⁰, který již více než pět let nepodporuje žádný z moderních prohlížečů. V důsledku toho jsou uživatelé tohoto portálu odkázáni na Internet Explorer, který je neméně zastaralý a dostupný pouze v operačním systému Windows.

Pokud Ministerstvo pro místní rozvoj bude poskytovat digitální služby prostřednictvím tohoto portálu, bude se jednat o porušení práva na digitální neutralitu. V tomto případě se však obávám, že se uživatelé svého práva úspěšně nedomůžou. Důvodem jsou v ZPDS stanovené široké výjimky, kdy technologickou neutralitu nelze vyžadovat. Jednou z nich je neúměrná ekonomická náročnost. V současné době by odstranění závislosti na klíčové technologii jako je MS Silverlight bylo nepochybně velmi drahé.

Dalšími výjimkami z technologické neutrality jsou bezpečnost informačního systému a jiný chráněný veřejný zájem. Vyloučení určité platformy nebo technologie budou moci poskytovatelé digitálních služeb tedy zdůvodnit s poukázáním na bezpečnostní riziko. Souhlasím s názorem autorů komentáře k tomuto zákonu, že by tyto výjimky měly být vykládány restriktivně²¹¹, aby bylo právo na digitální neutralitu zachováno v co největším rozsahu.

²¹⁰ MINISTERSTVO PRO MÍSTNÍ ROZVOJ. *NEN [Národní elektronický nástroj]: Ověření kompatibility* [online]. [cca 2022, cit. 20.6.2022]. Dostupné z: <https://nen.nipez.cz/CompatibilityCheck>.

²¹¹ DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. § 13 Právo na technologickou neutralitu. In: ZAJÍČEK. pozn. 156, s. 142.

V souvislosti s povinností poskytovat technologicky neutrální digitální služby jsem si položil ještě jinou otázku. Zda z tohoto práva vyplývá povinnost optimalizovat portály a jiné webové stránky, které slouží k poskytování digitálních služeb, pro mobilní zařízení. Pokud by užívání takového webu bylo na mobilních zařízeních úplně znemožněno, není pochyb, že by právo na technologickou neutralitu bylo porušeno. Ale častější situace je dle mé zkušenosti spíše absence optimalizace zobrazení a ovládání webu pro mobilní zařízení. Je to situace, kdy digitální služba je na všech platformách dostupná stejným způsobem, ale pro uživatele mobilních zařízení je využívání služeb složitější než pro ostatní. Domnívám se, že povinnost přizpůsobovat zobrazení a ovládání mobilním telefonům z § 13 odst. 1 ZPDS neplyne, protože toto ustanovení se omezuje pouze na povinnost zdržet se vyžadování konkrétní platformy či technologie při jejím poskytování.

4.7.6 Právo činit digitální úkon

Jelikož ZPDS pod pojem digitální služba zahrnuje jen úkony činěné směrem od orgánů veřejné moci, je nezbytné definovat komplementární pojem, který pojme úkony činěné vůči orgánu veřejné moci. Tím je podle § 2 odst. 3 ZPDS digitální úkon definovaný jako „*úkon vykonávaný uživatelem služby vůči orgánu veřejné moci v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě*“.

Právo činit digitální úkon je vyjádřeno v § 4 odst. 1 ZPDS. Oprávněným subjektem je uživatel služby vymezený stejně jako u práva na digitální službu. Zároveň jsou stanoveny způsoby činění digitálních úkonů prostřednictvím:

- datových schránek;
- kontaktních míst veřejné správy (Czech POINT);
- dokumentů podepsaných uznávaným elektronickým podpisem;
- informačních systémů veřejné správy (samoobslužných portálů);
- jiných způsobů, které stanoví právní předpis.

První čtyři způsoby jsou upraveny příslušnými zákony eGovernmentu. Tyto zákony určovaly povinnost orgánů veřejné moci přijímat úkony za stanovených podmínek již před přijetím ZPDS. Po jeho přijetí je nutné původní povinnosti považovat za provedení práva činit digitální úkon podle § 4 odst. 1 ZPDS. Z tohoto pohledu nedochází k významné změně, ale pouze ke zobecnění stávajících povinností a práv.

Ke drobné změně dochází v případě úkonů činěných prostřednictvím informačních systémů veřejné správy veřejné správy podle § 4 odst. 1 písm. d) ZPDS. Jde o vyjádření

obecného požadavku u každého digitálního úkonu provést elektronickou identifikaci a autorizaci uživatele a zaznamenat projev vůle, kterým uživatel úkon činí pro účely jeho zpětného prokázání. Při splnění tohoto požadavku se podle ZISVS považuje úkon za podepsaný. Fikce podpisu má původ ve změnovém zákonu DEPO.

Příkladem jiného způsobu činění digitálních úkonů, který stanoví právní předpis, je dříve rozebíraný přístup se zaručenou identitou podle ZISVS, který má uplatnění například v Portálu občana²¹².

§ 4 odst. 2 ZPDS pak rozšiřuje právo činit digitální úkon i na úkony, které sice nesplňují formální definici digitálního úkonu v § 2 odst. 3 ZPDS, ale u kterých jiný právní předpis nestanovil konkrétní způsoby činění úkonu. I takové úkony bude uživatel služby oprávněn činit vůči orgánům veřejné moci kterýmkoliv z prvních čtyř uvedených způsobů.

V § 14 odst. 5 ZPDS je řešena situace, kdy po 1. únoru 2025 nebude některý úkon evidován v katalogu služeb a povaha úkonu digitalizaci nevylučuje. V takovém případě bude mít orgán veřejné moci povinnost poskytovat službu digitálně vždy pokud to nebude v rozporu s povahou úkonu. Jde tedy o další rozšíření pojmu digitální úkon. Vzhledem k použití neurčitého slovního spojení „úkon, jehož povaha to nevylučuje“, lze očekávat po zmíněném datu nejistotu, zda některé úkony jsou digitální nebo ne.

Uživatelé se budou moci na základě tohoto ustanovení domáhat prostřednictvím správního soudnictví svého práva činit konkrétní digitální úkon, pokud budou tvrdit, že povaha úkonu nevylučuje digitální úkon. Správní soud toto posoudí jako právní otázku. Je těžké nyní předjímat, zda budou uživatelé služeb ochotni se s orgány veřejné moci soudit, nebo kvůli své právní jistotě raději upřednostní nedigitální způsob činění úkonu.

4.7.7 Digitální úkon jako volba

ZPDS nestanovuje obecnou přednost poskytování digitálních služeb ani činění digitálních úkonů před jejich nedigitálními alternativami. Podle § 14 odst. 1 ZPDS nesmějí být fyzické osoby povinny využívat digitální služby nebo činit digitální úkony. A contrario může být taková povinnost stanovena právnícké nebo fyzické podnikající osobě.

Uvedené ustanovení považuji za proklamativní, neboť využívání digitálních služeb a činění digitálních úkonů je již podle § 3 odst. 1 a § 4 odst. 1 a 2 ZPDS pro každého právem a nikoliv povinností. Také se může stát, že zvláštní zákon i přes zákaz v § 14 odst. 1 ZPDS

²¹² Tento způsob zakotvuje jako jeden z možných ustanovení § 6g odst. 3 ZISVS.

stanoví povinnost činit určitý digitální úkon fyzické osobě. Taková povinnost by byla podle mého názoru i přes uvedený zákaz vymahatelná, neboť by tím došlo k implicitní derogaci zákazu z pozice *lex specialis*.

V současném právním řádu je příkladem mandatorního digitálního úkonu povinnost některých nefyzických osob podávat elektronicky veškerá podání podle daňového řádu²¹³. Mimo daňovou oblast je takovým příkladem povinnost zaměstnavatele předkládat elektronicky evidenční listy důchodového pojištění České správě sociálního zabezpečení²¹⁴.

4.7.8 Katalog služeb

Katalog služeb je novým nástrojem zavedeným ZPDS, který by měl napomáhat procesu digitalizace služeb veřejné správy. Nejprve vysvětlím, co přesně se v tomto katalogu eviduje a následně se zamyslím nad významem tohoto katalogu pro další rozvoj eGovernmentu.

4.7.8.1 Obsah katalogu služeb

Podle § 2 odst. 4 ZPDS je katalogem služeb část údajů rozšiřující stávající evidenci registru práv a povinností. Jeho účelem je shromáždit údaje o všech službách a úkonech, které orgány veřejné moci poskytují či přijímají při výkonu veřejné moci. Mělo by se tedy jednat o úplný seznam:

- úkonů, které jsou oprávněny v rámci své agendy vykonávat orgány veřejné moci vůči jiným subjektům;
- úkonů jiných subjektů, které mohou být činěny osobami vůči orgánům veřejné moci.

Celkově je v katalogu služeb k 8. červnu 2022 evidováno 28 143 úkonů přiřazených k 6 709 službám ve 388 agendách. 94 % úkonů je označeno jako digitální²¹⁵.

U každého jednotlivého úkonu, který je evidován v rámci ohlášené agendy, je ohlašovatel povinen vyplnit několik atributů, které mají zásadní význam pro poznání tuzemského stavu eGovernmentu. Jsou jimi atributy, zda je již úkon digitální a zda je úkon

²¹³ Tato povinnost podle § 72 odst. 6 daňového řádu se týká osob, které mají zpřístupněnu datovou schránku ze zákona nebo mají ze zákona povinnost nechat účetní závěrku ověřit auditorem. Sankcí za nedodržení elektronické formy není neúčinnost nebo odmítnutí podání, ale dříve zmíněná elektropokuta podle § 247a odst. 2 daňového řádu.

²¹⁴ § 39 odst. 1 zákona č. 582/1991 Sb., České národní rady o organizaci a provádění sociálního zabezpečení.

²¹⁵ NAKIT, MINISTERSTVO VNITRA. Katalog služeb veřejné správy [Power BI Dashboard]. [cca 2022, cit. 8.6.2022]. Dostupné z: <https://app.powerbi.com/view?r=eyJrIjoiZTc3MDcwMWUtNTdkMC00NTM2LWI5MktMGJlNTQ5ODg2NWZjZlwiidCI6IjFkYjQxZDZmLTZmMzctNDZkYi1iZDNiLWM0ODNhYmI4MTA1ZCIslmMiOjh9>.

vhodný pro digitalizaci. Pokud je vhodný, musí být uvedeno, do kdy bude digitalizován. Pokud vhodný není, musí být uveden důvod. Zároveň jsou u každého úkonu evidovány existující i plánové obslužné kanály, což jsou konkrétní způsoby, kterými je nebo bude úkon poskytován. Z Katalogu služeb lze tedy přehledně zjistit, které úkony jsou poskytovány osobně nebo distančně pomocí datové schránky, dokumentu s uznávaným elektronickým podpisem nebo jinou formou dálkového přístupu.

Výše uvedené osvětlím na případu konkrétní ohlášené agendy občanských průkazů²¹⁶. V rámci této agendy je evidováno 21 konkrétních služeb veřejné správy vycházejících z agendového zákona o občanských průkazech.

Jednou z těchto služeb je vydání občanského průkazu. Tato služba se skládá ze dvou úkonů. Prvním je podání žádosti o vydání občanského průkazu, který činní žadatel vůči orgánu veřejné moci. Podání žádosti není digitální. Je poznamenána nevhodnost digitalizace z důvodu nezbytnosti osobní přítomnosti žadatele, kvůli pořízení jeho biometrických údajů. Ani následné předání občanského průkazu, což je úkon, který činní orgán veřejné moci vůči žadateli, není vhodný pro digitalizaci, neboť z agendového zákona vyplývá povinnost předat žadateli vyhotovený průkaz ve formě plastové karty osobně. Z toho vyplývá, že tato služba není vůbec digitální.

V této agendě je příkladem plně digitální služby poskytování údajů z evidence občanských průkazů jeho držitelů. Začáteční úkon v podobě podání žádosti vůči příslušnému orgánu veřejné moci je možné učinit jak osobně a poštou, tak i s pomocí datové schránky či dokumentu s uznávaným elektronickým podpisem. Do budoucna je plánováno umožnit podání žádosti i s pomocí samoobslužného portálu. Koncový úkon, který spočívá v poskytnutí údajů, může být proveden osobně, poštou nebo prostřednictvím datové schránky.

Přesto je téměř celá agenda v podstatě nedigitální. Možnosti digitalizování procesu vydání, odevzdání a zadržení občanského průkazu jsou závislé především na hmotné povaze občanských průkazů a požadavku pořízení biometrických údajů žadatele. Do budoucna se v ČR zamýšlí možnost alternativního prokazování se namísto plastové kartičky mobilní aplikací eDokladovka²¹⁷. To však nepovede ke změně u stávajících úkonů, neboť plastová kartička pravděpodobně zůstane zachována ve stejné podobě i do budoucna.

²¹⁶ VNITRA. Agenda Občanské průkazy (Kód A117) In: *Registr práv a povinností* [tabulky]. 2022 [cit. 20.6.2022]. Dostupné z: https://rpp-ais.egon.gov.cz/gen/agendy-detail/A117_10022022.xlsx.

²¹⁷ VLÁDA ČR. *Programové prohlášení vlády Petra Fialy* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://vlada.cz/cz/programove-prohlaseni-vlady-193547/>.

Důvody nevhodnosti digitalizace, které ohlašovatelé agendy uvádí v katalogu služeb, jsou relativně významné. Orgány veřejné moci s jejich pomocí totiž proklamují, že nemají povinnost některé úkony poskytovat digitálně. Údaj, zda je úkon vhodný k digitalizaci, je každý ohlašovatel agendy povinen udržovat aktuální a správný stejně jako jiné referenční údaje v Registru práv a povinností²¹⁸. V důsledku těchto výhrad se podle doslovného výkladu § 2 odst. 2 a 3 ZPDS nejedná ani o digitální službu a ani digitální úkon, protože v katalogu služeb nejsou vedeny jako úkony v elektronické podobě.

Některé výhrady nevhodnosti digitalizace považují u některých úkonů za problematické. Příkladem je povinnost uhradit osobně správní poplatek pomocí kolku²¹⁹ nebo osobně nahlédnout do spisu. V obou typech případů zní důvod nevhodnosti v podstatě stejně: zákon to neumožňuje. Přičemž objektivních důvodů, proč vůbec neumožnit nahlížení elektronicky třeba i za odpovídající poplatek, příliš není. I proto existuje rozdílný přístup napříč veřejnou správou. Přičemž nahlížení do spisu aktuálně většina orgánů veřejné moci považuje za úkon vhodný k digitalizaci²²⁰.

4.7.8.2 Zastoupení obslužných kanálů

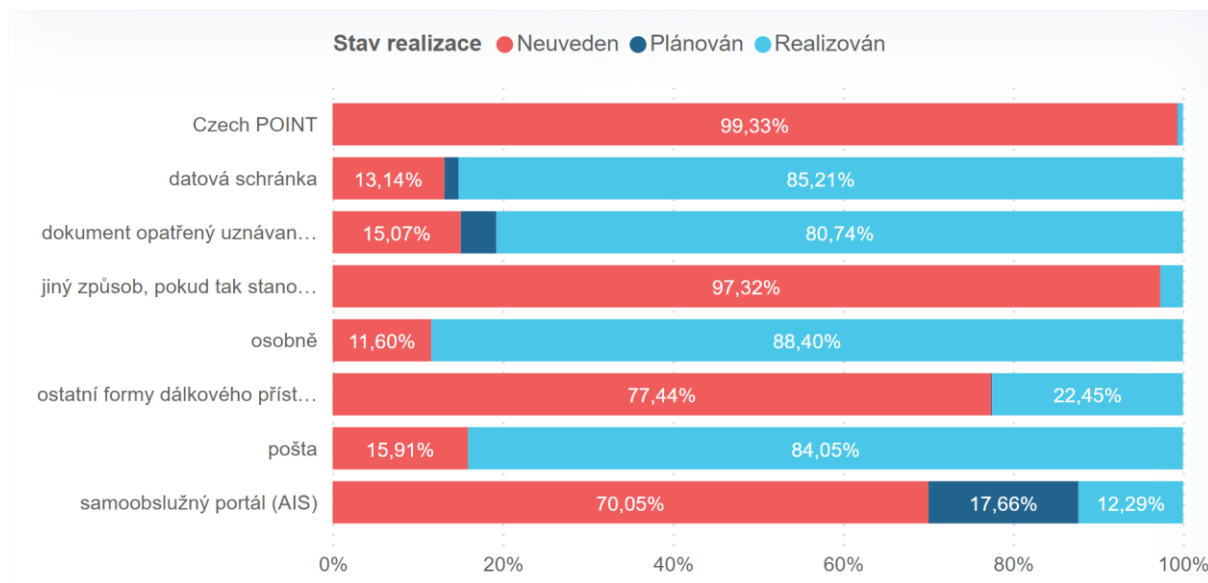
Katalog služeb nyní umožňuje nahlédnout, jak zásadně se liší dostupné obslužné kanály pro úkony, které činní orgány veřejné moci a pro úkony které činní jiné subjekty vůči těmto orgánům.

²¹⁸ MINISTERSTVO VNITRA. *Metodika pro evidenci služeb VS, jejich úkonů a plánu digitalizace* [online]. 2020, s. 2 [cit. 20.6.2022]. Dostupné z: <https://pma3.gov.cz/uploads/doc/Methodika-pro-evidenci-sluzeb.pdf>.

²¹⁹ Například:

MINISTERSTVO VNITRA. Agenda cizinecká a ochrany státních hranic (Kód A116): Úkon správního poplatku (Kód U7583). In: *Registr práv a povinností* [tabulky]. 2021 [cit. 20.6.2022]. Dostupné z: https://rpp-ais.ezon.gov.cz/gen/agendy-detail/A116_23012021.xlsx.

²²⁰ NAKIT, pozn. 215.



Graf č. 5: Obslužné kanály všech úkonů v katalogu služeb, které činí jiné subjekty vůči orgánům veřejné moci²²¹.

Ze srovnání zastoupení obslužných kanálů u všech úkonů, které činí jiné subjekty vůči orgánům veřejné moci, vyplývá, že nejvíce úkonů (88 %) je stále možné činit osobně. Ostatní úkony (12 %) se činí některým z distančních nebo jiných kanálů. Bez ohledu na to, zda je možné úkon činit osobně, přes 80 % úkonů lze učinit distančně poštou nebo s pomocí datové schránky či dokumentu s uznávaným elektronickým podpisem. U dvou posledně zmíněných obslužných kanálů by mělo jejich zastoupení do roku 2025 dále narůst o několik jednotek procent. Z toho lze na základě současné relativně vysoké hodnoty usuzovat, že povinnost orgánů veřejné moci přijímat takovéto digitální úkony těmito způsoby se v praxi již prosadila v široké míře. U očekávaného budoucího nárůstu, však nenacházím jakékoli indicie nasvědčující, že by se mělo jednat o důsledek nově přiznaných digitálních práv v ZPDS.

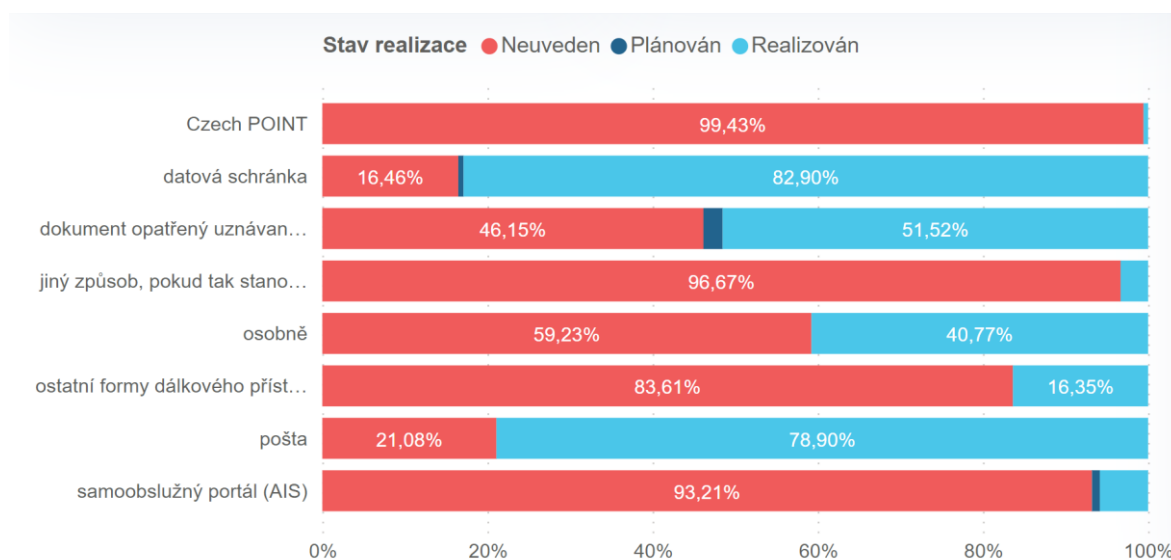
Mnohem zásadnější nárůst je očekáván u samoobslužných portálů. Do roku 2025 by se počet tímto způsobem dostupných úkonů měl více než zdvojnásobit. Jde o velmi výrazný trend, který má potenciál do digitální komunikace s veřejnou správou zapojit i osoby, které z různých důvodů nechtějí komunikovat prostřednictvím dokumentů s uznávaným elektronickým podpisem nebo prostřednictvím datových schránek. Navíc portály mohou při správném provedení být pro uživatele služeb konformnější a uživatelsky přívětivější v porovnání s datovými schránkami.

²²¹ Tamtéž.

Asistované univerzální kontaktní místo Czech POINT lze využít pouze pro marginální počet úkonů. Přesto jsou pobočky Czech POINT stále relevantní a jen během roku 2021 poskytly uživatelům téměř sedm set tisíc výpisů z trestního rejstříku²²².

Diskutované hodnoty je třeba interpretovat s ohledem na to, že nereflktují významnost, náročnost ani četnost činění jednotlivých úkonů.

Při srovnání zastoupení obslužných kanálů u úkonů, které činí orgány veřejné moci, lze vyčíst, že nejčastěji jsou úkony činěny poštou nebo datovými schránkami. To odpovídá způsobu doručování stanoveném v § 19 a násl. správního řádu. Ze stejného důvodu není u většiny úkonů uvedena možnost realizovat úkon osobně.



Graf č. 6: Obslužné kanály všech úkonů v katalogu služeb, které činí orgány veřejné moci při výkonu své působnosti²²³.

4.7.8.3 Význam katalogu služeb

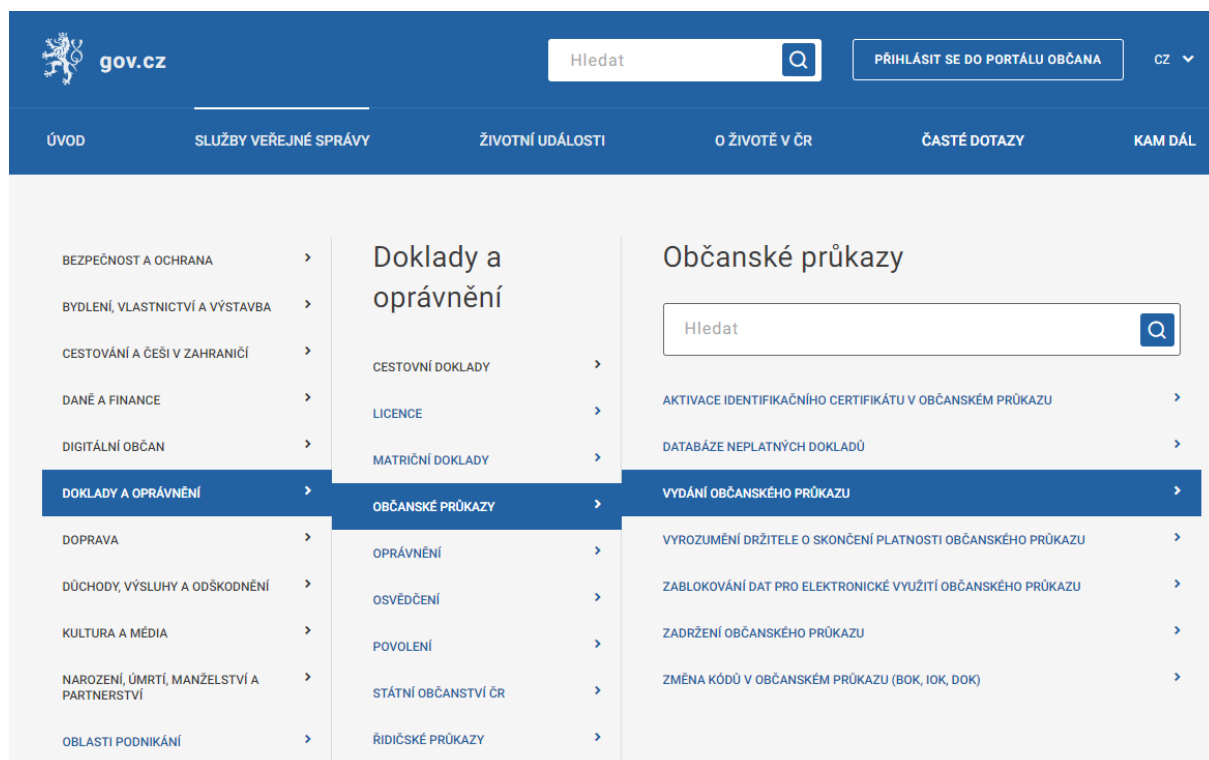
Katalog služeb má definiční význam pro většinu digitálních služeb a úkonů. Jejich evidování v katalogu služeb jako úkon v elektronické podobě je totiž jejich formálním předpokladem. Jiné než evidované úkony mohou být digitální jen při rozšíření pojmu digitální úkon podle § 4 odst. 2 a § 14 odst. 5 ZPDS

Další významy má katalog služeb jako celek. První z nich je informační význam. Před naplněním katalogu služeb nebyly centrálně shromážděny informace o tom, jakými obslužnými kanály jsou veřejné služby poskytovány a zda jsou nebo mohou být zdigitalizovány. Takto

²²² MINISTERSTVO VNITRA. Statistiky Czech POINT. In: *Czechpoint.cz* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://czechpoint.cz/public/statistiky-a-informace/statistiky-czp/>.

²²³ NAKIT, pozn. 215.

shromážděné informace mohou přinášet užitek i potenciálním uživatelům služeb. Příkladem je uživatelsky přívětivé procházení seznamu služeb na Portálu občana²²⁴. Ohlašovatelé agend mají podle zákona o základních registrech povinnost doplnit jednotlivé úkony detailními popisky v souladu s vyhlášenou osnovou²²⁵. Podle osnovy mají popisky obsahovat pro uživatele užitečné informace jako například: co je nutné k úkonu doložit, jaké hrozí případně sankce nebo jaké je možné využít opravné prostředky. Podle zjištění EGovernment Benchmarku z roku 2021 tuto povinnost neplnilo 65 % ohlašovatelů²²⁶.



Obrázek č. 3: Procházení seznamu služeb veřejné správy na Portálu občana²²⁷.

Za mnohem významnější než nové popisky však považují, že bude díky evidovaným informacím možné vyhodnocovat stav a proces digitalizace na základě alespoň nějakých dat napříč celou veřejnou správou. Předpokladem dlouhodobé využitelnosti je plnění povinnosti ohlašovatelů agend průběžně aktualizovat a doplňovat informace v katalogu.

²²⁴ Dostupné z: <https://portal.gov.cz/sluzby-verejne-spravy/>.

²²⁵ Vyhláška č. 515/2020 Sb. o struktuře informací zveřejňovaných o povinném subjektu a o osnově popisu úkonů vykonávaných v rámci agendy.

²²⁶ DZURILLA, Vladimír, TÝM OHA MV. *ICT benchmark veřejné správy 2021: podkladová data* [tabulky]. Archi.gov.cz, 2022. Poslední změna: 21.1.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/_media/benchmark_2021_data_final.xlsx.

²²⁷ MINISTERSTVO VNITRA. Služby veřejné správy. In: *Portál veřejné správy* [online]. 2022, zjednodušeno [cit. 20.6.2022]. Dostupné z: <https://portal.gov.cz/sluzby-verejne-spravy/>.

V souvislosti s katalogem služeb vznikl a průběžně se aktualizuje harmonogram digitalizace veřejné správy. Další aktualizace harmonogramu by měla být předložena vládě do poloviny listopadu 2022²²⁸. Podle stavu plnění harmonogramu k 8. červnu 2022 by mělo být do roku 2025 umožněno pomocí samoobslužných portálů činit dalších 2 399 úkonů²²⁹. V drtivě většině půjde o úkony, které jsou činěny vůči orgánům veřejné správy a které již alespoň jeden z digitálních obslužných kanálů nabízí.

Pokud však termín zůstane stejný, a přesto orgány veřejné moci plánované úkony na portálech včas nezpřístupní, mohlo by jít o porušení práv uživatelů služeb činit digitální úkon prostřednictvím informačních systémů veřejné správy podle § 4 odst. 1 písm. d) ZPDS. Zde pak nastane otázka, zda nepostačí orgánu veřejné moci namítnout, že z konkrétních objektivních příčin nebyl schopen portál včas dokončit popřípadě rozšířit o další digitální úkony.

4.7.9 Další práva související s digitálními úkony

Při činění digitálního úkonu jsou uživatelé služby a orgán veřejné moci ve fakticky nerovném informačním postavení. Orgán veřejné moci disponuje logy a dalšími informacemi z informačních systémů, které při zpracování digitálního úkonu využívá. S výraznou nerovností se uživatelé služeb musejí potýkat například u úkonů činěných prostřednictvím samoobslužných portálů, kde orgán veřejné moci má navrch, protože je zpravidla i provozovatelem tohoto portálu a má kompletní informace o chování uživatele, zatímco od uživatele služeb nelze očekávat, že by si činění svých digitálních úkonů zaznamenával způsobem umožňujícím jeho pozdější prokázání. Vyrovnanější je toto postavení u zasílání datových správ, kde uživatel služby disponuje doručenkou.

Tato nerovnost se může výrazně projevit zejména ve sporu, zda a kdy byl konkrétní digitální úkon učiněn. Proto § 5 ZPDS stanovuje uživatelům služeb právo na osvědčení digitálního úkonu. Osvědčení je veřejnou listinou v souladu s § 53 odst. 3 správního řádu, což ulehčí důkazní situaci uživatelům služeb.

Orgány veřejné moci, které jsou veřejnoprávními původci podle zákona o archivnictví a spisové službě, mají povinnost osvědčení poskytovat automaticky po přijetí digitálního

²²⁸ Usnesení vlády ČR č. 826/2021 k aktualizovanému harmonogramu a technickým způsobům provedení digitalizace služeb veřejné správy na období 2021 – 2025.

²²⁹ NAKIT, pozn. 215.

úkonu. Ostatní orgány veřejné správy jako například notáři vystaví osvědčení na žádost. Pro podání žádosti zákon nestanovuje konkrétní lhůtu.

Podle § 4 odst. 3 ZPDS má uživatel služby právo činit digitální úkon v několika různých datových formátech, pokud orgán veřejné moci nezveřejní elektronický formulář pro daný úkon. Blíže se tomuto právu budu věnovat v souvislosti s vymahatelností digitálních práv.

Některá ustanovení, která jsou v ZPDS uvozena: „uživatel služby má právo“, nestanovují žádná nová práva, ale spíše jen určují požadavky pro výkon stávajících práv a povinností. Příkladem je ustanovení § 12 ZPDS, které určuje výchozí minimální úroveň záruky prostředku pro elektronickou identifikaci na úroveň značná.

4.7.10 Právo na sdílení vedených údajů

Princip pouze jednou je od roku 2010 realizován pomocí povinnosti orgánů veřejné moci využívat při své činnosti ve stanoveném rozsahu referenční údaje vedené v příslušném základním registru. Nesouhlasím proto s tvrzením autorů komentáře, že „do účinnosti komentovaného ustanovení nebyla zákonem stanovena povinnost využívat tyto údaje namísto jejich opětovného vyžadování od dotčených osob“²³⁰. Pokud orgány veřejné moci vyžadovaly po osobách referenční údaje, přestože je byly oprávněny využívat, postupovaly v rozporu s tehdejším zněním § 5 zákona o základních registrech.

Nová právní úprava podstatně rozšiřuje množství údajů, které lze sdílet, a mění způsob nabytí právního titulu k jejich využívání a způsob stanovení jejich rozsahu. Dohromady se jedná o nejzásadnější změnu základních principů sdílení údajů mezi orgány veřejné moci od spuštění základních registrů. Podstata změn je zřetelná v ustanovení § 7 odst. 1 ZPDS, který zakazuje všem orgánům veřejné moci požadovat údaje vedené v základních registrech anebo v agendových informačních systémech (AIS), ke kterým mají přístup.

Sdílené budou nyní stejným způsobem nejen referenční údaje v základních registrech, ale i agendové údaje v AIS. Těch v roce 2019 NKÚ napočítal celkem 4 658²³¹. Agendové i referenční údaje tvoří dohromady propojený datový fond, ke kterému orgány veřejné moci přistupují pomocí svých AIS²³².

²³⁰ DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. § 7 Právo na využívání údajů. In: ZAJÍČEK. pozn. 156, s. 95–96.

²³¹ NKÚ. *Souhrnná zpráva o digitalizaci veřejné správy v ČR* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://nku.cz/assets/publikace-a-dokumenty/ostatni-publikace/zprava-o-digitalizaci-verejne-spravy.pdf>.

²³² Podrobnosti o propojeného datového fondu popisuje Národní architektonický plán. Součástí je i názorné grafické znázornění procesu sdílení údajů. Dostupné z: https://archi.gov.cz/nap:propojeny_datovy_fond.

Rozšíření množství údajů, které lze sdílet, promítl zákonodárce prostřednictvím změnových ustanovení ZPDS i do zákona o základních registrech. Část úpravy je proto společná pro referenční i agendové údaje. Ani u agendových údajů čerpající orgán veřejné moci není povinen ověřovat jejich správnost. Stejně jako u referenčních údajů jsou i taxativně stanovené důvody, kdy může orgán namísto využití sdílených údajů požadovat údaje od osob, které by jinak byly povinny údaje doložit. Zásadním důvodem je situace, kdy sdílené údaje nejsou uvedeny ve výčtu zpřístupněných údajů pro výkon agendy určitého orgánu veřejné moci, který je v souladu se zákazem § 7 odst. 1 ZPDS.

Podle staré právní úpravy byl přístup k agendovým údajům rozdílný podle toho, zda byl AIS zřízen zákonem, nebo ne. Právní titul pro čerpání údajů z AIS zřízených ze zákona nabývaly orgány veřejné moci rovněž ze zákona. Tento způsob vyžadoval, aby do agendových zákonů bylo inkorporováno množství zákonných výčtů údajů, ke kterým byl určitý orgán veřejné moci oprávněn přistupovat. Stejný způsob byl vyžadován i pro přístup k referenčním údajům v základních registrech.

Jak uvádí důvodová zpráva²³³ k DEPO zákonu, tento způsob byl ve světě ojedinělý. Vyznačoval se na jednu stranu vysokou transparentností, na druhou stranu však značnou rigidností, kdy nejdrobnější změna v zákonném výčtu údajů musela být provedena novelou zákona. Pro čerpání údajů z jiných AIS, které nevznikly zákonem, byl právní titul často nejasný. V některých případech byl odvozován od působnosti činit konkrétní úkon, jindy od obecných zásad spolupráce podle § 8 správního řádu. V důsledku těchto nejasností pak v praxi záleželo na subjektivním posouzení správců AIS.

Podle nové právní úpravy získá orgán veřejné moci přístup k vedeným údajům na základě jednoho ze dvou právních titulů. Prvním je registrace výkonu ohlášené agendy v Registru práv a povinností a druhým je souhlas uživatele služby.

Registrace výkonu ohlášené agendy podle zákona o základních registrech představuje přesně vymezený postup a také flexibilnější způsob určení rozsahu než dosavadní zákonné výčty. Orgán veřejné moci musí při registraci uvést k jaké činnosti údaje potřebuje. Transparentnost je zachována za pomoci veřejně zpřístupněných detailů agend včetně seznamu

²³³ VLÁDA ČR. Sněmovní tisk 756/0: Návrh zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci včetně důvodové zprávy. In: *Psp.cz* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=756>.

jednotlivých oprávnění k využívání referenčních a agendových údajů²³⁴. Registr práv a povinností se díky nové úpravě stává ještě významnějším nástrojem eGovernmentu.

Zrušení nezbytnosti uvádět v zákoně výčty údajů si vyžádalo změnu více než 140 agendových zákonů. Tuto změnu provedl zákon DEPO se shodně stanovenou účinností na 1. února 2022 jako u zbytku nové úpravy sdílení údajů v ZPDS a zákoně o základních registrech. V některých případech výčty z právního řádu zcela nevymizí. Například, pokud vedené údaje má využívat soukromoprávní uživatel údajů²³⁵ jako třeba poskytovatel bankovní identity.

Novinkou, kterou přinesl ZPDS, je oprávnění čerpat vedené údaje na základě souhlasu uživatelů služeb²³⁶. Přičemž musí jít o evidované údaje o osobě uživatele služby, o jejich právech či povinnostech nebo o právních skutečnostech, které se jí týkají. Rozsah a trvání souhlasu bude zpravidla vycházet ze žádosti orgánu veřejné moci, se kterou uživatel služby vyjádřil souhlas.

4.7.11 Další práva související s vedenými údaji

ZPDS stanovením několika souvisejících práv dále rozšiřuje a prohlubuje zákonnou realizaci univerzálního principu eGovernmentu pouze jednou. Vzhledem k množství nových práv je třídím do třech různých skupin.

Práva vycházející vyloženě z principu pouze jednou:

- Právo uživatele služby prokázat nebo osvědčit právní skutečnost odkazem na vedené údaje²³⁷, ke kterým má orgánu veřejné moci přístup, nebo původním elektronickým výpisem z informačního systému veřejné správy (§ 9 odst. 1 ZPDS);
- Právo uživatele služby namítnout, že není povinen předkládat rozhodnutí, doklad, průkaz nebo osvědčení, protože údaje o těchto skutečnostech jsou vedeny a orgán veřejné moci k nim má přístup (§ 9 odst. 2 písm. a ZPDS);

Práva rozšiřující množinu evidovaných údajů z vůle uživatele služby:

²³⁴ ŠEDIVÉC, pozn. 91.

²³⁵ § 5a zákona o základních registrech.

²³⁶ Detailní právní rozbor souhlasu k čerpání vedených dat je součástí komentáře:

DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. § 7 Právo na využívání údajů. In: ZAJÍČEK. pozn. 156, s. 96 a násl.

²³⁷ Připomínám, že vedenými údaji zkráceně označuji údaje vedené v základních registrech a AIS.

- Právo uživatele služby nechat si zapsat do Registru práv a povinností své údaje, které vyplývají z úkonu orgánu veřejné moci uvedeného v katalogu služeb a které dosud nejsou vedeny (§ 8 odst. 1 ZPDS);
- Právo uživatele služby nechat si zapsat kontaktní údaje, kterým je telefonní číslo a email, do základních registrů (§ 10 odst. 2 ZPDS);

Práva na informace související s vedenými údaji:

- Právo uživatele služby na přístup ke všem o něm vedeným údajům prostřednictvím Portálu občana (§ 11 odst. 1 ZPDS);
- Právo uživatele služby být upozorněn na změnu údajů vedených o jeho osobě nebo o jeho právech a povinnostech (§ 11 odst. 1 ZPDS);
- Právo uživatele služby být upozorněn na končící platnost některých průkazů a dokladů (§ 11 odst. 2 ZPDS).

Princip pouze jednou promítl změnové ustanovení § 18 ZPDS i do zásady správní činnosti v § 6 odst. 2 správního řádu. Ten v souladu s § 7 ZPDS rozšířil povinnost správních orgánů využívat primárně údaje z vlastní evidence na všechny vedené údaje, ke kterým má správní orgán přístup.

4.7.12 Vymahatelnost digitálních práv

„Chceme-li skutečně skokovou změnu v používání digitálních služeb (...), je nezbytné posílit práva občanů na digitální služby a nastavit právo na poskytnutí digitálních služeb včetně vymahatelnosti u soudu. (...) Zákony již spoustu povinností úřadům stanovují, ale nejsou vymahatelné a ani neexistuje způsob jak sankcionovat jejich nedodržení. (...) Jediné řešení je vytvořit tlak na státní instituce ze strany uživatelů digitálních služeb, tedy občanů“²³⁸ prohlásila ICT unie během přípravy ZPDS.

ZPDS však neobsahuje žádnou zvláštní úpravu sankcionování orgánů veřejné moci za nesplnění jejich povinností. Tento zákon neupravuje ani žádný zvláštní procesní postup, ve kterém by se mohl uživatel služeb svých digitálních práv domoci. Přesto by vymahatelnost stanovených práv a povinností měla být dle tvůrců zákona silnou stránkou nově přijaté úpravy. Nabízí se však otázka, zda tomu tak skutečně je a jaké konkrétní způsoby obrany může uživatel digitálních služeb využít.

²³⁸ ICT UNIE, pozn. 198.

4.7.12.1 Vymahatelnost neposkytnutí digitální služby

Nejprve se zamyslím nad situací, kdy je orgán veřejné moci povinen na základě § 3 ZPDS poskytnout uživateli konkrétní digitální službu, ale neučiní tak. K této situaci dochází buď faktickou nečinností anebo nesprávným rozhodnutím orgánu veřejné moci, pokud se vydává. Důsledkem je porušení subjektivní veřejné povinnosti orgánu veřejné moci, který měl digitální službu poskytnout. Zároveň je zasaženo do subjektivního veřejného práva uživatele. V této situaci je žádoucí, aby se uživatel mohl zaprvé domoci poskytnutí nerealizované digitální služby a zadruhé případné náhrady způsobené škody.

Uživatel služby má možnost domáhat se poskytnutí digitální služby pomocí právní ochrany ve správním soudnictví. Postup a žaloba se bude lišit podle toho, zda bylo vydáno správní rozhodnutí nebo nikoliv. Pokud bylo vydáno rozhodnutí ve správním řízení, je nezbytné před podáním žaloby proti rozhodnutí vyčerpat řádné opravné prostředky. V případě, že žádné žalovatelné rozhodnutí vydáno nebylo, lze podat žalobu proti nezákonnému zásahu.

Uživatel služby, do jehož práva bylo zasaženo a v souvislosti s tím mu vznikla škoda, která představuje odškodnitelnou majetkovou újmu, se může domáhat náhrady škody podle zákona o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem. O škodě bude rozhodovat příslušné ministerstvo nebo jiný ústřední správní úřad, v jehož odvětví působí orgán při jehož výkonu pravomoci škoda vznikla. Pokud bude uživateli v rozporu s § 3 ZPDS odepřeno poskytnutí digitální služby například v Portálu farmáře, bude příslušným k rozhodování ministerstvo zemědělství, protože portál slouží k výkonu moci v působnosti tohoto ministerstva.

Nesprávný úřední postup vymezuje teorie jako „*porušení pravidel předepsaných právními normami pro počínání státního orgánu při jeho činnosti, a to zejména takové, které nevede k vydání rozhodnutí*“²³⁹. Vzhledem k tomu, že zpravidla poskytování digitálních služeb nevyžaduje rozhodnutí orgánu veřejné moci, lze předpokládat, že výše popsaná forma odpovědnosti bude častější.

²³⁹ VOJTEK, Petr. § 13 [Nesprávný úřední postup státu]. In: VOJTEK, Petr, BÍČÁK, Vít. *Odpovědnost za škodu při výkonu veřejné moci*. 4. vydání. Praha: C.H. Beck, 2017, s. 147, marg. č. 1. ISBN: 978-80-7400-670-8.

4.7.12.2 Úvaha nad vymahatelností digitálních práv obecně

Pavel Mates označuje vymahatelnost práv za možnou Achillovu patu celého ZPDS²⁴⁰. S tímto názorem souzním. Navíc očekávám, že případné soudní spory nastanou pouze v situacích, kdy neposkytnutí digitální služby nebo neakceptování digitálního úkonu bude mít právní následky přesahující oblast eGovernmentu.

Na rozdíl od ICT Unie nepředpokládám, že projednání takových sporů ve správním soudnictví vytvoří významnější tlak na státní instituce ze strany uživatelů digitálních služeb. Hlavně proto, že nic nenasvědčuje tomu, že by mělo k nějakých významným sporům docházet. Přičemž vycházím ze zkušenosti, kterou jsem získal při seznámení se s judikaturou týkající se problematiky datových schránek a elektronických podpisů. V této souvislosti řešily tuzemské soudy především spory, kdy v důsledku porušení povinnosti orgánu veřejné moci bylo znemožněno uplatnit jiné procesní nebo hmotné právo žalobce. Příkladem jsou spory o okamžik, kdy je řádně učiněno podání zaslané emailem, kterými jsem se zabýval u výkladu o elektronických podpisech. Přestože tyto spory mají význam nejen pro adresáty rozhodnutí, ale i pro právní jistotu dalších uživatelů služeb, nezdá se, že by tato rozhodnutí byla zásadním tlakem na rozvoj eGovernmentu.

Vzhledem k tomu, že se jedná o novou úpravu, nelze vyloučit, že práva obsažená v ZPDS budou přeci jenom významně dotvořena činností soudů. Znění zákona k tomu ostatně samo vybízí použitím některých neurčitých pojmů. Například již zmíněné sousloví „*povaha to nevylučuje*“ nebo sousloví „*nepřiměřeně ekonomicky náročné*“ v § 13 odst. 1 ZPDS.

Obdobné závěry je zpravidla možné vztáhnout i na další digitální práva jako například právo činit digitální úkon nebo právo na technologickou neutralitu. Zásadní bude u každého práva volba odpovídajícího právního prostředku obrany uživatele služby.

Nad realizací a vymáháním jednotlivých digitálních práv se zamýšlel Pavel Mates i v jiném svém textu²⁴¹. Mates přitom za překážku při vymáhání práv běžnými adresáty považuje i příliš odbornou terminologii, která je typická pro eGovernment zákony a které běžný adresát nerozumí.

²⁴⁰ MATES, Pavel. Právo na digitální služby. In: *Revue pro právo a technologie* [online]. 2020, 11(21), 87-88 [cit. 20.6.2022]. ISSN 1805-2797. DOI: [10.5817/RPT2020-1-4](https://doi.org/10.5817/RPT2020-1-4).

²⁴¹ MATES, Pavel. Otazníky nad realizací práva na digitální služby. In: *Právní rozhledy* [online]. 2021, 20, 711-715 [cit. 20.6.2022]. ISSN: 1805-2797. Dostupné z: <https://beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpax4s7giyf6427g4ytc>.

4.7.12.3 Ojedinělý příklad konkrétní sankce v ZPDS

Výjimečným případem, kdy ZPDS stanoví konkrétní sankci za porušení povinnosti orgánu veřejné moci, je ustanovení § 4 odst. 3 ZPDS. To stanovuje primární povinnost orgánu veřejné moci zveřejnit elektronické formuláře, do kterých se automaticky propisují vedené údaje, ke kterým má orgán přístup a které jsou nezbytné pro učinění úkonu uživatelem. Při porušení této povinnosti vzniká orgánu veřejné moci sekundární povinnost akceptovat digitální úkon v jakémkoliv datovém formátu podle zákona o archivnictví a spisové službě.

Charakter této sankce je zajímavý a lze si dobře představit její dopady. Zpracování elektronických formulářů je pro orgány veřejné moci typicky administrativně méně náročné než zpracování jiných neformulářových podání. S pomocí elektronických formulářů je možné vyplněné údaje využít jako strukturovaná data v příslušném informačním systému, který je zpravidla přizpůsobený k efektivnímu vyřizování dané agendy. Zatímco zpracování různých datových formátů je většinou podstatně administrativně náročnější. Namísto výkonu podstaty dané agendy budou do svých informačních systémů úředníci ručně přepisovat nestrukturovaná data z nejrůznějších datových formátů. Přičemž některé přípustné formáty jsou známým obtížným zpracováním jako například PDF dokumenty s chybějící či poškozenou textovou vrstvou nebo obrázky zachycující obtížně čitelný text psaný rukou.

Tento nežádoucí stav zapříčiněný porušením primární povinnosti, by pro orgán veřejné moci měl být dostatečně motivující požadované elektronické formuláře vytvořit, propojit se svým informačním systémem a v souladu se zákonem zveřejnit uživatelům služeb. Problémem celé této sankční konstrukce je fakt, že nežádoucí stav může trvat neomezeně dlouho. Tlak na jeho nápravu se za dobu jeho trvání nemusí vůbec zvyšovat a v důsledku toho se nezavedou elektronické formuláře ani tam, kde by to bylo objektivně vhodné. Další nedostatek této sankce spatřuji v tom, že jde o tlak na nápravu nežádoucího stavu působí jen zevnitř veřejné moci, zatímco pro samotné uživatele může být nevýhodné nemít k dispozici snadno vyplnitelné a návodné elektronické formuláře bez možnosti domoci se nápravy.

De lege ferenda bych proto uvítal, aby orgán veřejné moci při zachování stávající podoby této sankce měl povinnost uvést v katalogu služeb důvod, proč elektronické formuláře nezveřejňuje a případně též jaké dopady má jejich nezveřejnění na uživatele služeb.

4.8 DEPO zákon

4.8.1 Specifika legislativního procesu

V případě DEPO zákona lze vysledovat dva zdroje původní iniciativy k přijetí tohoto změnového zákona.

Zprvé je jím legislativní činnost Ministerstva vnitra, které tímto zákonem zamýšlelo realizovat sliby obsažené v programovém prohlášení vlády a legislativní úpravy spojené s projektem Digitální Česko a obecně s dalším rozvojem eGovernmentu.

Za druhé jím byla paralelní aktivita skupiny poslanců a zmíněných lobbistických sdružení, která směřovala ke schválení ZPDS. Iniciativu formující výslednou podobu zákona DEPO vystihuje doprovodné usnesení č. 789 Poslanecké sněmovny k ZPDS vyzývající vládu, aby *„předložila návrh zákona (...) ve kterém navrhne zejména pravidla umožňující další rozšíření využití systému datových schránek, rozšíření a sdílení referenčních údajů v základních registrech, systematické využívání strojově čitelných formátů v rámci eGovernmentu a systematické využívání cloud computingu v oblasti veřejné správy“*²⁴².

Ještě než vláda předložila návrh DEPO zákona k projednání Poslanecké sněmovně, byla z něj vyňata řada významných změnových ustanovení týkajících se především sdílení údajů, které se později staly součástí poslaneckého návrhu ZPDS²⁴³. Vyňaté změny se týkaly jiných eGovernment zákonů jako například ZISVS, zákona o datových schránkách nebo zákona o základních registrech. V důsledku toho se jádrem změnového zákona staly změny, ke kterým Poslanecká sněmovna vyzvala vládu ve zmíněném usnesení.

Podoba návrhu, v jakém jej schválila vláda, doznala výrazných změn prostřednictvím poslaneckých pozměňovacích návrhů²⁴⁴. Výslednou podobu určily dva komplexní pozměňovací návrhy Výboru pro veřejnou správu a regionální rozvoj Poslanecké sněmovny

²⁴² POSLANECKÁ SNĚMOVNA. Doprovodné usnesení č. 789 ze dne 8. listopadu 2019 k návrhu na vydání ZPDS. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/text2.sqw?idd=164509>.

²⁴³ REDAKCE PRÁVNÍCH ROZHLEDŮ. Poslanecká sněmovna schválila návrh zákona upravujícího elektronizaci orgánů veřejné moci. In: *Právní rozhledy* [online]. 2021, č. 12, s. II-III [cit. 20.6.2022]. ISSN: 1805-2797. Dostupné z: <https://beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpaxa4s7gez6427nfuxayq>.

²⁴⁴ Podrobnosti o projednávání v Poslanecké sněmovně a jednotlivých pozměňovacích návrzích: POSLANECKÁ SNĚMOVNA. Sněmovní tisk 756. In: *Psp.cz* [online]. 2020 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/historie.sqw?o=8&t=756>.

a desítky pozměnovacích návrhů jednotlivých poslanců²⁴⁵ a nakonec i změny, které prosadil Senát.

4.8.2 Obsah zákona

Ve výsledku bych změny, které přináší DEPO zákon rozdělil na tři skupiny. První skupina jsou změny, které promítají do právního řádu principy nové právní úpravy v ZPDS, druhá skupina jsou změny, které modifikují tuzemský eGovernment nezávisle na ZPDS a třetí skupina jsou přílepký nesouvisící s eGovernmentem.

Příkladem takových přílepků jsou některé přijaté poslanecké pozměnovací návrhy. Mezi stovkami jiných změn lze nalézt například změnu advokátního zákona rozšiřující přestupky o nabízení právních služeb nebo prodloužení některých licencí pro rozhlasové a televizní vysílání²⁴⁶.

4.8.3 Změny promítající ZPDS

Nejzásadnější změnou, která tvoří podstatný obsah znění zákona, je bezpochyby zrušení jednotlivých zákonných výčtů v agendových zákonech opravňujících orgány veřejné moci čerpat údaje vedené v základních registrech a agendových informačních systémech. V souvislosti s tím zavádí pro předávání agendových údajů DEPO zákon úpravu čerpání vedených údajů soukromoprávními osobami a zcela nový informační systém sdílené služby.

4.8.4 Změny eGovernmentu

Na základě změny zákona o právu petičním je možné s pomocí portálu Občana vytvořit elektronickou petici a podepsat se pod ní s pomocí elektronické identifikace. Výrazné změny doznal i ZISVS. Poprvé je upraveno využívání cloudu ve veřejné správě. Vnitřní činnost veřejné správy ovlivní nový požadavek na atest elektronických systémů spisové služby. Mezi specifické novinky patří třeba změna regulace přístupu do centrálního registru zbraní.

Rozbor těchto změn je nad rámec této práce.

²⁴⁵ PETERKA, Jiří. Zprávy z Depa (1): Místo zmocnění v zákoně bude stačit jen zápis v registru. In: *Lupa.cz* [online]. Internet Info, 2021 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://lupa.cz/clanky/zpravy-z-depa-1-misto-zmocneni-v-zakone-bude-stacit-jen-zapis-v-registru/>.

²⁴⁶ REDAKCE PRÁVNÍHO ZPRAVODAJE. Další elektronizace veřejné správy (DEPO). In: *Právní zpravodaj* [online]. 2021, [cit. 20.6.2022]. Dostupné z: <https://beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpxa6s7ge2tq>.

Závěr

Digitalizace veřejné správy je velmi komplexní proces. Neexistuje žádná zaručená cesta k jeho završení. Cestu, kterou zvolila Česká republika, formovala zejména čtveřice původních projektů eGovernmentu, legislativa Evropské unie a činnost veřejné správy posledních dvaceti let.

Potřeba dalšího eGovernment zákona byla od počátku pochybná. Některé ambice vkládané do přijetí zákona o právu na digitální služby (ZPDS) nebyly naplněny. Slibovaná snadnější vymahatelnost digitálních práv je jen proklamovanou iluzí. ZPDS sice vyjasnil některá stávající digitální práva, avšak zároveň do právní úpravy eGovernmentu vnesl na jiných místech nové nejasnosti a pojmy, které je problematické jednoznačně vyložit.

Právo na digitální služby a právo na digitální úkon jsou v podstatě zobecněním dosavadní separátní úpravy jednotlivých způsobů digitální komunikace s veřejnou správou. Samotné jednoznačné přiznání těchto digitálních práv neznamená, že budou snadněji vymahatelná. Každý výkon těchto digitálních práv totiž musí být kromě ZPDS v souladu rovněž s eGovernment zákonem upravujícím způsob poskytování služby nebo činění úkonu, s agendovým zákonem, upravujícím konkrétní službu nebo úkon a případně též správním řádem, nebo jiným procesním předpisem. Dohromady tyto normy tvoří pro běžného uživatele služeb obtížně přehledný právní rámec plný specifické odborné terminologie. Navíc ZPDS v tomto ohledu neposkytuje uživatelům služeb žádné procesní ulehčení. Lze proto očekávat, že se běžní uživatelé služeb svých digitálních práv ve správním soudnictví spíše domáhat nebudou.

Za nejdůležitější přínos ZPDS považuji stanovení práva na technologickou neutralitu, které dosud upraveno vůbec nebylo, a zavedení registračního principu pro sdílení vedených údajů.

Registr práv a povinností se stal na úkor zákonodárné moci klíčovým flexibilní nástrojem registrace sdílených údajů z agendových informačních systémů. Jeho část označovaná jako katalog služeb plní funkci jedinečného přehledu digitalizovaných úkonů a dostupných obslužných kanálů napříč celou veřejnou správou. Posílením tohoto registru se posílilo i postavení jeho správce, Ministerstva vnitra, které je v současné době zároveň zodpovědné za koordinaci a koncepční plánování tuzemského eGovernmentu.

Dílčím přínosem jsou i nově definovaná práva související s digitálními úkony a s vedením údajů. Předpokladem je, že budou práva uživatelů realizována orgány veřejné správy dobrovolně. ZPDS nestanovuje až na jedinou velmi specifickou výjimku žádné faktické

sankce. Při porušení těchto digitálních práv je opět jediným nástrojem obrany odpovídající žaloba ve správním soudnictví.

Nová právní úprava nepřináší žádné přelomové změny. Jde pouze o částečnou evoluci realizující stále stejné principy. Tuzemský eGovernment je již delší dobu ve fázi konsolidace stávajících digitalizačních projektů. Výrazný nový projekt jako bankovní identita je spíše výjimkou, a i ten v zásadě pouze rozvíjí stávající možnosti elektronické identifikace.

Tuzemský eGovernment se i po přijetí nové právní úpravy potýká se stále stejnými problémy. V ČR je i nadále málo rozšířené proaktivní poskytování digitálních služeb. Nová právní úprava eGovernmentu se zaměřuje stejně jako dosavadní zákony na způsoby poskytování digitálních služeb, zatímco logika poskytování digitálních služeb zůstává pořád stejná. Podání žádosti občanem stále předchází poskytnutí digitální služby i v případech, kdy má veřejná správa k dispozici veškeré údaje, na jejichž základě by mohla digitální službu poskytnout automaticky.

Nově přijatá úprava nevyřeší ani stávající nedostatky veřejné správy v oblasti personální, řízení ICT ani v oblasti zadávání veřejných zakázek. Zásadní snaha o řešení těchto nedostatků, kterou by byla reforma veřejné správy, není ani předmětem současné politické diskuse. V dohledné době lze proto očekávat nanejvýš snahy o některá dílčí řešení. Příkladem může být aktuálně probíhající transformace koordinace a řízení digitalizace.

I přes výše uvedené nedostatky má ČR vybudovanou základní komunikační a technologickou infrastrukturu a funkční elektronické komunikační kanály, které umožňují existenci a budoucí rozvoj eGovernment.

Elektronická identifikace mezi populací je rozšířená a průběžně se navyšuje množství digitálních služeb, ke kterým ji lze využít. Nejčastějším místem, kde elektronickou identifikaci občan využije jsou samoobslužné portály veřejné správy. V této souvislosti však považují za velmi problematické automatické zřizování datových schránek fyzickým osobám při prvním použití prostředku elektronické identifikace, a to zejména kvůli povinnostem, které se pojí s datovými schránkami zřízenými ze zákona. Budoucí podobu elektronické identifikace může výrazně ovlivnit připravovaná novelizace nařízení eIDAS, která vychází z decentralizovaného pojetí elektronické identifikace, jenž není v souladu s jejím dosavadním centralizovaným pojetím.

Datové schránky zůstávají spolehlivým nástrojem elektronické komunikace jako plnohodnotná alternativa k doporučeným dopisům. Některé sporné otázky ohledně doručování datových správ pomohla vyjasnit činnost soudů.

Soudy nižších instancí v některých případech vykládaly normy související s elektronickými podpisy příliš formalisticky. Oproti tomu judikatura Nejvyššího soudu a Nejvyššího správního soudu je racionálnější a zohledňuje materiální hledisko elektronických institutů.

Současný právní řád poskytuje vhodný základ pro pokročilý eGovernment. Reálný stav eGovernmentu, který popisují indexy a benchmarky, svědčí o nedostatečném využití možností, které právní řád veřejné správě poskytuje. Je třeba mít na paměti, že na výslednou podobu celého eGovernmentu má zásadní vliv nejen přijatá legislativa, ale i množství vyčleněných finančních či technických prostředků, množství a kvalita lidského kapitálu a spousta dalších souvisejících faktorů.

Seznam použitých zdrojů

1. Seznam použité literatury

BEZPALEC, Pavel. *Management ICT systémů: Nové trendy v elektronických komunikacích* [online]. ČVUT, 2015 [cit. 20.6.2022]. Dostupné z: <https://entk.publi.cz/book/242-management-ict-systemu>.

FIALOVÁ, Eva. Právo na přístup k internetu. In: *Pravniprostor.cz* [online]. ATLAS, 2019 [cit. 20.6.2022]. ISSN: 2336-4114. Dostupné z: <https://www.pravniprostor.cz/clanky/pravo-it/pravo-na-pristup-k-internetu>.

HENDLER, Jim. Web 3.0 Emerging. In: *Computer* [online]. IEEE, 2009, 42(1) [cit. 20.6.2022]. ISSN: 1558-0814. Dostupné prostřednictvím IEEE Xplore. DOI: [10.1109/MC.2009.30](https://doi.org/10.1109/MC.2009.30).

HEEKS, Richard. *Implementing and Managing eGovernment* [online]. SAGE, 2006 [cit. 20.6.2022]. ISBN: 978-14-46220-19-1. Dostupné prostřednictvím SAGE Publishing. DOI: [10.4135/9781446220191](https://doi.org/10.4135/9781446220191).

HUSTEDT, Thurid, RANDMA-LIIV, Tiina, SAVI, Riin. Public Administration and Disciplines. In: *European Perspectives for Public Administration* [online]. Leuven, 2020 [cit. 20.6.2022]. ISBN: 978-94-6166-307-8. Dostupné prostřednictvím JSTOR. DOI: doi.org/10.2307/j.ctvv417th.11.

CHARALABIDIS, Yannis, LOUKIS, Euripidis, ALEXOPOULOS Charalampos, LACHANA Zoi. The Three Generations of Electronic Government. In: *Electronic Government* [online]. Springer, 2019 [cit. 20.6.2022]. ISBN 978-3-030-27325-5. DOI: [10.1007/978-3-030-27325-5_1](https://doi.org/10.1007/978-3-030-27325-5_1).

GERLOCH, Aleš. Teorie práva. 8. aktualizované vydání ed. Plzeň: Aleš Čeněk, 2021. ISBN: 978-80-7380-838-9.

GREGUŠOVÁ, Daniela. *Zákon o e-Governmente: komentár*. Bratislava: Eurokódex, 2018. ISBN: 978-80-8155-080-5.

JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. Správní řád. 6. vydání. Praha: C.H. Beck, 2019. ISBN 978-80-7400-751-4.

KITSING, Meelis. Scenarios as Thought Experiments for Governance. In: *European Perspectives for Public Administration* [online]. Leuven, 2020 [cit. 20.6.2022]. ISBN: 978-94-6166-307-8. Dostupné prostřednictvím JSTOR. DOI: [10.2307/j.ctvv417th.10](https://doi.org/10.2307/j.ctvv417th.10).

KMENT, Vojtěch. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? [online]. In: *Bulletin-advokacie.cz*. 2016 [cit. 20.6.2022]. ISSN: 1805-8280. Dostupné z: <http://www.bulletin-advokacie.cz/nahradi-elektronicky-podpis-prosty-ten-tradicni-vlastnorucni>.

KOLOUCH, Jan, BAŠTA, Pavel, KROPÁČOVÁ, Andrea, KUNC, Martin. Digitální služba. In: *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

KORBEL, František, KOVÁŘ, Dalibor, POTOČNÁK, Štefan, AMLER, Pavel. Elektronická identita při elektronickém (hmotně)právním jednání. In: *Právní rozhledy* [online]. 2019, 18 [cit. 20.6.2022]. ISSN: 1805-2797. Dostupné z: <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhfxa4s7ge4f6427gyzdm>.

KUSIAK-WINTER, Renata. Kierunki i etapy rozwoju e-administracji publicznej. In: *Ewolucja elektronicznej administracji publicznej*. [online] E-Wydawnictwo, 2021 [cit. 20.6.2022]. ISBN 978-83-66601-43-7. DOI: [10.34616/23.21.008](https://doi.org/10.34616/23.21.008).

LAYNE, Karen, LEE, Jungwoo. Developing fully functional E-government: A four stage model. In: *Government information quarterly* [online]. Elsevier, 2001, 18(2) [cit. 20.6.2022]. ISSN: 0740-624X. Dostupné prostřednictvím Science Direct. DOI: [10.1016/S0740-624X\(01\)00066-1](https://doi.org/10.1016/S0740-624X(01)00066-1).

LIPS, Miriam. *Digital Government: Managing Public Sector Reform in the Digital Era* [online]. Routledge, 2020 [cit. 20.6.2022]. ISBN: 978-13-15622-40-8. Dostupné z: <https://1lib.cz/book/17584618/07b207>.

MACINTOSH, Ann. Characterizing E-Participation in PolicyMaking. In: *Proceedings of the 37th Annual Hawaii International Conference on System Sciences* [online]. IEEE, 2004. [cit. 20.6.2022]. ISBN: 0-7695-2056-1. Dostupné prostřednictvím IEEE Xplore. DOI: [10.1109/HICSS.2004.1265029](https://doi.org/10.1109/HICSS.2004.1265029).

MÁCHOVÁ, Renáta, LNĚNIČKA, Martin. Reframing E-Government Development Indices with Respect to New Trends in ICT. In: *Review of economic perspectives* [online]. De Gruyter, 2015. 15(4) [cit. 20.6.2022]. ISSN: 1804-1663. DOI: [10.1515/revecp-2015-0027](https://doi.org/10.1515/revecp-2015-0027).

MATES, Pavel. Otazníky nad realizací práva na digitální služby. In: *Právní rozhledy* [online]. 2021, 20, 711-715 [cit. 20.6.2022]. ISSN: 1805-2797. Dostupné z: <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpxa4s7giyf6427g4ytc>.

MATES, Pavel. Právo na digitální služby. In: *Revue pro právo a technologie* [online]. 2020, 11(21), 87-88 [cit. 20.6.2022]. ISSN 1805-2797. DOI: [10.5817/RPT2020-1-4](https://doi.org/10.5817/RPT2020-1-4).

MATES, Pavel, SMEJKAL, Vladimír. *E-government v České republice: právní a technologické aspekty*. 2. podstatně přeprac. a rozš. vyd. ed. Praha: Leges, 2012. ISBN: 978-80-87576-36-6.

MASON, Stephen. *Electronic Signatures in Law* [online]. 4th edition. Institute of Advanced Legal Studies, 2016, [cit. 20.6.2022]. ISBN: 978-1-911507-01-7. Dostupné z: <https://humanities-digital-library.org/index.php/hdl/catalog/view/electronic signatures/1/86-1>.

MÜHLFEIT, František. Místo plastové kartičky datový záznam. EU chystá jednotnou peněženku digitálních identit. In: *E15.cz* [online]. CNC, 2021 [cit. 20.6.2022]. Dostupné z: <https://www.e15.cz/domaci/misto-plastove-karticky-datovy-zaznam-eu-chysta-jednotnou-penezenku-digitalnich-identit-1385271>.

HENDRYCH, Dušan aj. *Správní právo: Obecná část*. 9. vydání. Praha: C. H. Beck, 2016. ISBN: 978-80-7400-624-1.

PAVLÍK, Marek, ŠIMKA, Karel, POSTRÁNECKÝ, Josef, POMAHAČ, Richard. *Moderní veřejná správa: zvyšování kvality veřejné správy, dobrá praxe a trendy*. Praha: Wolters Kluwer, 2020. ISBN: 978-80-7598-048-9.

PETERKA, Jiří. ISSS 2022: Blíží se zemětřesení v eGovernmentu a tsunami datových schránek. In: *Lupa.cz* [online]. Internet Info, 2022 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://www.lupa.cz/clanky/iss-2022-blizi-se-zemetreseni-v-egovernmentu-a-tsunami-datovych-schranek/>.

PETERKA, Jiří. Zprávy z Depa (1): Místo zmocnění v zákoně bude stačit jen zápis v registru. In: *Lupa.cz* [online]. Internet Info, 2021 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://www.lupa.cz/clanky/zpravy-z-depa-1-misto-zmocneni-v-zakone-bude-stacit-jen-zapis-v-registru/>.

PETERKA, Jiří. Zprávy z Depa (2): Automatické zřízení datové schránky pro informačně gramotné. In: *Lupa.cz* [online]. Internet Info, 2021 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://lupa.cz/clanky/zpravy-z-depa-2-automaticke-zrizeni-datove-schranky-pro-informacne-gramotne/>.

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

RAGNEDDA, Massimo. DESTEFANIS, Giuseppe. Blockchain. A disruptive technologies. In: *Blockchain and Web 3.0* [online]. Taylor & Francis, 2019 [cit. 20.6.2022]. ISBN: 978-04-29029-53-0. DOI: [10.4324/9780429029530-1](https://doi.org/10.4324/9780429029530-1).

SEALED, TIME.LEX, SIEMENS. *Study on Cross-Border Interoperability of eSignatures* [online]. Publication office of the EU, 2010 [cit. 20.6.2022]. Dostupné z: <https://op.europa.eu/en/publication-detail/-/publication/280dc30e-6adb-4b83-af38-fe6083bffeaf>.

SKALICKÁ, Martina. Řízení ve věcech služby v digitalizované spisové službě [online]. In: *Epravo.cz*. 2021 [cit. 20.6.2022]. ISSN 1213-189X. Dostupné z: <https://www.epravo.cz/top/clanky/rizeni-ve-vecech-sluzby-v-digitalizovane-spisove-sluzbe-112403.html>.

STELLNER, František, VOKOUN, Marek, SOBĚHART, Radek. Smart government, smart administration a eGovernment v České republice. In: *Mladá Věda* [online]. Presov: 2021, 9(4) [cit. 20.6.2022]. ISSN: 1339-9318. Dostupné z: <https://www.proquest.com/docview/2617199270>.

ŠPAČEK, David. EGovernment: cíle, trendy a přístupy k jeho hodnocení. Praha: C.H. Beck, 2012. ISBN: 978-80-7400-261-8.

ŠPAČEK, David. Public Administration Reform in Czechia after 2000: Ambitious Strategies and Modest Results? In: *NISPAcee Journal of Public Administration and Policy* [online]. Sciendo, 2018, 11(1) [cit. 20.6.2022]. ISSN: 1337-9038. DOI: [10.2478/nispa-2018-0007](https://doi.org/10.2478/nispa-2018-0007).

TULÁČEK, Michal. *Elektronizace správy daní*. Praha: Leges, 2020. ISBN: 978-80-7502-434-3.

YILDIZ, Mete. E-government research: Reviewing the literature, limitations, and ways forward. In: *Government Information Quarterly* [online]. Elsevier, 2007, 24(3) [cit. 20.6.2022]. ISSN: 0740-624X. Dostupné prostřednictvím Science Direct. DOI: [10.1016/j.giq.2007.01.002](https://doi.org/10.1016/j.giq.2007.01.002).

VAŠEK, Jan. *Jak se vyznat v digitální terminologii* [online]. 2020 [cit. 20.6.2022]. Dostupné z: <https://kem.vscht.cz/digitalni-nakup-scm/archiv-2021/jak-se-vyznat-v-digitalni-terminologii>.

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. ISBN: 978-80-7400-670-8.

ZAJÍČEK, Zdeněk, KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel, DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. *Zákon o právu na digitální služby: komentář*. Praha: C.H. Beck, 2021. ISBN: 978-80-7400-822-1.

2. Seznam použitých internetových zdrojů

BAREŠOVÁ, Andrea. Miliarda! [prezentace]. In: *ISSS 2022* [online]. 2022 [cit. 20.6.2022]. Dostupné z: https://issc.cz/archiv/2022/download/prezentace/ceska-posta_baresova.pdf.

DZURILLA, Vladimír, TÝM OHA MV. *Informační koncepce České republiky* [online]. Ministerstvo vnitra: 2020. Poslední změna: 29.5.2020 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/soubor/informacni-koncepce-cr-2020.aspx>.

DZURILLA, Vladimír, TÝM OHA MV. *ICT benchmark veřejné správy 2021* [online]. Archi.gov.cz, 2022. Poslední změna: 21.1.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/_media/dokumenty:benchmark_2021_dc_final.pdf.

DZURILLA, Vladimír, TÝM OHA MV. *ICT benchmark veřejné správy 2021: podkladová data* [tabulky]. Archi.gov.cz, 2022. Poslední změna: 21.1.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/_media/benchmark_2021_data_final.xlsx.

EVROPSKÁ KOMISE. *Communication from the Commission...: The Role of eGovernment for Europe's Future* [online]. 2003 [cit. 20.6.2022]. CELEX: 52003DC0567. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52003DC0567>.

EVROPSKÁ KOMISE. DESI by components [tabulky] In: *Data Visualisation Tool* [online]. 2021 [cit. 20.6.2022]. Dostupné z: <https://digital-agenda-data.eu/charts/desi-components>.

EVROPSKÁ KOMISE. *Index digitální ekonomiky a společnosti (DESI) 2021: Česko* [online]. 2021 [cit. 20.6.2022]. Dostupné z: <https://ec.europa.eu/newsroom/dae/redirection/document/80581>.

EVROPSKÁ KOMISE. *EGovernment benchmark 2021: Source Data* [tabulky]. 2021 [cit. 20.6.2022]. Dostupné z: <https://ec.europa.eu/newsroom/dae/redirection/document/80571>.

EVROPSKÁ KOMISE. *EGovernment benchmark: Method Paper 2020-2023* [online]. Publications Office of the EU, 2021 [cit. 20.6.2022]. ISBN 978-92-76-36362-0. DOI: [10.2759/640293](https://doi.org/10.2759/640293).

EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES ze dne 15.12.2020* [online]. 2020 [cit. 20.6.2022]. CELEX: 52020PC0825. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0825>.

EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu ze dne 3. 6. 2021* [online]. 2021 [cit. 20.6.2022]. CELEX: 52021PC0281. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52021PC0281>.

EVROPSKÁ KOMISE. *Sdělení Komise...: Akční plán EU pro eGovernment na období 2016-2020* [online]. 2016 [cit. 20.6.2022]. CELEX: 52016DC0179. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52016DC0179>.

EVROPSKÁ KOMISE. *Systémy elektronické identifikace oznámené podle čl. 9 odst. 1 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu ze dne 27. dubna 2022* [online]. 2022 [cit. 20.6.2022]. CELEX: 52022XC0218(06). Dostupné z: [https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52022XC0218\(06\)](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52022XC0218(06)).

EVROPSKÁ KOMISE. *Zpráva Komise Evropskému parlamentu a Radě o hodnocení nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS) ze dne 3. června 2021* [online]. 2021 [cit. 20.6.2022]. CELEX: 52021DC0290. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021DC0290>.

GOLÁŇ Tomáš. In: SENÁT. *Stenozáznam z 2. dne 10. schůze* [online]. 2021 [cit. 20.6.2022]. Dostupné z: <https://senat.cz/xqw/webdav/pssenat/original/99360/83399/91229>.

ICT UNIE. Informace o stavu přípravy projednávání návrhu zákona o právech na digitální služby. In: *Ictu.cz* [online]. 2018 [cit. 20.6.2022]. Dostupné z: [http://www.ictu.cz/aktualne/detail-aktuality/?tx_ttnews\[tt_news\]=104](http://www.ictu.cz/aktualne/detail-aktuality/?tx_ttnews[tt_news]=104).

KOŘANOVÁ, Barbora aj. Sněmovní tisk 447/0: Návrh zákona o právu na digitální služby včetně důvodové zprávy. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=447>.

KUCHAR, Petr. Koordinace eGovernmentu z pohledu HAeG [prezentace]. In: *ISSS 2022* [online]. 2022 [cit. 20.6.2022]. Dostupné z: https://issc.cz/archiv/2022/download/prezentace/mvcr_kuchar.pdf.

MICROSOFT. Authentication vs. authorization. In: *Microsoft technical documentation* [online]. Microsoft: 2022. Poslední změna: 6.2.2022 [cit. 20.6.2022]. Dostupné z: <https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-vs-authorization>.

MINISTERSTVO PRO MÍSTNÍ ROZVOJ. *NEN [Národní elektronický nástroj]: Ověření kompatibility* [online]. [cca 2022, cit. 20.6.2022]. Dostupné z: <https://nen.nipez.cz/CompatibilityCheck>.

MINISTERSTVO VNITRA. Agenda cizinecká a ochrany státních hranic (Kód A116): Úkon správního poplatku (Kód U7583). In: *Registr práv a povinností* [tabulky]. 2021 [cit. 20.6.2022]. Dostupné z: https://rpp-ais.egon.gov.cz/gen/agendy-detail/A116_23012021.xlsx.

MINISTERSTVO VNITRA. Agenda občanské průkazy (Kód A117) In: *Registr práv a povinností* [tabulky]. 2022 [cit. 20.6.2022]. Dostupné z: https://rpp-ais.egon.gov.cz/gen/agendy-detail/A117_10022022.xlsx.

MINISTERSTVO VNITRA. eGON. In: *Mvcr.cz* [online]. Ministerstvo vnitra, [cca 2008, cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/clanek/egon-66.aspx>.

MINISTERSTVO VNITRA. *eGON News* [online]. Ministerstvo vnitra, 2008, 3 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/soubor/egon-news-3-pdf.aspx>.

MINISTERSTVO VNITRA. *Metodika pro evidenci služeb VS, jejich úkonů a plánu digitalizace* [online]. 2020 [cit. 20.6.2022]. Dostupné z: <https://pma3.gov.cz/uploads/doc/Metodika-pro-evidenci-sluzeb.pdf>.

MINISTERSTVO VNITRA. Organizační struktura. In: *Mvcr.cz* [online]. Ministerstvo vnitra, [cca 2022, cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/clanek/organizacni-struktura-362751.aspx>.

MINISTERSTVO VNITRA. *Portál občana: Přihlášení* [online]. 2022, verze 1.7.7. [cit. 20.6.2022]. Dostupné z: <https://obcan.portal.gov.cz/prihlaseni>.

MINISTERSTVO VNITRA. *Rozcestník vygenerovaných agend* [online]. 2022 [cit. 8.6.2022]. Dostupné z: <https://rpp-ais.egon.gov.cz/gen/agendy-detail/>.

MINISTERSTVO VNITRA. Služby veřejné správy. In: *Portál veřejné správy* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://portal.gov.cz/sluzby-verejne-spravy/>.

MINISTERSTVO VNITRA. Statistiky Czech POINT. In: *Czechpoint.cz* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://czechpoint.cz/public/statistiky-a-informace/statistiky-czp/>.

MINISTERSTVO VNITRA. *Strategický rámec rozvoje veřejné správy ČR pro období 2014-2020* [online]. Polygrafie Úřadu vlády ČR, 2017 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/soubor/strategicky-ramec-rozvoje-verejne-spravy-v-cr-pro-obdobi-2014-2020.aspx>.

MINISTERSTVO VNITRA. Snižování regulační zátěže občanů a veřejné správy. In: *Mvcr.cz* [online]. 2017 [cit. 20.6.2022]. Dostupné z: <https://mvcr.cz/clanek/snizovani-regulacni-zateze-obcanu-a-verejne-spravy.aspx>.

NAKIT, MINISTERSTVO VNITRA. Katalog služeb veřejné správy [Power BI Dashboard]. [cca 2022, cit. 20.6.2022]. Dostupné z: <https://app.powerbi.com/view?r=eyJrIjoiZTc3MDcwMWU0NTdkMC00NTM2LWI5MTktMGJINTQ5ODg2NWZjIiwidCI6IjFkYjQxZDZmLTNmMzctNDZkYi1iZDNiLWM0ODNhYmI4MTA1ZCIsImMiOiJh9>.

NKÚ. *Kontrolní závěr z kontrolní akce č. 17/22: Realizace projektů v oblasti ICT u MPSV* [online]. 2018 [cit. 20.6.2022]. Dostupné z: <https://nku.cz/assets/kon-zavery/k17022.pdf>.

NKÚ. *Souhrnná zpráva o digitalizaci veřejné správy v ČR* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://nku.cz/assets/publikace-a-dokumenty/ostatni-publikace/zprava-o-digitalizaci-verejne-spravy.pdf>.

OPEN-SOURCE ALIANCE. *Legislativa* [online]. 2021 [cit. 20.6.2022]. Dostupné z: <https://openczeg.cz/legislativa/>.

OSN. E-government survey 2020: *Digital Government in the Decade of Action for Sustainable Development*. [online]. 2020 [cit. 20.6.2022]. ISBN: 978-92-1-005145-3. Dostupné z: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>.

POSLANECKÁ SNĚMOVNA. Doprovodné usnesení č. 789 ze dne 8. listopadu 2019 k návrhu na vydání ZPDS. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/text2.sqw?idd=164509>.

POSLANECKÁ SNĚMOVNA. Sněmovní tisk 756. In: *Psp.cz* [online]. 2020 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/historie.sqw?o=8&t=756>.

REDAKCE EURO.CZ, NĚMEC, Jan. Upravený zákon jde do vlády. In: *Pravniprostor.cz* [online]. Internet Info, 2007 [cit. 20.6.2022]. ISSN 1212-9437. Dostupné z: <https://euro.cz/byznys/upraveny-zakon-jde-do-vlady-887462>.

REDAKCE PRÁVNÍCH ROZHLEDŮ. Poslanecká sněmovna schválila návrh zákona upravujícího elektronizaci orgánů veřejné moci. In: *Právní rozhledy* [online]. 2021, č. 12, s. 2-3 [cit. 20.6.2022]. ISSN: 1805-2797. Dostupné z: <https://beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgfpaxa4s7gezf6427nfuxayq>.

REKONSTRUKCE STÁTU: Nedigitální Česko [online]. 2021 [cit. 20.6.2022]. Dostupné z: https://rekonstrukcestatu.cz/download/3nQoIg/nedigitalni_cesko.pdf.

ŠEDIVEC, Tomáš. Referenční údaje. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 30.4.2021 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap:univerzalni_kontaktni_misto.

ŠEDIVEC, Tomáš. Slovník pojmů eGovernmentu. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019 [cit. 20.6.2022]. Poslední změna: 4.5.2022. Dostupné z: https://archi.gov.cz/slovník_egov.

ŠEDIVEC, Tomáš. Univerzální kontaktní místo. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 4.5.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap:univerzalni_kontaktni_misto.

ŠEDIVEC, Tomáš, RADA, Michal. Architektonická vize eGovernmentu ČR. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2018. Poslední změna: 31.5.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap_dokument:architektonicka_vize_e_governmentu_cr.

ŠEDIVEC, Tomáš, RADA, Michal. Informační koncepce ČR. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 21.7.2021 [cit. 20.6.2022]. Dostupné z: <https://archi.gov.cz/ikcr>.

ŠEDIVEC, Tomáš, RADA, Michal. Komunikační infrastruktura veřejné správy. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 1.6.2022 [cit. 20.6.2022]. Dostupné z: https://archi.gov.cz/nap:komunikacni_infrastruktura_veřejne_spravy.

ŠEDIVEC, Tomáš, RADA, Michal. Základní registry. In: *Archi.gov.cz* [online]. Ministerstvo vnitra: 2019. Poslední změna: 30.4.2021 [cit. 28.2.2022]. Dostupné z: https://archi.gov.cz/nap:zakladni_registry.

UNCITRAL. *Draft Model Law on the Use and Cross border Recognition of Identity Management and Trust Services: advance copy* [online]. UN, 2022 [cit. 20.6.2022]. Dostupné z: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/acn9-1112-e.pdf>.

ÚLOVEC, Jiří. Informace o současném stavu elektronických systémů spisové služby a informačních systémů pro správu [prezentace]. In: *ISSS 2019* [online]. 2019 [cit. 20.6.2022]. Dostupné z: https://isss.cz/archiv/2019/download/prezentace/mvcr_ulovec.pdf.

ÚŘAD VLÁDY ČR. *Akční plán pro Společnost 4.0* [online]. 2017 [cit. 20.6.2022]. Dostupné z: <https://databaze-strategie.cz/cz/urad-vlady/strategie/akcni-plan-pro-spolecnost-4-0-2017?typ=download>.

ÚŘAD VLÁDY ČR. *Akční plán rozvoje spisové služby Úřadu vlády České republiky* [online]. 2019, [cit. 20.6.2022]. Dostupné z: <https://vlada.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha-c--2---Akcni-plan-rozvoje-spisove-sluzby.pdf>.

VLÁDA ČR. Sněmovní tisk 1069/0: Návrh zákona o elektronické identifikaci včetně důvodové zprávy. In: *Psp.cz* [online]. 2008 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=7&ct=1069>.

VLÁDA ČR. Sněmovní tisk 447/1: Stanovisko vlády k návrhu zákona o právu na digitální služby. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=447&ct1=1>.

VLÁDA ČR. Sněmovní tisk 756/0: Návrh zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci včetně důvodové zprávy. In: *Psp.cz* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=756>.

VLÁDA ČR. Sněmovní tisk 928/0: Návrh zákona, kterým se mění Zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a další související zákony včetně důvodové zprávy. In: *Psp.cz* [online]. 2016 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/orig2.sqw?idd=116235>.

VLÁDA ČR. *Programové prohlášení vlády Petra Fialy* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://vlada.cz/cz/programove-prohlaseni-vlady-193547/>.

VLÁDA ČR. *Příloha č. 1 usnesení vlády ze dne 6. dubna 2022 č. 289: Projektový záměr „Transformace koordinace a řízení digitalizace* [online]. 2022 [cit. 20.6.2022]. Dostupné z: <https://apps.odok.cz/attachment/-/down/NANACDEH9J99>.

VRBA, Roman. Zpráva o stavu eGovernmentu pro rok 2022. In: *ISSS 2022* [zvuková nahrávka]. 2022, 53.-60. minuta [cit. 20.6.2022]. Dostupné z: <https://issz.cz/archiv/2022/download/audio/zprava-o-stavu-egovernmentu-pro-rok-2022.mp3>.

VÝBOR PRO VEŘEJNOU SPRÁVU A REGIONÁLNÍ ROZVOJ. Sněmovní tisk 447/0: Usnesení VSR ze dne 5. září 2019. In: *Psp.cz* [online]. 2019 [cit. 20.6.2022]. Dostupné z: <https://psp.cz/sqw/text/tiskt.sqw?o=8&ct=447&ct1=4>.

ZAJÍČEK Zdeněk. Zdeněk Zajíček (ICT Unie): Digitální ústava absolutně mění pohled na to, jak má stát fungovat. In: SLÍZEK, David. *Lupa.cz* [online]. Internet Info, 2018 [cit. 20.6.2022]. ISSN: 1213-0702. Dostupné z: <https://www.lupa.cz/clanky/zdenek-zajicek-ict-unie-digitalni-ustava-absolutne-meni-pohled-na-to-jak-ma-stat-fungovat/>.

3. Seznam použitých právních předpisů

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 (nařízení eIDAS), CELEX: 32014R0910.

Nařízení Komise (EU) 2015/806 ze dne 22. května 2015, kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru, CELEX: 32015R0806.

Příloha Usnesení vlády ČR č. 961/2014 o zřízení Rady vlády pro informační společnost (statut Rady vlády pro informační společnost).

Příloha zákona č. 549/1991 Sb., o soudních poplatcích, ve znění pozdějších předpisů.

Směrnice Evropského parlamentu a Rady (EU) 2016/2102 ze dne 26. října 2016 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru, CELEX: 32016L2102.

Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky (Listina), ve znění pozdějších předpisů.

Usnesení vlády ČR č. 289/2022 k realizaci projektu Transformace koordinace a řízení digitalizace.

Usnesení vlády ČR č. 826/2021 k aktualizovanému harmonogramu a technickým způsobům provedení digitalizace služeb veřejné správy na období 2021 – 2025.

Ústavní Zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů.

Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

Vyhláška č. 515/2020 Sb. o struktuře informací zveřejňovaných o povinném subjektu a o osnově popisu úkonů vykonávaných v rámci agendy.

Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy.

Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy.

Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů (ZPDS).

Zákon č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů.

Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky (kompetenční zákon), ve znění pozdějších předpisů.

Zákon č. 250/2017 Sb. o elektronické identifikaci, ve znění pozdějších předpisů.

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.

Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (DEPO zákon).

Zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (ZSVDET), ve znění pozdějších předpisů.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (zákon o datových schránkách), ve znění pozdějších předpisů.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ZISVS), ve znění pozdějších předpisů.

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

Zákon č. 549/1991 Sb., o soudních poplatcích, ve znění pozdějších předpisů.

Zákon č. 582/1991 Sb., České národní rady o organizaci a provádění sociálního zabezpečení.

4. Seznam použité judikatury

Nález Ústavního soudu ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99.

Nález Ústavního soudu ze dne 20. 5. 2014, sp. zn. II. US 2560/13

Nález Ústavního soudu ze dne 16. 6. 2015, sp. zn. I. ÚS 3930/14.

Nález Ústavního soudu ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99.

Nález Ústavního soudu ze dne 28. 6. 2021, sp. zn. II. ÚS 671/21.

Rozsudek Městského soudu v Praze ze dne 16.1.2013, čj. 10 A 320/2011-50.

Rozsudek Nejvyššího správního soudu ze dne 16. 5. 2019, č. j. 1 As 106/2018-45.

Rozsudek Nejvyššího správního soudu ze dne 16. 7. 2015, č. j. 9 As 261/2014-44.

Rozsudek Nejvyššího správního soudu ze dne 16. 12. 2010, č. j. 1 Ans 5/2010-172.

Rozsudek Nejvyššího správního soudu ze dne 17. 10. 2013, č. j. 6 Ans 1/2013-66.

Rozsudek Nejvyššího správního soudu ze dne 23. 3. 2016, č. j. 6 As 276/2015-31.

Rozsudek Nejvyššího správního soudu ze dne 31. 1. 2018, č.j. 5 As 295/2016-45.

Stanovisko Nejvyššího soudu ze dne 05.01.2017, sp. zn. Plsn 1/2015.

Stanovisko pléna Ústavního soudu ze dne 7. 9. 2021, sp. zn. Pl. ÚS-st. 53/21.

Usnesení Krajského soudu v Brně ze dne 12. 6. 2012, č. j. 47 Co 71/2010-249.

Usnesení Nejvyššího soudu ze dne 12. 9. 2018, č. j. 3 Tdo 1003/2018-37.

Usnesení Nejvyššího soudu ze dne 27.10.2020, sp. zn. 27 Cdo 143/2020.

Usnesení Nejvyššího správního soudu ze dne 15. 7. 2010, č. j. 9 Afs 28/2010-79.

Seznam grafů a obrázků

1. Seznam grafů

Graf č. 1: Layneův a Leeův čtyřfázový model budování eGovernmentu.	9
Graf č. 2: Vývoj úrovně poskytování digitálních veřejných služeb podle indexu DESI v porovnání s vybranými státy.	14
Graf č. 3: Schématické znázornění vrstev architektury tuzemského eGovernmentu.....	20
Graf č. 4: Pyramida zákonných předpisů relevantních pro eGovernment	29
Graf č. 5: Obslužné kanály všech úkonů v katalogu služeb, které činí jiné subjekty vůči orgánům veřejné moci.	70
Graf č. 6: Obslužné kanály všech úkonů v katalogu služeb, které činí orgány veřejné moci při výkonu své působnosti.	71

2. Seznam obrázků

Obrázek č. 1: Panáček eGON spolu s tehdejším ministrem vnitra Ivanem Langerem a jeho náměstkem Zdeňkem Zajíčkem.....	17
Obrázek č. 2: Přihlašovací stránka Portálu občana.	43
Obrázek č. 3: Procházení seznamu služeb veřejné správy na Portálu občana	72

Veřejná správa a eGovernment

Abstrakt

Diplomová práce *Veřejná správa a eGovernment* přináší jedinečný pohled na stávající i novou právní úpravu eGovernmentu ve veřejné správě. Podstatou práce je právní rozbor nově přijatého zákona o právu na digitální služby. Kritické úvaze je podroben samotný koncept tohoto zákona, který je dán specifickými okolnostmi vzniku, a také jednotlivá nově upravená digitální práva. Některá z těchto práv jsou zobecněním stávajících pravidel upravených v různých zákonech eGovernmentu, zatímco jiná jsou zcela nová a řeší dosud neřešené problémy digitalizace. Klíčovými digitálními právy, mezi které patří právo na digitální služby, právo činit digitální úkon a právo na sdílení vedených údajů, je v této práci věnována zásadní pozornost. Značná část nové úpravy je závislá na pojmech a právních institutech, které upravují stávající zákony eGovernmentu. V souvislosti s těmito instituty nabízí diplomová práce reflexi dosavadní právní úpravy a odpovědi na některé přetrvávající sporné otázky týkající se například přihlašování do portálů veřejné správy, automatického zřizování datových schránek některým fyzickým osobám nebo kvalifikovaných a nekvalifikovaných forem elektronického podání. Pro získání poznatků o aktuálním a plánovaném stavu digitalizace služeb veřejné správy byly využity i data z nově vzniklého katalogu služeb. Prostřednictvím indexů a benchmarků je právní úprava konfrontována se skutečným stavem eGovernmentu u nás i v zahraničí a jsou také identifikovány jeho nedostatky. Mnoho z těchto nedostatků přetrvává i po přijetí nové úpravy. Nebyly například naplněny ambice tvůrců zákona ohledně usnadnění vymáhání digitálních práv. Zároveň některé stávající problémy jako například nedostatečné proaktivní poskytování veřejných služeb nová úprava vůbec neřeší. Celkově zákon o právu na digitální služby nepřináší žádné významné revoluční změny. Nová právní úprava představuje pouze evoluci stávajících právních institutů eGovernmentu.

Klíčová slova: eGovernment, digitalizace veřejné správy, digitální veřejné služby.

Public Administration and eGovernment

Abstract

This diploma thesis Public Administration and EGovernment brings a unique perspective on the existing and new legal regulation of eGovernment. The essence of the thesis is a legal analysis of the newly adopted Digital Service Rights Act. The concept of the Act, which has been determined by specific circumstances of its creation, as well as the content of the Act, and the newly regulated digital rights, are critically analyzed. Some of these digital rights are only generalizations of existing rules regulated by various eGovernment acts, while other digital rights are wholly new and address previously unaddressed digitalization issues. The focus of this paper is on key digital rights such as the right to use digital services, the right to perform digital acts, and the right to share stored data. A crucial part of the new Act is dependent on legal institutes regulated by existing eGovernment laws. Concerning these legal institutes, the thesis offers a reflection of existing legal regulation and answers to some persistent legal questions concerning, for example, logging into public administration portals, the automatic setting up of data boxes for certain ordinary citizens, or qualified and non-qualified forms of electronic submission. Using international indexes and benchmarks, the present state legislation is confronted with the actual state of eGovernment in the Czech Republic. There are also identified deficiencies in the actual state of eGovernment. Furthermore, the newly established catalog of services is used to gain knowledge about the current and planned state of digitalization of public services. The significance of the chosen topic can be illustrated by the fundamental change in data sharing between public administration bodies, which has affected practically all areas of public administration. It was necessary to amend more than 140 other acts regulating the activities of public administration by a subsequent law.

Keywords: eGovernment, digitalization of public administration, digital public services