Západočeská univerzita v Plzni

Fakulta právnická

DIPLOMOVÁ PRÁCE

„Elektronizace veřejné správy – eGovernment v České republice“

MASTERS THESIS

„eGovernment in the Czech Republic “

Autor: Bc. Ondřej Škrabal

Vedoucí práce: JUDr. Tomáš Louda, CSc.

Plzeň, 2018

Zadání bakalářské práce

V **pevné vazbě** je na tomto místě vevázán **originál** Zadání.

V **termovazbě** (kroužkové vazbě) je na tomto místě vevázána **černobílá kopie** Zadání.

PODĚKOVÁNÍ

„Děkuji všem, kteří mě při vypracování diplomové práce podporovali, zvláště pak svému vedoucímu práce JUDr. Tomáši Loudovi, CSc. za trpělivost a cenné rady.“

25. března 2018 vlastnoruční podpis

ČESTNÉ PROHLÁŠENÍ

„Prohlašuji, že jsem zpracoval tuto bakalářskou práci samostatně a že jsem vyznačil použité zdroje informací, z nichž jsem při zpracování své práce čerpal.“

25. března 2018 vlastnoruční podpis

Obsah

Seznam použitých zkratek: **7**

Úvod **9**

1 Základní pojmy eGovernmentu **10**

1.1 Pojmy eGovernment, eGovernance a další 10

1.2 Veřejné elektronické služby 11

1.3 E-demokracie a e-participace 13

1.4 Informační systémy veřejné správy 14

2 Vývoj a trendy eGovernmentu v Evropské unii **16**

2.1 Vývoj eGovernmentu v politikách EU 16

2.2 Strategie Europe 2020 a eGovernment 17

3 Prvky eGovernmentu v České republice **21**

3.1 Historický vývoj 21

3.2 Portál veřejné správy 23

3.3 Czech POINT 25

3.3.1 Služby Czech POINT 26

3.4 Datové schránky 28

3.4.1 Zřizování datových schránek 28

3.4.2 Přístup do datové schránky 29

3.4.3 Přihlašování do datové schránky 30

3.4.4 Znepřístupnění datové schránky 31

3.4.5 Zneplatnění přístupových údajů 31

3.4.6 Zrušení datové schránky 32

3.4.7 Informační systém datových schránek 33

3.5 Autorizovaná konverze dokumentů 33

3.6 Základní registry 33

3.6.1 Vymezení pojmů základních registrů 34

3.6.2 Správa základních registrů 35

3.6.3 Vydávání ověřených výstupů 36

3.6.4 Registr obyvatel 36

3.6.5 Registr osob 37

3.6.6 Registr územní identifikace 38

3.6.7 Registr práv a povinností 39

3.6.8 Shrnutí 40

3.7 Registr smluv 41

3.8 Elektronický podpis 41

3.8.1 Historie elektronického podpisu 42

3.8.2 eIDAS – obecná ustanovení 42

3.8.3 Elektronický podpis ve světle současné úpravy 43
3.8.4 Elektronická časová razítka 44
3.8.5 Elektronické pečeti 45
3.8.6 Služby vytvářející důvěru a jejich poskytovatelé 45
3.9 Elektronické doporučené doručování 46
3.10 Elektronická identifikace 47
3.11 Portál občana 49
3.12 eSbírka a eLegislativa 49
3.13 Kyberbezpečnost 50
4 eGovernment České republiky a Evropská Unie 53
4.1 Benchmark a oblasti zkoumání 53
4.2 eGovernment benchmark 2016 54
4.3 eGovernment benchmark 2017 54
4.4 Shrnutí 55
5 Zhodnocení eGovernmentu České republiky 57
Závěr 61
Resumé 62
Seznam zdrojů 63

Seznam použitých zkratek:

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DAE2020	*A Digital Agenda for Europe.* COM(2010) 245 final
eGAP2020	*EU eGovernment Action Plan 2016-2020*: *Accelerating the digital transformation of government,* COM(2016) 179 final
eIDAS	Nařízení Evropského parlamentu a Rady (EU) 2014/910
ePodpis	Elektronický podpis
G2B	Government-to-Bussiness
G2C	Government-to-Customer
G2G	Government-to-Government
ICT	Informační a komunikační technologie
OTP	One Time Password
Registr obyvatel	Základní registr obyvatel
Registr osob	Základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci
Registr práv a povinností	Registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností
Registr územní identifikace	základní registr územní identifikace, adres a nemovitostí
SIP	Státní informační politika- cesta k informační společnosti
SIS	Komise vlády ČR pro státní informační poli-

	tiku
Směrnice NIS	Směrnice Evropského parlamentu a Rady (EU) 2016/1148
Zákon eID	Zákon č. 250/2017 Sb., *o elektronické identifikaci*, ve znění pozdějších předpisů
Zákon OP	Zákon č. 328/1999 Sb., *o občanských průkazech,* ve znění pozdějších předpisů
Zákon o eGovernmentu	Zákon č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů*, ve znění pozdějších předpisů
Zákon o ePodpisu	Zákon č. 227/2000 Sb., *o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)*, ve znění pozdějších předpisů
Zákon o ISVS	Zákon č. 365/2000 Sb., *o informačních systémech veřejné správy a o změně některých dalších zákonů*, ve znění pozdějších předpisů.
Zákon o kybernetické bezpečnosti	Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů*, ve znění pozdějších předpisů
Zákon o registru smluv	Zákon č. 340/2015 Sb., *o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv*, ve znění pozdějších předpisů
Zákon o sbírce zákonů	Zákon č. 222/2016 Sb., *o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv (zákon o Sbírce zákonů a mezinárodních smluv)*, ve znění pozdějších předpisů
Zákon o základních registrech	Zákon č. 111/2009 Sb., *o základních registrech*, ve znění pozdějších předpisů

Úvod

Tato diplomová práce se zabývá rozvojem eGovernmentu v České republice. Úvodem je nutné poznamenat, že oblast eGovernmentu je velice rozsáhlá a jednotlivé právní předpisy jsou většinou navzájem propojené, proto je obtížnější uchopit jednotlivé prvky eGovernmentu, jelikož v mnoha případech jeden bez druhého ztrácejí na významu. Tato práce má za úkol seznámit s vývojem eGovernmentu v České republice a jeho nástroji užitých v praxi. Nejprve je nutné vymezit několik základních pojmů užívaných v oblasti eGovernmentu, čímž se zabývá první kapitola této práce. Druhá kapitola se zabývá eGovernmentem v rámci Evropské unie, protože legislativa a projekty České republiky jsou v mnoha případech založeny na legislativě Evropské unie.

Třetí, nejobsáhlejší kapitola, se rozebírá jednotlivé nástroje eGovernmentu, které jsou využívány v České republice. Postupně řešenými současnými nástroji jsou portál veřejné správy, kontaktní místa Czech POINT, datové schránky, autorizovaná konverze dokumentů, základní registry, registr smluv a elektronický podpis. Tyto nástroje jsou v současné době v praxi užívané, ale existují i takové, jež teprve budou aplikovány. Těmito nástroji se třetí kapitola také zabývá a jsou jimi elektronické doporučené doručování, elektronická identifikace, portál občana a eSbírka a eLegislativa.

Předposlední kapitola se zabývá rozvojem eGovernmentu v České republice ve srovnání s Evropskou unií, tedy hodnocením úrovně eGovernmentu z relativního hlediska ve vztahu k průměru Evropské unie.

Poslední kapitola se zabývá finálním zhodnocením eGovernmentu České republiky a jeho současnými nedostatky s výhledem do budoucna.

Tato diplomová práce pracuje s právními předpisy účinnými k 25. 3. 2018, pokud se nejedná o právní předpisy k tomuto datu pouze platnými s pozdější účinností.

1 Základní pojmy eGovernmentu

Pro účely této práce je nutné nejprve vysvětlit základní pojmy eGovernmentu a elektronických služeb v rámci elektronizace veřejné správy, jelikož v české i mezinárodní literatuře se tyto pojmy liší podle autorů. Základní podstata elektronizace veřejné správy spočívá v zapojování informačních a komunikačních technologií (dále jen ICT) do činností veřejné správy.[1] Integrace takovýchto ICT se stala běžnou součástí reforem veřejné správy. Pro elektronizaci veřejné správy se v mezinárodním měřítku používá pojem eGovernment či eGovernance. Dále se tedy tato kapitola zabývá těmito a dalšími pojmy, které se vyskytují v soudobé literatuře.

1.1 Pojmy eGovernment, eGovernance a další

S rozvojem v této oblasti a zapojováním nástrojů New Public Management se stalo toto odvětví velmi populární. Díky tomu ale také začaly vznikat další pojmy a pododvětví, a to ať už v užším, či širším měřítku eGovernmentu.[2] Různorodá terminologie někdy pracuje s pojmem eGovernment jako věcnou oblastí, na kterou se zaměřují úvahy v rámci elektronizace veřejné správy. V užším pojetí to pak mohou být například pojmy jako e-health, e-environment, e-justice či e-participace v rámci e-demokracie. V širším záběru pak může být eGovernment chápán obecně pouze jako integrace ICT do veřejné správy, a to především internetu, jak je definováno OECD. OECD definovalo eGovernment jako použití informačních a komunikačních technologií, zvláště internetu, jako nástroje k dosažení lepší vlády.[3]

Distinkce mezi pojmy eGovernment a eGovernance spočívá v samotných pojmech v anglickém jazyce, tedy government (vláda) a governance (vládnutí), přičemž eGovernment je v rámci tohoto přístupu užším pojetím a zaměřuje se na rozvoj elektronických služeb občanům. Pojem eGovernance je v tomto pojetí širším konceptem rámcově zaměřeným na jednotlivé kroky vedoucí

[1] POMAHAČ, Richard. *Veřejná správa*, str. 183
[2] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*, str. 1
[3] OECD. *The e-Government Imperative*, str. 23

k implementaci a praxi těchto služeb mezi jednotlivými složkami vlády, jejich zaměstnanci a širokou veřejností. Ve zkratce lze pak dovodit, že pojem eGovernment je používán z institucionálního hlediska elektronizace veřejné správy, kdežto eGovernance je zaměřen na procesní stránku věci.[4]

Jak je uvedeno výše, v soudobé terminologii v rámci elektronizace veřejné správy se také lze setkat s pojmy jako e-health apod. Tyto pojmy označují jednotlivé sektory eGovernmentu jako odvětví veřejné politiky. Ovšem lze se setkat také s pojmem e-demokracie, který je z těchto pojmů nejmodernější. Pojmenovává tak různé snahy o větší demokratizaci s využitím ICT.[5] V rámci e-demokracie jsou vyjádřeny skoro vždy snahy o smíchání zastupitelské a přímé demokracie za účelem zvýšení účasti obyvatelstva na tvorbě politiky. Nejčastějšími formami e-demokracie je konzultování, vyjadřování názoru, a tento pojem zahrnuje dokonce i spolurozhodování či elektronické hlasování, ať už ve volbách, nebo v referendu.

Celkově vzato se literatura shoduje v podstatě eGovernmentu, která spočívá v zapojování ICT technologií do vnějších i vnitřních činností veřejné správy za účelem zlepšení své kvality a efektivity, jelikož veřejná správa je v moderním pojetí brána jako služba veřejnosti. Ideálním stavem pak je zajistit s využitím ICT naplňování svého účelu, a to i v oblastech, kde výkon veřejné správy nabývá vrchnostenské podoby.[6]

1.2 Veřejné elektronické služby

Elektronické veřejné služby hrají v oblasti eGovernmentu důležitou roli. Z obecného hlediska lze elektronickou službu, neboli e-službu, definovat jako interaktivní, na obsah zaměřenou a na internetu založenou zákaznickou službu, která je obsluhována zákazníkem a která je integrována s organizačními podpůrnými procesy a technologiemi za účelem posílit vztah zákazníka s poskytovatelem.[7] E-služba tedy zahrnuje interaktivní komunikaci jak se shora dolů, tak

[4] RILEY, Thomas B., SHERIDAN, William. *Comparing e-Government Vs. e-Governance*

[5] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*, str. 2

[6] Tamtéž, str. 3

[7] ANCARANI, Alessandro. *Towards quality e-service in the public sector: The evolution of web sites in the local public service sector*, str. 6

ze zdola nahoru. Kvalita takovéto služby je pak hodnocena hlavně dvěma kritérii. Prvním kritériem je technická kvalita, neboli jak je služba poskytována. Druhým kritériem je pak funkční kvalita, která se zabývá tím, co zákazník obdrží, tedy výsledkem využití této služby.[8]

V rámci hodnocení e-služeb je nutné také brát v úvahu do velké míry uživatelské rozhraní, které je tvořeno funkčností, vzhledem, logikou a použitelností dané internetové stránky, kde je služba umístěna.

Definující znaky společné v literatuře shrnuje na základě literatury J. Rowley.[9] E-služba je zprostředkována pomocí ICT a interakce uživatele s organizací. Tato interakce neprobíhá tváří v tvář, čímž jsou sice překonány klasické překážky jako vzdálenost instituce od uživatele nebo otevírací doba instituce. Na druhou stranu se uživatelé v tomto případě mohou spolehnout hlavně na svůj zrak.[10]

E-služba má hlavně informační hodnotu. To znamená, že uživatel prostřednictvím internetu vyhledává určité informace. Snadnost vyhledávání a získávání těchto informací se pak promítá v konečném hodnocení e-služeb uživatelem. Posledním definujícím znakem e-služby je její samoobslužný charakter, což znamená, že při poskytování informací neprobíhá přímá asistence nebo interakce se zaměstnancem organizace či osobou pověřenou. Tato vlastnost klade pak na uživatele novou roli, a to jak se vypořádá s e-službou sám uživatel, se pak také promítá do výsledného hodnocení.[11]

Ancarani pak rozděluje úroveň e-služeb do několika úrovní dle užité technologie použité v čase. Nejzákladnější úrovní je poskytování obecných informací, jakými mohou být kontakty, základní činnosti a umístění dané instituce. Vyšší úrovní se pak chápe jednoduchá jednosměrná komunikace instituce s uživatelem. Jednosměrná komunikace spočívá v poskytování aktualit, tiskových vyjádření, technických informací či užitečných odkazů. Na další úrovni pak probíhá komplexnější jednosměrná a jednoduchá obousměrná komunikace. Komplexní jednosměrná komunikace spočívá v poskytování finančních informací,

[8] ANCARANI, Alessandro. *Towards quality e-service in the public sector: The evolution of web sites in the local public service sector*, str. 8
[9] ROWLEY, Jennifer. *An analysis of the e-service literature: Towards a research agenda*
[10] POMAHAČ, Richard. *Veřejná správa*, str. 184
[11] Tamtéž, str. 185

často pokládaných otázek či nabídkou práce. Jednoduchá obousměrná komunikace se pak sestává z dotazníků, podáváním doporučení a online formuláři. Na nejvyšší úrovni probíhá už komplexní obousměrná interakce a transakce, což znamená například posílání stížností a v rámci transakcí účetní operace a uzavíraní smluv.[12] Jak lze vypozorovat, z jednotlivých úrovní by se měly e-služby postupně stávat propracovanější a od základního poskytování informací by se přes interakční prvky měly vyvinout až ve služby poskytující i transakční prvky.

Oblast e-služeb se nevztahuje pouze na komunikaci s uživatelem vně veřejné správy, ale také na instituce veřejné správy mezi sebou. Dělení dle subjektů komunikace se pak v rámci literatury rozlišuje na e-služby pro veřejnost a e-správu. V rámci e-služby pro veřejnost probíhají dva komunikační kanály, kterými jsou government-to-citizen (G2C) a government-to-bussiness (G2B). Do této kategorie patří přímé e-služby. E-služby by měly ale uživatelům sloužit i nepřímo, a proto se v terminologii také hovoří o tzv. e-správě, kam spadá komunikace government-to-government (G2G), tedy zdokonalení a modernizování vládních řídících procesů, systémů a podsystémů s využitím ICT, s čímž se také pojí nutnost organizačních změn a změna správních procesů.[13]

Závěrem lze konstatovat, že veřejné e-služby se oproti klasickým e-službám liší v jeho poskytovateli, kterým je organizace či instituce veřejné správy, které jsou specifické právě tím, jak jsou zakládány, řízeny a zabezpečovány. Poskytované veřejné e-služby musí tedy mít oporu v příslušných právních normách.

1.3 E-demokracie a e-participace

Z pojmu demokracie vyplývá státní uspořádání, kde vládne lid. Občané se zapojují do otázek veřejného dění a vlastní správy výkonem úřadů. Postupem času a hlavně v moderním období není přímá demokracie v antickém pojetí možná. To vyplývá hlavně z hlediska geografického a demografického, kterým je vzdálenost centra od periferií a počet obyvatel. V současné době informační a

[12] ANCARANI, Alessandro. *Towards quality e-service in the public sector: The evolution of web sites in the local public service sector,* str. 13
[13] POMAHAČ, Richard. *Veřejná správa,* str. 187

značně elektronizované se v rámci eGovernmentu vyvíjejí snahy a trendy zapojovat občany více do politického dění. E-demokracie a e-participace, jakožto odvětví eGovernmentu, spočívají právě v odstraňování bariér zásahu občanů do rozhodování vlády a tvoření veřejné politiky. Nejčastějšími prostředky jsou konzultace, spolurozhodování či elektronické hlasování v referendu nebo volbách. V současné době představuje toto odvětví mladou oblast, ale do budoucna může být velice důležitá.

Pojmy e-participace a e-demokracie jsou v literatuře často spojovány i oddělovány, ale v principu zůstávají jejich cíle stejné. Hlavním cílem je posílit důvěru obyvatelstva ve vládu a instituce veřejné správy. Literatura také spojuje nástroje e-participace a e-demokracie spíše s projekty typu G2C a G2B. Účelem není posilování komunikace G2G, ale vnášení prvku přímé demokracie do demokracie zastupitelské.[14]

1.4 Informační systémy veřejné správy

Pod pojmem systém se obecně vzato rozumí určitý ucelený a uspořádaný celek, který má své vnitřní a vnější vztahy. Jádro a účel informačního systému pak tkví v organizovaném způsobu uspořádání informací (dat) a jejich následnému zpřístupňování a předávání ostatním účastníkům.[15] Celý systém tedy má být přehledný, uživatelsky přívětivý a skrze tento systém by měla být možná komunikace všech se všemi.

Začátkem je nutno podotknout, že v rámci informačních systémů veřejné správy v České republice se v literatuře hovoří o dvou obdobích. Prvním obdobím se rozumí období do roku 2000 a dále o období následujícím. Toto dělení se odvíjí v souvislosti na rozvoji národní politiky v rámci elektronizace veřejné správy. Rok 2000 je důležitý kvůli přijetí zákona č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen „zákon o ISVS), jehož předmětem je stanovit práva a povinnosti orgánů veřejné správy v rámci vytváření, provozu, správy a užívání informačních systémů ve veřejné správě. Zde už také existuje

[14] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*, str. 8

[15] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*, str. 48

plnohodnotná právní definice informačních systémů veřejné správy, která zní: „*Informačním systémem veřejné správy je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností…*“[16] Problematikou informačních systému veřejné správy a jejich zavádění se pak dále zabývá následující kapitola této práce.

V této kapitole tedy byly stručně vymezeny a přiblíženy základní pojmy eGovernmentu z teoretického hlediska, které jsou používány v následujících kapitolách této práce. Zákon o ISVS je nutné brát jako jeden z prvních nástrojů rozvoje eGovernmentu a tudíž má funkci zastřešující pro mnoho dalších projektů.

[16] Zákon o ISVS, § 2 písm. b)

2 Vývoj a trendy eGovernmentu v Evropské unii

Tato kapitola se zabývá vývojem politiky eGovernmentu v EU a současné trendy členských zemí EU. Na začátek bude blíže popsán vývoj a strategie EU až po současnost. Další část se pak bude zabývat agendou jednotného digitálního trhu 2020.

2.1 Vývoj eGovernmentu v politikách EU

Současné pojetí politiky eGovernmentu v EU dosud velmi vychází z původních iniciativ. eGovernment je v evropských informačních politikách brán jako jeden z nástrojů k vytvoření informační společnosti. Tyto politiky musí být pro správné fungování také do jisté míry standardizovány, aby mohl vzniknout jednotný digitální trh nabízející více či méně stejné e-služby v každém členském státu.

První iniciativou EU byla „*eEurope – An Information Society For All*“, která byla připravena Evropskou komisí v prosinci 1999 a předložena jako dokument na summitu Rady v Lisabonu v roce 2000. Tato iniciativa byla schválena jako akční plán eEurope 2002. V tomto plánu se již objevovaly prvky eGovernmentu ve formě elektronického přístupu k veřejným službám (alespoň těm základním).[17] Úkolem veřejné správy pak mělo být rychlé přizpůsobení se k novým metodám výkonu činnosti, včetně spolupráce se soukromým sektorem, rozšíření elektronického podpisu, elektronizace nejzákladnějších transakcí s Evropskou komisí a základních veřejných údajů.[18]

Státy střední a východní Evropy uznaly strategické cíle lisabonského summitu a dohodly se přijmout akční plán eEurope v rámci pozdější iniciativy eEurope+. V červnu 2002 byla představena další strategická iniciativa eEurope 2005, která se začala soustředit na jednotlivé uživatele. Zdůrazňoval se cíl zabezpečit občanům širokopásmové připojení. Členské státy měly mimo jiné do konce ro-

[17] POMAHAČ, Richard. *Veřejná správa,* str. 191
[18] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*, str. 24

ku 2005 zajistit, aby byly přes širokopásmové připojení k internetu připojeny veškeré instituce veřejné správy.[19]

V září 2003 byl publikován dokument *The Role of eGovernment for Europe's Future*. eGovernment byl vnímán jako nástroj pro větší efektivitu, otevřenost a pružnost veřejného sektoru. Byl zde zdůrazňován propastný rozdíl počítačové gramotnosti ve společnosti. Dále bylo jako cíl vnímáno zvýšení interoperatibility institucí uvnitř států i mezi státy navzájem, což je jedním z hlavních cílů i v současnosti.

V červnu 2005 přijala Evropská komise dokument i2010, který pak přijala v roce 2006 jako i2010 eGovernment Action Plan,[20] který obsahoval 5 hlavních priorit, které měl být splněny do roku 2010. První prioritou bylo poskytnutí přístupu všem složkám obyvatelstva, aby nedocházelo k vyloučení jistých sociálních skupin, které jsou znevýhodněny. Druhou prioritou bylo zvýšit efektivitu administrativy zapojováním informačních technologií do procesu výkonu veřejné správy. Třetí prioritou byla elektronizace zadávání veřejných zakázek, kde se státy zavázaly do roku 2010 mít 100% veřejných zakázek dostupných elektronicky a alespoň 50% jich tak zadávat. Čtvrtou prioritou bylo zajistit realizaci klíčových prvků pro eGovernment, což byla elektronická identita, elektronické podepisování dokumentů a elektronické archivování. Poslední prioritou bylo zvýšit participaci a demokratizaci procesu přijímání rozhodnutí (e-participace).[21]

2.2 Strategie Europe 2020 a eGovernment

V rámci přijetí strategického dokumentu Evropa 2020 byla jako její součást přijata Digitální agenda pro Evropu, jejíž cílem je zajistit udržitelný hospodářský a sociální přínos jednotného digitálního trhu založeného na rychlém a superrychlém internetu a interoperabilních aplikacích.[22] Digitální agenda pro Evropu (dále jen „DAE2020") je jedna ze sedmi hlavních iniciativ strategie Evro-

[19] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*, str. 26
[20] EUROPEAN COMMISSION, i2010 *eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*
[21] Tamtéž
[22] EUROPEAN COMMISSION, *A Digital Agenda for Europe*, str. 3

pa 2020, která byla vypracovaná s cílem vymezit roli zavádění informačních a komunikačních technologií. Na základě konzultací s různými subjekty určila komise v DAE2020 sedm nejvýznamnějších překážek, kterými jsou roztříštěnost digitálních trhů, nedostatečná interoperabilita, rostoucí kyberkriminalita a riziko nízké důvěry, nedostatečné investice do sítí, nedostatečný výzkum a inovace, nedostatky v oblasti počítačové gramotnosti a počítačových dovedností a nakonec promarněné příležitosti při řešení společenských výzev.

Roztříštěnost digitálních trhů je dle DAE2020 nemožnost využívat jednotného digitálního trhu, protože oblast e-služeb toliko nepřesahují hranice, jak by mohly. Je tedy zapotřebí odstranit regulační překážky a usnadnit elektronické platby a elektronické fakturace.

Nedostatečnou interoperabilitou se rozumí nedostatky v normalizaci, zadávání veřejných zakázek a koordinaci veřejných orgánů. Digitální služby a nástroje by měly být založeny na otevřených platformách a podobných normách, aby spolu mohly lépe komunikovat.

Rostoucí kyberkriminalitou a nízkou důvěrou v sítě znamená, že se občané nebudou zapojovat do stále více propracovanějších e-služeb, pokud nebudou mít v on-line prostředí důvěru. Evropa se proto musí zabývat otázkou kybernetických trestných činů, které sahají od dětské pornografie až po krádež identity. Se zvyšujícím se počtem informačních systémů a údajů v nich uložených je nutné vypracovat odpovídající ochranné mechanismy, aby se zamezilo útokům.

Dalším problémem jsou *nedostatečné investice do sítí*. DAE2020 předpokládá, že rychlé a superrychlé internetové sítě budou do budoucna jádrem ekonomiky, a proto je potřeba zavádět a šířit stále rychlejší internetová připojení pro všechny. Evropa by měla podněcovat soukromé investice doplněné veřejnými investicemi.

Nedostatečný výzkum a inovace spočívá v investicích a spolupráci při výzkumu nových informačních a komunikačních technologií, aby mohly IT společnosti v Evropě vytvářet produkty světové kvality.

Předposledním problémem jsou *nedostatky v oblasti počítačové gramotnosti a počítačových dovedností*. Evropa dle DAE2020 trpí rostoucím nedostatkem odborných znalostí v oblasti IT a počítačové gramotnosti, což způsobuje vy-

loučení občanů z digitální společnosti a ekonomiky. Tyto nedostatky pak zpomalují růst produktivity, které zavádění IT technologií má.

Promarněné příležitosti při řešení společenských výzev ve zkratce znamenají zabývat se těmi nejožehavějšími společenskými tématy, kterými jsou např. změna klimatu, životní prostředí, stárnoucí obyvatelstvo a rostoucí zdravotní náklady, aby se naplnil plný potenciál informačních a komunikačních technologií.

Cíle pro DAE byly pak specifikovány v Evropském akčním plánu „eGovernment" na období 2011 – 2015[23]. V tomto dokumentu byly specifikovány čtyři politické priority, které měly být do konce roku 2015 splněny. První prioritou bylo umožnit občanům a podnikům používat veřejné e-služby a zlepšit přístup k veřejným informacím a zlepšit transparentnost. Mobilita na jednotném trhu byla další prioritou, jež měla být zajištěna pohodlným poskytováním e-služeb pro zřizování a provozování podniků, pro studium, práci, pobyt a důchod kdekoli v Evropské unii. Třetí prioritou bylo podporovat využívání elektronické správy za účelem snížení administrativní zátěže a zlepšení organizačních procesů. Poslední priorita spočívala ve vytváření vhodných klíčových prostředků a nezbytných právních a technických předpokladů.[24]

V současnosti stanoví cíle v rámci strategie DAE2020 Evropský akční plán „eGovernment" na období 2016 – 2020 (dále jen „eGAP2020"), jehož vizí je, že do roku 2020 budou orgány veřejné správy otevřené a měly by nabízet vstřícné, účinné a komplexní e-služby všem občanům a podnikům v EU. Tento plán má za cíl modernizovat veřejnou správu, dosáhnout jednotného digitálního trhu a zapojit více občany a firmy při vytváření vysoce kvalitních veřejných služeb.[25]

Aby se dosáhlo těchto cílů a vizí, stanoví eGAP2020 tři hlavní priority, kterými jsou modernizace veřejné s využitím klíčových digitálních technologií, umož-

[23] EUROPEAN COMMISSION, *The European eGovernment Action Plan 2011-2015: Harnessing ICT to promote smart, sustainable & innovative Government*
[24] Tamtéž, str. 3
[25] MINISTERSTVO VNITRA. *Akční plán pro eGovernment na období 2016-2020*

nění přeshraniční mobility občanů a firem pomocí interoperabilních veřejných služeb a usnadnění digitální interakce mezi orgány veřejné správy a uživateli.[26]

Dokument eGAP2020 obsahuje celkem 20 opatření rozdělených do těchto tří priorit. V rámci první priority jimi jsou podpora přechodu členských států k plnému zavedení elektronických veřejných zakázek a využití registru smluv, zavedení služby eID, revize současného Evropského rámce interoperability, společné stavební prvky a koordinace rozvoje prototypu pro evropský katalog standardů informačních a komunikačních technologií pro veřejné zakázky.[27]

V rámci priority druhé jsou jimi například *Single Digital Gateway*, což je v podstatě evropský portál veřejné správy, dále *European eJustice Portal* (nástroj přímé komunikace mezi občany a soudy jiných členských států), rozvoj elektronického propojení insolvenčních rejstříků skrze *European eJustice Portal* a povinné propojení obchodních rejstříků všech členských států.[28]

Hodnocení využití principu „*pouze jednou*“ pro občany v přeshraničním styku,[29] urychlit rozvoj a přijetí směrnice INSPIRE (standardizované sbírání, využívání a popis dat týkajících se prostorových informací jako jsou podzemní vody, teplota vzduchu, dopravní sítě a využití půdy) a transformace webových stránek pro podporu většího zapojení občanů a podniků při vytváření politiky EU jsou pak cíli v rámci poslední priority.

[26] EUROPEAN COMMISSION, *EU eGovernment Action Plan 2016-2020: Accelerating the digital transformation of government*

[27] Tamtéž, str. 6 – 9

[28] Tamtéž, str. 9 – 11

[29] Princip „only once“ znamená, že občané jiných členských států budou muset své údaje poskytnout a potvrdit správnost pouze jednou a nebudou takto muset činit znovu, protože budou vedeni v národních evidencích.

3 Prvky eGovernmentu v České republice

Tato kapitola se zabývá procesem elektronizace veřejné správy v České republice. Nejprve je vymezen historický vývoj, od kterého se pak odvíjí rozbor a představení nástrojů eGovernmentu v praxi užívaných.

3.1 Historický vývoj

Jak bylo uvedeno výše, proces elektronizace veřejné správy se dle literatury dělí do několika období. První programová prohlášení vlády, ať už republiková, či federální, byla zaměřena hlavně na reformaci veřejné správy a v rámci eGovernmentu pouze na dobudování komunikace mezi finančními a daňovými správami.[30] V roce 1991 byla vytvořena *Komise vlády ČR pro Státní informační systém* (dále jen „SIS“). Tato komise měla za úkol zajistit odstranění roztříštěnosti informačních systémů veřejné správy a koordinovat vytvoření jednotného informačního systému.[31] Do roku 2000 si totiž mohl každý resort nakupovat vlastní výpočetní techniku a zřizovat své informační systémy, které ale pak meziresortně nekomunikovaly, nebo byla komunikace obtížná.[32]

Řešení SIS počítalo hlavně s rozhodující úlohou registru občanů, nemovitostí, hospodářských subjektů, územně identifikačního registru a s ohledem na státní politiku také s jednotným státním informačním systémem. Kompetence komise pak přešly na ministerstvo hospodářství a po jeho zrušení na Úřad vlády ČR. V roce 1996 pak byl vytvořen Úřad pro státní informační systém. Postavení tohoto úřadu bylo slabé, protože jednotliví správci informačních systémů byli stále resortní. S cílem koordinovat státní informační politiku byla pak v roce 1998 zřízena Rada vlády pro informační politiku, jejímž účelem bylo zpracovat a předložit vládě strategický dokument Státní informační politika, ve kterém byla obsažena také koncepce budování informačních systému veřejné správy.

[30] POMAHAČ, Richard. *Veřejná správa,* str. 208

[31] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*, str. 53

[32] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*, str. 48

Dokument *Státní informační politika – cesta k informační společnosti* (SIP) je dle literatury považován za první zlomový dokument v rámci eGovernmentu, jelikož přináší první ucelené koncepce elektronizace veřejné správy.[33] Tato koncepce již počítala s vytvářením portálů veřejné správy, vznikem základních registrů občanů, nemovitostí, elektronických podpisů a kontaktních míst veřejné správy.

Na SIP pak navazovala koncepce budování informačních systémů veřejné správy, kde byla koordinace a propojení těchto informačních systémů samostatnou prioritou. Realizaci zmíněných konceptů měl pak dále napomoci zákon č. 365/2000 Sb., o informačních systémech veřejné správy.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy stanoví práva a povinnosti související s vytvářením, užíváním, správou a rozvojem informačních systémů veřejné správy. Tento zákon mimo jiné v současné době upravuje také Portál veřejné správy a kontaktní místa veřejné správy Czech POINT.

Tento zákon lze brát v potaz jako obecný zastřešující právní rámec informačních systémů veřejné správy. Ustanovení § 2 tohoto zákona vymezuje základní pojmy jako informační činnost, informační systém veřejné správy, uživatel, provozovatel a správce informačního systému a například i referenční rozhraní.

Zákon mimo to, že hovoří o informačních systémech obecně, rozlišuje ještě tři specifické druhy takovýchto systémů. Rozlišuje portál veřejné správy, veřejný informační systém a provozní informační systém. Portál veřejné správy je takový informační systém, který usnadňuje získávání základních informací o činnosti veřejné správy uživatelům skrze dálkový přístup. Veřejným informačním systémem je systém vedený orgánem veřejné správy poskytující služby, které mají vazbu na informační systémy. Provozním informačním systémem se potom rozumí informační systém, který zajišťuje informační a komunikační služby uvnitř příslušného orgánu. Tedy služby související s provozem daného orgánu, které nesouvisejí přímo s výkonem veřejné správy.

Mimo to je důležité upozornit, že tento zákon se nevztahuje na informační systémy vedené zpravodajskými službami, Národním bezpečnostním úřadem, Ná-

[33] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*, str. 55

rodním úřadem pro kybernetickou a informační bezpečnost a na informační systémy sloužícími pro potřeby nakládání s utajovanými informacemi.[34]

Důležitým zlomem v oblasti eGovernmentu bylo zřízení Ministerstva informatiky České republiky zřízené s účinností zákona č. 517/2002 Sb., ve znění pozdějších předpisů. V souvislosti se zřízením tohoto ministerstva se hovořilo o snaze vlády zastřešit celý rozvoj eGovernmentu pod jednu instituci. Ministerstvo informatiky bylo ústředním orgánem státní správy pro informační a komunikační technologie, zabývalo se rovnou soutěží na telekomunikačním trhu a rozvojem elektronického obchodu, mělo podporovat počítačovou gramotnost, a hlavně bylo koordinátorem v rozvoji eGovernmentu, a to i v rámci meziresortní spolupráce. Ministerstvo informatiky bylo zrušeno k 1. 6. 2007 zákonem č. 110/2007 Sb., a jeho kompetence přešly na Ministerstvo vnitra, Ministerstvo průmyslu a obchodu a Ministerstvo pro místní rozvoj. Zrušením ministerstva informatiky začíná další etapa rozvoje eGovernmentu v České republice. Takto tedy vypadal stručný vývoj eGovernmentu do roku 2006 a nyní už je vhodné se soustředit na jednotlivé projekty.

3.2 Portál veřejné správy

Portál veřejné správy přístupný na adrese http://portal.gov.cz byl spuštěn do provozu 6. 10. 2003. V obecném slova smyslu se portálem rozumí vstup většinou honosně vyzdobený. V rámci eGovernmentu se jím také rozumí vstup, který poskytuje utříděné a vzájemné propojené informace o institucích, jejich činnostech a výsledcích.[35] Zatímco původně portály označovaly místa na internetu, která měla slučovat všechny služby do jednotného rozhraní, v dnešním slova smyslu jsou portály spíše sbírkou odkazů nebo uzavřeným informačním systémem, ačkoliv hlavní znak, kterým je dálkový přístup, zůstává.[36]

Správcem portálu veřejné správy je Ministerstvo vnitra. Portál veřejné správy je mezi ostatními portály nejvýznamnější hlavně kvůli své univerzálnosti a obsáhlosti. Portálem veřejné správy je dle zákona o ISVS informační systém ve-

[34] Zákon o ISVS, § 1 odst. 2
[35] VODIČKA, Milan. *3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli*, str. 132
[36] MATES, Pavel a Vladimír SMEJKAL. *E-government v českém právu*, str. 70

řejné správy zajišťující přístup k informacím státních orgánů, orgánů územních samosprávných celků a orgánů veřejné moci, které nejsou orgány státní ani orgány územně samosprávných celků.[37]

První funkcí portálu veřejné správy je zajišťování přístupu k informacím získaným na základě informační činnosti[38] veřejných orgánů zejména v oblasti sociálního zabezpečení, zdravotnického zabezpečení, správy veřejných financí, dotací, veřejných zakázek, státní statistické služby, evidence a identifikace osob, jejich součástí a práv a povinností těchto osob či jejich součástí a tvorby a publikace právních předpisů.[39]

Další funkcí se pak rozumí zajišťování komunikace uživatelů s orgány veřejné správy prostřednictvím datových schránek a kontaktních míst veřejné správy.[40] Dochází zde tedy k provázání portálu veřejné správy se systémem datových schránek, které jsou jako další projekt v rámci eGovernmentu specifikovány dále. Poslední funkcí portálu veřejné správy je přístup k informacím fyzických a právnických osob, a to především díky elektronickým formulářům, a komunikace s těmito osobami.[41] Takovéto zpřístupnění informací pak probíhá za úplatu, která je příjmem státního rozpočtu.

Po otevření portálu veřejné správy lze ihned spatřit jeho základní dělení. Portál veřejné správy se dělí do čtyř kategorií, jimiž jsou občan, podnikatel, cizinec a úředník.[42] Pro každou z kategorií se dále portál veřejné správy dělí na oblast průvodce životními situacemi, služby a užitečné odkazy. Průvodce životními situacemi se dělí na další oblasti podle předmětu. Například občan bude chtít vědět více o změně jména či příjmení, stačí se postupně skrze oddíl rodina dostat až na změnu jména a příjmení, přičemž výsledkem je stručný návod jak změnu provést.

Občan se tedy dozví základní informace, kdo je oprávněn v této věci jednat, na které instituci tuto věc řešit či dle jakých právních předpisů se postupuje. Důle-

[37] Zákon o ISVS, § 6f
[38] Tamtéž, § 2 písm. a)
[39] Tamtéž, § 6f odst. 2
[40] Tamtéž, § 6f odst. 3
[41] Tamtéž, § 6f odst. 4
[42] VODIČKA, Milan. *3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli*, str. 153

žité je zmínit, že u každého návodu nechybí poslední aktualizace a také orgán, který odpovídá za správnost daného návodu. V případě změny jména či příjmení odpovídá za správnost návodu Ministerstvo vnitra, konkrétně odbor všeobecné správy, oddělení státního občanství a matrik.

Mezi poskytované služby portálu veřejné správy patří věstníky, formuláře, seznam datových schránek, povinně zveřejňované informace obcí. Formuláře lze vyplnit online, ale prozatím je podmínkou vlastnit datovou schránku.

Portál veřejné správy je tedy v celku univerzální portál zaměřující se na poskytování informací uživatelům s prvky komplexnější jednosměrné a jednoduché obousměrné komunikace. Přínos lze spatřit hlavně v průvodci životními situacemi, který opravdu poskytuje stručný a srozumitelný návod na chování v různých situacích, které mohou nastat u každého.

3.3 Czech POINT

Dalším projektem v rámci eGovernmentu jsou kontaktní místa veřejné správy upravené § 8a zákona o ISVS. Prostřednictvím kontaktního místa lze v rozsahu a za podmínek stanovených jinými právními předpisy činit podání správním orgánům. Kontaktní místo také může doručovat dokumenty veřejných orgánů. Czech POINT je zkratkou pro Český podací ověřovací informační národní terminál.[43]

Dle zákona o ISVS jsou kontaktními místy notáři, krajské úřady, matriční úřady, obecní úřady (včetně úřadů městských částí nebo obvodů statutárních měst a hlavního města Prahy), zastupitelské úřady stanovené prováděcím předpisem, držitel poštovní licence, Hospodářská komora České republiky a banka, která k tomu byla autorizována Ministerstvem vnitra.

Významným institutem v rámci Czech POINTu je vydávání ověřených výstupů z informačních systémů veřejné správy, což ve zkratce znamená, že provozova-

[43] Zákon o ISVS, § 8a odst. 1

tel informačního systémů z něho na požádání vydává částečné nebo úplné výpisy.[44]

Zákon o ISVS pak v této souvislosti rozlišuje mezi veřejnými a neveřejnými evidencemi, rejstříky a seznamy. Do první kategorie patří především často používané informační systémy, jakými jsou například obchodní rejstřík a katastr nemovitostí. Do druhé kategorie pak můžeme zařadit evidenci rejstříků trestů, matriky či základní registry. Institut vydávání ověřených výstupů kontaktními místy je důležitý hlavně v jeho právní závaznosti, jelikož je takovýto výstup dle § 9 odst. 4 zákona o ISVS veřejnou listinou. Co je veřejnou listinou, vymezuje například § 53 zákona 500/2004 Sb., *Správní řád*. Veřejnou listinou se rozumí listina vydaná soudy, jinými státními orgány, orgány územně samosprávných celků a listina, která je zvláštním právním předpisem označena za veřejnou. U veřejné listiny platí presumpce správnosti, a pokud někdo tvrdí opak, musí unést důkazní břemeno. Správnost poskytovaného výstupu se pak potvrzuje ověřovací doložkou, kde kromě potvrzení totožnosti výstupu se záznamem v informačním systému nalezneme údaj o tom, z kolika listů se výstup skládá, místo a datum vyhotovení doložky, pořadové číslo a otisk úředního razítka a podpis ověřujícího.[45]

3.3.1 Služby Czech POINT

V současné době lze služby Czech POINTu rozdělit do následujících kategorií:

1) Poskytování výpisů z informačních systémů veřejné správy
2) Podání vůči státní správě
3) Základní registry
4) Datové schránky
5) Konverze na žádost a související služby
6) Zprostředkovaná identifikace osoby[46]

V rámci první kategorie, kromě již výše zmíněných výpisů, lze získat na kontaktních místech také výpis z insolvenčního rejstříku, výpis z bodového hodno-

[44] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*, str. 73
[45] Zákon o ISVS, § 9a
[46] CZECHPOINT. *Jaké služby poskytuje Czech POINT?*

cení řidiče, výpis z veřejných rejstříků (rejstříky spolků, nadací, ústavů atd.) a výpis z živnostenského rejstříku. V rámci druhé kategorie je možné využít Czech POINT k registraci do MA ISOH[47], kvůli evidenci autovraků a nakládání s nimi. Další službou v rámci této kategorie je podání podle živnostenského zákona.[48] Tedy ohlásit živnost, ohlásit nebo změnit údaje vedené v živnostenském rejstříku, podat žádost o udělení koncese a podat žádost o změnu rozhodnutí o udělení koncese. Třetí kategorií jsou základní registry, konkrétně základní registr obyvatel (registr obyvatel) a základní registr osob (registr osob). V rámci této agendy lze požadovat výpis, změnu údajů či výpis o využití referenčních údajů.

Další kategorií služeb jsou datové schránky. Datové schránky lze na místech Czech POINT zřizovat, znepřístupnit, přidat ověřenou osobu či zneplatnit takovéto osobě přístup. Datové schránky jsou rozebrány v další části této práce. Předposlední kategorií služeb Czech POINTu je konverze na žádost a s tím související služby. Konverzí se myslí úplné převedení dokumentu v listinné podobě do elektronické podoby způsobem, který zajistí obsahovou shodu těchto dokumentů, s připojením doložky o provedení konverze a převedení dokumentu v elektronické podobě do podoby listinné. Souvisejícími službami této agendy pak jsou evidence ověřovacích doložek a úschova konvertovaných dokumentů. Poslední kategorií je zprostředkovaná identifikace osoby, kterou se rozumí ověření totožnosti žadatele. Výstupem tohoto procesu je vystavení veřejné listiny o identifikaci.[49]

Jak lze z popisu vidět, kontaktní místa veřejné správy Czech POINT je projekt, který má usnadnit a zastřešit základní služby poskytované veřejnou správou. Důležité je zmínit, že Czech POINT zavedl také rozhraní CzechPOINT@home a CzechPOINT@office. První ze zmíněných je určen pro fyzické osoby, které mají zřízenou vlastní datovou schránku. Občan může v tomto rozhraní požádat o výpis nebo změnu údajů týkajících se základních registrů nebo požádat o vý-

[47] Modul Autovraky Informačního systému odpadového hospodářství
[48] Zákon č. 455/1991 Sb., o živnostenském podnikání
[49] CZECHPOINT. *Jaké služby poskytuje Czech POINT?*

pis z ostatních rejstříků ať už veřejných, či neveřejných.[50] V rámci CzechPOINT@office mohou úředníci v rámci svého výkonu působnosti požadovat výpis a opis z rejstříku trestů, výpis ze základních registrů, konverzi dokumentů z moci úřední a vykonávat úkony v rámci matrik, ohlašoven a soudů.[51]

3.4 Datové schránky

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (dále jen „zákon o eGovernmentu“) přinesl první úpravu datových schránek určených pro elektronickou komunikaci mezi orgány veřejné moci a fyzickými a právnickými osobami a mezi orgány veřejné moci navzájem. Datovou schránkou je dle § 2 zákona o eGovernmentu elektronické úložiště určené k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci a dodávání dokumentů fyzických osob, fyzických osob podnikajících a osob právnických. Správcem a zřizovatelem datových schránek je Ministerstvo vnitra.

3.4.1 Zřizování datových schránek

Zákon v případě datových schránek rozlišuje datové schránky fyzických osob, podnikajících fyzických osob, právnických osob a datových schránek orgánů veřejné moci. Datové schránky orgánů veřejné moci, právnických osob zapsaných v obchodním rejstříku a právnických osob zřízených ze zákona jsou zřízeny povinně ze zákona Ministerstvem vnitra. Datovou schránku také bezplatně zřídí Ministerstvo vnitra advokátu, statutárnímu auditorovi, daňovému poradci a insolvenčnímu správci bezodkladně po obdržení informace o jeho zápisu do zákonem stanovené evidence. Datovou schránku mohou na žádost také získat ostatní právnické osoby, fyzické osoby a fyzické osoby podnikající.

Rozdíly nejsou pouze v zákonné povinnosti zřizovat datové schránky, ale také v možném počtu datových schránek na jeden subjekt. Fyzické osoby, fyzické osoby podnikající a právnické osoby mají nárok na zřízení jedné datové

[50] CZECHPOINT. *CzechPOINT@home*
[51] CZECHPOINT. *Služby pro úředníky*

schránky, kdežto orgány veřejné moci a orgány územních samosprávných celků mohou požádat o zřízení další datové schránky.

Zákon stanovil povinnou komunikaci mezi orgány veřejné moci pomocí datových schránek, pokud to umožňuje povaha dokumentu a nedoručuje-li se na místě. Dále také stanovil takovouto formu i při doručování písemností ve správním řízení.[52] Správní orgán v první řadě doručuje písemnosti veřejnou datovou sítí do datových schránek. Teprve nelze-li takto doručit, může správní orgán písemnost doručit prostřednictvím provozovatele poštovních služeb. Provádění úkonů vůči orgánům veřejné moci ale ze zákona povinné není.[53]

3.4.2 Přístup do datové schránky

Subjekty oprávněné k přístupu do datové schránky se liší tím, pro jaký subjekt byla zřízena. Osoby oprávněné k přístupu do datové schránky stanovil § 8 zákona o eGovernmentu. K přístupu do datové schránky fyzické osoby a fyzické osoby podnikající je oprávněna osoba, pro kterou byla tato schránka zřízena. Do datové schránky právnické osoby je oprávněn statutární orgán právnické osoby, člen statutárního orgánu právnické osoby nebo vedoucí organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku. U orgánu veřejné moci je pak oprávněn vedoucí tohoto orgánu. Výše uvedené osoby jsou ze zákona zmocněny žádat o znepřístupnění a opětovné zpřístupnění datové schránky, proto jsou dle literatury označovány jako osoby primární.[54]

Primární osoby mohou dále určit, že úkony, které jsou jim ze zákona vyhrazeny ve vztahu k pověřeným osobám a k ministerstvu, může činit fyzická osoba k tomu pověřená a označovaná jako administrátor. Dále také mohou primární osoby a administrátor pověřit jinou fyzickou osobu k přístupu do datové schránky, a to v rozsahu jimi stanoveném.

[52] Zákon č. 500/2004 Sb., Správní řád, § 19

[53] Zákon o eGovernmentu, § 18

[54] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*, str. 189

3.4.3 Přihlašování do datové schránky

Přihlásit se do datové schránky lze v současné době několika způsoby. Přihlášení probíhá prostřednictvím přístupových údajů nebo elektronických prostředků, elektronicky čitelných identifikačních dokladů či elektronických prostředků třetích osob.

Prvním ze zmíněných, tedy přístupové údaje, je přihlášení pomocí uživatelského jména a hesla. Tento způsob je nejjednodušší a nabízí základní zabezpečení ověření identity. Přístupové údaje zajišťuje Ministerstvo vnitra.[55] Ministerstvo vnitra zašle do vlastních rukou přístupové údaje oprávněné osobě bezodkladně po zřízení datové schránky. Datová schránka se pak aktivuje prvním přihlášením oprávněné osoby nebo uplynutím patnáctého dne po dni doručení přístupových údajů.[56]

Přihlásit se k datové schránce lze také pomocí strojově čitelných dokladů. V současné době se tento způsob týká hlavně občanských průkazů se strojově čitelnými údaji a s kontaktním elektronickým čipem, ve kterém jsou zapsány údaje uvedené v § 3 odst. 2 písm. a) až c) a v odstavci 5 téhož paragrafu zákona č. 328/1999 Sb., o občanských průkazech.

Další způsob přihlašování do datové schránky je pomocí certifikátu, který lze zakoupit na pobočkách Czech POINT. Certifikát lze mít nainstalovaný v počítači či ho typicky mít uložený na datovém nosiči. Po provedené registraci certifikátu v datové schránce pak už není možné se přihlásit pouze prostřednictvím přístupových údajů. Takovýto způsob je bezpečnější, ale vyžaduje mít certifikát buď nainstalovaný v daném počítači, nebo ho nosit stále u sebe.[57]

Datové schránky pak nabízí ještě další způsoby přihlašování, kterými jsou SMS autentizace a OTP (One Time Password) autentizace. Tento typ autentizace probíhá prostřednictvím mobilních zařízení, a to formou zasílání textových zpráv s bezpečnostním kódem či použitím generátoru jednorázových kódů.

---

[55] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*, str. 191

[56] Zákon o eGovernmentu, §§ 9 a 10

[57] DATOVÉ SCHRÁNKY. *Rozšířená autentizace*

3.4.4 Znepřístupnění datové schránky

Ministerstvo vnitra znepřístupní datovou schránku v případech uvedených v § 11 odst. 1 až 5 zákona o eGovernmentu. Nejprve je nutné si uvědomit, že znepřístupnění není to samé jako zrušení. V případě znepřístupnění datové schránky se jedná o její deaktivaci a následné nemožnosti do datové schránky doručovat či skrze ni činit právní úkony. Samotná datová schránka v tomto případě není zrušena a v určitých případech ji lze znovu zpřístupnit.

Obecně Ministerstvo vnitra zruší datovou schránku fyzické osoby a podnikající fyzické osoby, dnem jejího úmrtí, prohlášením za mrtvého, nabytím právní moci rozhodnutí o zbavení nebo omezení svéprávnosti anebo dnem, kdy byla tato osoba omezena na osobní svobodě z důvodu vzetí do vazby, výkonu trestu odnětí svobody, zabezpečovací detence nebo ochranného léčení. Pro fyzické osoby podnikající stejně jako pro právnické osoby pak dále platí, že ministerstvo zruší danou datovou schránku ke dni výmazu dané osoby ze zákonem stanovené evidence. Ministerstvo také znepřístupní datové schránky soukromoprávním uživatelům a orgánům veřejné moci ke dni jejich zrušení popř. pozastavení nebo přerušení působnosti. Ve výše zmíněných případech je zákonem umožněno znepřístupnit datovou schránku i zpětně.

Zákon také umožňuje znepřístupnit datovou schránku na základě podání žádosti ministerstvu. Takto lze zrušit pouze datové schránky, které vznikly na základě žádosti a ne ze zákona. Například lze takto zrušit datové schránky fyzických osob, fyzických osob podnikajících (kromě osob uvedených v § 4 odst. 3 zákona), tzv. ostatních právnických osob neuvedených v § 5 odst. 1 a u orgánů veřejné moci to lze pouze u dalších datových schránek.

Jak již bylo zmíněno výše, znepřístupněnou datovou schránku lze znovu zpřístupnit, a to na žádost oprávněné osoby, pokud byla datová schránka znepřístupněna na žádost. V případě orgánů veřejné moci a soukromoprávních uživatelů s pozastavenou nebo přerušenou působností se datová schránka zpřístupní ke dni vymazání takového údaje z příslušné evidence.

3.4.5 Zneplatnění přístupových údajů

Zneplatnění údajů je institut využívaný při ztrátě přístupových údajů či jejich odcizení. Zneplatnit údaje lze také statutárním orgánům právnických osob nebo

jejím jednotlivým členům, pokud už statutárním orgánem nejsou nebo pozbyli danou funkci. Zneplatnění probíhá neprodleně po oznámení oprávněnou osobou a současně s tím jsou této osobě zaslané nové přístupové údaje.

3.4.6 Zrušení datové schránky

Dle § 13 zákona o eGovernmentu ministerstvo zruší datovou schránku fyzické osoby po uplynutí 3 let ode dne úmrtí fyzické osoby, případně dne, který je v rozhodnutí soudu o prohlášení za mrtvého uveden jako den úmrtí, datovou schránku podnikající fyzické osoby po uplynutí 3 let ode dne výmazu podnikající fyzické osoby ze zákonem stanovené evidence, datovou schránku právnické osoby po uplynutí 3 let ode dne zániku právnické osoby nebo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, které nemají právního nástupce, případně ode dne jejich výmazu ze zákonem stanovené evidence, datovou schránku orgánu veřejné moci po uplynutí 3 let ode dne po jeho zrušení a v případě, že orgán veřejné moci zaniká výmazem z evidence podle jiného právního předpisu, po uplynutí 3 let ode dne uvedeného v rejstříku orgánů veřejné moci a soukromoprávních uživatelů údajů jako den jeho zániku.

Po dobu těchto 3 let sice už nebudou datové schránky dostupné bývalým oprávněným osobám, ale s jejich obsahem se v případě nutnosti lze seznámit (např. při správním či soudním řízení).[58] Ovšem problém lze v tomto případě spatřit v archivaci datových zpráv. Každá datová zpráva se po uplynutí 90 dní od jejího doručení vymaže.[59] Doručením se dle zákona rozumí okamžik přihlášení osoby, s ohledem na rozsah její oprávnění, s přístupem k dané datové zprávě, nebo uplynutí lhůty 10 dnů od dodání datové zprávy (doručení fikcí). Z toho vyplývá, že oprávněné osoby by si měly ve svém zájmu zprávy archivovat či využít konverze dokumentů.

[58] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*, str. 198
[59] DATOVÉ SCHRÁNKY. *Všeobecné dotazy*

3.4.7 Informační systém datových schránek

Informační systém datových schránek je informačním systémem veřejné zprávy dle zákona o ISVS. Tento informační systém obsahuje informace o datových schránkách, jejich uživatelích a veškeré činnosti týkající se obsahu datových schránek dle § 14 zákona o eGovernmentu. Obsah zpráv je nepřístupný, ale lze se zde dozvědět např. datum a čas odeslání datové zprávy, datum přihlášení oprávněné osoby či datum odeslání dokumentu včetně hodiny a sekundy. Správcem tohoto informačního systému je Ministerstvo vnitra a provozovatelem je Česká pošta, s. p.

3.5 Autorizovaná konverze dokumentů

Zákon o eGovernmentu pojednává také o konverzi dokumentů, což je nedílnou součástí užívání datových schránek. Konverzí se dle § 22 zákona rozumí úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě a naopak, přičemž se dokument konvertuje takovým způsobem, aby byla zajištěna shoda obsahu těchto dokumentů, a následně se připojí doložka o provedení konverze. Zákon zde taky jasně stanoví, že dokument, který konvertováním vznikne, se označuje „výstup“ a má stejné právní účinky jako dokument, ze kterého vznikl.

Konverze dokumentů na žádost se provádí na kontaktních místech veřejné správy dle zákona o ISVS a také ji mohou provádět advokáti za podmínek stanovených zákonem č. 85/1996 Sb., *o advokacii*. Konverzi dokumentů z moci úřední pak provádějí orgány veřejné moci pro výkon své působnosti. Účelem konverze dokumentů jako nástroje je zajistit takový postup, který převede dokument z jedné formy do druhé, aniž by u něj došlo k oslabení funkce důkazního prostředku.[60]

3.6 Základní registry

Už od poloviny 90. let byla diskutována potřeba zřídit informační systém, který by obsahoval systematicky uspořádané údaje, u kterých by nebyla potřeba ově-

[60] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*, str. 225

řovat jejich správnost. Účelem bylo zajistit využívání údajů, které by mohly být danými subjekty aktualizovány a sdíleny, aby nedocházelo k roztříštěnosti informací a jejich případné nesprávnosti. Tento záměr byl realizován až v roce 2009 zákonem č. 111/2009 Sb., o základních registrech (dále jen „zákon o základních registrech). Tento zákon vymezuje obsah základních registrů, informačního systému základních registrů, informačního systému územní identifikace a stanoví práva a povinnosti související s jejich vytvářením, užíváním a provozem. Dále také zřizuje Správu základních registrů.

3.6.1 Vymezení pojmů základních registrů

Zákon o základních registrech přinesl v té době mnoho nových pojmů, které jsou dnes sice už více zažité, ale je dobré je na začátek vymezit. Základním registrem je dle § 2 tohoto zákona informační systém veřejné správy dle zákona o ISVS. Základních registrů je hned několik. Dle § 3 zákona jsou jimi základní registr obyvatel (registr obyvatel), základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (registr osob), základní registr územní identifikace, adres a nemovitostí (registr územní identifikace) a posledním je základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností (registr práv a povinností).

Institutem pro funkci základních registrů je také referenční údaj, kterým je dle § 2 zákona o základních registrech údaj vedený v základním registru, který je jako referenční údaj označen. Referenční údaje se liší dle příslušného základního registru. Obecně vzato je referenční údaj státem garantovaný správný údaj v daném základním registru, ze kterého čerpají orgány veřejné moci při své činnosti, aniž by musely ověřovat správnost těchto údajů.[61]

Orgánem veřejné moci je státní orgán, územní samosprávný celek a fyzická nebo právnická osoba se svěřenou působností v oblasti veřejné správy. Zákon také definuje soukromoprávního uživatele, který není orgánem veřejné moci, ale bylo mu na základě zvláštních předpisů svěřeno oprávnění využívat údajů ze základních registrů.

[61] SPRÁVA ZÁKLADNÍCH REGISTRŮ. *Referenční údaj*

Agenda je dalším institutem, kterým se rozumí ucelená oblast působnosti orgánu veřejné moci nebo ucelená oblast působení soukromoprávního uživatele údajů. Na tento institut navazuje agendový informační systém, což je informační systém veřejné správy sloužící k výkonu agendy, využívání elektronických formulářů nebo elektronické identifikace. Z toho dále vychází pojem editor, což je orgán veřejné moci oprávněný zapisovat a provádět změny v základním registru.

Zákon také zavádí informační systém základních registrů jako informační systém veřejné správy, který slouží ke sdílení dat mezi jednotlivými registry navzájem, základními registry a agendovými informačními systémy a agendovými informačními systémy navzájem.

3.6.2 Správa základních registrů

Zákon o základních registrech zřídil Správu základních registrů se sídlem v Praze jakožto správní úřad podřízený Ministerstvu vnitra. Dle § 7 zákona je tento úřad správcem informačního systému základních registrů a mezi jeho hlavními úkoly je zajišťovat provoz základních registrů, realizovat vazby mezi základními registry, realizovat vazby mezi základními registry a agendovými informačními systémy a realizovat vazby mezi agendovými informačními systémy navzájem. To vše skrze informační systém základních registrů. Dále také vede záznamy o událostech souvisejících s provozováním základních registrů, zpřístupňuje referenční údaje obsažené v základních registrech, agendových informačních systémech. V neposlední řadě také zveřejňuje aktuální údaje o provozním stavu základních registrů.

Správa základních registrů je v podstatě pouze technickým pracovištěm Ministerstva vnitra a není oprávněna k přístupu k obsahu referenčních údajů v základních registrech s výjimkou přístupu v rámci její agendy. Správa základních registrů pak dále v případě důvodného podezření, že orgán veřejné správy nebo soukromoprávní uživatel neoprávněně přistupuje k referenčním údajům, informuje neprodleně Úřad pro ochranu osobních údajů.

3.6.3 Vydávání ověřených výstupů

Osobám se poskytují údaje, které jsou o nich vedeny v základních registrech dle zákona o ISVS. Dále mají tyto osoby nárok na poskytnutí záznamu o využívání jejich údajů v základním registru. V prvním případě se tak děje prostřednictvím ověřeného výstupu z informačního systému veřejné správy. Poskytování záznamu o využívání údajů lze získat i prostřednictvím datové schránky. Pokud má daná osoba zřízenou datovou schránku, zasílá se jí záznam o využívání jejich údajů bezplatně, vždy za uplynulý kalendářní rok.

Při změně referenčního údaje se také zasílá bezplatně dané osobě bezplatně výpis referenčních údajů z příslušného základního registru. Komunikace v tomto případě probíhá pouze skrze datové schránky. Pokud daná osoba nemá zřízenou datovou schránku, výpis se neposkytuje.

Pokud daná osoba dále zjistí nesoulad referenčních údajů o ní vedených se skutečným stavem, může bezplatně požádat o změnu referenčních údajů příslušného editora. Žádost může daná osoba podat i prostřednictvím kontaktního místa veřejné správy.

3.6.4 Registr obyvatel

Dle §16 až § 17 zákona o základních registrech se v registru obyvatel nachází údaje o fyzických osobách (subjekty registru obyvatel), jimiž jsou státní občané České republiky, cizinci v rámci trvalého pobytu, dlouhodobého víza nebo dlouhodobého pobytu. Dále jsou jimi občané členských států Evropské unie, občané států, které jsou vázány mezinárodní smlouvou sjednanou s Evropským společenstvím, a občané států v rámci Evropského hospodářského prostoru a jejich rodinní příslušníci, kteří hodlají na území České republiky pobývat déle než 3 měsíce. V registru obyvatel jsou také vedeni cizinci, kterým byla na území České republiky udělena mezinárodní ochrana formou azylu či doplňkové ochrany. Poslední kategorií jsou fyzické osoby, o nichž tak stanoví zvláštní právní předpis.

V registru obyvatel se vedou příjmení, jméno, adresa místa pobytu (případně též adresa na doručování písemností), datum, místo a okres narození (u osob narozených v cizině datum, místo a rodný stát). Dále se vedou údaje o úmrtí (datum, místo a okres, popř. stát úmrtí), údaje o státním občanství (popř. více

státních občanství), čísla a druhy elektronicky čitelných identifikačních dokladů a typ a identifikátor datové schránky, je-li tato datová schránka zpřístupněna. Výše zmíněné údaje jsou údaji referenčními.

Kromě referenčních údajů se také v registru obyvatel vedou provozní údaje, kterými jsou záznam o využívání údajů z registru obyvatel pro potřeby agendových informačních systémů, záznam o poskytnutí údajů příslušnému subjektu a o poskytnutí údajů jiné fyzické nebo právnické osobě. Dále mezi provozní údaje patří datum poslední změny každého údaje v registru obyvatel a záznam o udělení nebo odvolání souhlasu subjektu o poskytnutí údajů jiné fyzické nebo právnické osobě.

Správcem registru obyvatel je Ministerstvo vnitra, které je zároveň i editorem údajů o občanech České republiky, které zapisuje prostřednictvím agendového informačního systému evidence obyvatel, občanských průkazů nebo cestovních dokladů. U cizinců a občanů členských států EU atd. je editorem Policie České republiky. Ministerstvo vnitra je pak editorem ještě u jiných fyzických osob podle zvláštních předpisů.

Speciální postavení zde mají obecní úřady obcí s rozšířenou působností v rámci výkonu volebního práva občana. Tyto úřady mají na základě dotazu okrskové volební komise ze zákona oprávnění využívat referenčních údajů v rozsahu čísla a druhu elektronicky čitelných identifikačních dokladů, jména, příjmení a adresy místa pobytu. Tyto údaje pak neprodleně sdělí okrskové volební komisi.

3.6.5 Registr osob

Dalším ze základních registrů je registr osob, jehož subjekty jsou právnické osoby, organizační složky a organizační jednotky státu a právnických osob, podnikající fyzické osoby, svěřenské fondy a zahraniční osoby a jejich organizační složky za podmínky, že jsou zapsány v některé z evidencí, jako jsou obchodní rejstřík, živnostenský rejstřík atd.

Co se týče referenčních údajů, jsou v jistém směru podobné jako u registru obyvatel. Jedná se o obchodní firmu nebo název, jméno a příjmení u fyzických osob podnikajících, které nejsou zapsány v obchodním rejstříku. U podnikajících fyzických osob a zahraničních osob se zapisuje jméno a příjmení. Dalšími

referenčními údaji je pak identifikační číslo osoby (IČO), datum vzniku nebo zápisu a datum zániku nebo výmazu z evidence podle jiných právních předpisů, první forma, typ datové schránky a její identifikátor (pokud je zpřístupněna), statutární orgán, adresa sídla, adresa místa provozovny, datum zahájení a ukončení provozování činnosti v provozně a adresa místa pobytu v České republice.

Mnoho těchto údajů je vyjádřeno formou referenční vazby, což jsou kódy nebo identifikátory, kterými se odkazuje na referenční údaje v ostatních základních registrech. Tím nedochází k duplikování údajů. Platí to např. u jmen fyzických osob (registr obyvatel) nebo sídla (registr územní identifikace).

Mezi provozní údaje v tomto případě patří kód agendy, identifikační číslo editora, datum prvotního zápisu osoby editora, datum poslední změny údaje v registru osob a záznam o využívání údajů z registru osob. Správcem tohoto registru je Český statistický úřad.

3.6.6 Registr územní identifikace

Tento registr obsahuje údaje o základních územních prvcích, čímž se rozumí část zemského povrchu vymezená hranicí nebo výčtem jiných územních prvků, adresní místo nebo stavební objekt.

Registr územní identifikace obsahuje údaje o území státu, území regionu soudržnosti podle jiného právního předpisu, území vyššího územního samosprávného celku, území kraje, území okresu, správní obvod obce s rozšířenou působností, správní obvod obce s pověřeným obecním úřadem, území obce, území vojenského újezdu, správní obvod v hlavním městě Praze, území městského obvodu v hlavním městě Praze, území městské části v hlavním městě Praze, území městského obvodu a městské části územně členěného statutárního města, katastrální území, území základní sídelní jednotky, stavební objekt, adresní místo a pozemek v podobě parcely.

Referenčními údaji jsou v tomto případě dle § 38 zákona identifikační údaje, údaje o vazbách na ostatní územní prvky, případně územně evidenční jednotky, údaje o druhu a způsobu využití pozemku a jeho technicko-ekonomické atribu-

ty, údaje o typu a způsobu využití stavebního objektu, údaje o typu a způsobu ochrany nemovitostí a adresy.

V registru územní identifikace se vedou objekty nejrůznější povahy a zákonná úprava spíše připomíná prováděcí předpis. Vzhledem k rozsahu těchto údajů bylo nutné zavést agendový informační systém územní identifikace na podporu registru územní identifikace. Správcem tohoto informačního systému, stejně jako registru územní identifikace, je Český úřad zeměměřičský a katastrální.

3.6.7 Registr práv a povinností

Registr práv a povinností obsahuje údaje o orgánech veřejné moci, soukromoprávních uživatelích údajů, agendách a právech a povinnostech fyzických a právnických osobách, pokud jsou jejich údaje vedeny v základních registrech. Jde tedy o registr, který plní ve vztahu k ostatním základním registrům úlohu spíše servisní, jelikož registr práv a povinností slouží jako zdroj údajů pro informační systémy základních registrů a řízení přístupu uživatelů k nim. V praxi to znamená, že pokud se někdo nebo nějaká instituce bude snažit získat z registrů jakýkoliv údaj či bude chtít nějaký údaj změnit, tak bude systém posuzovat, zda na to má daná instituce právo.

Obsahem tedy jsou referenční údaje o působnosti orgánů veřejné moci, o jejich agendách, které vykonávají, o informačních systémech, které pro výkon agend využívají, a o rozsahu oprávnění k referenčním údajům základních registrů.[62] Referenčními údaji o právech a povinnostech osob jsou pak dále údaje o rozhodnutích nebo jiných úkonech orgánů veřejné moci (včetně veřejnoprávních smluv a opatření obecné povahy), které mění referenční údaje v registru osob nebo registru obyvatelstva.

Obecně vzato platí, že referenčními údaji jsou identifikátor orgánu veřejné moci (popř. soukromoprávního uživatele), název osoby, typ datové schránky a identifikátor datové schránky, číslo a název právního předpisu a označení ustanovení, na jehož základě je vykonávána daná působnost, a název a kód agendy.

[62] SPRÁVA ZÁKLADNÍCH REGISTRŮ. *Registr práv a povinností*

Aby mohl příslušný orgán veřejné moci využívat údajů v základních registrech, je nutné tuto agendu zaregistrovat dle § 53 a § 54 zákona o základních registrech. Registrace probíhá tak, že ústřední správní úřad ohlásí agendu ve své působnosti Ministerstvu vnitra. Pokud se jedná o podřízený správní úřad, ohlašuje tak prostřednictvím svého ústředního správního úřadu. Agenda vykonávaná orgány územních samosprávných celků v přenesené působnosti nebo soukromoprávními uživateli údajů se ohlašuje prostřednictvím věcně příslušného ústředního úřadu. V posledním případě, pokud je agenda vykonávaná orgány územních samosprávných celků v rámci samostatné působnosti, provede ohlášení ústřední správní úřad, pro jehož oblast působnosti je tato agenda nejbližší.

Pokud shledá Ministerstvo vnitra, že je ohlášení bezvadné, a získá od správce základního registru a správce agendového informačního systému kladné stanovisko z hlediska oprávněnosti přístupu k požadovanému rozsahu údajů, provede registraci agendy, přidělí kód agendy a údaje o agendě zařadí do číselníku agend.

Po úspěšné registraci agendy se mohou orgány veřejné moci přihlašovat k výkonu činnosti v působnosti dané agendy. Podmínkou je, že přihlašující se orgán veřejné moci je buďto editorem referenčních údajů, nebo požaduje získávání údajů ze základních registrů, nebo požaduje získávání údajů z agendových informačních systémů jiných správců. Pokud Ministerstvo vnitra neshledá žádné nedostatky, zaregistruje příslušný orgán veřejné moci do výkonu agendy a vyrozumí ho.

3.6.8 Shrnutí

Jak lze vidět, základní registry jsou obsáhlým projektem České republiky a v rámci eGovernmentu patří mezi ty větší. Zákonná úprava je velmi technická a pro normálního člověka může být až nesrozumitelná. Účelem základních registrů je sloužit především jako zdroj informací pro orgány veřejné moci, ale přináší prospěch i soukromým osobám. Otázkou je potom zabezpečení jednotlivých registrů, které spadá pod jejich správce. A jak bylo zmíněno výše, využívání údajů ze základních registrů je obklopeno pojistkami, které by měly zaručit pouze oprávněné užití k výkonu činnosti veřejné správy.

3.7 Registr smluv

Registr smluv je informační systém zřízený zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „zákon o registru smluv“) účinným od 1. 7. 2016.

Registr smluv je informační systém veřejné správy dle zákona o ISVS, který slouží k uveřejňování soukromoprávních smluv, smluv o poskytnutí dotace nebo návratné finanční výpomoci, jejichž stranou jsou subjekty specifikované v § 2 odst. 1 zákona o registru smluv. Jedná se o veřejnoprávní korporace a právnické osoby, v níchž má stát nebo jiný veřejnoprávní subjekt většinovou majetkovou účast. Zveřejnění smlouvy prostřednictvím registru smluv je spojeno s nabytím její účinnosti, takže bez řádného uveřejnění je smlouva neúčinná. Správcem registru smluv je Ministerstvo vnitra.

Uveřejňování probíhá tak, že dle § 5 zákona o registru smluv povinné subjekty bezodkladně zašlou uzavřenou smlouvu správci registru smluv, nejpozději však do 30 dnů od uzavření smlouvy. Správce pak bezodkladně smlouvu uveřejní prostřednictvím registru smluv, k čemuž dochází zpravidla automatizovaně.

Do registru smluv je ze zákona zaručený bezplatný dálkový přístup na internetové adrese https://smlouvy.gov.cz. Portál registru smluv nabízí jak klasické, tak i podrobné vyhledávání. V detailním náhledu jsou identifikovány smluvní strany, hodnota smlouvy (pokud nějakou má) a podrobné informace o smlouvě. Samozřejmostí je také úplné znění příslušné smlouvy.

3.8 Elektronický podpis

Elektronický podpis by se měl dát využít všude, kde se využívá vlastnoruční podpis.[63] Pokud v dnešní době můžeme jakýkoliv dokument převést do elektronické podoby, je potřeba s tímto převedeným dokumentem spojit stejné právní účinky jako v listinné podobě. K tomu slouží elektronický podpis (ePodpis). Elektronický podpis patří společně s datovými schránkami mezi základní nástroje elektronické komunikace s orgány veřejné moci.[64]

[63] MATES, Pavel a Vladimír SMEJKAL. *E-government v českém právu*, str. 123
[64] VODIČKA, Milan. *3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli*, str. 34

3.8.1 Historie elektronického podpisu

Dříve než byl přijat zákon o ISVS, byl přijat zákon č. 227/2000 Sb. O elektronickém podpisu (dále jen „zákon o ePodpisu“), který definoval elektronický podpis jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.[65] Dále také rozlišil prostý elektronický podpis, zaručený elektronický podpis a uznávaný elektronický podpis.

Formou prostého elektronického podpisu mohl být i ruční podpis naskenovaný a vložený do datové zprávy. Zaručeným elektronickým podpisem pak byl elektronický podpis, který zaručil, že byl jednoznačně spojen s podepisující osobou, umožnil identifikaci podepisující osoby ve vztahu k datové zprávě, byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, a byl k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.[66]

Uznávaným elektronickým podpisem byl zaručený elektronický podpis založený na kvalifikovaném certifikátu, který vydával akreditovaný poskytovatel certifikátů.

Tento zákon byl ale zrušen přímo účinným nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (dále jen „eIDAS“) účinným od 1. 7. 2016. Tento právní rámec pokrývá elektronickou identifikaci, elektronický podpis a související služby vytvářející důvěru. Dále se tedy bude tato kapitola zabývat nařízením eIDAS a k němu příslušným prováděcím předpisům.

3.8.2 eIDAS – obecná ustanovení

Nařízení eIDAS bylo vydáno s cílem zajistit řádné fungování jednotného trhu (respektive naplňovat strategii jednotného digitálního trhu) a usilovat o odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci. Z hle-

[65] Zákon o ePodpisu, § 2 písm. a
[66] Zákon o ePodpisu, § 2 písm. b

diska obsahu nařízení je nutné si uvědomit, že v prvním případě se jedná o harmonizační právní normu, která stanoví stejný standard elektronické identifikace a s ní spojených právních jednání. V celku jde tedy o zajištění stejné úrovně, vzájemné přeshraniční interoperability a uznávání elektronické identifikaci mezi členskými státy navzájem.

Článek 3 nařízení definuje základní pojmy nutných k dalšímu porozumění.

Elektronickou identifikací se rozumí postup používání osobních identifikačních údajů v elektronické podobě, které jednoznačně určí fyzickou či právnickou osobu (případně fyzickou osobu zastupující osobu právnickou). *Prostředkem pro elektronickou identifikaci* je hmotná či nehmotná jednotka, která obsahuje osobní identifikační údaje sloužící k autentizaci pro účely e-služeb. *Osobními identifikačními prostředky* se dle nařízení rozumí soubor údajů umožňujících zjistit totožnost dané osoby. *Systémem elektronické identifikace* je systém, na jehož základě se osobám vydávají prostředky pro elektronickou identifikaci. *Autentizací* je postup umožňující potvrdit elektronickou identifikaci osob.

Nařízení v rámci elektronického podpisu rozlišuje elektronický podpis zaručený a kvalifikovaný. *Zaručený elektronický podpis* je zde definován jako podpis splňující požadavky dle článku 26 nařízení a *kvalifikovaný elektronický podpis* je pak vyšší stupeň zaručeného podpisu, který je založený na *kvalifikovaném certifikátu*, což je certifikát splňující požadavky dle přílohy I nařízení.

3.8.3 Elektronický podpis ve světle současné úpravy

Nařízení eIDAS změnilo definici elektronického podpisu oproti předešlé úpravě zmíněné výše. Dle dikce nařízení jsou elektronickým podpisem „*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*“.[67] Dle tohoto znění už není elektronický podpis pouze identifikátor podepisující osoby, ale můžeme ho chápat jako podpis vlastnoruční, což znamená stvrzující projev vůle, který vede k platnosti určitého dokumentu.

[67] Čl. 3 bod 10 nařízení eIDAS

Zaručeným elektronickým podpisem je elektronický podpis, který je jednoznačně spojen s podepisující osobou, umožňuje identifikaci dané osoby, je vytvořen pomocí dat pro vytváření elektronických podpisů s vysokou úrovní důvěry dané osoby a je k dokumentům, které jsou tímto podpisem podepsány, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu obsahu dokumentu.

Kvalifikovaný elektronický podpis je definován v čl. 3 odst. 12 nařízení jako „*zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy*“.

Obecně vzato jsou elektronické podpisy vydávány kvalifikovanými poskytovateli služeb vytvářejících důvěru, kteří uzavírají smlouvu orgánem dohledu dané země. Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce definuje, že orgánem dohledu je Ministerstvo vnitra. Kvalifikované poskytovatele služeb pak lze zjistit na stránkách tohoto ministerstva.[68]

Elektronický podpis nesmí být podle čl. 25 nařízení odmítán jako důkaz v soudním ani správním řízení jen z toho důvodu, že se jedná o elektronickou podobu podpisu. Dále je zde kvalifikovaný elektronický podpis postaven na úroveň podpisu vlastnoručního a samozřejmě nechybí ustanovení o vzájemném uznávání kvalifikovaných elektronických podpisů členskými státy navzájem.

3.8.4 Elektronická časová razítka

Elektronická časová razítka jsou už v právním řádu České republiky od roku 2004. Dle čl. 3 bodu 33 jsou elektronickým časovým razítkem elektronická data spojující jiná data s určitým okamžikem, a tím prokazují, že daná data v tomto okamžiku již existovala. Nařízení pak v čl. 42 definuje kvalifikovaná časová razítka, která spojují datum a čas s daty takovým způsobem, že bude přiměřeně zamezeno nezjistitelné změny těchto dat. Dalším požadavkem časového razítka je podmínka přesného času spojeného s časem světovým. Konečným požadavkem je podepsání časového razítka zaručeným elektronickým podpisem, zaručenou elektronickou pečetí nebo jiným rovnocenným způsobem.

[68] Viz http://www.mvcr.cz/e-podpis-povinne-zverejnovane-informace.aspx

3.8.5 Elektronické pečeti

Dřívější právní úprava EU neznala elektronické značky na rozdíl od české právní úpravy, kde byl tento institut zaveden, i když pouze ve formě uznávané elektronické značky.[69] Elektronická pečeť je definována čl. 3 nařízení eIDAS obdobně jako elektronický podpis, avšak s tím rozdílem, že pečetící osobou může být pouze osoba právnická. Elektronická pečeť je tedy jakýmsi průkazem původu dat (např. institucí, podniků atd.) a k pečetění dochází spíše mechanicky, stejně jako při razítkování listinných dokumentů.[70] Nařízení rozeznává také kvalifikovanou elektronickou pečeť, založenou na kvalifikovaném certifikátu.

3.8.6 Služby vytvářející důvěru a jejich poskytovatelé

Nařízení eIDAS se nezabývá pouze elektronickými podpisy, ale také dalšími instituty, a proto vyvstala nutnost obecného pojmu. Službou vytvářející důvěru je e-služba (poskytována zpravidla za úplatu), která spočívá ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb doporučeného doručování a certifikátů s tím souvisejících. Dále pak spočívá ve vytváření, ověřování shody a platnosti certifikátů v rámci autentizace internetových stránek a v uchovávání elektronických podpisů, pečetí nebo certifikátů s e-službami souvisejícími. Poskytovatelem je pak fyzická nebo právnická osoba, která poskytuje jednu či více těchto služeb, a to buď jako kvalifikovaný, nebo nekvalifikovaný poskytovatel.

Služby, stejně jako poskytovatelé, mohou být kvalifikovaní, což lze chápat jako akreditovaní či certifikovaní. Rozdíl pak je v právní síle poskytovaných služeb, respektive užití těchto služeb v právním jednání.

Doprovodným zákonem k nařízení eIDAS v oblasti elektronických podpisů je zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Zákon upravuje v návaznosti na nařízení eIDAS některé postupy poskytovatelů služeb vytvářejících důvěru, některé požadavky na služby vytvářející

[69] Zákon o ePodpisu, § 111

[70] SMEJKAL, Vladimír, KODL, Jindřich, UŘIČAŘ, Miroslav. Elektronický podpis podle nařízení eIDAS, *Revue pro právo a technologie*, str. 215

důvěru, působnost Ministerstva vnitra v této oblasti a sankce za delikty v této oblasti.

Jelikož je nařízení eIDAS přímo účinné v členských státech upravuje tento zákon jen zbytkovou působnost. Dle § 2 zákona poskytuje kvalifikovaný poskytovatel služeb vytvářejících důvěru kvalifikovanou službu na základě písemné smlouvy. Smlouva se uzavírá s orgánem dohledu, kterým je dle § 13 odst. 1 Ministerstvo vnitra. Seznam kvalifikovaných poskytovatelů služeb je pak dostupný způsobem umožňujícím dálkový přístup.[71]

Zajímavá je zde úprava elektronických podpisů v § 5 zákona. Orgány veřejné moci (veřejnoprávní podepisující) a ostatní osoby při výkonu své působnosti musí při podepisování dokumentů, kterými se právně jedná, užít pouze kvalifikovaný elektronický podpis. Pokud ale někdo právně jedná ve své působnosti vůči veřejnoprávnímu podepisujícímu, musí použít uznávaný elektronický podpis, kterým se dle zákona rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu nebo kvalifikovaný elektronický podpis. Zachovala se zde tedy terminologie z předešlého zákona o elektronickém podpisu.

Pro elektronické pečetě zde pak platí obdobná úprava dle § 8 – § 10 zákona. Veřejnoprávní podepisující při právním jednání používá kvalifikovanou elektronickou pečeť. Osoby jednající ve své působnosti vůči veřejnoprávnímu podepisujícímu užívají zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu nebo kvalifikovanou pečeť.

V obou případech (podpis i pečeť) lze užít i jiného typu podpisu, pokud dané osoby nejednají ve své působnosti.

Zákon dále v § 14 umožnil Správě základních registrů poskytovat služby vytvářející důvěru, a to i jako hospodářskou činnost.

3.9 Elektronické doporučené doručování

Jak bylo zmíněno výše, nařízení eIDAS se nevztahuje pouze na elektronické podpisy, ale v rámci České republiky přináší nové instituty eGovernmentu. Jedním z nových nástrojů eGovernmentu je elektronické doporučené doručo-

[71] Viz http://www.mvcr.cz/e-podpis-povinne-zverejnovane-informace.aspx

vání, kterým se dle čl. 3 bodu 36 rozumí služba, která umožňuje přenášet elektronická data mezi osobami a poskytuje důkazy o nakládání s těmito daty, včetně dokladu o odeslání a přijetí dat.

Do budoucna by tedy mělo být možné obdržet elektronické dokumenty jiným způsobem než skrze datovou schránku. Takto doručené dokumenty musí mít sílu důkazního prostředku a mohou se užít ve všech správních i soudních řízeních. Do budoucna se rozvoj této služby očekává až se zajištěním elektronické identifikace (identity).

3.10 Elektronická identifikace

Elektronická identifikace je jedním z důležitých předmětů nařízení eIDAS řešených v článku 6 – 12. Zákonodárce v návaznosti na eIDAS přijal zákon č. 250/2017 Sb., o elektronické identifikaci s účinností od 1. 7. 2018 (dále jen „zákon eID“). Předmětem toho zákona je možnost využití elektronické identifikace, působnost Ministerstva vnitra a Správy základních registrů a přestupky na úseku elektronické identifikace.

Hned z ustanovení § 2 zákona eID je zřejmé, že prokázat totožnost osoby lze i prostřednictvím kvalifikované elektronické identifikace. Kvalifikovanou elektronickou identifikací se rozumí elektronická identifikace prostřednictvím kvalifikovaného systému elektronické identifikace.

Kvalifikovaným systémem je dle § 3 zákona eID systém elektronické identifikace spravovaný kvalifikovaným správcem a splňujícím požadavky nařízení eIDAS. Kvalifikovaným správcem může být pouze státní orgán nebo osoba, které byla udělena akreditace. Kontrolním orgánem je Ministerstvo vnitra.

Zákon tedy umožňuje vydávat prostředky elektronické identifikace specifikované nařízením eIDAS. Povinností držitele prostředku elektronické identifikace je dle § 17 zákona eID ověřit správnost údajů a počínat si tak, aby nemohlo dojít ke zneužití, a případnou ztrátu prostředku nebo jeho zneužití ohlásit kvalifikovanému správci.

Zřizuje se také tzv. národní bod, což je informační systém veřejné správy dle zákona o ISVS podporující proces elektronické identifikace. Jeho správcem je Správa základních registrů. Národní bod slouží také k plnění požadavků inte-

roperability v rámci EU. V národním bodu se dle § 21 zákona eID vede identifikátor prostředku, agendový identifikátor držitele prostředku a identifikátor držitele v rámci kvalifikovaného systému.

V souvislosti se zavedením elektronické identifikace byla přijata novela zákona č. 328/1999 Sb., o občanských průkazech (dále jen „zákon OP“). Zákon č. 195/2017 Sb., *kterým se mění zákon OP a související zákony*, přináší změnu v rámci občanských průkazů.

Novela zavádí oproti současné úpravě pouze dva typy občanských průkazů, kterými jsou občanské průkazy se strojově čitelnými údaji a s kontaktním elektronickým čipem a občanský průkaz bez strojově čitelných údajů. To znamená, že každý občanský průkaz vydaný v klasickém režimu bude mít zabudovaný kontaktní čip s kvalifikovaným certifikátem splňujícím podmínky prostředku elektronické identifikace pro komunikaci s informačními systémy veřejné správy.[72]

Přístup k údajům v kontaktním elektronickém čipu bude chráněn identifikačním osobním kódem držitele. Zákon rozlišuje 3 typy osobních kódů. Prvním je bezpečností osobní kód (§ 8a), který slouží k autentizaci držitele při fyzickém prokázání jeho totožnosti. Druhým je identifikační osobní kód (§ 8b), který slouží k přístupu k identifikačnímu certifikátu a ke vzdálené autentizaci držitele. Třetím je pak deblokační osobní kód (§ 8c), který slouží k odblokování přístupu k identifikačnímu certifikátu v případě, že držitel třikrát po sobě zadá špatný identifikační kód.

Tato právní úprava je velice důležitá v rámci eGovernmentu, jelikož elektronická identifikace otevírá dveře zavádění dalších nástrojů eGovernmentu, zejména nástrojů e-participace a e-demokracie. Jedním z dalších projektů v rámci eGovernmentu bude spuštění tzv. portálu občana, kterým se zabývá další podkapitola.

[72] Zákon o občanských průkazech ve znění zákona č. 195/2017 Sb., § 2

3.11 Portál občana

Portál občana je nový nástroj České republiky v rámci eGovernmentu. Vzniknout mohl díky zavedení elektronické identifikace osob a s tím souvisejícími změnami. V současné době je projekt v pilotní testovací fázi, ale do konce roku 2018 by měl být v plném provozu.

Principem portálu občana je umožnit občanům komunikaci s jednotlivými úřady prostřednictvím dálkového přístupu. Portál občana by měl umožnit lidem vyřizovat záležitosti, kvůli kterým se musí chodit na příslušný úřad nebo kontaktní místo veřejné správy.[73]

Přes internet tedy půjde získat stejné výpisy jako na kontaktních místech Czech POINT a projekt také počítá i s transakčními e-službami, jako jsou místní poplatky, správní poplatky, soudní poplatky. Portál bude taky upozorňovat na konec platnosti ostatních dokladů.

K přístupu na portál bude nutný výše zmíněný nový občanský průkaz s kontaktním čipem s kvalifikovaným certifikátem. Přihlašovat na portál se bude pomocí elektronické čtečky, kterou si budou muset zájemci zakoupit. Cena této čtečky by se měla pohybovat okolo 200 – 300 Kč. Ze zavedení portálu občana neplyne povinnost tyto služby využívat. Zájemci si budou muset tuto službu aktivovat v rámci nového občanského průkazu a zadat si bezpečnostní identifikační a deblokační kód.

Důležitým principem je, že k používání portálu občana nebude nutné si zřídit datovou schránku.

3.12 eSbírka a eLegislativa

Nástroj eGovernmentu eSbírka a eLegislativa jsou projektem, jehož cílem je zajistit lepší dostupnost, přehlednost a srozumitelnost platného práva. Projekt je legislativně upraven zákonem č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv (dále jen „zákon o sbírce zákonů“). Zákon o sbírce záko-

[73] AKTUÁLNĚ.CZ. *Česko za rok spustí portál pro online komunikaci s úřady, lidé budou potřebovat občanku s čipem*

nů přináší mnoho změn. Mezi ty nejdůležitější patří spojení Sbírky zákonů a Sbírky mezinárodních smluv do jedné. V rámci eGovernmentu je pak nejdůležitější elektronický systém Sbírky zákonů a mezinárodních smluv.

Elektronický systém Sbírky zákonů a mezinárodních smluv je dle § 6 zákona informační systém veřejné správy (dle ISVS), jehož správcem je Ministerstvo vnitra. Prostřednictvím tohoto systému se vede Sbírka zákonů a mezinárodních smluv v elektronické podobě, která se zpřístupňuje veřejnosti způsobem umožňujícím dálkový přístup (eSbírka), a databáze informací o aktech též zpřístupněná způsobem umožňujícím dálkový přístup (eLegislativa).

Jak lze vidět, projekt se dělí na dvě části. V eSbírce nalezneme závazná elektronická znění právních aktů včetně právně závazných úplných znění. Nástroj eSbírka bude řešena internetovým portálem, eLegislativa je určena pro pružnou práci s aktuálními a minulými úplnými zněními právních předpisů, včetně souvisejících předpisů (výkladová stanoviska, komentáře atd…).[74]

Z právnického hlediska nejde pouze o projekt v rámci eGovermentu a zjednodušení práce s právními předpisy, ale dle § 1 odst. 2 zákona o sbírce zákonů má listinná i elektronická podoba stejné právní účinky. eSbírka tedy bude pramenem práva a stát je odpovědný za správnost jejího obsahu. V současné době nejsou elektronická úplná znění právních předpisů pramenem práva a při rozporu mezi listinnou a elektronickou podobou má listinná podoba navrch.

Zákon o sbírce zákonů vejde v účinnost 1. 1. 2020, přičemž Ministerstvo vnitra počítá s tím, že projekt bude dokončen k 31. 12. 2019.[75]

3.13 Kyberbezpečnost

Se zvyšováním a prohlubováním eGovernmentu musí jít ruku v ruce také úroveň zabezpečení digitální sítě a informačních systémů. V roce 2016 byla EU přijata směrnice upravující opatření k zajištění společné úrovně bezpečnosti sítí a informačních systémů (dále jen „směrnice NIS“).[76] Tato směrnice určila

[74] MINISTERSTVO VNITRA. *eSbírka a eLegislativa*

[75] MINISTERSTVO VNITRA. *eSbírka a eLegislativa*

[76] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké úrovně bezpečnosti sítí a informačních systémů v Unii

členským státům povinnosti týkající se standardu zabezpečení a orgánů zajišťujících bezpečnost. Směrnice stanovila závazné datum naplnění cílů na 8. 5. 2018. Zákonodárce na to reagoval novelou zákona č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“). Zákon o kybernetické bezpečnosti vymezuje základní pojmy a povinné osoby (dohromady 8) v oblasti kybernetické bezpečnosti. Dále specifikuje v ustanovení § 4 bezpečností opatření, kterým se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti sítí a služeb elektronické komunikace. Příslušným orgánem kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost se sídlem v Brně.

Nutno podotknout, že už v době přijetí směrnice EU byla úroveň kybernetické bezpečnosti v ČR na vysoké úrovni. I tak ale přinesla směrnice o NIS několik změn. Například zavedla CSIRT (Computer Security Incident Response Team) pro všechny členské země, jejichž úkolem je zvládání rizik a rešení incidentů. Dle zákona o kybernetické bezpečnosti tuto úlohu plní CERT (Computer Emergency Response Team), které jsou rozlišené na národní a vládní. Národní CERT mohou provozovat právnické osoby za podmínek stanovených v § 18 na základě veřejnoprávní smlouvy s Národním úřadem pro kybernetickou a informační bezpečnost. Mimo národních CERT existuje také vládní CERT zřízený v rámci zmíněného úřadu. CSIRT celé EU mezi sebou komunikují a vyměňují si informace.

3.14 Shrnutí

Jak lze z předešlého textu vidět, nástrojů eGovernmentu užívaných v praxi je v současné době mnoho. Tyto nástroje jsou ve většině případů vzájemně propojené. Informační systémy veřejné správy je zastřešující nástroj, bez kterého by nebyl další vývoj možný, protože na něm staví např. základní registry, registr smluv a další. Největší posun lze v současné době pozorovat v souvislosti s nařízením eIDAS. Elektronická identifikace a nové občanské průkazy posunou eGovernment v ČR vpřed a poskytnou nové možnosti občanů využívat e-služeb veřejné správy. Snad budou tyto nástroje hojně využívány. Z právního hlediska bude mít velký přínos projekt eSbírka a eLegislativa, která bude obsa-

hovat oficiální elektronické právní prameny, které usnadní práci jak advokátům, tak úředníkům.

4 eGovernment České republiky a Evropská Unie

Předchozí kapitoly ukázaly, jaké trendy v rámci eGovernmentu existují v EU a jaké nástroje eGovernmentu jsou v České republice použity, respektive budou v blízké době užívány. Tato kapitola se zabývá hodnocením celkové úrovně eGovernmentu z pohledu Evropy.

4.1 Benchmark a oblasti zkoumání

Evropská komise si každoročně nechává zpracovat eGovernment benchmarking, vždy za uplynulý rok, který hodnotí jednotlivé země EU (+ země Evropského hospodářského prostoru). Tyto benchmarky hodnotí eGovernment z hlediska jeho hloubky, dostupnosti atd. Každoročně je zpracovává společnost Capgemini[77] s dalšími partnery.

Zmíněné benchmarky se zaměřují na eGovernment ve 4 hlavních oblastech, jimiž jsou zaměřenost na uživatele, transparentnost, přeshraniční mobilita a klíčové předpoklady.

Zaměřenost na uživatele indikuje, v jakém rozsahu jsou služby poskytovány online a jak jsou vnímány. Jednotlivými hodnocenými kategoriemi v této oblasti jsou online dostupnost a online použitelnost.

V rámci *transparentnosti*, která indikuje v jaké míře je veřejná správa transparentní vzhledem ke svému výkonu činnosti, procesu výkonu činnosti a nakládáním s uživatelskými daty.

V oblasti *přeshraniční mobility* se zkoumá přeshraniční dostupnost služeb a jejich využitelnost. *Klíčovými předpoklady* se rozumí jednotlivé technické podmínky potřebné k užívání e-služeb, kterými jsou zejména elektronická identifikace, elektronické dokumenty, ověřené zdroje nebo například elektronické doručování.[78]

[77] Pro více info o skupině Capgemini: https://www.capgemini.com/company-profile-key-figures/

[78] EUROPEAN COMMISSION. *EU eGovernment Report 2016*

4.2 eGovernment benchmark 2016

Zpráva z eGovernment benchmarku z roku 2016[79] ukazuje, že veřejné e-služby jsou v posledních letech čím dál tím více dostupné, ale jednotlivé zkoumané oblasti ukazují, že zlepšují nerovnoměrně, a to jak v jednotlivých zemích, tak na úrovni EU. Tento benchmark byl zlomový v tom, že byl proveden v půlce období DAE2020, na jeho základě pak byl vytvořen eGAP2020.

Česká republika je z pohledu EU spíše konzervativnější a umírněnější, avšak postupem času se lepší a lze říci, že patří spíše do podprůměru. V oblasti zaměření na uživatele vyšlo pro ČR celkové skóre 69, což je pod celkovým průměrem EU (77), ale vychází zde najevo celkové zlepšení, hlavně v kategorii použitelnosti, které odpovídá průměru EU.

Oblast transparentnosti je pro ČR celkově největší nedostatek, a to jak v objektivním hodnocení, tak ve srovnání s průměrem EU. Největší nedostatek je užívání osobních dat, kde ČR dosahuje skóre 11 (nedostatečný) oproti průměru EU (55).

V oblasti přeshraniční mobility dosahuje ČR průměrného hodnocení. Na druhou stranu v kategorii použitelnosti e-služeb dosahuje hodnocení nadprůměrného. Oblast klíčových předpokladů je dalším nedostatkem, jelikož celkové výsledky dosahují polovičních hodnot oproti průměru EU.[80]

4.3 eGovernment benchmark 2017

Benchmark z roku 2017 je zatím nejnovějším dokumentem a stejně jako ten předchozí se věnuje již zmíněným čtyřem klíčovým oblastem s tím, že přeshraniční mobilita je rozdělena dle subjektů (občan, podnik). Zajímavé je spíše porovnat, v čem se ČR dokázala zlepšit a v čem naopak zase zaostává.

V oblasti zaměřenosti na uživatele se ČR drží pořád pod průměrem EU. Sice lze pozorovat zlepšení v online dostupnosti služeb, ale už zaostává v jejich použitelnosti. V tomto benchmarku byla také v rámci této oblasti hodnocena přívětivost e-služeb pro mobilní zařízení (telefon, tablet), kde ČR velmi zaostává.

---

[79] EUROPEAN COMMISSION. *EU eGovernment Report 2016*

[80] EUROPEAN COMMISSION. *EU eGovernment Report 2016: Country Factsheet*

Naopak ke zlepšení došlo v rámci transparentnosti. ČR se sice pořád drží lehce pod průměrem EU, ale došlo k velkému zlepšení v rámci užívání osobních dat, kde získala nadprůměrné hodnocení. Nejhorším indikátorem v této oblasti byla transparentnost poskytování služeb, které stagnuje na stejné úrovni jako v minulých letech.

V přeshraniční mobilitě občanů se ČR drží na průměru. Ve srovnání s EU si ČR vede dobře v přeshraniční mobilitě eID (elektronická identifikace, elektronický podpis), což znamená uznávání standardů eID ostatních členských států a naopak. Evropské státy jsou ale aktivnější v rámci přeshraniční mobility elektronických dokumentů veřejné správy, kterou nemá ČR žádnou.

Trochu jiná situace nastává v rámci přeshraniční mobility podniků. Celkové hodnocení této oblasti je zase průměrná, avšak oproti přeshraniční mobilitě občanů je zde obrácený stav v indikátorech eID a elektronických dokumentů. Přeshraniční pohyb elektronických dokumentů je vysoko nad průměrem EU (70 oproti 43). Na druhou stranu je nedostatečná mobilita eID podniků.

V poslední oblasti je ČR podprůměrná. Zkoumanými klíčovými předpoklady byly eID, elektronické dokumenty, elektronické doručování a ověřené zdroje (základní registry s principem *pouze jednou*). Elektronická identifikace je zde hodnocena průměrně a elektronické dokumenty podprůměrně. Ověřené zdroje jsou naopak nadprůměrné a elektronické doručování zaostává.[81]

4.4 Shrnutí

Jak z benchmarků vyplývá, je ČR spíše umírněná v prohlubování nástrojů eGovernmentu, proto je v rámci EU průměrná až podprůměrná. Z hodnocení vyplývá, že ČR zaostává hlavně v transparentnosti dat a informací, hlavně z hlediska poskytování služeb. ČR je naopak obecně v rámci EU vyzdvihována, kvůli projektu základních registrů.[82] Základní registry patří mezi projekty, které byly iniciovány českou vládou. Hlavními benefity jsou pružná reakce na změnu údajů, efektivní sdílení údajů a vzdálený přístup do registru územní

[81] EUROPEAN COMMISSION. *EU eGovernment Report 2017: Country Factsheet*
[82] EUROPEAN COMMISSION. *EU eGovernment Report 2017: Background report,* str. 48

identifikace. Základní registry totiž splňují princip interoperability mezi systémy veřejné správy, opětovné použití údajů a zajišťují princip *pouze jednou.*[83]

V relativním hodnocení s podobnými státy EU vyplývá, že ČR má nevyužitý potenciál v rámci průniku služeb a digitalizace. Pro ČR se tak doporučuje využít plného potenciálu informačních a komunikačních technologií, jelikož zázemí na to má odpovídající. Zbývá jen přijmout takovou politiku, která by směřovala k většímu užívání nástrojů eGovernmentu. Je nutné taky připomenout, že nejnovější eGovernment benchmark pracuje s daty za předešlý rok, tedy za rok 2016. V nejbližší době bude plně účinné nařízení eIDAS a nařízení GDPR,[84] což zapříčiní zlepšení ČR v jejich nejslabších oblastech, kterými jsou eID a jejich přeshraniční mobilita, elektronické dokumenty a nakládání s osobními daty.

Se zavedením elektronické identifikace bude moci každý občan činit úplné elektronické podání a díky komunikaci se základními registry bude mít přístup k záznamům o využívání jeho referenčních údajů z pohodlí domova. V současnosti si lze tento záznam na pobočkách Czech POINT, ke kterému se váže správní poplatek za vydání, nebo musí mít fyzické osoby zřízeny datovou schránku, což není lákavé z hlediska doručování, protože do datové schránky lze doručit i fikcí. Každopádně díky oběma nařízením budou mít občané větší přehled a pohodlí. Na druhou stranu je nutné provést osvětu veřejnosti a online služby poskytovat uživatelsky přívětivě, aby eID a portál občana (respektive portál veřejné správy) využívalo co nejvíce lidí, jinak se projekt mine účelem a lidé budou stále chodit vyřizovat své věci osobně.

[83] EUROPEAN COMMISSION. *EU eGovernment Report 2017: Background report,* str. 48
[84] Nařízení Evropského parlamentu a Rady (EU) 2016/679 účinné od 25. 5. 2018

5 Zhodnocení eGovernmentu České republiky

Hodnocení eGovernmentu ČR není vůbec jednoduché. Na jedné straně totiž pomalu ale jistě vláda zavádí nástroje eGovernmentu, ale nevyužívá jejich plný potenciál a nerozvíjí je. V této souvislosti se ČR propadla v rámci eGovernmentu ve světě z 25. místa až na 50. místo během jednoho roku.[85]

Jak již bylo zmíněno, ČR zaostává hlavně v rámci transparentnosti poskytování služeb a atraktivitě e-služeb. Datové schránky, které jsou určeny ke komunikaci s orgány veřejné moci, jsou povinné pouze pro vymezený okruh subjektů. Pro fyzické osoby se v současnosti datová schránka nevyplatí, jelikož je s ní spojená i určitá zodpovědnost. Fyzické osob tak musejí pravidelně svou datovou schránku kontrolovat, stahovat a zálohovat si dokumenty v ní obsažené. Prostřednictvím datové schránky lze totiž dle zákona o datových schránkách doručit i fikcí. Rozdílem mezi právnickými osobami a fyzickými osobami jsou v tom, že právnická osoba má povětšinou někoho pověřeného, kdo doručenou poštu a datovou schránku kontroluje, takže je možné, aby majitel firmy odjel na dlouhou dovolenou, protože za něj tuto agendu může někdo vyřídit. Kdežto u fyzické osoby, která odjede na delší dobu ze země, nemá nikdo jiný do datové schránky přístup a tím, že se nedoručuje prostřednictvím poskytovatele poštovních služeb, se daná osoba ani nemusí o doručení dozvědět od rodinných příslušníků či osob sdílejících adresu bydliště. Tedy v režimu doručování v listinné podobě se poskytovatel poštovních služeb snaží fyzicky daný dokument doručit a zanechává v poštovní schránce alespoň upomínku. Do budoucna při elektronickém doručování bude důležité tento problém vyřešit, protože do datové schránky, pokud je zpřístupněná, lze doručit vždy, kdežto prostřednictvím poskytovatele poštovních služeb lze dokument uložit až po neúspěšném pokusu o doručení.

S probíhající digitalizací pak vyvstává otázka relevance kontaktních míst Czech POINT, protože pokud do budoucna bude čím dál více subjektů využívat internetových portálů a eID, skrze které by mělo vyřídit v podstatě skoro

[85] AKTUÁLNĚ.CZ. *Česko je až padesáté na světě podle elektronizace veřejné správy*

všechny agendy veřejné správy včetně transakcí, budou místa Czech POINT ztrácet na významu a užitku. Možná by bylo k užitku tato místa v dlouhodobém hledisku přetvářet na školící a poradní centra.

Dalším problémem je v ČR dostupnost rychlého a superrychlého internetu každému. Rychlý a stabilní internet je základ pro budoucí vývoj eGovernmentu a využitelnost veřejných e-služeb občany a podniky. V současné době je venkov v podstatě odříznut, nebo je závislý na jednom poskytovateli internetu, který už nemusí mít zájem služby vylepšovat. Ministerstvo průmyslu sice vypsalo dotační výzvu, jelikož EU poskytla na budování sítí ČR 11,5 miliardy Kč, ale projekt by měl být splněn do roku 2020, tak jak je to specifikováno v DAE2020. V ČR je podle posledních průzkumů 84 % obyvatel připojeno k internetu rychlostí nižší než 10 Mbit/s a reálně cca 2 % obyvatel dosahuje rychlosti 30 Mbit/s.[86] Do roku 2020 dle vize DAE2020 má být 50 % domácností připojeno rychlostí alespoň 100 Mbit/s a 100 % populace by mělo být připojeno rychlostí alespoň 30 Mbit/s.

Pokud se podaří v rámci tohoto období rozšířit internetové sítě i na venkov, vyvstává otázka, jak na tom budou střední a malá města, protože na ty se tyto dotace nevztahují. Paradoxně může dojít k tomu, že venkov bude mít o mnoho rychlejší internetové připojení než městské oblasti.

Zajímavou oblastí bude také budoucí atraktivita veřejných e-služeb ve smyslu přívětivosti uživatelského rozhraní. Pokud totiž budou jednotlivé portály složité a budou připomínat spíše databázi, nebudou uživatelé mít o tyto služby zájem. V celé EU se portálová řešení soustřeďují na vznik tzv. životních událostí (life events), které fungují jako třídník, který uživatele postupně navede ke konkrétnímu požadavku. V atraktivitě také pomůže optimalizace internetových portálu pro mobilní zařízení. Optimalizace pro mobilní zařízení není v ČR na takové úrovni, na které by být měla. Například portál veřejné správy je jakž takž optimalizován. Optimalizovány jsou i stránky Ministerstva průmyslu a obchodu, ale stránky Ministerstva Vnitra, které hraje vedoucí úlohu v prosazování eGovernmentu, optimalizované není vůbec. Stránky Ministerstva spravedlnosti sice mobilní verzi stránky obsahují, ale nefungují.

[86] SEZNAM.CZ. *Mapa rychlosti internetu v ČR*

Budoucí vývoj eGovernmentu v ČR lze spatřovat v zavádění nástrojů eDemokracie a e-participace, a to jak na lokální úrovni, tak na úrovni národní. Prvky přímé demokracie formou referend a konzultací by mělo přispět ke snižování demokratického deficitu, který je v poslední době znatelnější. Díky zavedení elektronické identifikace je možné tyto nástroje aplikovat. Jedním z hlavních nástrojů je eVoting, tedy elektronické hlasování. Na toto téma existuje mnoho protichůdných názorů. Na jedné straně by bylo volit z pohodlí domova velmi přínosné, hlavně z hlediska přilákání voličů, kterým se nechce nebo se nemohou v den konání voleb dostavit do volebních místností a svůj hlas odevzdat. Pokud pomineme občany, kteří k volbám neprojevují zájem, mohli by dočasně indisponovaní občané, nebo občané nacházející se mimo území ČR, hlasovat prostřednictvím internetu a jejich hlasy by tak nepropadly.

Na druhou stranu je nutné vyřešit zabezpečení hlasování, aby nedocházelo k ovlivňování voleb, a také je zde problém neformální nátlaku ze strany rodiny atd. Nejdále se v této oblasti dostalo z evropských zemí Estonsko, kde proběhly první elektronické volby už v roce 2005 a v současné době je skrze eVoting odevzdáváno 30 % hlasů.[87] Samozřejmě Estonsko není jedinou zemí, kde takovéto projekty byly zaváděny. Elektronické volby se konaly například i ve Francii a Německu, kde ale vyvstaly vážné pochybnosti z hlediska manipulace s průběhem a výsledky voleb. Ve Francii bylo od eVotingu odstoupeno z obav kyberkriminality.[88] V Německu bylo elektronické hlasování dokonce shledáno neústavním.[89] Nizozemí se rokem 2017 vrátilo zpět k papírovému hlasování a fyzickému počítání hlasů.[90] Závěrem je teda nutné vylepšit do budoucna evropskou digitální síť, tak aby byla důvěryhodná a eGovernment se mohl dále rozvíjet.

Transponováním směrnice NIS by mělo dojít ke standardizaci bezpečnostní úrovně digitálních sítí a informačních systémů, aby bylo možné v budoucnu dále eGovernment prohlubovat. Do té doby by bylo nejlepší se soustředit na zvyšování digitalizace a úrovně e-služeb tak, aby zajišťovaly i transakční prvky

[87] E-ESTONIA. *E-governance: i-voting*
[88] REUTERS. *France drops electronic voting for citizens abroad over cybersecurity fears*
[89] DEUTSCHE WELLE. *German Court Rules E-Voting Unconstitutional*
[90] THE GUARDIAN. *Dutch will count all election ballots by hand to thwart hacking*

a komplexní obousměrnou komunikaci. Dalším možným směrem, kam se v nejbližší době uchýlit, je implementace prvků e-participace občanů v rozhodovacích procesech vlády, tak aby docházelo alespoň ke konzultacím a získáváním veřejného mínění, místo toho, aby bylo nutné projevovat veřejné mínění formou petičního práva.

Česká republika má do budoucna velký potenciál, jelikož i samostatné projekty jako jsou základní registry, které byly vytvořeny z iniciativy České republiky, jsou stabilní a v podstatě předběhly svou dobu. Jejich úprava je místy až moc technicky zaměřená, což by bylo lepší nechat na prováděcích předpisech z hlediska flexibility a případných změn. Nicméně to nemění nic na tom, že základní registry jsou plně využívány a další projekty jako elektronická identifikace na nich staví.

Závěr

Nástroje eGovernmentu pomáhají k větší efektivitě a úspoře času při výkonu veřejné správy. Zavádění nástrojů eGovernmentu má už poměrně dlouhou historii. Jak lze z této práce poznat, Česká republika nezaostává toliko v implementaci nových nástrojů, ale v jejich stagnaci a nulovém nebo minimálním rozvoji. V mnoha případech jsou nástroje eGovernmentu implementovány na základě legislativy či doporučení EU, což dokazuje postoj zákonodárce k modernizaci veřejné správy. Česká republika je v rámci eGovernmentu, dle terminologie EU, umírněná, což v realitě znamená rigidní a neinovativní. Důvodů může být spousta, ale nejspíše je tato rigidita způsobená nechutí vlád pouštět se do větších projektů, pokud nemusí.

Mnoho občanů a podnikatelů určitě ocení budoucí vývoj v rámci elektronického podání, jelikož zrychluje jednání s orgány veřejné moci. Případné transakční služby také přijdou vhod všem občanům, kteří nebudou zdrženliví v užívání nových občanských průkazů.

Tato diplomová práce se zabývá současnými nástroji eGovernmentu, které jsou v praxi používány na území České republiky s tím, že neopomenula zmínit ani nástroje, které budou aplikovány v nejbližší době.

Oblast eGovernmentu není závislá pouze na právní úpravě v dané zemi, ale také na technickém zázemí jednotlivých orgánů veřejné moci a celkovým technologickým rozvojem informačních a komunikačních technologií včetně internetových sítí.

Tato práce postupně představila základní pojmy eGovernmetu a představila obecné trendy EU. V největší kapitole byly rozebrány jednotlivé nástroje eGovernmentu. V posledních dvou kapitolách byla ČR zhodnocena z hlediska unijního a obecného.

Závěrem lze poznamenat, že eGovernment je jako téma věčné, ale velmi dynamické jelikož se rychle rozvíjí. Tím získává tato oblast na atraktivitě v rámci zkoumání. Na druhou stranu jsou nutné pravidelné benchmarky a dostupná literatura se stává velmi rychle zastaralou.

Resumé

The eGovernment area is a very extensive and currently interesting field of research. Today's world is gradually digitized and people use mainly electronic means to communicate. In this respect, public administration is also developing.

This master thesis deals with eGovernment in the Czech Republic. Individual chapters represent eGovernment as an area of research. Firstly, the basic concepts of eGovernment are introduced. The next chapter deals with eGovernment in the European Union. The third chapter deals with the eGovernment tools used in the Czech Republic. These tools include the public administration portal, Czech POINT contact points, data boxes, authorized document conversions, basic registers, contracts register and electronic signature. Some of the tools described will still be applied. The tools which will be applied in the near future include electronic recommended delivery, electronic identification, citizen's portal, and eCollection and eLegislation. The penultimate chapter deals with the evaluation of the level of the Czech Republic in terms of the European Union. This chapter uses the official benchmarks of the European Union. The last chapter deals with eGovernment evaluation in the Czech Republic and its problems. It also deals with future developments and barriers.

Seznam zdrojů

Literatura a internetové zdroje (všechny internetové zdroje byly přístupné k 25. 3. 2018):

AKTUÁLNĚ.CZ. *Česko je až padesáté na světě podle elektronizace veřejné správy*, 4. 8. 2016. [online] Dostupné z: https://zpravy.aktualne.cz/ekonomika/cesko-je-az-padesate-na-svete-podle-elektronizace-verejne-sp/r~02c5b38c5a5111e6a3e5002590604f2e/

AKTUÁLNĚ.CZ. *Česko za rok spustí portál pro online komunikaci s úřady, lidé budou potřebovat občanku s čipem,* 18. 7. 2017. [online] Dostupné z: https://zpravy.aktualne.cz/domaci/novy-obcansky-prukaz-s-chipem-umozni-snazsi-komunikaci-s-ura/r~ff84b0b86ba411e793d0002590604f2e/?redirected=1521890613

ANCARANI, Alessandro. *Towards quality e-service in the public sector: The evolution of web sites in the local public service sector*. Managing Service Quality, 15, str. 6-23, [online], 2005. Dostupné z: https://www.researchgate.net/publication/235307489_Towards_quality_e-service_in_the_public_sector_The_evolution_of_web_sites_in_the_local_public_service_sector

CZECHPOINT. *CzechPOINT@home*, [online], 2018. Dostupné z: http://www.czechpoint.cz/public/verejnost/czechpointhome/

CZECHPOINT. *Jaké služby poskytuje Czech POINT?*, [online], 2018. Dostupné z: http://www.czechpoint.cz/public/verejnost/sluzby/

CZECHPOINT. *Služby pro úředníky*, [online], 2018. Dostupné z: http://www.czechpoint.cz/public/urednik/sluzby-pro-uredniky/

DATOVÉ SCHRÁNKY. *Rozšířená autentizace*, [online], 2018. Dostupné z: https://www.datoveschranky.info/zakladni-informace/rozsirena-autentizace

DATOVÉ SCHRÁNKY. *Všeobecné dotazy*, [online], 2018. Dostupné z: https://www.datoveschranky.info/zakladni-informace/vseobecne-dotazy

DEUTSCHE WELLE. *German Court Rules E-Voting Unconstitutional*. 3. 3. 2009. [online] Dostupné z: http://www.dw.com/en/german-court-rules-e-voting-unconstitutional/a-4069101

E-ESTONIA. *E-governance: i-voting*. 2018. [online] Dostupné z: https://e-estonia.com/solutions/e-governance/i-voting/

MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.

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

MINISTERSTVO VNITRA. *Akční plán pro eGovernment na období 2016-2020*, [online], 2016. Dostupné z: http://www.mvcr.cz/mvcren/docDetail.aspx?docid=22026119&docType=ART&chnum=2

MINISTERSTVO VNITRA. *eSbírka a eLegislativa*, [online], 2018. Dostupné z: http://www.mvcr.cz/clanek/esbirka-a-elegislativa.aspx

OECD. *The e-Government Imperative*, OECD Publishing, Paris [online], 2003. Dostupné z: http://www.oecd-ilibrary.org/governance/the-e-government-imperative_9789264101197-en

POMAHAČ, Richard. *Veřejná správa*. V Praze: C.H. Beck, 2013. Beckovy mezioborové učebnice. ISBN 978-80-7400-447-6.

REUTERS. *France drops electronic voting for citizens abroad over cybersecurity fears.* 6. 3. 2017. [online] Dostupné z: https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233

RILEY, Thomas B., SHERIDAN, William. *Comparing e-Government Vs. e-Governance*, Geospatial World, [online], 2017. Dostupné z: https://www.geospatialworld.net/article/comparing-e-government-vs-e-governance/

ROWLEY, Jennifer. *An analysis of the e-service literature: Towards a research agenda*, Internet Research, Vol. 16 Issue: 3, str. 339-359, [online], 2006. Dostupné z: https://www.emeraldinsight.com/doi/pdfplus/10.1108/10662240610673736

SEZNAM.CZ. *Mapa rychlosti internetu v ČR.* 2016. [online] Dostupné z: https://www.seznam.cz/mapa-rychlosti-internetu

SMEJKAL, Vladimír, KODL, Jindřich, UŘIČAŘ, Miroslav. Elektronický podpis podle nařízení eIDAS, *Revue pro právo a technologie*, 2015, 11(6), 189 – 235. ISSN: 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/3586/R_2015_11_TEMA_Smejkal

SPRÁVA ZÁKLADNÍCH REGISTRŮ. *Referenční údaj*, [online], 2018. Dostupné z: http://www.szrcr.cz/referencni-udaj

SPRÁVA ZÁKLADNÍCH REGISTRŮ. *Registr práv a povinností*, [online], 2018. Dostupné z: http://www.szrcr.cz/registr-prav-a-povinnosti

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

VODIČKA, Milan. *3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli*. Vydání první. Praha: Wolters Kluwer, 2014. 189 stran. ISBN 978-80-7478-671-6.

THE GUARDIAN. *Dutch will count all election ballots by hand to thwart hacking*. 2. 2. 2017. [online] Dostupné z: https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking

Právní předpisy České republiky:

Zákon č. 328/1999 Sb., *o občanských průkazech*, ve znění pozdějších předpisů

Zákon č. 227/2000 Sb., *o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)*, ve znění pozdějších předpisů

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

Zákon č. 517/2002 Sb., *kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé zákony*, ve znění pozdějších předpisů

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

Zákon č. 110/2007 Sb., *Zákon o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů*, ve znění pozdějších předpisů

Zákon č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů*, ve znění pozdějších předpisů

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

Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),* ve znění pozdějších předpisů

Zákon č. 340/2015 Sb., *o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv)*, ve znění pozdějších předpisů

Zákon č. 222/2016 Sb., *o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv (zákon o Sbírce zákonů a mezinárodních smluv)*, ve znění pozdějších předpisů

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

Zákon č. 195/2017 Sb., *kterým se mění zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a další související zákony*

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

Dokumenty a právní předpisy Evropské unie (řazené chronologicky):

EUROPEAN COMMISSION. *A Digital Agenda for Europe.* COM(2010) 245 final, 2010. Dostupné z: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC0245

EUROPEAN COMMISSION. *EU eGovernment Action Plan 2016-2020*: *Accelerating the digital transformation of government*, COM(2016) 179 final , 2016. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0179

EUROPEAN COMMISSION. *EU eGovernment Report 2016.* 3. 10. 2016, [online]. Dostupné z: https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016-shows-online-public-services-improved-unevenly

EUROPEAN COMMISSION. *EU eGovernment Report 2016: Country Factsheet*, 3. 10. 2016, [online]. Dostupné z: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17864

EUROPEAN COMMISSION. *EU eGovernment Report 2017: Background report, 27. 11. 2017.* [online] Dostupné z: https://ec.europa.eu/digital-single-market/en/news/new-study-egovernment-services-europe-improving-cross-border-availability-services

EUROPEAN COMMISSION. *EU eGovernment Report 2017: Country Factsheet, 27. 11. 2017.* [online] Dostupné z: https://ec.europa.eu/digital-single-market/en/news/new-study-egovernment-services-europe-improving-cross-border-availability-services

EUROPEAN COMMISSION. i2010 eGovernment Action Plan: *Accelerating eGovernment in Europe for the Benefit of All*, COM(2006) 173 final, 2006. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0173

EUROPEAN COMMISSION. The European eGovernment Action Plan 2011-2015: *Harnessing ICT to promote smart, sustainable & innovative Government*, COM(2010) 743 final, 2010. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52010DC0743

EUROPEAN UNION. Nařízení Evropského parlamentu a Rady (EU) 2014/910 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*. In: *Úřední věstník EU.* L 257/73, 28. 8. 2014. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

EUROPEAN UNION. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. L 119/1. 4. 5. 2016. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679

EUROPEAN UNION. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké úrovně bezpečnosti sítí a informačních systémů v Unii. In: *Úřední věstník EU.* L 194/1, 19. 7. 2016. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L1148&from=EN