Univerzita Karlova
Právnická fakulta

# DISERTAČNÍ PRÁCE

Bohumír Štědroň

# Občanské soudní řízení sporné a využití informačních technologií a právních informačních systémů

Bohumír ŠTĚDROŇ



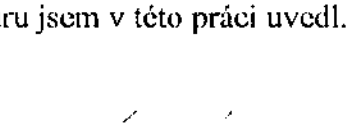
**DISERTAČNÍ PRÁCE**

**Poděkování**

Rád bych poděkoval paní doc. JUDr. Aleně Mackové, PhD., své školitelce, za cenné rady, ochotu a veškerou pomoc při psaní této práce.

**Čestné prohlášení**

Prohlašuji na svou čest, že jsem tuto disertační práci vypracoval samostatně a veškerou použitou literaturu jsem v této práci uvedl.

V Praze, dne ..... 

.....
Bohumír Štědroň

**Obsah**


**1. Úvod ..... 8**
*1.1. Předmět a cíl práce ..... 8*
*1.2. Terminologický slovník ..... 8*
*1.3. Právní rámec upravující problematiku E-Justice ..... 16*
1.3.1. Právní předpisy ..... 16
1.3.2. Metodické pokyny týkající se ISVS ..... 17
1.3.3. Přehled bývalých standardů ISVS ..... 17
1.3.4. Prováděcí právní předpisy k ISVS ..... 18
1.3.5. Resortní předpisy (Ministerstvo spravedlnosti ČR) ..... 18
1.3.6. Seznam stanovisek Úřadu pro ochranu osobních údajů ..... 19
1.3.7. Seznam norem a standardů týkajících se bezpečných elektronických systémů 19
**2. Současný stav justice a možnosti při nasazení informačních technologií a informačních právních systémů ..... 21**
*2.1. Obecné zhodnocení ..... 21*
*2.2. Projekt „E-Justice" v ČR ..... 26*
*2.3. V současné době nejčastěji využívané právní informační systémy ..... 31*
2.3.1. Systém ASPI ..... 31
2.3.2. LexDATA – právní informační systém ..... 31
2.3.3. LexGalaxy – právní informační systém ..... 33
*2.4. Resortní informační a komunikační systémy ..... 33*
2.4.1. ISOR - Informační systém obchodního rejstříku ..... 33
2.4.2. ISKOS – informační systém obchodního soudnictví ..... 33
2.4.3. ISAS – informační systém pro administrativu okresních soudů ..... 34
2.4.4. IRES – informační systém pro vedení ekonomických agend ..... 34
2.4.5. ISYZ – informační systém pro státní zastupitelství ..... 34
2.4.6. ISNS – informační systém Nejvyššího soudu ..... 35
2.4.7. ISKONK – informační systém agendy konkursů ..... 35
2.4.8. Evidence znalců a tlumočníků ..... 35
2.4.9. Evidence Rejstříku trestů ..... 35
*2.5. Další informační systémy využívané v právní praxi ..... 35*
2.5.1. AKWin (BaumSoft) - softwarový produkt určený pro advokátní kanceláře ..... 35
2.5.2. ISAP - Informační systém pro aproximaci práva ..... 36
2.5.2. FinKalk 2001 ..... 36
**3. Využití informačních technologií a systémů v občanském soudním řízení sporném ..... 37**
*3.1. Procesní úkony účastníků řízení a soudu ..... 37*
3.1.1. Úvod ..... 37
3.1.2. Nasazení elektronického podpisu a jeho úprava v právním řádu ..... 37
3.1.3. Jak správně vyřizovat emaily a vést jejich evidenci ..... 39
3.1.4. Pravidla pro tvorbu přístupných webových stránek orgánů justice (soudů) ..... 50
3.1.5. Elektronické podání - žaloba (nález ÚS) ..... 52
*3.2. Dokazování ..... 56*
3.2.1. Úvod ..... 56
3.2.2. Použití elektronických dokumentů (např. e-mailu) jako důkazního materiálu 57
3.2.3. Prokázání doručení elektronické (datové) zprávy ..... 59
3.2.4 Elektronické vedení a archivování soudních spisů a jiných dokumentů (důkazů) ..... 60
3.2.5 Obchodní věstník online ..... 61

3.2.6. Nahlížení do katastru nemovitostí online ... 61
3.2.7. Dálkový přístup k údajům katastru nemovitostí ČR ... 62
3.2.8. Elektronický návrh na zápis do katastru nemovitostí ... 63
*3.3. Rozhodnutí ... 63*
3.3.1. Úvod ... 63
3.3.2. Elektronické rozhodnutí a doručení rozhodnutí elektronickou cestou ... 64
3.3.3. Elektronický platební rozkaz ... 66
*3.4. Výkon rozhodnutí ... 68*
3.4.1. Úvod ... 68
3.4.2. Elektronický formulář pro podání návrhu na exekuci ... 69
*3.5. Další možnosti využití informačních technologií a systému (ICT) v soudním řízení 70*
3.5.1. Využití elektronického podpis a certifikátů – technický exkurs ... 70
3.5.2. Doporučení Transparency International k elektronizaci soudnictví ... 88
3.5.3. Elektronický evropský soudní atlas ve věcech občanských ... 89
3.5.4. Elektronická evropská soudní síť v občansko-právních a obchodních záležitostech ... 89
3.5.5. Rozhodčí řízení online (mimosoudní způsob řešení sporů) ... 89
3.5.5. Elektronický formulář pro evropský zatýkací rozkaz (trestní řízení) ... 91
*3.6. Elektronizace soudních agend a ochrana osobních údajů ... 93*
3.6.1. Právní kvalifikace pojmu osobní údaj ... 93
3.6.2. Používání rodného čísla v elektronických databázích ... 94
3.6.3. Elektronické zpracování osobních údajů zemřelých osob ... 95
3.6.4. Kontrola práce zaměstnance prostřednictvím telekomunikační techniky, ochrana soukromí a osobních údajů zaměstnance ... 96
3.6.5. Poskytnutí informací a získání souhlasu subjektu údajů v elektronické komunikaci ... 102
3.6.6. Elektronická spisová služba u Policie ČR a ochrana osobních údajů ... 103
**4. Vybrané statistické ukazatele (rychlost rozhodování soudů a vývoj elektronizace veřejné správy v ČR) ... 111**
*4.1. Úvod ... 111*
*4.2. Přehled o průběhu řízení – občanskoprávní agenda ... 111*
*4.3. Přehled o průměrných délkách řízení ode dne nápadu do dne právní moci ve dnech – náhrada škody ... 112*
*4.4. Přehled o průměrných délkách řízení ode dne nápadu do dne právní moci ve dnech – vlastnické vztahy ... 112*
*4.5. Stížnost pro porušení zákona – rychlost vyřizování podnětů ze strany státního zastupitelství ... 113*
*4.6. Rychlost vyřizování podnětů ze strany státního zastupitelství u ostatních řízení .. 113*
*4.7. Státní zastupitelství – rychlost vyřizování netrestních věcí ... 114*
*4.8. Státní zastupitelství – rychlost vyřizování odvolání ... 115*
*4.9. Využívání IT, internetu a počítačů v domácnostech (ČSÚ) ... 115*
**5. Výhody open source řešení a otevřených formátů při elektronizaci justice ... 120**
*5.1. Otevřené formáty ve veřejné správě ... 120*
*5.2. Otevřený standard pro elektronizaci soudnictví – pravidla a doporučení ... 120*
5.2.1. Doporučení ... 120
5.2.2. Pravidla pro otevřený IT standard v resortu justice ... 121
*5.3. Nasazení Open Source software v justici ... 122*
5.3.1. Pojem Open Source software ... 122
5.3.2. Zdrojový a objektový kód ... 123
5.3.3. Vztah mezi Open Source a Free Software (svobodným software) ... 123

5.3.4. Pojem licence (licenční ujednání) ... 124
5.3.5. K některým dalším pojmům ... 124
*5.4. Důvody pro využívání Open Source software v justici ... 125*
*5.5. Příklady nejčastěji užívaných Open Source aplikací ... 126*
**6. Příklady komerčních řešení informačních systémů vhodných k využití v resortu justice ... 127**
*6.1. Úvod ... 127*
*6.2. Informační systém Gordic GINIS ... 127*
6.2.1. Obecně ... 127
6.2.2. Podatelna (POD) ... 128
6.2.3. Univerzální spisový uzel (USU) ... 129
6.2.4. Vedoucí (VED) ... 130
6.2.5. Výpravna (VYP) ... 130
6.2.6. Spisovna (SPI) ... 132
6.2.7. Generátor podacích deníků (TPD) ... 132
6.2.8. Úkoly (UKO) a Usnesení a porady (USN) ... 133
6.2.9. Užití digitálních dokumentů a převod dokumentů do digitální podoby ... 133
*6.3. Objentis Software Integration ... 136*
6.3.1. DM Systémy dnes ... 136
6.3.2. Co je DMSs? ... 137
6.3.3. Použití DMSs ... 138
6.3.4. Dokument v DMSs ... 143
6.3.5. Samopopisné Objekty ... 144
*6.4. Unicorn Enterprise System ... 145*
6.4.1. Co je systém UES ... 145
6.4.2. Klíčové funkční oblasti ... 146
6.4.3. Artefakt ... 150
**7. Závěr ... 154**
**8. Použitá a doporučená literatura ... 155**
*8.1. Psaná literatura ... 155*
*8.2. Online veřejně přístupná literatura a zdroje ... 156*
*8.3. Metodiky, předkládací zprávy, studie proveditelnosti a návrhy zákonů ... 157*

# 1. Úvod

## 1.1. Předmět a cíl práce

Předmětem této práce, která má mezioborový charakter (procesní právo a informační technologie) je zmapování současného stavu české justice s ohledem na možnost efektivního využívání informačních technologií a systémů (ICT). Využívání ICT bude dokumentováno v rámci občanského soudní řízení sporného, jakožto jednoho z nejčastěji využívaných soudních řízeních, kde je zároveň hlavní iniciativa při vedení řízení (sporu) na samotných účastnících řízení. Pod pojem justice je v této práci chápána především soustava těchto orgánů:

- Ministerstvo spravedlnosti,
- soudy všech stupňů a státní zastupitelství.

Dále se projekt elektronizace justice dotkne těchto dalších orgánů (složek veřejné moci):

- Policie ČR,
- Probační a mediační služby,
- rejstříku trestů,
- Institut pro kriminologii a sociální prevenci,
- Justiční akademie,
- orgánů vykonávající správní řízení.

Cílem práce je poukázat na v současné době nedostatečné využívání ICT a navrhnout konkrétní možnosti nasazení ICT v české justici s cílem práci soudů a celého resortu zkvalitnit, zrychlit, zlevnit, zamezit současným častým „nešvarům" české justice (jako např. vykrádání[1] a ztrácení spisů atd.) a učinit komunikaci v rámci justice bezpečnější. Právě uvedené cíle lze dle názoru autora této práce vhodným nasazením ICT dosáhnout.[2] Zároveň jsou v práci prezentovány nové přístupy a trendy, kterými by se česká justice dle názoru autora měla vyvíjet (např. využívání otevřených standardů a open source software).

## 1.2. Terminologický slovník

**3G** - 3rd Generation, třetí generace technologií mobilních telefonů. Pod pojmem 3G se skrývají širokopásmové technologie, které umožní přenos textu, grafiky, videa, a zvuku.

**ADSL** – Asymmetric Digital Subscriber Line, jde o technologii pro vysokorychlostní připojení k Internetu realizované na klasické telefonní lince. Podmínkou použití je telefonní přípojka a připojení k ústředně, která je vybavena potřebnou technologií.

---

[1] Podrobněji viz. rozhovor s Ministrem spravedlnosti ČR Jiřím Pospíšilem na serveru www.ejustice.cz (20.6.2007).

[2] Úspěšně proběhla plná elektronizace soudnictví např. v Izraeli (Electronic Court System) – viz. http://prague.mfa.gov.il. Důvodem k elektronizaci byla i nelichotivá skutečnost, že z přibližně milionu spisů ročně zakládaných izraelskými soudy se přibližně polovina nikdy nedostala k soudci.

**All-in-One** – označení pro ERP systémy schopné pokrýt a integrovat všechny čtyři základní podnikové procesy (výroba, vnitřní logistika, personalistika a ekonomika).

**Anonymní surfování** – některé společnosti nabízí software (často i zdarma), který umožňuje vytvořit falešnou identitu a poté lze např. anonymně surfovat po webových serverech, vyměňovat si e-maily a účastnit se chatových diskusí.

**Archiv** - zařízení podle zákona č. 499/2004 Sb., o archivnictví a spisové službě (tzv. zákon o spisové službě), které slouží k ukládání archiválií a péči o ně.

**Archiválie** - takový záznam, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán ve veřejném zájmu k trvalému uchování a byl vzat do evidence archiválií; archiváliemi jsou i pečetidla, razítka a jiné hmotné předměty související s archivním fondem či s archivní sbírkou, které byly vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrány a vzaty do evidence (definice dle zákona č. 499/2004 Sb., o archivnictví a spisové službě - tzv. zákon o spisové službě).

**Archivnictví** - obor lidské činnosti zaměřený na péči o archiválie jako součásti národního kulturního dědictví a plnící funkce správní, informační, vědecké a kulturní.

**Atest** - úřední doklad osvědčující kladný výsledek atestace.

**Atestace** - stanovení způsobilosti pro použití v informačních systémech veřejné správy na základě shody se stanovenými standardy, technickými normami požadovaným stupněm bezpečnosti nebo na základě dosažení vyšší úrovně technických a užitných vlastností, než požadují standardy a technické normy. Atestace provádí atestační středisko.

**Atestační středisko** - právnická nebo fyzická osoba provádějící atestace na základě pověření k výkonu atestací. Pracuje na základě smlouvy uzavřené s žadatelem o atestaci a za úhradu.

**Blacklist, whitelist nebo greylist** - těmito pojmy jsou obvykle označovány seznamy objektů (počítače, uživatelé, adresy apod.) na něž jsou uvaleny restrikce. Whitelist (bílá listina) obsahuje subjekty, kterým je příslušná operace povolena, blacklist (černá listina) obsahuje subjekty, kterým je příslušná operace zakázána a greylist (šedá listina) provádí podrobnější dělení (některé operace povoleny, jiné zakázány).

**B2B – Business-to-Business**, systémy elektronické komerce uplatňované mezi podnikatelskými subjekty.

**B2C – Business-to-Costumer**, systémy elektronické komerce uplatňované mezi podnikatelskými subjekty a koncovými zákazníky.

**B2E** - Business-To-Employee, souhrn služeb založených na internetových standardech a protokolech zaměřených na zaměstnance podniku (organizace) zvyšujících jejich informovanost, motivaci, znalosti a produktivitu práce.

**BI** - Business Inteligence, nástroje pro podporu rozhodování, někdy označované také jako e-intelligence. Řešení opírající se o datové sklady a analýzu dat, které umožňují dělat správná rozhodnutí na základě získaných přesných a komplexních informací o dané organizaci.

**Blog** - je zkrácenou podobou slova weblog. Jedná se o publikační web, který je udržován a spravován pro osobní potřebu autora a má podobu internetového média. Blogy obvykle reprezentují osobu jejich tvůrce, kterému se říká blogger.

**Bluetooth** - bezdrátový komunikační standard, který je určen k propojení přenosných zařízení, jako jsou mobilní telefony, notebooky a kapesní počítače.

**bullying** (týrání) - šikanování a ponižování jednotlivců nebo skupin formou osobních útoků vedených prostřednictvím kanálů elektronické komunikace, jako je např. e-mail, instant messaging nebo textové zprávy (SMS).

**Citlivý údaj** - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, dále o zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů (podrobněji viz. zákon č. 101/2000 Sb., o ochraně osobních údajů).

**CMS** - Content Management System (systém pro správu obsahu) je označení pro software zajišťující správu dokumentů typicky webového obsahu. V dnešní době se jako CMS zpravidla chápou webové aplikace, někdy s případným doplňkovým programovým vybavením u klienta. Pro CMS se někdy používají i oborově podobné termíny „redakční či publikační systém". Základní funkce CMS se obvykle člení na administrátorské a uživatelské.

**Cookies** (koláčky) – jednoduché textové soubory s informacemi, uchovávané v jednoduchých textových souborech, umístěných na váš počítač z webové sítě. Cookies mohou být čteny webovými stránkami během vašich pozdějších návštěv. Informace uložená v cookie může mít vztah k vašemu chování při procházení webové stránky, nebo obsahovat jedinečné identifikační číslo, takže si vás webová stránka bude moci „pamatovat" při vaší příští návštěvě.

**CRM** - Customer Relationship Management, systém pro řízení vztahu se zákazníky.

**Customizace** – tvorba zakázkového řešení nebo úprav podle konkrétního přání zákazníka.

**Cyberspace** - označení virtuálního světa vytvářeného moderními technologiemi (počítači, telekomunikačními sítěmi apod.) paralelně ke světu „reálnému".

**Cyber stalking** - (kybernetický lov) – zneužívání online komunikace k obtěžování a zastrašování vybraných uživatelů. Oběti tohoto typu chování jsou pak pronásledovány a obtěžovány spamem, zanecháváním různých (často urážlivých) vzkazů v návštěvních knihách na webových stránkách, na chatu, zasíláním virů, apod.

**Čárový kód** - je prostředek pro automatizovaný sběr dat. Je tvořen černotiskem vytištěnými pruhy (v některých novějších verzích kódu mozaikou) definované šířky, umožňujícími přečtení pomocí technických prostředků - čteček či skenerů.

**Dálkový přístup** - přístup do informačního systému prostřednictvím zařízení určeného pro elektronickou komunikaci - telekomunikačního zařízení (například prostřednictvím sítě Internet).

**Data warehouse** - datový sklad, Data warehouse poskytuje uživatelům mnoharozměrný pohled na data získaná z mnoha zdrojů a pomáhá transformovat „surová data" získaná z informačních systémů na informace vhodné a potřebné k rozhodování.

**Digitální podpis** - je podskupinou elektronického podpisu. Jedná se o bezpečnostní mechanismus, který má v zásadě sloužit jako ekvivalent „vlastnoručního" podpisu pro užití v rámci elektronické komunikace.

**DMS** – Dokument Management System je systém, který dokáže ukládat, evidovat, prohledávat a zabezpečit dokumenty.

**Domain Name System** - je internetová služba zajišťující překlad doménových jmen na IP adresy a obráceně.

**Dokument** - každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či digitální.

**DSS** - Systémy na podporu rozhodování (Decision Support Systems) pomáhají svým uživatelům (manažerům) při realizaci řídících a rozhodovacích činností. Uživatel tu může srovnávat dílčí výsledky řešení se svými představami a podle toho ovlivňovat další průběh řešení.

**E-business (e-commerce, elektronické komerce)** – souhrnné označení pro podporu a realizaci podnikání prostřednictvím internetu.

**eGovernment (E-Government)** - série procesů, umožňující výkon veřejné správy a uplatňování občanských práv a povinností fyzických a právnických osob, realizovaných elektronickými prostředky. Cílem je rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům (občanům).

**E-Justice** - viz. Elektronická justice.

**E-podpis (elektronický podpis)** – v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu se jedná o 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 (totožnosti) podepsané osoby ve vztahu k datové zprávě.

**E-procurement** – označení pro elektronické tržiště nebo pro podporu elektronické formy zprostředkování nabídky nákupu v informačních systémech (včetně zadávání veřejných zakázek pomocí elektronických informačních a komunikačních systémů).

**Elektronická justice (E-Justice)** - znamená využití informačních technologií a systémů v prostředí justice (resortu spravedlnosti), především pak zavedení elektronické formy komunikace, výměny a zpracování informací mezi subjekty, nacházejícími se v prostředí

justice nebo vstupujícími do kontaktů s resortem justice (účastníci řízení, jiné orgány veřejné moci).

**Elektronická podatelna** - pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv.

**Elektronická značka** - obdoba zaručeného elektronického podpisu, elektronickou značkou však může k označení dat použít i právnická osoba nebo organizační složka státu, a to automatizovaně (viz. zákon č. 227/2000 Sb., o elektronickém podpisu).

**ERP**- Enterprise Resource Planning, informační systém orientovaný na firemní finanční plánování. Je určen pro plánování zdrojů potřebných k přijetí, zhotovení, dodání a zaúčtování zakázky.

**EU Extranet** - je informační systém Generálního sekretariátu Rady EU (GSC) pro distribuci oficiálních elektronických dokumentů z GSC do Ministerstev zahraničí členských zemí, Stálých misí v Bruselu a Evropské komisi.

**FAQ** - Frequently Asked Questions nebo-li často kladené dotazy a odpovědi na ně. Obvyklá forma nápovědy na webových stránkách.

**FTP** - File Transfer Protocol, protokol pro přenos souborů mezi počítači v Internetu.

**HTML** - zkratka z anglického Hyper Text Markup Language, značkovací jazyk pro hypertext. Je jedním z jazyků pro vytváření stránek v systému World Wide Web, který umožňuje publikaci stránek na Internetu.

**HTTP** - HyperText Transport Protocol, který je využíván ke komunikaci mezi prohlížečem a web serverem. Umožňuje přenášet html stránky z www k uživateli.

**Informační systém** - funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností.

**Informační systém pro aproximaci práva (ISAP)** - je určen pro informační podporu aktivit souvisejících s procesem harmonizace českých právních předpisů s předpisy Evropského společenství. Jeho hlavním cílem je poskytovat uživatelům zejména aktuální informace o platné legislativě ES/EU a ostatních souvisejících dokumentech a jejich českých překladech.

**Informační systémy veřejné správy (ISVS)** - jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů (např. živnostenský zákon nebo obchodní zákoník).

**Internet** - globální síť spojující miliony počítačů ve více než stovce zemí na celém světě. Internet není jinak centrálně řízen a jedná se o decentralizovanou síť, ve které je každý prvek naprosto samostatný a nezávislý. Síť vznikla v šedesátých letech dvacátého století jako projekt americké armády, který měl nabídnout možnost komunikace se zbytkem světa za jakýchkoliv okolností. V tomto duchu pracuje internet dodnes.

**IP adresa** – identifikační detaily pro konkrétní počítač (nebo poskytovatele internetového připojení), vyjádřené v kódu „internetového protokolu" (např. 192.168.72.34). Každý počítač připojený k internetu má jedinečnou IP adresu, ačkoliv adresa nemusí být stejná při každém připojení se k internetu.

**ISEJ** - informačního systém elektronické justice.

**ISVS** – viz. **Informační systémy veřejné správy.**

**JPEG** - Joint Photographic Experts Group, grafický formát, nejčastěji je používán pro ukládání fotografií (obrázků).

**Kancelářský balík** - označení pro skupinu kancelářského software prodávaného jako celek, který nabízí i určitý vyšší stupeň vzájemného propojení jejich funkcí a poskytování více možností než ty, co nabízí operační systém. Kancelářský balík obvykle obsahuje textový procesor, tabulkový procesor a některé další programy jako program na tvorbu prezentací, databázový systém a grafické a komunikační nástroje.

**Kvalifikované časové razítko** - důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

**Kvalifikovaný certifikát** - datová zpráva, která je vydána kvalifikovaným poskytovatelem certifikačních služeb. Spojuje data pro ověřování elektronických podpisů s podepisující resp. označující osobou a umožňuje ověřit její identitu.

**Kyberprostor** – viz. cyberspace.

**Linux** - volně šiřitelný operační systém UNIXového typu. Autorem je Linus Torvalds a tisíce dobrovolných programátorů z celého světa. Představuje alternativu k MS Windows.

**MIČR** – Ministerstvo informatiky ČR, dnes již neexistuje, nástupnická organizace pro eGovernment je Ministerstvo vnitra ČR.

**MVČR** – Ministerstvo vnitra ČR, získalo agendu eGovernmentu po zrušeném Ministerstvu informatiky ČR.

**Nigerijské dopisy** - pod pojmem „nigerijské dopisy" rozumíme tištěné dopisy či e-mailové zprávy, ve kterých cizinec tvrdí, že disponuje značnými finančními prostředky, k jejichž faktickému získání ale potřebuje pomoc další osoby. Obrací se proto na adresáta zprávy a za pomoc při převodu mu nabízí provizi ve výši několika procent z částky. Ve skutečnosti je cílem získat údaje o bankovním účtu adresáta zásilky, který bude následně vykraden.

**OCR** - Optical Character Recognition (optické rozpoznávání znaků) je specializovaný software zabývající se snímáním tištěných dokumentů pomocí skeneru a převodem textového obsahu do tvaru, který je editovatelný počítačem.

**ODF** - Formát OpenDocument (ODF) neboli OASIS Open Document Format for Office Applications (OASIS otevřený formát dokumentu pro kancelářské aplikace) je otevřený souborový formát určený pro ukládání a výměnu dokumentů vytvořených kancelářskými

aplikacemi. ODF zahrnuje textové dokumenty (jako např. poznámky, knihy, dopisy aj.), prezentace, tabulky, grafy a databáze. Formát OpenDocument je standardizován Mezinárodní organizací pro normalizaci jako standard ISO/IEC 26300.

**Osobní údaj** - jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu (viz. zákon č. 101/2000 Sb., o ochraně osobních údajů).

**Orgány veřejné správy** - jsou ministerstva, jiné správní úřady a orgány územní samosprávy.

**Označující osoba** - fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou (viz. zákon č. 227/2000 Sb., o elektronickém podpisu).

**Pharming** - jedna z variant krádeže osobních údajů, které jsou získávány po infikování počítače zákeřným programem. Uživateli je pak např. místo požadované oficiální stránky banky podstrčena falešná stránka, která sbírá přístupové údaje a osobní data k jejich dalšímu zneužití.

**Phishing** - krádež citlivých informací, např. údajů o platební kartě či krádež jména a hesla k nějaké službě. Nejtypičtějším příkladem je falešný e-mail, tvářící se jako odeslaný z vaší banky, v němž je požadavek o ověření totožnosti. Po kliknutí na odkaz je uživatel zaveden na falešnou stránku (která se ovšem tváří, že je v pořádku), kde odevzdá své údaje a následně přijde o peníze. Phishing je tak elektronickou obdobou tzv. „nigerijských dopisů".

**Podepisující osoba** - fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby. Nejčastěji občan nebo zaměstnanec orgánu veřejné správy (viz. zákon č. 227/2000 Sb., o elektronickém podpisu).

**Portál veřejné správy** - informační systém vytvořený a provozovaný se záměrem usnadnit veřejnosti dálkový přístup k informacím z veřejné správy pro ni potřebným.

**Provozní informační systém** - informační systém zajišťující informační činnosti nutné pro vnitřní provoz příslušného orgánu, například účetnictví, správu majetku, a nesouvisející bezprostředně s výkonem veřejné správy.

**Provozovatel ISVS** - subjekt, který provádí alespoň některé informační činnosti související s informačním systémem. Provozováním informačního systému veřejné správy může správce pověřit jiné subjekty, pokud to jiný zákon nevylučuje.

**Původce** - podle zákona č. 499/2004 Sb., o archivnictví a spisové službě (tzv. zákon o spisové službě) každý, z jehož činnosti dokument vznikl.

**RFID čipy** - Radio Frequency Identification, čipy umožňující identifikace na rádiové frekvenci (RFID) jsou další generací identifikátorů navržených např. k identifikaci zboží (navazuje na systém čárových kódů).

**Rodné číslo** - jednoznačný číselný identifikátor přidělovaný obyvatelům v České republice. Lze z něj mj. vyčíst datum narození a pohlaví příslušné osoby.

**RSS** - Really Simple Syndication, je formát souboru založený na XML, který slouží pro tzv. syndikaci -- tedy pro přebírání anotací článků zpravodajských serverů.

**SME** - Small and Medium Enterprises, označení pro malé a střední podniky.

**Spam** – obecný výraz pro hromadně rozesílanou, nevyžádanou elektronickou poštu.

**Spoofing** – technika, při které určitý počítač v rámci sítě internet předkládá falešnou IP adresu a vydává se tak za někoho jiného. Cílem je získat přístup k informacím, které by jinak uživatel získat nemohl (např. placené webové stránky), nebo zabránit své vlastní identifikaci.

**Správce ISVS** - subjekt, který určuje účel a prostředky zpracování informací a za informační systém odpovídá. Jsou to ministerstva, jiné správní úřady, orgány územní samosprávy a další státní orgány (souhrnně nazývané „orgány veřejné správy").

**Standard ISVS** - soubor pravidel pro výkon odborných činností spojených s vytvářením, rozvojem a využíváním informačních systémů veřejné správy uveřejněný ve Věstníku MIČR.

**Systém** - souhrn souvisejících prvků, sdružený do jednoho celku. V latině a řečtině znamená termín „system" kombinovat, uspořádat, sdružovat.

**TCO** – Total Costs of Ownership, celkové náklady vlastnictví.

**Uživatel** - osoba nebo organizace, která používá provozovaný systém k vykonávání specifické funkce.

**Veřejný informační systém** - informační systém vedený správci ISVS, nebo jiný informační systém poskytující služby veřejnosti, který má vazby na informační systémy veřejné správy.

**VoIP** – Voice over IP, technologie umožňující přenos hlasu pomocí internetového protokolu (v prostředí internetu)

**Výkon spisové služby** - zajištění odborné správy dokumentů došlých a vzešlých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností.

**W3C** - World Wide Web Consortium (W3C) je mezinárodní konsorcium, jehož členové společně s veřejností vyvíjejí webové standardy pro World Wide Web (více informací na www.w3c.org).

**Whois** - program, který umí v internetové NIC databázi hledat lidi a další internetové entity jako jsou domény, sítě a jednotlivé stroje.

**XML** - eXtensible Markup Language (česky rozšiřitelný značkovací jazyk) je obecný značkovací jazyk, který byl vyvinut a standardizován konsorciem W3C. Umožňuje snadné

vytváření konkrétních značkovacích jazyků pro různé účely a široké spektrum různých typů dat.

**Základní registry** - mají zabezpečit dostupnost základních zdrojů dat v soustavě informačních systémů veřejné správy.

**Zaměstnanec** - osoba ve služebním poměru, pracovněprávním nebo jiném obdobném vztahu.

**Zaručený elektronický podpis** („e-podpis") - elektronický podpis, který je jednoznačně spojen s podepisující osobou a umožňuje její identifikaci, podepisující osoba ho může udržet pod svou výhradní kontrolou a je k datové zprávě připojen tak, že je možno zjistit jakoukoliv její následnou změnu. Je určen pouze fyzickým osobám. V praxi se používá zejména při komunikaci občana s orgánem veřejné správy (viz. zákon č. 227/2000 Sb., o elektronickém podpisu).

## 1.3. Právní rámec upravující problematiku E-Justice

### *1.3.1. Právní předpisy*

- Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů
- Zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů
- Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů
- Zákon č. 283/1991 Sb., o Policii ČR
- Zákon č. 513/1991 Sb., obchodní zákon, ve znění pozdějších předpisů
- Zákon č. 328/1991 Sb., o konkursu a vyrovnání, ve znění pozdějších předpisů
- Zákon č. 328/1991 Sb., o konkursu a vyrovnání, ve znění pozdějších předpisů
- Zákon č. 436/1991 Sb., o některých opatřeních v soudnictví, o volbách přísedících, jejich zproštění a odvolání z funkce a o státní správě soudů České republiky
- Zákon č. 549/1991 Sb., o soudních poplatcích, ve znění pozdějších předpisů
- Zákon č. 563/1991 Sb., o účetnictví ve znění pozdějších změn a doplňků
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla)
- Zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích
- Zákon č. 29/2000 Sb., o poštovních službách
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- Zákon č. 127/2005 Sb. o elektronických komunikacích
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

- Vyhláška Ministerstva spravedlnosti č. 23/1994 Sb., o jednacím řádu státního zastupitelství, zřízení poboček některých státních zastupitelství a podrobnostech o úkonech prováděných právními čekateli
- Vyhláška č. 496/2004 Sb., k elektronickým podatelnám
- Vyhláška č. 646/2004 Sb., o podrobnostech výkonu spisové služby
- Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- Vyhláška č. 336/2005 Sb., o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv
- Vyhláška č. 522/2005 Sb, kterým se stanoví seznamy utajovaných informací (příloha 1 a 9)
- Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků
- Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací
- Nařízení vlády č. 173/2006 Sb., o zásadách stanovení úhrad a licenčních odměn za poskytování informací podle zákona o svobodném přístupu k informacím
- Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb
- Poštovní podmínky České pošty, s.p., platné od 1.6.2007
- Problematiku spisové služby v podmínkách Policie České republiky upravují dále interní akty řízení vydané Ministerstvem vnitra a interní akty vydané Policií České republiky ve formě závazných pokynů

### *1.3.2. Metodické pokyny týkající se ISVS*

- Metodika tvorby XML schémat v oblasti informačních systémů veřejné správy
- Metodický pokyn pro tvorbu a přidělování doménových jmen třetí úrovně v doméně gov.cz
- Metodika evidence využívání počítačových programů
- Metodický pokyn pro popis datových prvků
- Metodický pokyn pro popis elektronických informačních zdrojů
- Best practice - pravidla pro vyřizování elektronické pošty
- Best practice - Pravidla pro tvorbu přístupného webu
- Metodický předpis pro strukturu standardů ISVS
- Pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů

### *1.3.3. Přehled bývalých standardů ISVS*[3]

- Standard ISVS pro strukturu a výměnný formát digitální technické mapy města (č. 001/01.02)

[3] Standardy ISVS byly k 1.1.2007 zrušeny zákonem č. 81/2006 Sb., kterým se mění zákon č. 365/2000 Sb., o ISVS.

- Standard ISVS pro komunikaci informačních systémů na bázi protokolů TCP/IP (č. 002/01.04)
- Standard ISVS pro náležitosti životního cyklu informačního systému (č. 005/02.01)
- Standard ISVS pro pověřování k výkonu atestací a pro náležitosti provozu atestačních středisek (č. 006/03.01)
- Standard ISVS pro náležitosti procesu a metodiky atestace jakosti produktů (č. 007/01.02)
- Standard ISVS k prostorové identifikaci (č. 008/04.02)
- Standard ISVS pro zveřejňování vybraných informací o veřejné správě způsobem umožňujícím dálkový přístup (č. 012/01.02)
- Standard ISVS pro informační systémy v oblasti personální a platové (č. 013/04.01)
- Standard ISVS pro atestace shody informačních systémů veřejné správy se standardy ISVS (č. 014/01.02)
- Standard ISVS pro transkripci neběžných latinských znaků do znaků podle kódové tabulky ISO Latin 2 (015/01.03)
- Standard ISVS stanovující povinné požadavky na metodiku atestace shody IS se Standardem ISVS pro náležitosti životního cyklu IS (č. 017/01.01)

### *1.3.4. Prováděcí právní předpisy k ISVS*

- Nařízení vlády č. 594/2006 Sb., o přepisu znaků do podoby, ve které se zobrazují v informačních systémech veřejné správy
- Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích
- Vyhláška č. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy
- Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy
- Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS
- Vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní
- Vyhláška č. 53/2007 Sb., o referenčním rozhraní

### *1.3.5. Resortní předpisy (Ministerstvo spravedlnosti ČR)*

- Instrukce MSp č. 1100/98 OOD, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy
- Instrukce MSp č. 75/99 OI, kterou se vydává ukládací řád počítačových údajů
- Pokyn obecné povahy nejvyššího státního zástupce ze dne 4.12.1996, kterým se vydává kancelářský řád státního zastupitelství, ve znění pozdějších předpisů
- Instrukce MSp č. 26/2000 OI, kterou se stanoví postup při předávání dat obchodního rejstříku externím odběratelům
- Instrukce MSp č. 96/96 OI, o vnitřním informačním systému resortu justice

*1.3.6. Seznam stanovisek Úřadu pro ochranu osobních údajů*[4]

- Stanovisko č. 1/2007 - K aplikaci práva na ochranu osobních údajů při poskytování informací o činnosti orgánů veřejné správy
- Stanovisko č. 8/2006 - K využívání elektronických karet
- Stanovisko č. 7/2006 - Dozorové pravomoci Úřadu pro ochranu osobních údajů v souvislosti s výkonem advokacie
- Stanovisko č. 6/2006 - Nahlížení do kandidátních listin a poskytování informací o kandidátech voleb do obecních zastupitelstev
- Stanovisko č. 5/2006 - Poskytování osobních údajů při kontrolní činnosti
- Stanovisko č. 4/2006 - Zveřejňování osobních údajů v dražební vyhlášce
- Stanovisko č. 3/2006 - Dálkový (elektronický) přístup obecní policie k osobním údajům z informačního systému evidence obyvatel, registru provozovatelů a řidičů motorových a přípojných vozidel
- Stanovisko č. 2/2006 - Zpracování osobních údajů v rámci vědy
- Stanovisko č. 1/2006 - Provozování kamerového sytému z hlediska zákona o ochraně osobních údajů
- Stanovisko č. 1/2005 - Činnost pojišťovacích zprostředkovatelů a oznamovací povinnost
- Stanovisko č. 6/2004 - Kopírování dokladů z pohledu zákona o ochraně osobních údajů
- Stanovisko č. 5/2004 - Uplatnění částky zaplacených odborových příspěvků jako odečitatelné položky od daně z příjmu
- Stanovisko č. 4/2004 - Aplikační výklad k části zákona č. 133/2000 Sb. o evidenci obyvatel a rodných číslech a o změně některých zákonů
- Stanovisko č. 3/2004 - Zpracování osobních údajů v souvislosti s prováděním klinického hodnocení léčiv a léčivých přípravků
- Stanovisko č. 2/2004 - Zpřístupňování a zveřejňování osobních údajů z jednání zastupitelstev a rad obcí a krajů
- Stanovisko č. 1/2004 - Evidence při vstupech do budov
- Stanovisko č. 2/2002 - Zpracovávání osobních údajů v souvislosti s činností knihovny
- Stanovisko č. 1/2002 - Zpracování osobních údajů v souvislosti se zajišťováním zdravotní péče
- Stanovisko č. 2/2001 - Zpracování citlivého osobního údaje členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací
- Stanovisko č. 1/2001 - Zveřejňování jmen dlužníků
- Stanovisko č. 1/2000 - Vedení dokumentace pacientů ve zdravotnictví

*1.3.7. Seznam norem a standardů týkajících se bezpečných elektronických systémů*

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

[4] Text stanovisek je k dispozici v elektronické podobě na stránkách Úřadu pro ochranu osobních údajů – www.uoou.cz.

- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.
- ČSN ETSI TS 102 023 - Elektronické podpisy a infrastruktury; Požadavky na postupy autorit časových razítek.
- ČSN ISO/IEC 17799 - Informační technologie - Soubor postupů pro management bezpečnosti informací.
- ČSN BS 7799-2 - Systém managementu bezpečnosti informací - Specifikace s návodem pro použití.
- ČSN ISO/IEC TR 13335 - Informační technologie - Směrnice pro řízení bezpečnosti IT 1-3.
- ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.
- CWA 14167-2 - Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.
- CWA 14167-4 - Cryptographic module for CSP signing operations - Protection profile - CMCSO PP.
- CWA 14169 - Secure signature-creation devices "EAL 4+".
- FIPS PUB 140-1 - Security Requirements for Cryptographic Modules.
- FIPS PUB 140-2 - Security Requirements for Cryptographic Modules.

# 2. Současný stav justice a možnosti při nasazení informačních technologií a informačních právních systémů

## 2.1. Obecné zhodnocení

Současný stav v oblasti justice v ČR je charakteristický tím, že existující informační systémy a technologie se prakticky výlučně zaměřují na oblast organizace a řízení justice.[5] Přípravné i vlastní soudní řízení jak na občanskoprávním, tak trestním úseku zatím stále probíhá výlučně v listinné podobě, s minimální provázaností prostřednictvím elektronické komunikace, a to jak mezi jednotlivými články resortu justice a soudy, tak i mezi jednotlivými složkami veřejné správy a účastníky soudního nebo správního řízení.

Podání elektronickou poštou na soudy je v současné době již možné.[6] Elektronicky podepsaná podání musí mít připojen kvalifikovaný certifikát vystavený akreditovaným poskytovatelem certifikačních služeb. Fungování elektronické podatelny je řešeno zákonem a informace o elektronické podatelně musí být na webových stránkách.[7]

Neexistuje ovšem plně funkční e-komunikace mezi státními zastupitelstvími, soudy, účastníky soudního řízení a ostatními orgány veřejné moci (včetně Policie ČR). E-podatelna je dnes zpravidla prvním a současně posledním místem elektronického zpracování dokumentu (podání). Nadále totiž zůstává zásadní upřednostňování papírové formy oběhu dokumentů, která setrvává v podstatě jako jediný nosič informací pro soudní a správní řízení. Pokud se do oběhu výjimečně dostane elektronický dokument, je ihned „zprocesněn" vytisknutím na papír a vložením do spisu, který dále koluje jako originál v papírové formě.

Zjevné nevýhody papírové formy:[8]

- je méně bezpečná proti manipulaci či padělání,
- je snadněji zničitelná (záplavy, plísně, hlodavci apod.),
- občas se „ztrácí" či je odcizena,
- ztráta spisu přitom obvykle znamená nemožnost ukončit řízení,
- obtížněji se transportuje (zasílá, předává),
- kdo chce nahlédnout do spisu, musí se osobně dostavit do lokality jeho fyzického uložení,
- list papíru je vždy dražší než jeho elektronický obraz,
- velké množství papíru nešetří životní prostředí.

---

[5] Viz a podrobněji: Ministerstvo spravedlnosti ČR, Popis modulární struktury včetně jejich vazeb a návaznosti a harmonogram vybudování elektronické justice - studie proveditelnosti, 2007.

[6] Na elektronické adrese podatelny posta@msp.justice.cz - tato přijímá datová média (FDD nebo CD) a datové zprávy ve formátu DOC nebo RTF.

[7] Povinnost k provozování elektronických podatelen je stanovena obecně pro orgány veřejné moci zákonem 227/2000 Sb., o elektronickém podpisu, v provedení nařízením vlády 495/2004 Sb. Postup při přijímání a odesílání datových zpráv prostřednictvím elektronických podatelen upravuje vyhláška č. 496/2004 Sb., o elektronických podatelnách.

[8] Tamtéž (Popis modulární struktury … … studie proveditelnosti ).

Nasazení informačních technologií a systémů pro podporu činnosti české justice není v současné době evidentně optimálně využito. Elektronizace činnosti soudů probíhá pouze pozvolna. Základní příčiny tohoto stavu lze hledat v povaze relativně rigidního soudního systému. Procesní postupy jednotlivých typů soudního řízení se řadu let opíraly o jediný dostupný způsob zpracování písemností klasickou papírovou formou. Přinejmenším desítky let precizované postupy pro činění podání, zasílání a předávání písemností i pro oběh písemností uvnitř soudního systému vytvořily poměrně dobře fungující systém, který však z hlediska propustnosti i úrovně sdílení a ochrany informací dosáhl svého maxima.[9] S uvolněním společenských poměrů a zvýšeným ekonomickým i sociálním pohybem došlo a stále dochází k razantnímu růstu počtu soudně řešených kauz. Vyspělé země světa (v rámci EU i mimo ni) se vydaly cestou masivní elektronizace svých soudních systémů, což vytváří tlak na uplatnění stejného postupu i v našich podmínkách, z důvodu vzájemné informační a technické kompatibility.[10]

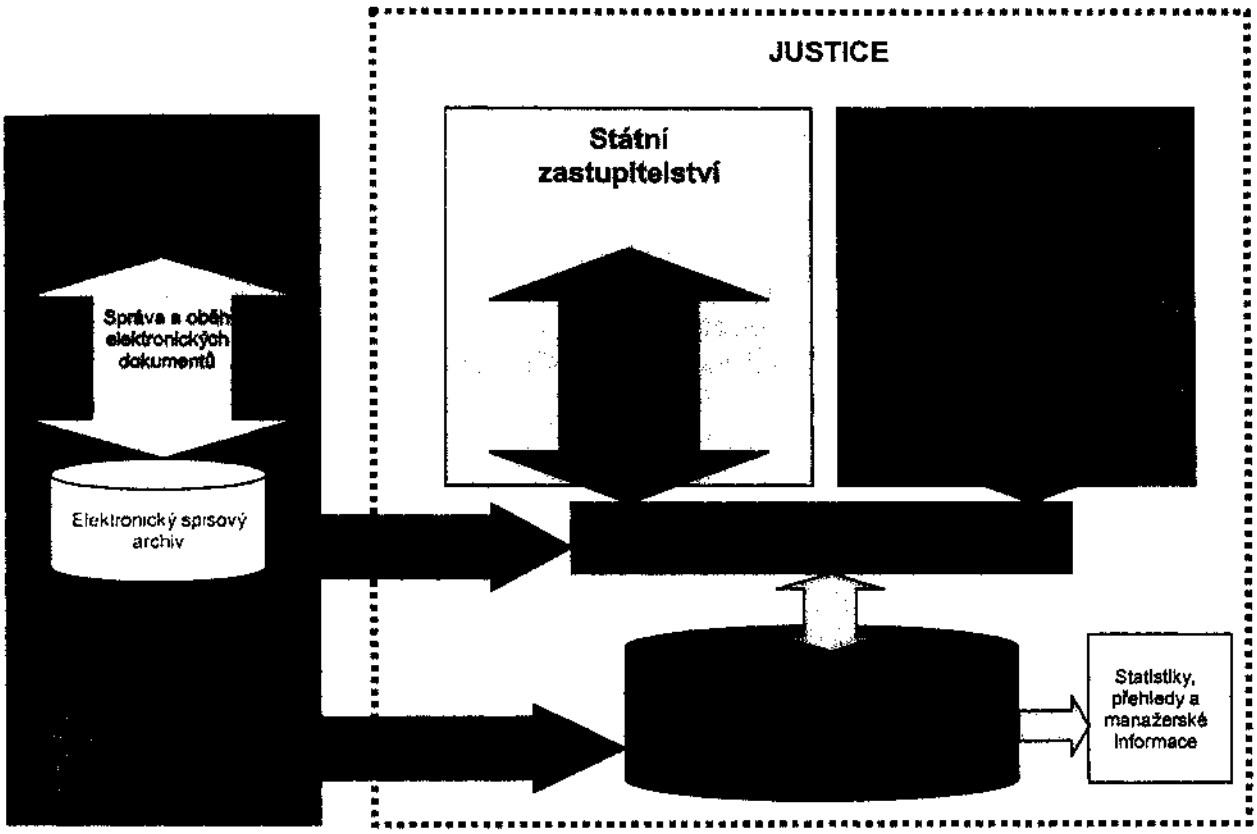
Při současném stavu české justice je možno ze systémového hlediska rozdělit zpracování a oběh písemností na tři základní části:[11] (1) písemnosti na vstupu do soudního sytému, (2) písemnosti zpracovávané uvnitř soudního systému a (3) informace na výstupu ze soudního systému.

Pokud jde o písemnosti na vstupu do soudního systému, obecné informace může tazatel získat v elektronické formě. Civilní soudní podání lze podle § 41 odst. 1 zákona č. 99/1963 Sb., občanského soudního řádu, ve znění pozdějších předpisů, činit písemně, ve stanovených případech ústně, a dále mj. též elektronicky. V tomto případě však musí být podání doplněno předložením papírového originálu nebo papírovým podáním stejného znění. Elektronické podání tak plní funkci předběžného podání, ke kterému soud bez dodatečného písemného potvrzení nepřihlíží.[12] Trestní řád (zákon č. 141/1961 Sb., ve znění pozdějších přepisů) umožňuje podání v písemné i v kvalifikované elektronické formě. Podání musí být podepsáno zaručeným elektronickým podpisem ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Tím je zaručena originalita podání (všechny změny podání jsou zjistitelné) a obsah podání jako datové zprávy je spojen nezaměnitelným způsobem s podepisující osobou. Podání jsou doručována na elektronické podatelny soudů. Povinnost k provozování elektronických podatelen je stanovena obecně pro orgány veřejné moci zákonem 227/2000 Sb., o elektronickém podpisu, v provedení nařízením vlády 495/2004 Sb. Postup při přijímání a odesílání datových zpráv prostřednictvím elektronických podatelen upravuje vyhláška č. 496/2004 Sb., o elektronických podatelnách.

Pro písemnosti zpracovávané uvnitř soudního systému je z hlediska efektivity soudního řízení (samostatně stojí oblast elektronizace vlastní administrativy soudů) rozhodující možnost vedení soudního spisu v elektronické podobě. Zdlouhavost rozhodování soudů je zčásti zapříčiněna administrativními průtahy způsobenými pomalým oběhem papírových písemností mezi soudními instancemi i soudy stejné úrovně. Soudy se v době oběhu soudního spisu cestou poštovního styku dostávají do stavu vynucené nečinnosti ve vztahu k řešení dané

[9] Tamtéž (Popis modulární struktury … … studie proveditelnosti ).
[10] Tamtéž (Popis modulární struktury … … studie proveditelnosti ).
[11] Tamtéž (Popis modulární struktury … … studie proveditelnosti ).
[12] §42 3 OSŘ: *„Podání obsahující návrh ve věci samé učiněné telegraficky je třeba písemně doplnit nejpozději do tří dnů, je-li písemné podání učiněno telefaxem nebo v elektronické podobě, je třeba v téže lhůtě jej doplnit předložením jeho originálu, případně písemným podáním shodného znění. K těmto podáním, pokud nebyla ve stanovené lhůtě doplněna, soud nepřihlíží. Stanoví-li to předseda senátu, je účastník povinen soudu předložit originál (písemné podání shodného znění) i jiných podání učiněných telefaxem.“*

kauzy. Elektronické vedení soudního spisu přináší rovněž v praxi významné zásadní zvýšení zabezpečení soudního spisu proti neoprávněné manipulaci s ním – především proti krádeži listin ze spisu, který často není proti takovému postupu dostatečně zabezpečen. V případě vhodného zajištění elektronického soudního spisu je možnost neoprávněné manipulace s jeho obsahem vyloučena.[13]




*Obrázek: Ukázka oběhu elektronického dokumentu v rámci policie a justice. Zdroj: Ministerstvo spravedlnosti ČR.*

Na výstupu ze soudního systému se v současné době objevují v elektronické formě pouze informace organizačního charakteru nebo informace, které nejsou pro justici specifické (úřední deska, seznamy pracovníků, údaje podle zákona č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a další). Již delší dobu se diskutuje otázka zveřejňování soudních rozhodnutí v plném rozsahu (s výjimkou specifických případů).[14] Vedle obecného zvýšení informovanosti o rozhodování soudů by se tím zvýšila i kontrola činnosti soudců s pozitivní zpětnou vazbou na kvalitu jejich práce. Kvalitní, jednotný způsob zveřejňování rozhodování soudů napomůže prostřednictvím snadnější dostupnosti soudních rozhodnutí i ke snížení míry nejednotnosti judikatury.[15]

[13] Tamtéž (Popis modulární struktury ... ... studie proveditelnosti ).
[14] Viz. např. volební program SNK Evropští demokraté - http://www.snked.cz/index.php?dok=1288.
[15] Tamtéž (Popis modulární struktury ... ... studie proveditelnosti ).

Při vysokých nárocích na ochranu, snadnou a současně selektivní dostupnost zpracovávaných, přenášených a uchovávaných dat, vznikajících činností justice, je zřejmé, že odpovídající zajištění výše uvedených postupů může být realizováno efektivním způsobem pouze v rámci komplexního, jednotně připraveného, vedeného a odpovídajícím způsobem procesně zajištěného projektu elektronizace české justice E-Justice.[16] Komplexní informační řešení z tohoto projektu vzešlé musí mj. zajistit ochranu příslušných dat na úrovni rámcově odpovídající např. standardům v oblasti bankovnictví.

V současné době využívané komunikační kanály v rámci veřejné správy (včetně justice):

- Osobní setkání
  V rámci veřejné správy je stále běžným způsobem, jak komunikovat s úřadem, osobní setkání, tedy kdy se občan osobně dostaví na konkrétní úřad a záležitost vyřídí s příslušným úředníkem. Cílem eGovernmentu a E-Justice je tyto případy minimalizovat a umožnit občanovi, aby většinu agendy mohl vyřizovat prostředky komunikace na dálku. Každý úřad pro osobní komunikaci s občanem stanovuje tzv. úřední hodiny.

- Informační kancelář
  Informační kancelář poskytuje potřebná sdělení jak při telefonických dotazech, tak při osobních návštěvách občanů. Tyto služby jsou ve stanoveném rozsahu poskytovány bezplatně.

- Úřední deska
  Podle § 26 odst. 1 zákona 500/2004 Sb., správního řádu je povinen každý správní orgán zřídit úřední desku, která musí být nepřetržitě veřejně přístupná, a obsah úřední desky se zveřejňuje i způsobem umožňujícím dálkový přístup, tedy jinými slovy na internetu. V případě obcí se na úřední desce obligatorně publikují např. obecně závazné vyhlášky a nařízení obce, záměry obce prodat, směnit nebo darovat nemovitý majetek, pronajmout jej nebo poskytnout jako výpůjčku, dále rozhodnutí krajského úřadu, resp. Ministerstva vnitra o odejmutí (části) výkonu přenesené působnosti, oznámení o počtu členů obecního zastupitelstva, který má být volen v následujícím volebním období, oznámení o místě, době a navrženém programu připravovaného zasedání zastupitelstva obce atd. S publikací některých z uvedených dokumentů pak zákon č. 128/2000 Sb., o obcích spojuje závažné právní důsledky – v případě právních předpisů obce nabytí jejich platnosti, resp. účinnosti, v případě oznámení o majetkoprávních úkonech naopak možnou neplatnost příslušného právního úkonu. Obdobným způsobem a s obdobnými právními důsledky je publikace těchto dokumentů upravena i v zákoně č. 129/2000 Sb., o krajích a v zákoně 131/2000 Sb., o hl. m. Praze. Dále např. podle § 76 zákona č. 166/1999 Sb., o veterinární péči se vyhláška o mimořádných opatřeních vyhlásí tak, že se vyvěsí na úřední desce krajského úřadu a všech dotčených obecních úřadů nebo podle § 12 zákona č. 26/2000 Sb., o veřejných dražbách se u dražeb nemovitostí předpokládá uveřejnění oznámení o dražbě též na úřední desce příslušného obecního úřadu.

- Podatelna (klasická)

[16] Podrobněji např. viz. rozhovor s Ministrem spravedlnosti ČR Jiřím Pospíšilem na serveru www.ejustice.cz (20.6.2007).

Klasické podatelny fungující na každém úřadu pro příjem listin a dokumentů. Úřady jsou také povinny informovat občana o úředních hodinách podatelen. Úředník podatelny na požádání potvrdí příjem příslušné listiny.

- Elektronická podatelna (e-podatelna)
  Záležitosti elektronických podatelen jsou v současné době legislativně upraveny zákonem č. 227/2000 Sb., o elektronickém podpisu, nařízením vlády č. 495/2004 Sb., kterým se provádí zákon o elektronickém podpisu, a vyhláškou č. 496/2004 Sb., o elektronických podatelnách. V těchto dokumentech je stanovena povinnost provozovat elektronickou podatelnu a přijímat jejím prostřednictvím podání opatřená zaručeným elektronickým podpisem. Kromě příjmu elektronických podání opatřených zaručeným elektronickým podpisem upravuje správní řád i příjem nepodepsaných elektronických podání. Takové podání je postaveno na úroveň podání pomocí jiných technických prostředků, zejména dálnopisu nebo telefaxu. Znamená to, že nepodepsané elektronické podání musí být do 5 dnů potvrzeno písemně, ústně do protokolu nebo též opět elektronicky, ale již se zaručeným elektronickým podpisem.

- Telefon, Fax (včetně Call Centra)
  Jsou klasickými komunikačními kanály veřejné správy, které mají oporu i v zákoně. Podání na orgány veřejné správy je možné učinit i faxem.

- Pošta (klasická)
  Klasická pošta vedle podatelny je zatím stále nejrozšířenější komunikační kanál, pokud občan vyžaduje potvrzení o přijetí svého podání (např. formou doporučeně s dodejkou).

- Média (televize, rádio, rozhlas, tisk)
  Media poskytují veřejné správě také široké spektrum komunikačním kanálů vůči občanovi. Kromě veřejnoprávní televize zvažuje veřejná správa i zřízení speciální kabelové televize. Stejně tak orgány veřejné správy využívají tištěná media jako komunikační prostředek (např. noviny pražského magistrátu).

- Internet (email, webové stránky, RSS, VoIP)
  Internet a jeho možnosti (email, webové prezentace atd. včetně IP telefonie) by se měly stát do budoucna hlavním komunikačním kanálem jak v rámci veřejné správy, tak i mezi veřejnou správou a občanem.

- Vyvolávací systémy
  Vyvolávací systém je častý komunikační kanál, který slouží pro určení pořadí v případech, že v určitou dobu se na orgány veřejné správy obrací více žadatelů (občanů).

- Interní oběžníky
  Obsahují texty a informace určené pro interní potřebu uzavřené skupiny pracovníků (např. v rámci určitého ministerstva nebo podniku).

- Intranet, Extranet
  Intranet a Extranet jsou počítačové sítě, které používají stejné technologie (TCP/IP, HTTP) jako internet. Jde ale o tzv. „soukromé" sítě, tzn., že jsou určeny pro použití pouze malé skupiny uživatelů (například pracovníci určitého úřadu). Vnější přístup k

takovéto počítačové síti je zabezpečen a kontrolován. Smyslem intranetu a extranetu je zpřístupnění zvolených informací a programů vybraným subjektům za účelem zefektivnění vzájemné spolupráce.

- SMS brány, automatizované terminály (kiosky) atd.
  Mezi další komunikační kanály lze řadit např. SMS brány nebo různé druhy (informačních) kiosků a terminálů. Tyto druhy komunikačním kanálů se zatím používají okrajově, nicméně jejich počet v budoucnu nepochybně vzroste.

## 2.2. Projekt „E-Justice" v ČR

V souladu s informační politikou Ministerstva spravedlnosti ČR byly vytyčeny tyto strategické cíle v oblasti informatiky:[17]

- výstavba informační a komunikační infrastruktury pro interní i externí potřeby složek resortu (včetně personálního zajištění oživujícího tuto infrastrukturu);
- dostupnost a využitelnost potřebných informací pro řídicí a rozhodovací procesy („information management");
- vytvořit předpoklady pro přechod od řízení informací („information management") k řízení znalostí („knowledge management");
- vytvořit předpoklady pro uplatnění informačních technologií při řídicích procesech;
- zajištění vzdělávání pro odborný personál a uživatele informačních a komunikačních technologií, včetně stanovení požadavků na rozvoj a řízení lidských zdrojů k využívání informací;
- zajištění přístupu k informacím z resortu pro občany.

Splnění těchto cílů je ale vždy dlouhodobý proces podmíněný součinností a vhodnou koordinací mnoha faktorů: organizačních, personálních, technických a finančních. Zvýšená pozornost úloze informačních a komunikačních technologií je také vyjádřena v mnoha dokumentech Evropské unie i vlády České republiky.

Jeden z nejvýznamnějších projektů (strategických cílů) se začal realizovat dne 21. prosince 2005, kdy vláda ČR vyslovila svým usnesením č. 1652 souhlas s přípravou informačního systému elektronické justice (E-Justice) v České republice (resp. jeho 1. etapy, tedy elektronického soudního spisu). O necelý rok později 6. prosince 2006 pak vláda České republiky usnesením č. 1390 vzala na vědomí materiál „Návrh zavedení informačního systému elektronické justice (ISEJ) v České republice" a zároveň uložila úkol připravit a předložit Vládě ČR k projednání materiál zajišťující provázanost informačního systému elektronické justice se systémem eGovernmentu v celé veřejné správě.[18]

Hlavním cílem projektu elektronické justice v České republice je vytvořit takové legislativní, technické a organizační podmínky, aby bylo možno primárně vést všechny soudní spisy v

[17] Podrobněji viz. dokument „Informační politika civilní části resortu spravedlnosti", www.justice.cz.
[18] Popularizací elektronizace českého soudnictví (eJustice) se dlouhodobě zabývá např. server www.ejustice.cz.

elektronické podobě a zajistit možnost bezpečného přístupu k obsahu spisu pro oprávněné osoby.[19]

Materiál „Návrh postupu pro zavedení informačního systému elektronické justice (ISEJ) v České Republice", který vláda vzala v roce 2006 na vědomí, obsahuje popis potřeb resortu justice na přípravu tohoto informačního systému v návaznosti na systém eGovernmentu. Materiál rovněž obsahuje podrobný popis postupů, které je nezbytné při vývoji informačního systému dodržovat. Předmětný materiál navrhuje mimo jiné i časový, věcný a finanční harmonogram dalších postupových kroků.

Zavedení informačního systému elektronické justice je odůvodněno zejména z níže uvedených důvodů:[20]

1. zvýšení průchodnosti a dostupnosti české justice;
2. snížení doby vyřizování soudních případů;
3. zefektivnění meziresortní spolupráci - především mezi rezorty Ministerstva spravedlnosti ČR a Ministerstva vnitra ČR (včetně Policie ČR) při vyřizování trestní agendy;
4. zlepšení dohledu na průběh soudního řízení;
5. zajištění lepšího sdílení informací mezi státním zastupitelstvím, soudem a případně probační a mediační službou;
6. možnost sdílení informací (soudních spisů) mezi jednotlivými soudy;
7. zlepšení komunikace veřejnosti s justicí (možnost komunikace v elektronické podobě);
8. zlepšení přístupu osob k informacím ze soudních spisů i prostřednictvím sítě internetu.

*Časový harmonogram (etapy) zavedení informačního systému elektronické justice:*[21]

- *I. etapa:* zavedení elektronického soudního spisu. Zahájení implementačních prací v roce 2008. Pilotní implementace: konec roku 2008. Zkušební provoz 30. 6. 2009. Postupné zahájení rutinního provozu systému elektronické justice – rok 2010
- *II. etapa:* ověření funkčnosti systému elektronického trestního řízení a přenosu dat mezi Policií a Státním zastupitelství a soudy – 30. 6. 2009
- *III. etapa:* komplexní řešení elektronické justice včetně výměny informací se všemi orgány státní správy – zahájení etapy 30. 6. 2009

Finanční náklady na přípravu informačního systému elektronické justice jsou odhadovány následovně:[22]

| Rok | Náklady v mil. Kč |
|---|---|

[19] K pojmu E-Justice (e-justice, Ejustice) též např. Vladimír Smejkal, Řekněme ANO procesním analýzám v justici!, www.ejustice.cz (5.3.2006).
[20] Viz. Předkládací zpráva „Provázanost informačního systému elektronické justice se systémem eGovernment v celé veřejné správě", Ministerstvo spravedlnosti ČR, 2007, č.j. 67/2007 OIS SP.
[21] Tamtéž (Předkládací zpráva „Provázanost ..." ).
[22] Tamtéž (Předkládací zpráva „Provázanost ..." ).

| | |
|---|---|
| 2007 | 135 |
| 2008 | 235 |
| 2009 | 100 |
| 2010 | 100 |
| **Celkem** | **570** |

Mezi nejvýznamnější dílčí úkoly, které jsou v přímé vazbě na elektronickou justici, budou dále patřit:[23]

1. *Bezpečnost datových sítí a serverů*
   Zvýšení zabezpečení datových sítí a serverů všech složek resortu Ministerstva spravedlnosti. Pro splnění tohoto úkolu je nutné zavedení důvěryhodné výpočetní základny na všech složkách resortu.

2. *Dohled nad provozem informačních systémů*
   Zajistit další rozvoj komplexní systémové správy jako nástroje pro dohled datových sítí a informačních systémů s důrazem na možnost aktivního dohledu a zvýšení efektivnosti využití.

3. *Stabilita serveru a stanic*
   Zabezpečit zvýšenou stabilitu klientských stanic a serverů. K zajištění tohoto úkolu zabezpečit jasná pravidla obnovy techniky resortu a zavést pravidelný cyklus obnovy PC a serverů.

4. *Sdílení informací resortních informačních systémů*
   Zlepšit komunikaci mezi jednotlivými informačními systémy, které jsou v resortu justice provozovány. Dopracovat informační systémy o takové komunikační rozhraní, aby bylo možné efektivně sdílet zpracovávané informace. Zajistit propojení resortních systémů s externími datovými zdroji s využitím standardizovaného formátu.

5. *Výpisy z evidence obchodního rejstříku a Rejstříku trestů*
   Umožnit poskytování výpisů z evidence obchodních rejstříků a Rejstříku trestů oprávněným osobám a orgánům veřejné správy. Zajistit podmínky pro poskytování výpisů i na jiných zákonem vyjmenovaných místech (CZECH POINT).

6. *Výměna informací o odsouzených osobách v rámci EU*
   Připojení Rejstříku trestů do ověřovacího provozu vybraných států EU (Německo, Francie, Španělsko, Belgie, Lucembursko), jehož cílem je vzájemně sdílet informace z těchto evidencí.

7. *Insolvenční rejstřík*
   Zajištění vývoje informačního systému insolvenčního rejstříku, ověření na vybraných pilotních soudech a zahájení rutinního provozu u všech krajských a vrchních soudů.

8. *Bezpečné připojení uživatelů informačních systémů*

[23] Tamtéž (Předkládací zpráva „Provázanost ...“ ).

Zajištění bezpečného připojení pro zaměstnance jednotlivých složek resortu k vybraným informačním systémům pomocí veřejné datové sítě Internet tak, aby byla zajištěna plnohodnotná reakce na podání k soudům i v mimopracovní době.

9. *Formuláře pro obchodní rejstřík*
Změna formulářů pro podání návrhu do Obchodního rejstříku, zajištění takových služeb, aby bylo možné podání doručit i elektronicky (s využitím zaručeného elektronického podpisu).

10. *Elektronické platební rozkazy*
Vývoj a nasazení systému, který umožní přijímat a vydávat platební rozkazy v elektronické podobě.

11. *Informace o stavu soudních řízení*
Zpřístupnění informací o stavu jednotlivých soudních řízení, a to prostřednictvím sítě Internetu.

12. *Informace o jednáních v jednacích síních soudů*
Zpřístupnění informací o jednotlivých soudních jednáních v jednacích síních, a to prostřednictvím sítě Internetu.

13. *Evidence soudních rozhodnutí (judikatura)*
Změna koncepce systému evidence soudních rozhodnutí a zapojení Nejvyššího soudu do tohoto procesu. Zpřístupnění evidence oprávněným osobám.

14. *Centrální evidence stíhaných osob*
Rozvoj Centrální evidence stíhaných osob a integrace tohoto systému s rutinně provozovanými systémy soudů.

15. *Centrální podatelna pro resort justice*
Zajištění projektu nasazení centrální podatelny resortu a její integrace do provozních systémů Ministerstva spravedlnosti ČR, soudů a státních zastupitelství.

16. *Využití eLearningu*
Zajištění vývoje a provozu eLearningu jako jedné z hlavních forem vzdělávání v rámci resortu justice.

17. *Záložní komunikační uzel*
Vybudování záložního informačního a komunikačního uzlu sítě s cílem zajištění maximální dostupnosti a bezpečnosti poskytovaných služeb systémy resortu.

18. *Úřední desky složek resortu*
Zajištění projektu nasazení informačního systému úředních desek jednotlivých složek resortu. Nákup elektronických kiosků pro složky resortu tak, aby bylo možné udržovat úřední desky v elektronické podobě.

**Harmonogram zavedení informačního systému elektronické justice z hlediska časové náročnosti**
*(Zdroj: Ministerstvo spravedlnosti ČR)*

| Krok | Popis | Období |
|---|---|---|
| 0. | Zpracování procesní analýzy | Q3 2007 |
| 1. | Zajištění metodického dohledu (MD) projektu elektronické justice v souladu se zákonem č. 137/2006 Sb., o veřejných zakázkách, v platném znění | Q4 2007 |
| 2. | Zajištění generálního dodavatele (GD) systému elektronické justice v souladu se zákonem č. 137/2006 Sb., o veřejných zakázkách, v platném znění | Q1 2008 |
| 3. | Implementace I. etapy - elektronického soudního spisu | 2008–2009 |
| 3.1 | Dílčí projektové úlohy implementace:<br>• Analýza 1. etapy projektu<br>• Dílčí projektová úloha – personální analýza ve vztahu k problematice elektronického soudního spisu<br>• Dílčí projektová úloha – analýza legislativních změn ve vztahu k problematice elektronického soudního spisu | Q1 2008 |
| 3.2 | Předložení návrhu novel zákonů umožňujících zavedení elektronické justice vládě ČR v termínu do 31.12.2007 | Q1 2008<br>Schválení návrhů |
| 3.3 | • Vybudování datového úložiště - evidence eSpisu<br>• Bezpečnost eSpisu<br>• Oběh dokumentů eSpisu<br>• Řízení přístupu, sdílení a postupování eSpisu<br>• Pilotní implementace | 2008 |
| 3.4 | • Integrace s existujícími IS MSP<br>• Zkušební provoz<br>• Centrální skenování spisového archivu MSP<br>• Proces vybavování subjektů resortu MSP vybavením pro eSpis<br>• Digitalizace archivu spisů MSP | 2008 - 2009 |
| 3.5 | • Digitalizace archivu spisů MSP<br>• Zahájení rutinního provozu<br>• Analýza 2. etapy | 2009 |
| 4. | Zahájení implementace II. etapy – mezirezortní spolupráce | 2009 – 2013 |

## 2.3. V současné době nejčastěji využívané právní informační systémy

### *2.3.1. Systém ASPI*

Systém ASPI[24] (automatizovaný systém právních informací) je komplexní systém pro práci s právními informacemi.

Systém obsahuje:

- všechny předpisy současné české a slovenské Sbírky zákonů, Sbírky mezinárodních smluv, Sbírky zákonů a nařízení ČSR
- právní předpisy vydané samosprávnými celky – kraji
- předpisy ministerstev a ústředních orgánů (např. texty předpisů publikované ve Finančním zpravodaji, Cenovém věstníku, věstnících ministerstva průmyslu a obchodu, zdravotnictví, školství a řada dalších)
- nálezy Ústavního soudu publikované ve Sbírce zákonů
- předpisy vydané před rokem 1945 včetně zákonů bývalého Rakouska-Uherska

Všechny texty jsou dostupné v aktuálním znění se zachováním jednotlivých historických časových znění textu až po jeho původní podobu.

Ve verzi pro ČR jsou uvedeny i informace o předpisech vydaných v SR po 1.1.1993 a naopak; lze provozovat současně obě verze a porovnávat např. předpisovou úpravu v ČR a v SR. Firemní software umožňuje přebírání autentických textů z tiskárny Sbírky zákonů a zvyšuje tak podstatně přesnost textu i vysokou aktuálnost.

Systém dále obsahuje literaturu a judikaturu:

- právnická a ekonomická literatura
- současné i historické komentáře a výklady k předpisům
- komentáře předních autorů k aktuálním předpisům a jejich novelám
- důvodové zprávy k návrhům zákonů
- systematicky zpracované prameny od roku 1990
- zařazeny i některé komentáře z období před rokem 1948
- provázáno na ustanovení příslušných právních předpisů
- veškerá judikatura a stanoviska soudů s provázaností vzhledem k právním předpisům
- ve spolupráci s Ústavním soudem zařazovány i nálezy a usnesení Ústavního soudu nad rámec tištěné Sbírky nálezů a usnesení Ústavního soudu
- zařazována jsou i rozhodnutí Evropského soudu pro lidská práva

### *2.3.2. LexDATA – právní informační systém*

Právní informační systém LexDATA[25] je moderní systém s unikátním rozsahem právních databází.

[24] Zdroj: www.aspi.cz.

Systému LexDATA obsahuje následující databáze:

- předpisy Sbírky zákonů – jedna z nejrozsáhlejších databází právních předpisů vydávaných ve Sbírce zákonů od roku 1918 a také vybrané významné právní normy publikované před rokem 1918
- předpisy Sbírky mezinárodních smluv včetně cizojazyčných verzí
- aktualizovaná znění Sbírky zákonů a Sbírky mezinárodních smluv v časovém řezu jejich vývoje

Judikatura obsahuje:

- judikaturu oficiální Sbírky soudních rozhodnutí a stanovisek a další judikaturu na základě doporučení soudců Nejvyššího soudu ČR od roku 1961
- judikaturu oficiální Sbírky rozhodnutí Nejvyššího správního soudu
- judikaturu oficiální Sbírky nálezů a usnesení Ústavního soudu
- judikaturu Sbírky soudních rozhodnutí Evropského soudu pro lidská práva ve Štrasburku
- judikaturu uveřejňovanou nakladatelstvím C. H. Beck v Souboru rozhodnutí Nejvyššího soudu a v jednotlivých časopisech
- judikaturu Sbírky rozhodnutí Nejvyššího soudu Československé republiky ve věcech občanských z let 1919 – 1948.

Věstníky a zpravodaje obsahují:

- archivy celých ročníků oficiálních periodik ministerstev a ústředních orgánů státní správy
- publikované důvodové zprávy

Předpisy místní samosprávy obsahují předpisy hlavního města Prahy, statutárních měst a všech krajů

Literatura obsahuje:

- plné texty článků uveřejněných v časopisech nakladatelství C. H. Beck: Právní rozhledy, Soudní rozhledy, Trestněprávní revue, Ad Notam a Právní zpravodaj
- přehled literatury obsahující anotace důležitých článků z periodik: Bulletin advokacie, Justiční praxe, Právní rádce a Právník
- přehled literatury obsahující bibliografické záznamy důležitých knih a periodik

Celní sazebník je ve formě elektronické knihy od roku 1997

Předpisy Evropské unie:

- ze Sbírky zákonů odkazy na související předpisy EU ve všech oficiálních jazycích (databáze EurLEX)

---

[25] Zdroj: www.lexdata.cz.

- možnost fulltextového vyhledávání v revidovaných českých překladech předpisů EU publikovaných na serveru vlády ČR (systém ISAP)
- odkaz na vyhledávání na českém portálu EU - EurLEX

### *2.3.3. LexGalaxy – právní informační systém*

LexGalaxy[26] je právní informační systém o českých právních dokumentech od roku 1784 včetně historických právních památek od roku 992. LexGalaxy obsahuje kompletní rejstřík cca 100.000 dokumentů a podstatný výběr textů dokumentů ze Sbírky zákonů od roku 1918; kompletní sbírky Ústavního soudu; oficiální prameny judikatury (od roku 1918); Finanční zpravodaje; správní rozhodnutí; spousty věstníků ústředních a jiných orgánů státní správy a samosprávy a další důležité právní zdroje nejen české, ale i evropské či mezinárodní. Zahrnuje i velmi žádaná a praktická rekonstruovaná úplná znění (neoficiální) řady zákonů a vyhlášek. Velký důraz je kladen i na mezinárodní smlouvy a dohody. Součástí systému jsou i vybrané informace o evropském právu (EU) a právu Rady Evropy (Evropský soud pro lidská práva).

## 2.4. Resortní informační a komunikační systémy

Ministerstvo spravedlnosti ČR zabezpečuje vývoj a údržbu informačních systémů, které jsou plošně nasazovány u jednotlivých složek resortu. V této kapitole budou popsány nejdůležitější informační systémy, které jsou již rutinně provozovány.[27]

### *2.4.1. ISOR - Informační systém obchodního rejstříku*

Informační systém obchodního rejstříku slouží pro evidenci a vyřizování agendy obchodních rejstříků. Pomocí této aplikace jsou prováděny všechny zápisy do databáze. Aplikace umožňuje vyhotovovat výpisy a úplné výpisy z databází a zároveň její nadstavba zabezpečuje vedení veškerých podání v této agendě a vedení evidence materiálů, které jsou uloženy ve sbírce listin. Aplikace je nasazena u všech rejstříkových soudů a je v rutinním provozu od roku 1995. Je to typická terminálová aplikace, která pracuje v prostředí znakových terminálů. Je provozována v prostředí databázového systému Informix a je vytvořena s pomocí nástroje Informix 4GL. Součásti informačního systému je i modul, který zabezpečuje aktualizaci databází v rámci jednotlivých rejstříkových soudů tak, že každý den ráno je na každém z těchto soudů vytvořena totožná databáze všech údajů ze všech rejstříkových soudů. Pro noční aktualizaci údajů je využívána rozlehlá datová síť Ministerstva financí. Přenosové trasy vyčleněné pro potřeby resortu spravedlnosti jsou pro současné potřeby z hlediska přenosové kapacity již nedostačující; obdobně nedostačující je i spolehlivost sítě a dohled nad činností sítě zajišťovaný Ministerstvem financí.

### *2.4.2. ISKOS – informační systém obchodního soudnictví*

[26] Zdroj: www.lexgalaxy.cz.
[27] Zdroj: Informační politika civilní části resortu spravedlnosti v letech 2001-2005.

Informační systém obchodního soudnictví je rutinně provozován na úseku obchodního soudnictví na krajských soudech a na vrchních soudech v České republice. Slouží k evidenci a vyřizování obchodní agendy těchto soudů. Obsahuje nástroje, které výrazně usnadňují práci a zjednodušují zpracování této agendy. Aplikace je připravena pomocí vývojových prostředků Informix 4GL a je provozována v prostředí znakových terminálů s využitím databázového systému Informix.

### *2.4.3. ISAS – informační systém pro administrativu okresních soudů*

Speciální informační systém určený pro vedení administrativy okresních soudů. Hlavní přínos spočívá ve sjednocení způsobu evidence a zvýšení efektivnosti práce soudů, zejména u rutinních opakujících se činností. Systém řeší veškerou administrativu okresních soudů, od nápadu přes automatické přidělení soudci, vedení rejstříku a zpracování dokumentů po zpracování rozsudků, statistiky a výkazů.

### *2.4.4. IRES – informační systém pro vedení ekonomických agend*

Systém využívá databázový stroj Oracle a je určen pro ucelené zpracování ekonomiky všech složek resortu. Je složen z těchto modulů:

- Rozpočet
- Peněžní deník
- Majetek
- Zásoby
- Smlouvy
- Výkaznictví
- Faktury
- Účetnictví
- Pokladna
- Banka
- Pohledávky a závazky
- Výkaznictví
- Vazba na mzdy

Jednotlivé moduly lze provozovat samostatně, přičemž celý informační systém je provázán s informačním systémem pro administrativu okresních soudů, informačním systémem pro státní zastupitelství, informačním systémem Nejvyššího soudu a informačním systémem agendy konkursů.

### *2.4.5. ISYZ – informační systém pro státní zastupitelství*

Speciální informační systém vyvinutý pro všechny stupně státních zastupitelství. Systém zpracovává administrativu státních zastupitelství, tedy rejstříky pro jednotlivé druhy řízení vedené na státním zastupitelství a ostatní evidenční pomůcky (např. kniha vazeb, kniha úschov apod.). Systém obsahuje modul pro sledování různých vybraných rizikových věcí.

### *2.4.6. ISNS – informační systém Nejvyššího soudu*

Speciální informační systém pro vedení administrativy Nejvyššího soudu. Systém řeší veškerou administrativu soudu, od nápadu přes automatické přidělení soudci, vedení rejstříku a zpracování dokumentů po zpracování rozsudků, statistiky a výkazů. Součásti systému jsou funkce pro podporu správy Nejvyššího soudu a kanceláře předsedy Nejvyššího soudu. Společným modulem je katalog rozhodnutí a evidence judikatury, který představuje speciální podporu pro práci s rozhodnutími a stanovisky, která kolegia Nejvyššího soudu zpracovávají v rámci své sjednocovací činnosti a publikují ve Sbírce soudních rozhodnutí a stanovisek. Systém využívá databázový stroj Oracle a je určen pro práci v prostředí MS Windows. Pro zpracování dokumentů využívá možnosti textového editoru MS WORD.

### *2.4.7. ISKONK – informační systém agendy konkursů*

Speciální informační systém pro vedení agendy konkursů u krajských soudů. Systém je určen pro práci v prostředí MS Windows a pro zpracování dokumentů využívá možnosti textového editoru MS WORD.

### *2.4.8. Evidence znalců a tlumočníků*

Speciální informační systém pro vedení agendy znalců a tlumočníků u krajských soudů. Vytvořená databáze je pravidelně pololetně v souladu s instrukcí Ministerstva spravedlnosti postupována všem okresním soudům a dalších resortním i mimoresortním organizacím. Pro prohlížení databáze slouží samostatné programové vybavení, které je nedílnou součásti systému.

### *2.4.9. Evidence Rejstříku trestů*

Tento informační systém slouží pro evidenci všech trestních listů, na kterých jsou údaje o trestech vynesených soudy České republiky. Systém umožňuje tisk záznamu o odsouzení z této evidence.

## 2.5. Další informační systémy využívané v právní praxi

### *2.5.1. AKWin (BaumSoft) - softwarový produkt určený pro advokátní kanceláře*

AK4Win - Advokátní kancelář[28] pro MS Windows je programovým celkem vytvořeným speciálně pro advokátní kanceláře. Jeho účelem je evidovat veškeré dění od příchodu klienta

[28] Zdroj: www.aspi.cz.

až po závěrečné vyúčtování. Umí ale také vést účetní evidenci kanceláře a vytvořit daňové přiznání.

Základním prvkem je spisová evidence, tj. kartotéka klientů a spisů. Každý klient má svoji kartu se svými údaji a u každého klienta je možné vést libovolné množství spisů. Také každý spis má svoji kartu a na ní je evidováno vše, co se od data nápadu na spise odehrálo.

### 2.5.2. *ISAP - Informační systém pro aproximaci práva*

Informační systém pro aproximaci práva – ISAP[29] je určen pro informační podporu aktivit souvisejících s procesem harmonizace českých právních předpisů s předpisy Evropského společenství. Jeho hlavním cílem je poskytovat uživatelům zejména aktuální informace o platné legislativě ES/EU a ostatních souvisejících dokumentech a jejich českých překladech. Obsahuje rovněž pomocné nástroje pro analýzu a komparaci právních předpisů, postižení vzájemných vztahů a monitorování průběhu aproximačního procesu, sledování legislativního procesu z hlediska aproximace a podpůrné prostředky pro překladatelskou a revizní činnost.

### 2.5.2. *FinKalk 2001*

FinKalk 2001[30] představuje sadu specializovaných kalkulaček pro různé výpočty (úroky z prodlení, advokátní tarif, notářské poplatky, ap.).

[29] Zdroj: isap.vlada.cz.
[30] Zdroj: www.juristic.cz.

# 3. Využití informačních technologií a systémů v občanském soudním řízení sporném

## 3.1. Procesní úkony účastníků řízení a soudu

### *3.1.1. Úvod*

Občanské soudní řízení sporné se zahajuje na návrh, tzv. žalobou. Občanský soudní řád (OSŘ) upravuje tři definice účastníků řízení (obvykle tzv. žalobce a žalovaného).[31] První definice je dle § 90 OSŘ, kde se stanoví, že účastníky řízení jsou žalobce a žalovaný. Dále § 94 stanoví, že v řízení, které může být zahájeno i bez návrhu, jsou účastníky i navrhovatel a ti, o jejichž právech nebo povinnostech má být v řízení jednáno. Jde-li však o řízení o neplatnost manželství nebo o určení, zda tu manželství je či není, jsou účastníky pouze manželé (tzv. druhá definice). V neposlední řadě jsou účastníky řízení také navrhovatel a ti, které zákon za účastníky označuje (třetí definice).

Procesní úkony lze definovat jako úkony (projevy nebo jednání subjektů řízení),[32] které ovlivňují zahájení, průběh a ukončení procesu (řízení).[33] Procesními úkony soudu jsou všechny úkony, které soud činí v průběhu řízení, od jeho zahájení až do pravomocného skončení (tedy soudní rozhodnutí nebo opatření soudu). Procesní úkony účastníků řízení se nazývají podáním (např. žaloba) a vždy směřují vůči soudu.[34] Podání dle § 42 OSŘ je možno učinit písemně, ústně do protokolu, v elektronické podobě, telegraficky nebo telefaxem. Ústně do protokolu je možno pak podání učinit, jde-li o návrh na zahájení řízení o povolení uzavřít manželství, o určení a popření rodičovství, o určení, zda je třeba souhlasu rodičů dítěte k jeho osvojení, o osvojení a řízení, které lze zahájit i bez návrhu, a návrhy na výkon rozhodnutí v těchto řízeních vydaných.

### *3.1.2. Nasazení elektronického podpisu a jeho úprava v právním řádu*

Elektronický podpis[35] je jedním z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu. Postupně stále více právních předpisů umožňuje jeho používání v oblasti orgánů veřejné správy, a to jak při komunikaci mezi úřady navzájem, tak i při komunikaci občanů s jednotlivými úřady.

---

[31] Podrobněji viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 157 an.

[32] Subjekty řízení jsou soud (na jedné straně) a účastníci řízení (na straně druhé).

[33] Podrobněji viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 188 an.

[34] Podrobněji viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 198 an.

[35] K elektronickému podpisu se vztahují zejména tyto prováděcí právní předpisy: (1) vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, (2) nařízení vlády č. 495/2004 Sb, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů a (3) vyhláška č. 496/2004 Sb. k elektronickým podatelnám.

Elektronický podpis[36] představují podle zákona o elektronickém podpisu (ZEP) *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 (totožnosti) podepsané osoby ve vztahu k datové zprávě.* V tomto pojetí se může elektronickým podpisem rozumět i podpis v textu e-mailové zprávy.[37] Zákon o elektronickém podpisu upravuje především náležitosti zaručeného elektronického podpisu a elektronickým podpisem ve smyslu předchozí definice se dále nezabývá. Z toho důvodu se v praxi pod pojmem elektronický podpis většinou rozumí zaručený elektronický podpis. Zaručený elektronický podpis jsou tedy digitální data, která podepisující osoba vytváří pomocí svého soukromého klíče a zajišťuje jimi integritu a nepopiratelnost původu podepsaných dat.

V současné době nemá elektronický podpis podle zákona v českém právním řádu při všech právních úkonech stejné účinky jako podpis vlastnoruční. V oblasti soukromého práva lze činit právní úkony elektronicky a tyto úkony elektronicky podepisovat tam, kde právní předpis či jiné platné ujednání (dohoda zúčastněných stran) nedovozuje neplatnost tohoto úkonu,[38] pokud není dodržena listinná forma.[39]

V praxi lze rozlišovat tyto druhy elektronických podpisů (e-podpisů):

1) *„prostý" elektronický podpis* (§ 2, písm. a) ZEP)

   Za takovýto e-podpis může být považováno i podepsaní se v textu emailové zprávy.

2) *zaručený elektronický podpis* (§ 2, písm. b) ZEP)

   Zaručeným elektronickým podpisem je dle ZEP elektronický podpis, který splňuje následující požadavky:

   a) je jednoznačně spojen s podepisující osobou,
   b) umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
   c) byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
   d) je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

3) *uznávaný elektronický podpis* (§ 11 ZEP)

[36] Pro mezinárodně právní komparaci srov. např. Štědroň, B., Electronic Signature in USA, Common Law Review, Vol 3, No 5, Autumn 2003, str. 54-56, ISSN 1213-4678 (úprava e-podpisu v právu USA) nebo Štědroň, B., Právní úprava elektronického podpisu v Rusku, www.itpravo.cz, IT Právo – server o internetovém a počítačovém právu, 11.04. 2003, Společnost pro právo informačních technologií (SPIT), ISSN 1801-4089 (úprava e-podpisu v Rusku) atd.

[37] Podrobněji viz www.micr.cz (i po zrušení Ministerstva informatiky ČR jsou stránky stále v provozu a obsahují řadu užitečných informací).

[38] Například pokud občanský zákoník stanoví, že vlastnoruční závěť musí být napsaná vlastní rukou a vlastní rukou podepsaná, jinak je neplatná, potom v tomto případě nelze substituovat vlastnoruční podpis za elektronický.

[39] Podrobněji viz (zdroj): www.micr.cz – často kladené otázky k e-podpisu.

> Uznávaný elektronický podpis představuje nejvyšší zákonem požadovaný stupeň bezpečnosti a může být vydáván pouze tzv. akreditovanými poskytovateli certifikační služeb.[40]

Zákon (ZEP, § 11) dále stanoví, že v oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (tzv. „uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám.

S pojmem elektronický podpis se někdy zaměňuje pojem „elektronická značka". Z technologického hlediska je elektronická značka stejná jako zaručený elektronický podpis, tj. jedná se o digitální podpis.[41] Pro vlastní vytváření elektronických značek nebo pro přijímání datových zpráv jimi označených není tedy potřeba pořizovat jiný software. Odlišnost elektronické značky a zaručeného elektronického podpisu má především právní charakter. Elektronický podpis vytváří fyzická osoba (stejně jako vlastnoruční), elektronickou značkou může datové zprávy označovat i právnická osoba nebo organizační složka státu. Lze ji přirovnat k otisku úředního razítka. Zákon (ZEP) stanoví, že (§11) písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.[42]

### *3.1.3. Jak správně vyřizovat emaily a vést jejich evidenci*

Elektronická pošta (e-mail, email, e-pošta)[43] se stále více prosazuje jako prostředek doručování písemností veřejné správě na úkor listovní pošty. Po novele hlavních procesně právních předpisů je nutné vzít v úvahu i skutečnost, že takto doručené písemnosti mají stejný význam a plynou z nich stejné právní důsledky jako z podání doručených v listinné podobě. Některé z těchto písemností jsou zároveň elektronicky podepsány. Je proto nezbytné, aby se pracovníci soudu naučili s písemnostmi v elektronické podobě zacházet a používat prostředky elektronické komunikace k jejich přijímání a doručování. Význam a množství úřední korespondence v elektronické podobě bude v budoucí době pouze narůstat.

#### *1. E-podatelna soudu jako efektivní nástroj pro přijímání / odesílání elektronické pošty*

E-podatelna je místem, které slouží k přijímání/vstupu a vypravování/výstupu elektronických písemností do/z úřadu. Pro úřady je klíčové nahlížet na e-podatelnu jako na alternativu

---

[40] V praxi není samozřejmě vydáván elektronický podpis jako takový, ale nástroje pro vytváření a kontrolu elektronického podpisu (tzv. soukromý a veřejný klíč). Samotný elektronický podpis je pouze číslo vygenerované počítačem, které je při každém procesu podpisu jiné.

[41] Digitální podpis je bezpečnostní mechanismus, který má v zásadě sloužit jako ekvivalent „vlastnoručního" podpisu pro užití v elektronické komunikaci. Digitální podpis je podskupinou elektronického podpisu.

[42] Podrobněji k problematice e-podpisu viz. www.micr.cz (často kladené otázky k e-podpisu).

[43] Tato kapitola vychází ze zásad pro vyřizování elektronické pošty, které Ministerstvo informatiky vydalo jako „best practice", a které jsou určeny zejména orgánům státní správy a samosprávy, jakož i dalším právním subjektům, které rozhodují jako orgány veřejné moci (dále „úřady") a kterým jsou doručovány písemnosti ve smyslu zákona o archivnictví a spisové službě prostřednictvím elektronické pošty.

listovní podatelny, neboť zde naleznou odpověď na většinu otázek, které pojem e-podatelny v uživatelích často vyvolává.

E-podatelnou je třeba rozumět souhrn technického vybavení, umožňujícího připojit se prostřednictvím sítě na poštovní server e-podatelny, stáhnout elektronickou poštu do své e-mailové schránky v poštovním klientu, uložit a evidovat doručenou elektronickou poštu a postoupit ji k dalšímu vyřízení, dále obsluha e-podatelny a pravidla pro zacházení s elektronickými písemnostmi, nejčastěji ve formě spisového řádu a návodů pro obsluhu technického vybavení.

Obecně lze říci, že:

a) čím více úřad sjednotí postupy zpracování pošty v listinné podobě s postupy při zpracování elektronické pošty, tím srozumitelnější prostředí pro své pracovníky vytvoří,

b) čím více elektronické pošty bude do úřadu vstupovat prostřednictvím e-podatelny, tím menší budou „ztráty" této pošty, neboť došlá pošta bude podléhat jedné evidenci a bude s ní manipulovat omezený a kontrolovaný počet pracovníků, které není problém vyškolit. Obdobně to platí i pro poštu odesílanou. Bude-li došlá i odesílaná pošta procházet tímto jedním kanálem, bude možné jednoduše zkontrolovat, jak je došlá pošta vyřizována.

### 2. *Nakládání s elektronickou poštou musí být upraveno ve spisovém a skartačním řádu*

Spisový a skartační řád,[44] jako základní předpis upravující oběh písemností v úřadu, je základním dokumentem, který definuje postupy pro práci s elektronickými písemnostmi. Je třeba, aby v něm úřad upravil, které datové zprávy jsou v působnosti spisového řádu a stávají se písemnostmi úřadu a které nikoli.[45] Množinu těchto písemností můžeme definovat jako elektronickou poštu, která souvisí s výkonem kompetencí daného úřadu. Mezi datové zprávy, které není třeba považovat za písemnosti určené úřadu, bezpochyby patří soukromá sdělení adresovaná zaměstnancům úřadu, spam nebo interní e-mailová komunikace (např. komunikace mezi nadřízenými a podřízenými).

Elektronickou poštu nelze ze spisového řízení vyčlenit a považovat ji za zvláštní kategorii komunikace. Naopak je s ní třeba nakládat stejně obezřetně, a v souladu se spisovým a skartačním řádem, jako s poštou v listinné podobě. Pokud spisový a skartační řád nebo jiné interní směrnice elektronickou poštu ignorují a příslušné postupy neupravují, nelze očekávat, že s ní bude náležitě nakládáno.

Vymezení toho, jaké datové zprávy podléhají spisovému řízení, je úkolem spisového řádu. Dalším úkolem je určení postupů pro jejich evidenci a vyřizování.

---

[44] Zákon o archivnictví a spisové službě § 66 odst. 2: *„Určení původci vydají vnitřní předpis pro výkon spisové služby, který obsahuje základní pravidla pro manipulaci s dokumenty u určeného původce* (dále jen „spisový a skartační řád")..."

[45] Vyhláška o podrobnostech výkonu spisové služby § 2 odst. 2: „...Určený původce uvede ve svém spisovém a skartačním řádu seznam dokumentů, které z hlediska jeho činnosti nejsou úředního charakteru; tyto dokumenty pak nepodléhají evidenci."

3. *Postupy musí být upraveny jak pro poštu, která do úřadu vstupuje prostřednictvím e-podatelny, tak pro poštu, která dochází jednotlivým pracovníkům na jejich jména do jim přidělených e-mailových schránek.*

E-podatelna by měla být hlavním místem, kudy vstupují do úřadu elektronické písemnosti. Někdy se stává, že podání (žádosti, oznámení, stížnosti) doručují osoby nikoliv na adresu e-podatelny (např. posta@justice.cz), ale přímo do e-mailových schránek zaměstnanců.[46] I v takovém případě musí písemnost projít e-podatelnou, protože právě zde musí dojít k její evidenci a k ověření e-podpisu, pokud je k datové zprávě přiložen. Spisový a skartační řád musí pamatovat i na tuto situaci a ukládat zaměstnancům, aby písemnost do e-podatelny sami doručili. Zpráva musí být přeposlána včetně všech jejích součástí, kterými mohou být přílohy, ale i e-podpis, pokud jím je zpráva opatřena, a certifikát, je-li ke zprávě přiložen.

Přeposlání lze provést uložením dané datové zprávy ve formátu, který zachovává všechny její součásti (např. standardizovaný formát .eml, případně formát .msg), a následným odesláním této zprávy v příloze.

Přeposílat naopak není nutné datové zprávy, které jsou svým obsahem a rozsahem obdobou telefonického rozhovoru. Taková pošta se neeviduje. Pokud však má úřad zájem, aby určitý přehled o této poště existoval, může vést její evidenci například v rámci jednotlivých organizačních útvarů na nižší úrovni řízení (např. oddělení). Tato evidence může posloužit pro kontrolu, zda bylo na došlou poštu reagováno a zda se tak stalo bez zbytečného prodlení, nebo pro namátkovou kontrolu, jakým způsobem jsou požadavky, dotazy apod. vyřizovány. Je vhodné, aby tato došlá i odeslaná pošta byly ukládány tak, aby k nim měl přístup bezprostředně nadřízený pracovník (např. k tomuto účelu vyhrazený adresář se sdíleným přístupem).

Na straně zaměstnanců je pak třeba dbát na to, aby byly správně rozlišeny datové zprávy, které mají být evidovány a ukládány a které nikoliv. Spisový a skartační řád by měl toto rozlišení formulovat co nejjasněji, aby každý pracovník uměl bez problémů rozlišit, která z doručených zpráv podléhá spisové evidenci (zejména podání podle správního řádu či jiného předpisu, žádost o informaci podle zákona o svobodném přístupu k informacím, stížnost apod.).

Doručování dokumentů či písemností, které mají úřední charakter, do e-mailových schránek zaměstnanců, je vždy komplikací a zbytečným zatížením úředního procesu. Vyloučit však tyto případy v praxi nelze. Navíc zde vždy existuje nebezpečí, že v důsledku nepřítomnosti pracovníka zůstane doručená datová zpráva po určitý čas nepovšimnuta. Preventivním opatřením je v této věci dobrá informovanost těch, kteří úřadu podání zasílají. Na webových stránkách úřadu je třeba jasně deklarovat, že pro doručování se používá daná adresa e-podatelny, jak tato e-podatelna na podání odpovídá apod. Občan tak získá konkrétní

[46] Vyhláška o podrobnostech výkonu spisové služby § 1 odst. 6: *„Pokud je v adrese na obálce dokumentu uvedeno na prvním místě jméno a příjmení fyzické osoby, předá se adresátovi, popřípadě jím určené osobě, neotevřená. Zjistí-li adresát po otevření zásilky, která mu byla takto doručena, že obsahuje dokument úředního charakteru, zabezpečí jeho dodatečné zaevidování a dále postupuje podle spisového a skartačního řádu určeného původce. Pokud je dokument úředního charakteru doručen v digitální podobě přímo do e-mailové schránky adresáta, postupuje se podle věty druhé obdobně.“*

představu o způsobu, jak je jeho podání zpracováno, a má větší motivaci jej zaslat právě na tuto adresu místo odesílání dokumentů konkrétnímu zaměstnanci.

### 4. *Úřad má možnost zřídit více e-podatelen pro příjem datových zpráv různého obsahu*

Soud (úřad) má možnost se rozhodnout, že zřídí více e-podatelen, z nichž každá je učena pro příjem datových zpráv předem stanoveného obsahu (např. pro příjem podání podle správního řádu, pro příjem žádostí o informace podle zákona o svobodném přístupu k informacím, pro příjem dotazů atd.). Dosavadní praxe však ukazuje, že takové opatření nemusí vždy přinést očekávaný efekt. Odesilatelé zpráv se často nezabývají tím, zda má úřad více e-podatelen, a zprávu zašlou na elektronickou adresu, kterou znají, nebo na první, kterou mají k dispozici (zpravidla na webových stránkách úřadu).

V této souvislosti je nutné si uvědomit, že odesilatel nemá zákonnou povinnost zasílat datové zprávy úřadu výlučně prostřednictvím e-podatelny, případně jedné z několika e-podatelen.[47] Podání je zásadně učiněno v okamžiku, kdy se o něm úřad dozví, a tímto okamžikem se stává účinným.[48] To znamená v době, kdy je přijato na jakoukoliv elektronickou adresu úřadu, nikoliv až tehdy kdy jej obdrží e-podatelna, případně e-podatelna, kterou úřad zřídil pro příjem zpráv určitého obsahu. Jiný postup by připadal v úvahu jen tehdy, pokud by některý zákon stanovil, že podání je účinné pouze tehdy, pokud je doručeno konkrétní e-podatelně.

Určitou výhodu mají úřady, které postupují podle právních předpisů stanovujících, že podání je možné podat pouze na jimi zveřejněném tiskopisu (např. daňová přiznání). E-podatelna (resp. aplikace), která taková podání přijímá, má možnost prakticky neumožnit zaslání jiného podání a naopak nabízí výhodu (zveřejněný formulář, event. další služby aplikace) těm, kteří ji využijí.

Pokud se tedy úřad rozhodne provozovat více e-podatelen, měl by najít způsob, jakým zainteresovat odesilatele, aby zaslal datovou zprávu na „správnou" e-podatelnu. Může to být forma adresy (stavebni_rizeni@urad.cz), příslib rychlé reakce (např. pokud svůj dotaz zašlete na adresu dotazy@urad.cz, vyřídíme jej do tří dnů) aj. Praktické zkušenosti při uplatnění takových postupů však prozatím nejsou.

V případě, že úřad provozuje více e-podatelen, může s ohledem na úspornost provozu interně stanovit, že pouze jedna z podatelen provede předepsané postupy při doručování datových zpráv (odeslání potvrzení o doručení apod.). V takovém případě, na těch e-podatelnách, které nebudou předepsané postupy provádět, musí dojít k uložení datové zprávy ve formátu, který zachová všechny její součásti (viz výše), a k jejímu odeslání na e-podatelnu, která tyto postupy provádět bude, ve formě přílohy.

### 5. *Ve spisovém řádu je vhodné upravit nakládání s poštou, která je dodána na technickém nosiči (disketě, kompaktním disku atd.)*

---

[47] Zákon o elektronickém podpisu, v § 11 odst. 3 stanoví, že orgán veřejné moci přijímá a odesílá datové zprávy prostřednictvím e-podatelny. Jedná se tedy o povinnost úřadů, nikoliv těch, kteří jim zprávy zasílají. Podle zákona č. 500/2004 Sb., správní řád, platí od 1. 1. 2006, že se podání činí u orgánu věcně a místně příslušného, přičemž e-podatelna není „orgánem", ale souborem technicko-organizačních pravidel (viz nařízení vlády, kterým se provádí zákon o elektronickém podpisu č. 495/2004 Sb.).

[48] Správní řád § 37 odst. 6: „*...Podání je učiněno dnem, kdy tomuto orgánu došlo.*"

Je-li technický nosič přílohou pošty doručené v listinné podobě, je nezbytné, aby byl evidován jako její nedílná příloha a tak s ním bylo i nakládáno. Je-li doručen pouze technický nosič, je vhodné, aby byl evidován „klasickou" podatelnou jako zásilka, a předán e-podatelně ke zpracování datové zprávy uložené na tomto nosiči. S datovou zprávou se dále manipuluje obdobně, jako by byla doručena e-podatelně prostřednictvím sítě.

6. *Mezi odesílatelem datové zprávy a e-podatelnou musí být na straně úřadu „kontrolní mechanismus", kterým je antivirová ochrana včetně ochrany proti datovým zprávám, které mají chybný formát*

Internet, který je hlavním prostředím pro připojení e-podatelen, je velmi málo regulovaným médiem. Každý z připojených uživatelů se zde vystavuje riziku neoprávněného přístupu do systému nebo zasažení škodlivým kódem,[49] a proto je nutné se těmto hrozbám bránit.

Úřad musí tedy před přijetím jakékoli datové zprávy do e-podatelny ověřit, zda daná zpráva neobsahuje škodlivý software nebo zda její formát nemůže poškodit její aktiva. Pokud by k této kontrole nedošlo a zprávy zasažené viry nebo jiným škodlivým kódem byly e-podatelnou přijaty, mohly by způsobit nenapravitelné škody. Takto zasažené zprávy mohou být uloženy jen mimo e-podatelnu, a to pouze tehdy, není-li tím ohrožena bezpečnost informačního systému úřadu ani bezpečnost zpracovávaných informací. Pokud je v možnostech úřadu tyto zprávy odděleně a bezpečně uložit, například do antivirových trezorů, je vhodné, aby uloženy byly, a tak byly k dispozici pro možnost případného řešení sporů a dokazování.

Je na uvážení úřadu, zda bude informovat odesílatele o přijetí takto poškozené datové zprávy. Doporučuje se však maximální obezřetnost, neboť řada „zavirovaných" zpráv při doručení „maskuje" elektronickou adresu odesílatele. V takovém případě by prosté „odpovězení" bylo zasláno na elektronickou adresu, ze které zpráva nebyla odeslána.

Datové zprávy, které neprošly úspěšně výše uvedenou kontrolou, nejsou považovány za doručené.

7. *U doručených datových zpráv je nezbytné stanovit a zaznamenat čas jejich doručení*

V okamžiku, kdy datová zpráva dojde e-podatelně, je jí tzv. dostupná. To znamená, že e-podatelna zprávu přijala a může s ní dále nakládat (např. evidovat ji, ověřit e-podpis, pokud je připojen atd.). Za dostupnou se tedy považuje datová zpráva, pokud je uložena již na e-mailovém serveru ve schránce e-podatelny.

Pro některé další úkony je nutné určit a zaznamenat přesný čas doručení. Jedná se o čas doručení, nikoliv čas počátku zpracování. Časem doručení může být například pátek 20:00:00 SEČ,[50] kdy byla datová zpráva e-podatelně doručena, i když bude poprvé otevřena až v pondělí na začátku pracovní doby. Úřad tedy musí počítat veškeré lhůty od času doručení.

[49] Podle vyhlášky o elektronických podatelnách se kontroluje výskyt počítačového programu, který je způsobilý přivodit škodu na informačním systému nebo na informacích zpracovávaných orgánem veřejné moci, nebo chybný formát přijaté datové zprávy (souhrnně „škodlivý kód").

[50] Středoevropský čas, též CET (Central European Time).

Organizačně ani technicky nelze se 100% úspěšností zajistit, že podání budou na úřad docházet výhradně na e-podatelnu. Jak již bylo uvedeno, bude se stávat, že podání přijdou přímo do e-mailové schránky zaměstnance úřadu. Tento zaměstnanec má pak povinnost přijatou datovou zprávu zaslat e-podatelně k zaevidování. Časem doručení bude i v tomto případě čas, kdy datová zpráva došla na e-mailový server, ze kterého si datovou zprávu do své e-mailové schránky zaměstnanec stáhl.

8. *Způsob zacházení s nevyžádanými obchodními sděleními (spam) by měl být upraven spisovým a skartačním řádem. Obecně platí, že nemusí podléhat spisovému řízení*

Zákon o některých službách informační společnosti zakazuje všem subjektům, až na malé výjimky, šířit bez souhlasu adresáta obchodní sdělení. Tento „nešvar" způsobuje v současné době velmi podstatné zvýšení objemu dat přenášených po Internetu. Zpracování těchto dat v e-podatelnách může znamenat zbytečné zatížení jak technického vybavení, tak jeho obsluhy. Uvedený zákon o některých službách informační společnosti nemůže ale spam z prostředí českého Internetu zcela odstranit, a proto je třeba problém řešit. Jednou z možností, která je v souladu s legislativou, je nastavit e-podatelnu tak, aby odmítala nevyžádaná obchodní sdělení a tyto datové zprávy nebyly e-podatelnou ukládány a evidovány. Podmínkou je, aby antispamový filtr byl dobře nastavený, a nemohlo se stát, že dojde k odmítnutí důležité písemnosti (např. podání).
Ačkoli se to může zdát jednoduché, vždy zde bude určité riziko odmítnutí platného podání, a proto může úřad uvážit také druhou variantu. Tou je přijímání i obchodních sdělení od odesilatelů, kteří nejsou na tzv. opt-in seznamu, a následné posouzení těchto sdělení, tj. zda se budou dále zpracovávat nebo budou odmítnuta a případně bude upozorněn Úřad pro ochranu osobních údajů na jejich doručení. V každém případě se doporučuje použít určitý filtr, který rozdělí doručenou poštu na platné písemnosti a spam (ten poté může být předmětem posouzení, odstranění, nebo i následného zpracování). Zvolené řešení je vhodné popsat ve spisovém a skartačním řádu. Pro použití konkrétního filtru a jeho nastavení je nutné se dobře seznámit s funkcemi daného filtru, případně konzultovat použití s dodavatelem.

9. *Doručené datové zprávy se ukládají do úložiště doručených datových zpráv ve tvaru, ve kterém byly přijaty, včetně všech příloh a případných jiných součástí*

Je-li k datové zprávě připojen kvalifikovaný certifikát a zaručený e-podpis založený na tomto certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále „uznávaný e-podpis") nebo kvalifikovaný systémový certifikát[51] a elektronická značka založená na tomto certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále „uznávaná e-značka"), ukládají se spolu se zprávou.

Používá-li úřad pro stažení pošty z poštovního serveru např. poštovní klient MS Outlook Office, je třeba pro uložení datové zprávy použít formát, který zachovává všechny vlastnosti dané zprávy. V tomto případě se jedná o formát .msg. Při použití ostatních e-mailových klientů je možno zprávu uložit ve formátu .eml.

[51] Zjednodušeně: kvalifikovaný certifikát je vydáván pro fyzickou osobu, která se bude jménem úřadu podepisovat. Kvalifikovaný systémový certifikát se vydává pro úřad. Je obdobou razítka úřadu.

Pokud je k datové zprávě připojen jiný druh e-podpisu nebo certifikátu, je vhodné je také uložit spolu se zprávou (jsou její součástí), i když není nutné s nimi dále pracovat a ověřovat jejich platnost.

Pro zajištění bezpečnosti úložiště a datových zpráv, které jsou v něm uloženy, je nutné aby:

1) byla data zálohována a zabezpečena proti ztrátě a neoprávněnému pozměnění, a
2) byli určeni pracovníci, kteří mají do úložiště přístup a odpovídají za ně.

### *10. Datové zprávy se v e-podatelně evidují a opatřují identifikátorem e-podatelny*

Doručené datové zprávy se v e-podatelně evidují v souladu se spisovým a skartačním řádem úřadu. Kromě obvyklých náležitostí takové evidence se zaznamenává přesný čas doručení, a to s přesností na sekundu. Tento údaj má zásadní význam při ověřování platnosti uznávaného kvalifikovaného certifikátu.[52]

Evidence může být jak v elektronické (v praxi častější, jelikož ji lze nezpochybnitelným způsobem navázat na elektronickou poštu), tak i v listinné podobě, pokud je úřad schopen zajistit jednoznačný vztah mezi listinnými záznamy o elektronické poště a elektronickou poštou jako takovou (odkazem na číslo hlavičky datové zprávy, identifikací jejího odesilatele a přesného času doručení apod.).

Následně je datová zpráva opatřena identifikátorem e-podatelny, který je obdobou podacího razítka. Jeho účelem je zachytit informace o dané zprávě pro další řízení, a to zejména informace týkající se e-podpisu, případně časového razítka. Důležité je, aby identifikátor obsahoval výsledek ověření platnosti e-podpisu[53] a zmíněný čas doručení. Je žádoucí, aby zaznamenání uvedených informací proběhlo co nejdříve po doručení datové zprávy. Nezjistí-li úřad předmětné skutečnosti a nezaznamená je do identifikátoru, bude je následně velmi obtížně získávat, eventuálně dokazovat.

Forma identifikátoru není předepsána, ale je výhodné, pokud je v elektronické podobě. Úřady, které přijímají datové zprávy ojediněle, jej mohou pořizovat i v listinné formě v rámci jejich listinné evidence. V každém případě je nutné dbát na bezpečnost údajů, které jsou v identifikátoru uvedeny. Platí zde stejné zásady jako pro úložiště doručených zpráv.

### *11. Doručení datové zprávy e-podatelna potvrzuje odesílateli zasláním zprávy o doručení*

Učiní tak v případě, že je možné z doručené datové zprávy zjistit elektronickou adresu odesilatele. Potvrzení musí obsahovat:

1) datum a čas s uvedením hodiny, minuty a sekundy, kdy byla datová zpráva doručena (čas doručení včetně sekundy je uveden v hlavičce zprávy, většinou ji lze zobrazit v možnostech dané zprávy),

---

[52] V oblasti orgánů veřejné moci lze podle §11 zákona o elektronickém podpisu za účelem podpisu používat jen kvalifikované certifikáty vydané akreditovaným poskytovatelem certifikačních služeb.

[53] Podrobněji viz. Matejka, J., Chum, V., K právní úpravě elektronického podpisu, Bulletin Advokacie, 3/2002, s. 27-41, ISSN 1210-6348.

2) charakteristiku doručené datové zprávy umožňující její identifikaci (např. číslo jednací nebo jiný identifikační znak, hash, případně i plný text doručené zprávy).

Potvrzení by mělo být podepsáno uznávaným e-podpisem pracovníka e-podatelny nebo uznávanou e-značkou úřadu. Toto je důležité pro právní jistotu odesilatele. Prostředí Internetu nedává záruky za doručení, proto by mělo být doručení pokaždé potvrzeno. Je to obdoba potvrzení doručení listovního podání "klasické" podatelně, například ve formě razítka podatelny na kopii písemnosti.

V případě, že je takto reagováno na datovou zprávu, která byla doručena s uznávaným e-podpisem nebo uznávanou e-značkou, je toto podepsání/označení podle vyhlášky o elektronických podatelnách povinné.

*12. E-podatelna zjišťuje a zaznamenává náležitosti doručených datových zpráv, tedy především vlastnosti e-podpisu. Pro tento krok musí být obsluha e-podatelny proškolena*

Tato činnost je pro pracovníky e-podatelen poměrně nová a v řadě případů je dosud prováděna nesprávně nebo neúplně. Z tohoto důvodu je zde popsána detailně. Je třeba poznamenat, že následující řádky jsou určeny především poučeným laikům, projektantům softwaru pro e-podatelny nebo informatikům, kteří by měli nastavit software e-podatelny ke správnému fungování a proškolit obsluhu.

Zjišťuje se, zda datová zpráva odpovídá technickým parametrům, které úřad stanovil jako přípustné. Každá e-podatelna má určité programové vybavení, které ve větší nebo menší míře omezuje škálu datových zpráv, které je schopna zpracovávat. Je tedy důležité, aby každý úřad popsal, jaké technické náležitosti musí mít doručované písemnosti, a tuto informaci zveřejnil na svých webových stránkách nebo na jiném veřejném a navštěvovaném místě. Mezi tyto informace musí bezpochyby patřit formát datových zpráv, případně jejich velikost. Každý úřad vybavený ICT by jistě měl umět otevřít a pracovat se soubory ve formátu pdf, txt, html.

Dále se zjišťuje, zda je k datové zprávě připojen uznávaný e-podpis nebo uznávaná e-značka, případně zda je připojeno kvalifikované časové razítko. Uznávaná e-značka a kvalifikované časové razítko budou v současné době k datovým zprávám připojeny pouze výjimečně, protože novela zákona o elektronickém podpisu jejich užívání umožnila, ale žádný jiný právní předpis zatím nestanovil povinnost jejich užívání pro konkrétní typy podání. E-podpis bude stále běžnější součástí přijímaných datových zpráv. E-podatelna by za účelem práce s e-podpisem měla být vybavena aplikací, která dokáže pracovat s kryptografickými funkcemi operačního systému, uloženými v tzv. kryptografickém jádře OS, a která umí pracovat s formátem .p7s podle normy PKCS#7. Běžné kancelářské softwarové balíky, které v sobě mají poštovního klienta, tyto požadavky bez problémů splňují. V návodu k nim je možné nalézt i popis kroků vedoucích ke zjištění, zda je e-podpis k doručené zprávě připojen, či nikoliv.

Poté se musí také prověřit, zda je zaručený e-podpis platný a zda jeho kvalifikovaný certifikát nebyl zneplatněn nebo e-značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn, případně zda je platné kvalifikované časové razítko. Řada produktů, které jsou popsané dále v publikaci, umožňuje, aby ověření platnosti zaručeného e-podpisu nebo e-značky provedla aplikace sama a ohlásila, pokud podpis platný není.[54]

Pokud tedy pracovník e-podatelny zjistí, že:

1) aplikace (poštovní klient) ohlásila, že e-podpis je neplatný, protože došlo ke změně obsahu podepsaných dat, neboli k porušení integrity, nebo
2) certifikát, na jehož základě je e-podpis vytvořený, přestal být platný ještě před časem doručení datové zprávy, nebo
3) certifikát se nachází na seznamu zneplatněných certifikátů s časem zneplatnění, který předchází času doručení,

potom výsledkem ověření e-podpisu bude výrok, že e-podpis je neplatný a tuto skutečnost je nutné napsat do identifikátoru e-podatelny. I v tomto případě je nutné zaznamenat údaj o tom, zda certifikát podepisující osoby je kvalifikovaný a zda jej vydal akreditovaný poskytovatel certifikačních služeb. Tyto informace jsou uvedeny v certifikátu.

Důsledky neplatnosti e-podpisu dovodí příslušný úředník, který danou písemnost zpracovává. Nutné však je, aby se o této skutečnosti dozvěděl. Zdrojem informací jsou pro něj údaje zaznamenané v identifikátoru.

Pokud všechna uvedená ověření skončí dobře, tj. s kladným výsledkem, je možné považovat e-podpis za platný.[55] Jak už bylo uvedeno, čas, ke kterému se platnost certifikátu ověřuje, je čas doručení datové zprávy. Ojediněle může dojít k situaci, že e-podatelna zjistí, že kvalifikovaný certifikát byl v době doručení datové zprávy neplatný, ale lze usuzovat, že zaručený e-podpis byl vytvořen v době platnosti tohoto certifikátu. Například: v podepsané zprávě je uvedeno, že byla odeslána v 8:00 hodin (z toho usuzujeme, že podpis byl vytvořen před tímto časem), certifikát byl zneplatněn v 8:03 a ověřování probíhá 8:10 hodin. Úřad nemůže na takový certifikát spoléhat, protože nemá k dispozici věrohodný údaj, kdy byla skutečně zpráva podepsána (s časem odeslání lze lehce manipulovat, takže podpis mohl být vytvořen i v 8:05). V tomto případě by úřad mohl na certifikát spoléhat, pokud by bylo k datové zprávě připojeno platné kvalifikované časové razítko a toto razítko by bylo vytvořeno před okamžikem zneplatnění certifikátu datové zprávy (pro uvedený příklad dříve než v 8:03). Pokud by platné časové razítko k datové zprávě připojeno nebylo, úřad uvědomí podepsanou osobu, že nemá možnost provést veškeré úkony potřebné k tomu, aby ověřil, že zaručený e-podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn před vytvořením zaručeného e-podpisu. Se zprávou je tedy nutné nakládat tak, jako by podepsána nebyla.

V souhrnu si můžeme vyjmenovat, které údaje se do identifikátoru musí zaznamenávat:

1) datová zpráva odpovídá technickým parametrům – ANO x NE
2) je připojen uznávaný elektronický podpis – ANO x NE

[54] Viz. též Matejka, J., Odpovědnost za provoz nezabezpečené počítačové sítě, DATA SECURITY MANAGEMENT, 5/2002, s.22 - 24, ISSN 1211-8737.
[55] Viz. též Matejka, J., Úprava elektronického podpisu v právním řádu ČR, Právník, 5/2001, s.582 – 611, ISSN 0231-6625.

3) je připojena uznávaná elektronická značka – ANO x NE
4) je připojeno kvalifikované časové razítko – ANO x NE
5) zaručený elektronický podpis je platný – ANO x NE
6) elektronická značka je platná – ANO x NE
7) její kvalifikovaný systémový certifikát nebyl zneplatněn – ANO x NE
8) připojené kvalifikované časové razítko je platné – ANO x NE
9) je připojen kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát – ANO x NE
10) je uveden akreditovaný poskytovatel, který certifikát vydal a vede jeho evidenci – ANO x NE
11) obsahuje kvalifikovaný certifikát údaje, na jejichž základě je možné osobu, která podepsala datovou zprávu, jednoznačně identifikovat – ANO x NE
12) bylo odesláno potvrzení o doručení datové zprávy – ANO x NE
13) bylo odesláno sdělení, že úřad nemá možnost provést veškeré úkony potřebné k tomu, aby ověřil, že zaručený elektronický podpis nebo elektronická značka jsou platné a jejich kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nebyly zneplatněny před vytvořením zaručeného elektronického podpisu nebo elektronické značky – ANO x NE.

E-podatelna tyto skutečnosti zjistí a zapíše do identifikátoru, ale dále se jimi nezabývá. Pokud úřad nestanoví interním předpisem jinak, e-podatelna tedy nezjišťuje, zda datová zpráva měla být podle zvláštního právního předpisu podepsána uznávaným e-podpisem, zda mělo být připojeno kvalifikované časové razítko atd. Pouze uvedené skutečnosti konstatuje a předává je k řešení příslušným útvarům, které se vyřízením obsahu zprávy zabývají. Po splnění všech výše uvedených úkonů e-podatelna předává datovou zprávu příslušným útvarům úřadu k vyřízení.

Je na rozhodnutí úřadu, a tedy úpravě ve spisovém a skartačním řádu, zda je datová zpráva předána v elektronické podobě nebo vytištěna a předána v listinné podobě. V takovém případě musí být vytištěn a ke zprávě připojen i identifikátor e-podatelny, ve kterém jsou uvedeny všechny předepsané údaje. Údaje o času doručení, ověření e-podpisu a jiné údaje, které identifikátor obsahuje, totiž mohou mít pro další vyřizování zásadní význam. V každém případě musí být datová zpráva uložena v elektronické podobě ve tvaru, ve kterém byla přijata.

### *13. Datová zpráva, která je z úřadu odesílána, se v e-podatelně ukládá do úložiště vypravených datových zpráv ve tvaru, ve kterém byla odeslána*

Pokud je k datové zprávě připojen uznávaný e-podpis oprávněného zaměstnance úřadu a jeho kvalifikovaný certifikát nebo uznávaná e-značka úřadu a její kvalifikovaný systémový certifikát, ukládají se spolu se zprávou.[56] Podepsat datovou zprávu uznávaným e-podpisem může pouze zaměstnanec, který je k tomu oprávněn. Na rozdíl od podepisování potvrzení o doručení zprávy, které bude zpravidla podepisovat pracovník e-podatelny, se zde bude jednat o podpis pracovníka, který je oprávněn takto stvrdit určitý úkon úřadu . Pokud tak úřad stanoví, může být odesílaná zpráva včetně tohoto podpisu, „přepodepsána" jako celek

[56] Viz. též Matejka, J., K využití elektronického podpisu v pracovněprávních vztazích, Právo a zaměstnání, 5/2001, s.5 – 11, ISSN 1211-1139.

pracovníkem e-podatelny. Tím stvrdí, že zprávu z e-podatelny odeslal se všemi jejími součástmi.
Před odesláním z úřadu prochází datová zpráva kontrolou, zda neobsahuje škodlivý kód. Odesílaná datová zpráva se v e-podatelně eviduje v souladu s vnitřními předpisy úřadu, které upravují evidenci vypravovaných písemností. Čas odeslání zprávy je zaznamenán s přesností na sekundu.

### *14. Zveřejňování údajů*

Aby ti, kdo elektronickou poštu na úřady zasílají, měli k dispozici potřebné údaje, ukládá nařízení vlády, kterým se provádí zákon o elektronickém podpisu, úřadům povinnost příslušné údaje zveřejnit. Jedná se o tyto údaje:

a) elektronická adresa e-podatelny (e-mail, případně url) a informace o tom, zda je e-podatelna určena výhradně pro příjem datových zpráv určitého obsahu (např. daňová přiznání), nebo nikoliv,
b) kontaktní údaje pro přijímání datových zpráv na technických nosičích (adresa, úřední hodiny apod.),
c) případné další možnosti doručování datových zpráv (pokud existují), zejména prostřednictvím technického zařízení v sídle úřadu nebo v jeho organizačních jednotkách,
d) pravidla pro potvrzování doručení datových zpráv (např. max. doba, která může uplynout od přijetí zprávy do odeslání potvrzení) a vzor zprávy, kterou se doručení potvrzuje,
e) technické parametry:[57]
   - datových zpráv, pro jejichž přijetí má e-podatelna technické a programové vybavení (např. rtf, doc, pdf, jpg nebo html, dále se může jednat o komunikační protokoly); některé úřady preferují jimi zveřejněné elektronické formuláře (např. Automatizovaný daňový informační systém, žádosti o dávky státní sociální podpory) – nastavení se odvozuje od vybavení daného úřadu a od požadavků (např. bezpečnostních) na provoz ICT,
   - technických nosičů, na nichž lze předávat datové zprávy,
f) postup v případě, že u přijaté datové zprávy je zjištěn škodlivý software nebo chybný formát zprávy,
g) způsob, jakým jsou vyřizovány dotazy týkající se provozu e-podatelny, včetně kontaktních údajů (e-mailová adresa, telefon apod.),
h) aktuální seznam zaměstnanců, kterým byly vydány kvalifikované certifikáty,
i) seznam právních předpisů, podle kterých je možné vůči úřadu činit právní úkony v elektronické podobě a náležitosti těchto úkonů, zejména náležitosti týkající se použití uznávaného e-podpisu.

V této souvislosti je nutné zdůraznit, že úřad není oprávněn omezovat druhou stranu v úkonech, které hodlá činit elektronicky. Pokud tedy právní předpis stanoví, že určitý úkon vůči úřadu je možné činit elektronicky, úřad musí pro příjem takových datových zpráv vytvořit příslušné podmínky. Na druhé straně není úřadu bráněno v tom, aby umožnil příjem i jiných datových zpráv, například takových, jejichž náležitosti nejsou právními předpisy upraveny. Naopak v elektronické podobě nelze přijímat taková podání, u nichž právní předpis

[57] Srov. též. Štědroň, B., Open source best option for e-gov't, Czech Business Weekly, 24.7.2006, ISSN 1214-8415.

výslovně stanoví povinnost přijímat je pouze v klasické listinné podobě, nebo stanoví takové podmínky, že je nelze provést elektronicky (např. úředně ověřený podpis).

### *3.1.4. Pravidla pro tvorbu přístupných webových stránek orgánů justice (soudů)*

Tato kapitola obsahuje doporučení pro tvorbu WWW stránek ve veřejné správě[58] a stanoví podmínky pro zveřejňování informací dálkovým přístupem ve shodě s takzvanými pravidly WAI (Web Accessibility Initiative, Iniciativa pro bezbariérový přístup). Pravidla mají doporučující charakter, mají být vodítkem pro zadavatele webových stránek a inspirací pro jejich správce.[59]

Všichni uživatelé internetu nejsou stejní. Existují specifické skupiny uživatelů, které mají i specifické potřeby. V praxi to jsou většinou zrakově a sluchově postižení, případně uživatelé se sníženou hybností rukou nebo poruchami soustředění. Tito uživatelé využívají pomocné technologie, například hlasové výstupy a braillské řádky, které informace z WWW stránek zprostředkovávají. Aby tyto pomůcky fungovaly, je třeba, aby webová stránka splňovala kritéria přístupného webu. Správně přístupný web navíc neslouží pouze zdravotně postiženým, ale i lidem využívajícím méně obvyklá zobrazovací zařízení, operační systémy nebo softwarové vybavení.

V prostředí veřejné správy není možné, aby byl kdokoli v přístupu k informacím diskriminován. Respekt k pravidlům přístupného webu navíc nepředstavuje žádné dodatečné finanční náklady. Stačí znát základní pravidla pro tvorbu WWW stránek a řídit se jimi.

*Obsah webových stránek je dostupný a čitelný*

1. Každý netextový prvek nesoucí významové sdělení má svou textovou alternativu.
2. Informace sdělované prostřednictvím skriptů, objektů, appletů, kaskádových stylů, obrázků a jiných doplňků na straně uživatele jsou dostupné i bez kteréhokoli z těchto doplňků.
3. Informace sdělované barvou jsou dostupné i bez barevného rozlišení.
4. Barvy popředí a pozadí jsou dostatečně kontrastní. Na pozadí není vzorek, který snižuje čitelnost.
5. Předpisy určující velikost písma nepoužívají absolutní jednotky.
6. Předpisy určující typ písma obsahují obecnou rodinu písem.

*Práci s webovou stránkou řídí uživatel*

7. Obsah WWW stránky se mění, jen když uživatel aktivuje nějaký prvek.

---

[58] Vychází z Best practice - Pravidla pro tvorbu přístupného webu, MIČR, 2006. Best practice – Pravidla pro tvorbu přístupného webu připravila pracovní skupina složená ze zástupců Metodického centra informatiky, Sjednocené organizace nevidomých a slabozrakých (SONS), odborných konzultantů a pracovníků Ministerstva informatiky.

[59] Pravidla pro tvorby přístupného webu se neustále aktualizují. Aktuální podrobná verze pravidel je k dispozici na internetových stránkách www.pravidla-pristupnosti.cz. K přepracovávání pravidel došlo v rámci výzkumného úkolu projektu vědy a výzkumu vypsaném v roce 2006 Ministerstvem informatiky.

8. Webová stránka bez přímého příkazu uživatele nemanipuluje uživatelským prostředím.
9. Nová okna se otevírají jen v odůvodněných případech a uživatel je na to předem upozorněn.
10. Na webové stránce nic nebliká rychleji než jednou za sekundu.
11. Webová stránka nebrání uživateli posouvat obsahem rámů.
12. Obsah ani kód webové stránky nepředpokládá ani nevyžaduje konkrétní způsob použití ani konkrétní výstupní či ovládací zařízení.

*Informace jsou srozumitelné a přehledné*

13. Webové stránky sdělují informace jednoduchým jazykem a srozumitelnou formou.
14. Úvodní webová stránka jasně popisuje smysl a účel webu. Název webu či jeho provozovatele je zřetelný.
15. Webová stránka i jednotlivé prvky textového obsahu uvádějí své hlavní sdělení na svém začátku.
16. Rozsáhlé obsahové bloky jsou rozděleny do menších, výstižně nadepsaných celků.
17. Informace zveřejňované na základě zákona jsou dostupné jako textový obsah webové stránky.
18. Na samostatné webové stránce je uveden kontakt na technického správce a prohlášení jasně vymezující míru přístupnosti webu a jeho částí. Na tuto webovou stránku odkazuje každá stránka webu.

*Ovládání webu je jasné a pochopitelné*

19. Každá webová stránka má smysluplný název, vystihující její obsah.
20. Navigační a obsahové informace jsou na webové stránce zřetelně odděleny.
21. Navigace je srozumitelná a je konzistentní na všech webových stránkách.
22. Každá webová stránka (kromě úvodní webové stránky) obsahuje odkaz na vyšší úroveň v hierarchii webu a odkaz na úvodní WWW stránku.
23. Všechny webové stránky rozsáhlejšího webu obsahují odkaz na přehlednou mapu webu.
24. Obsah ani kód webové stránky nepředpokládá, že uživatel již navštívil jinou stránku.
25. Každý formulářový prvek má přiřazen výstižný nadpis.
26. Každý rám má vhodné jméno či popis vyjadřující jeho smysl a funkčnost.

*Odkazy jsou zřetelné a návodné*

27. Označení každého odkazu výstižně popisuje jeho cíl i bez okolního kontextu.
28. Stejně označené odkazy mají stejný cíl.
29. Odkazy jsou odlišeny od ostatního textu, a to nikoli pouze barvou.
30. Obrázková mapa na straně serveru je použita jen v případě, že nebylo možné pomocí dostupného geometrického tvaru definovat oblasti v obrázkové mapě. V ostatních případech je použita obrázková mapa na straně uživatele. Obrázková mapa na straně serveru je vždy doprovázena alternativními textovými odkazy.
31. Uživatel je předem jasně upozorněn, když odkaz vede na obsah jiného typu, než je webová stránka. Takový odkaz je doplněn sdělením o typu a velikosti cílového souboru.

*Kód je technicky způsobilý a strukturovaný*

32. Kód webových stránek odpovídá nějaké zveřejněné finální specifikaci jazyka HTML či XHTML. Neobsahuje syntaktické chyby, které je správce webových stránek schopen odstranit.
33. V metaznačkách je uvedena použitá znaková sada dokumentu.
34. Prvky tvořící nadpisy a seznamy jsou korektně vyznačeny ve zdrojovém kódu. Prvky, které netvoří nadpisy či seznamy, naopak ve zdrojovém kódu takto vyznačeny nejsou.
35. Pro popis vzhledu webové stránky jsou upřednostněny stylové předpisy.
36. Je-li tabulka použita pro rozvržení obsahu webové stránky, neobsahuje záhlaví řádků ani sloupců. Všechny tabulky zobrazující tabulková data naopak záhlaví řádků a/nebo sloupců obsahují.
37. Všechny tabulky dávají smysl čtené po řádcích zleva doprava.

### *3.1.5. Elektronické podání - žaloba (nález ÚS)*

Dne 24. 4. 2006 vydal Ústavní soud pro elektronickou komunikaci se soudy významný nález sp. zn. IV. ÚS 319/05, v němž výkladem § 42 odst. 1 a 3 OSŘ překlenul pochybení zákonodárce, kterého se dopustil při novelizaci občanského soudního řádu.[60] Ústavní soud tak podpořil přímý přístup k soudům prostřednictvím elektronických podání.[61] V předmětném nálezu Ústavní soud dovodil:

*„Povinnost stěžovatele uvedená v ustanovení § 42 odst. 3 občanského soudního řádu, tedy písemně doplnit své elektronické podání do tří dnů, se nevztahuje na podání v elektronické podobě, jestliže je k němu připojen uznávaný elektronický podpis dle § 11 odst. 1 zákona č. 227/2000 Sb., o elektronickém podpisu a změně některých dalších zákonů."*

Právní zástupce stěžovatelů v předmětném sporu zaslal dne 3.6.2005 Ústavnímu soudu podání označené jako ústavní stížnost v elektronické podobě se zaručeným elektronickým podpisem prostřednictvím akreditovaného poskytovatele certifikačních služeb.[62] Toto písemné podání právní zástupce stěžovatelů ve lhůtě tří dnů písemně nedoplnil. Ústavní soud byl tedy postaven před otázku, zda podání má procesní účinky, a je návrhem na zahájení řízení. Návrh na zahájení řízení se podává písemně Ústavnímu soudu (ustanovení § 34 odst. 1 věta prvá zákona o Ústavním soudu ). Ústavní soud odloží podání, která nejsou návrhy na zahájení řízení [ustanovení § 41 písm. a) zákona o Ústavním soudu ]. Ústavní soud v dosavadní praxi vykládal písemnou formu extenzivně za přiměřeného použití ustanovení § 42 odst. 3 občanského soudního řádu, a byla tak akceptována i podání telegrafem, pokud byla písemně doplněna nejpozději do tří dnů, i podání telefaxem, pokud byl ve stejné lhůtě předložen originál, případně písemné podání shodného znění. Vzhledem k tomu, že úprava podání v elektronické podobě není v zákoně o Ústavním soudu obsažena, je i tady nutno přiměřeně použít úpravu obsaženou v občanském soudním řádu (ustanovení § 63 zákona o Ústavním soudu ). Ustanovení § 42 odst. 1 věta prvá občanského soudního řádu zní : *„Podání je možno učinit písemně, ústně do protokolu, v elektronické podobě, telegraficky nebo telefaxem."*

Ustanovení § 42 odst. 3 občanského soudního řádu zní: *„Podání obsahující návrh ve věci samé učiněné telegraficky je třeba písemně doplnit nejpozději do tří dnů, je-li písemné podání*

---

[60] Podrobněji viz Černý, P., Procesní účinky elektronického podání v občanském soudním řízení, Právní rozhledy 12/2006, C.H.Beck, ISSN 1210-6410.
[61] Podrobněji např. viz „Elektronické žaloby – už žádné výmluvy ", www.ejustice.cz.
[62] Dále citováno z předmětného nálezu sp. zn. IV. ÚS 319/05.

*učiněno telefaxem nebo v elektronické podobě, je třeba v téže lhůtě jej doplnit předložením jeho originálu, případně písemným podáním shodného znění. K těmto podáním, pokud nebyla ve stanovené lhůtě doplněna, soud nepřihlíží. Stanoví-li to předseda senátu, je účastník povinen soudu předložit originál (písemné podání shodného znění) i jiných podání učiněných telefaxem.*"

Za použití pouze jazykového výkladu shora uvedených ustanovení občanského soudního řádu by Ústavní soud nemohl k elektronickému podání stěžovatelů přihlížet a muselo by být odloženo. Ústavní soud byl však přesvědčen, že za použití dalších metod výkladu právních norem lze dojít k závěru, že povinnost stěžovatele uvedená v ustanovení § 42 odst. 3 občanského soudního řádu, tedy písemně doplnit své elektronické podání do tří dnů, se nevztahuje na podání v elektronické podobě, jestliže je k němu připojen uznávaný elektronický podpis dle ustanovení § 11 odst. 1 zákona č. 227/2000 Sb., o elektronickém podpisu a změně některých dalších zákonů (dále jen „zákon o elektronickém podpisu" nebo ZEP).

První metodou výkladu, kterou Ústavní soud použil, byl výklad historicko-teleologický. Historicko-teleologickým výkladem je zjišťován účel, k němuž měla právní úprava sloužit v době svého přijetí. Směřuje tedy ke zjištění skutečného úmyslu, který zákonodárce měl při přijetí právního předpisu. Záměr zákonodárce lze nalézt v důvodových zprávách, neboť pokud není prokázán opak, je třeba mít za to, že zákonodárce přijal se samotným předpisem i jeho záměr.

Zákon o elektronickém podpisu deklaroval, že jeho účelem je (dle ustanovení § 1) upravit v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. Relevantní právní úpravou Evropských společenství je směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (Úřední list ES z 19.1.2000, L 13/12). Cílem této směrnice je odstranit překážky pro elektronickou komunikaci a elektronický právní styk, které vyplývají z různých pravidel o právním uznání elektronických podpisů a o akreditaci tzv. ověřovací služby v členských státech. V čl. 5 směrnice o zásadách Společenství pro elektronické podpisy jsou členské státy zavázány, aby tzv. zaručené elektronické podpisy založené na kvalifikovaných osvědčeních a vytvořené pomocí prostředků pro bezpečné vytváření podpisu byly po právní stránce spojeny se stejnými právními následky jako vlastnoruční podpisy, které jsou na papírovém podkladu. Smyslem a účelem této směrnice je tedy ulehčení použitelnosti elektronického podpisu a docílení jeho rovnocenného postavení s podpisem vlastnoručním. V důvodové zprávě k zákonu o elektronickém podpisu (III. volební období Poslanecké sněmovny, 1999, tisk 415/0) je v oddíle věnovanému odůvodnění hlavních principů návrhu zákona uvedeno, že hlavním principem navrhovaného zákona je zajistit, že datové zprávy nesmí být diskriminovány, tj. že nesmí existovat rozpor v zacházení mezi datovými zprávami a dokumenty na papíře. Důvodová zpráva k ustanovení § 2 zákona o elektronickém podpisu uvádí, že zaručený elektronický podpis jako jeden z druhů elektronického podpisu představuje ekvivalent „ověřeného podpisu" na papíru a využívá takových technologických postupů, které umožňují jednoznačnou identifikaci a autentizaci osoby, která podpis vytvořila.[63] K ustanovení § 3 je dále uvedeno, že zaručený elektronický podpis zaručuje, že datovou zprávu podepsala oprávněná osoba. Zaručené elektronické

[63] Srov. též Matejka, J., **Krádež elektronického podpisu, aneb s čím tvůrci zákona (ne)počítali**, Server ROOT.cz, rubrika Bezpečnost, 17.10.2000.

podpisy podložené osvědčením vydaným ověřovatelem informací (poskytovatelem certifikačních služeb) budou uznány jako vlastnoruční podpis v případech, kdy takový vlastnoruční podpis požadují právní předpisy nebo dohoda stran.[64]

Historický vývoj ustanovení upravujících podání v elektronické podobě v § 42 občanského soudního řádu byl následující. Zákonem o elektronickém podpisu bylo ustanovení § 42 odst. 1 věta první občanského soudního řádu novelizováno (s účinností k 1.10.2000) tak, že: „*Podání je možno učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky nebo telefaxem.*" Dle procesualistické teorie mělo podání v elektronické podobě procesní účinky jen tehdy, jestliže bylo také elektronicky podepsáno způsobem stanoveným v zákoně o elektronickém podpisu. Neobsahovalo-li podání také náležitý elektronický podpis, soud k němu nepřihlížel.[65] Vzhledem k tomu, že zákon o elektronickém podpisu nenovelizoval i ustanovení § 42 odst. 3 občanského soudního řádu, nebylo možné podat soudu podání v jiné elektronické podobě než se zaručeným elektronickým podpisem.

Zákonem č. 226/2002 Sb., kterým byly novelizovány procesní předpisy v souvislosti s elektronickým doručováním, byla v ustanovení § 42 odst. 1 občanského soudního řádu zrušena slova „podepsané elektronicky podle zvláštních předpisů" a do ustanovení § 42 odst. 3 občanského soudního řádu byla za slova „učiněno telefaxem" vložena slova „nebo v elektronické podobě", přičemž tato úprava trvá od účinnosti zákona (1.7.2002) dodnes.[66] Tím byla připuštěna elektronická podání i bez připojeného zaručeného elektronického podpisu, avšak za podmínky, že budou písemně doplněna nejpozději do tří dnů. Novelizace procesních předpisů zavedená zákonem č. 226/2002 Sb. měla dle důvodové zprávy k tomuto zákonu (III. volební období Poslanecké sněmovny, 2002, tisk 1225) sledovat promítnutí koncepce elektronického způsobu komunikace zakotvené v zákonu o elektronickém podpisu a mělo dojít k dalšímu zpřesnění v předmětné oblasti.

Je tedy zřejmé, že úmyslem zákonodárce při přijetí novely č. 226/2002 Sb. nebylo negovat použití elektronického podpisu jako institutu rovnocenného písemnému vlastnoručnímu podpisu, ale pouze rozšířit komunikaci se soudní mocí na možnost učinit podání v elektronické podobě i bez zaručeného elektronického podpisu.

Objektivně-teleologickým výkladem, jehož úlohou je vystihnout smysl a účel právní normy v souvislosti s potřebami společnosti v aktuální situaci, v níž se má norma realizovat, nutno dojít k závěru, že původní účel této právní normy je i nadále zachován. Jejím cílem je i v současnosti usnadnit doručování podání prostřednictvím elektronické komunikace tak, aby byla v co největší míře zajištěna rovnost elektronických podání s podáními v písemné podobě na papíře. Z toho lze vyvodit, že výklad ustanovení § 42 odst. 1 věta prvá o.s.ř. po novele provedené zákonem o elektronickém podpisu č. 227/2000 Sb. je i nadále zachovatelný a podání v elektronické podobě splňující výše uvedené požadavky zákona o elektronickém podpisu je podáním rovnocenným s podáním v písemné podobě na papíře s vlastnoručním podpisem, zatímco elektronicky učiněné podání bez zaručeného elektronického podpisu je nutné do 3 dnů doplnit.

---

[64] Viz. též Matejka, J., Chum, V., K právní úpravě elektronického podpisu, Bulletin Advokacie, 3/2002, s. 27-41, ISSN 1210-6348.

[65] Bureš, J., Drápal, L., Mazanec, M., Občanský soudní řád. Komentář. 5. vydání. Praha: C. H. Beck, 2001, str. 152.

[66] Viz. též Matejka, J., K novele zákona o elektronickém podpisu, Právní zpravodaj, 12/2002.

K tomuto závěru přispívá i systematický výklad v rámci dalších procesních předpisů, neboť normu nelze vykládat izolovaně, ale též v souvislostech celého právního řádu. Dle ustanovení § 37 odst. 2 zákona č. 150/2002 Sb. , soudního řádu správního, ve znění účinném k 3.6.2005, lze podání obsahující úkon, jímž se disponuje řízením nebo jeho předmětem, provést písemně, ústně do protokolu, popřípadě v elektronické formě podepsané elektronicky podle zvláštního zákona. Podání je možno učinit i v elektronické podobě bez elektronického podpisu, musí být však do tří dnů potvrzeno písemným podáním shodného obsahu.

Rovněž podle zákona č. 141/1961 Sb., trestního řádu, ve znění účinném k 3.6.2005, je možné učinit podání v elektronické podobě. Dle ustanovení § 59 odst. 2 trestního řádu ten, kdo činí podání v elektronické podobě podle zvláštního právního předpisu, uvede současně poskytovatele certifikačních služeb, který jeho certifikát vydal a vede jeho evidenci, nebo certifikát připojí k podání. Podání splňující tyto požadavky není nutné dále doplňovat.

Zákon č. 500/2004 Sb., správní řád, ve znění platném k 3.6.2005 a účinném od 1.1.2006, umožňuje v ustanovení § 37 odst. 4 učinit podání písemně nebo ústně do protokolu anebo v elektronické podobě podepsané zaručeným elektronickým podpisem. Podání v elektronické podobě bez zaručeného elektronického podpisu je třeba doplnit do 5 dnů.

Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění účinném k 3.6.2005, v ustanovení § 21 odst. 4 umožňuje učinit podání v elektronické podobě podle zvláštního předpisu, současně musí být uveden poskytovatel certifikačních služeb, který certifikát vydal a vede příslušnou evidenci, nebo je povinen certifikát připojit k podání. Podání v elektronické podobě nesplňující tyto požadavky musí být do tří dnů po odeslání opakováno písemně nebo ústně do protokolu (ustanovení § 21 odst. 5 zákona o správě daní a poplatků).

I systematický výklad relevantních ustanovení dalších procesních předpisů tedy ukazuje, že elektronické podání s připojeným elektronickým podpisem splňujícím specifické požadavky uvedené v zákoně o elektronickém podpisu má procesní účinky bez dalšího.

Zákon o elektronickém podpisu obsahuje několik druhů elektronického podpisu, a to kromě „běžného" elektronického podpisu (ustanovení § 2 písm. a)) i několik variant zaručeného elektronického podpisu. Ústavní soud byl postaven před otázku, který z druhů zaručeného elektronického podpisu je způsobilým vyvolat procesní účinky bez písemného doplnění podání. Dle názoru Ústavního soudu jím je „uznávaný elektronický podpis" dle ustanovení § 11 zákona o elektronickém podpisu.[67] Ten totiž zajišťuje dostatečnou jistotu, že podání vytvořila osoba, která je pod ním podepsána, a zákonodárce jeho užití v obdobných případech předpokládá. V ustanovení § 11 odst. 1 věta prvá zákona o elektronickém podpisu je uvedeno, že v oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen „uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná.

Nejvyšší verifikační hodnotu ze zaručených elektronických podpisů má tedy právě uznávaný elektronický podpis. Zatímco u vlastnoručního podpisu se vychází především z toho, že je výsledkem individuálního a relativně stálého písemného projevu člověka, u zaručeného

[67] Srov. též Matejka, J., Expertiza k § 11 zákona o elektronickém podpisu (žadatel: Úřad pro ochranu osobních údajů), Ústavu státu a práva Akademie věd České republiky.

elektronického podpisu jde pouze o schopnost provést nějaký úkon, který je vázán na dostupnost prostředku pro vytvoření takového podpisu. Zatímco v případě vlastnoručních podpisů je možno znalecky dokazovat skutečnost, že určitý podpis náleží určité osobě, v případě zaručeného elektronického podpisu toto možné není. Znalec zde potvrzuje pouze skutečnost, že datová zpráva byla podepsána prostřednictvím konkrétních prostředků, a nikoli skutečnost, že ji podepsala určitá konkrétní osoba. Z těchto důvodů je třeba klást na podání prostřednictvím veřejné datové sítě zvýšené požadavky, jak je to ostatně reflektováno i ve shora uvedeném ustanovení § 11 zákona o elektronickém podpisu.

Ústavní soud tak ve výše uvedeném nálezu poskytl soudům podporu pro jejich postup spočívající v přijímání elektronických podání podepsaných zaručeným elektronickým podpisem a dal jim jasný signál, kterou z variant zaručeného elektronického podpisu považuje za nejvhodnější.[68] Je ale dále nutno upozornit na skutečnost, že potenciální přijímání jiných elektronických podání než s připojeným uznávaným elektronickým podpisem nezaručuje dostatečnou verifikaci osoby (ověření totožnosti osoby) činící podání a je třeba před takovýmto postupem varovat.[69]

## 3.2. Dokazování

### *3.2.1. Úvod*

Rozhodnutí soudu v konkrétní sporné věci (sporu), k němuž činnost soudu směřuje, musí být přirozeně racionálně opřeno o určité vědomosti, resp. poznatky soudu. Účelem dokazování v rámci procesu je proto dobrat se pokud možno pravdivých poznatků o rozhodujících skutečnostech, jejichž poznání poslouží soudu jako podklad pro spravedlivé, správné a zákonné rozhodnutí.[70] Pro míru dokazování objektivní pravdy ale neexistuje žádné měřítko a proto platí, že pravdivými jsou ty poznatky o skutečnostech, o jejichž pravdivosti je soudce (soud) subjektivně přesvědčen.[71] Platí tedy obecná zákonná zásada, že důkazy hodnotí soud podle své úvahy, a to každý důkaz jednotlivě a všechny důkazy v jejich vzájemné souvislosti. Zároveň soud pečlivě přihlíží ke všemu, co vyšlo za řízení najevo, včetně toho, co uvedli účastníci.[72]

Ohledně důkazní povinnosti platí tyto zákonné zásady:[73]

- účastníci jsou povinni označit důkazy k prokázání svých tvrzení a soud rozhoduje, které z navrhovaných důkazů provede,
- ve věcech, v nichž lze zahájit řízení i bez návrhu, jakož i v řízení o povolení uzavřít manželství, v řízení o určení a popření rodičovství, v řízení o určení, zda je třeba souhlasu rodičů dítěte k jeho osvojení, v řízení o osvojení, v řízení o jmenování

[68] Viz. Černý, P., Procesní účinky elektronického podání v občanském soudním řízení, Právní rozhledy 12/2006, C.H.Beck, ISSN 1210-6410.
[69] Viz. Černý, P., Procesní účinky elektronického podání v občanském soudním řízení, Právní rozhledy 12/2006, C.H.Beck, ISSN 1210-6410.
[70] Viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 238 an.
[71] Viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 239 an.
[72] §132 OSŘ.
[73] § 120 a §121 OSŘ.

rozhodce nebo předsedajícího rozhodce, v řízení o přivolení k výpovědi z nájmu bytu, v řízení o zákonnosti zajištění cizince a o jeho propuštění a v řízení o některých otázkách obchodních společností, družstev a jiných právnických osob je soud povinen provést i jiné důkazy potřebné ke zjištění skutkového stavu, než byly účastníky navrhovány,
- soud může též vzít za svá skutková zjištění shodná tvrzení účastníků.
- není třeba dokazovat skutečnosti obecně známé nebo známé soudu z jeho činnosti, jakož i právní předpisy uveřejněné nebo oznámené ve Sbírce zákonů České republiky.

Ohledně provádění důkazů platí dále zákonné zásady:[74]

- dokazování provádí soud při jednání,
- je-li to účelné, může být o provedení důkazu dožádán jiný soud nebo předseda senátu může důkaz z pověření senátu provést mimo jednání. Účastníci mají právo být přítomni u takto prováděného dokazování. Jeho výsledky je třeba vždy při jednání sdělit,
- senát může vždy rozhodnout, aby provedené důkazy byly doplněny nebo před ním opakovány,
- účastníci mají právo vyjádřit se k návrhům na důkazy a ke všem důkazům, které byly provedeny,
- dokazování je třeba provádět tak, aby byla šetřena povinnost zachovávat mlčenlivost o utajovaných informacích chráněných zvláštním zákonem a jiná zákonem stanovená nebo státem uznávaná povinnost mlčenlivosti.

Za důkaz (důkazní prostředek) mohou sloužit všechny prostředky, jimiž lze zjistit stav věci, zejména výslech svědků, znalecký posudek, zprávy a vyjádření orgánů, fyzických a právnických osob, notářské nebo exekutorské zápisy a jiné listiny, ohledání a výslech účastníků.[75] Pokud není způsob provedení důkazu předepsán, určí jej soud.[76] Závisí-li rozhodnutí na posouzení skutečností, k nimž je třeba odborných znalostí, ustanoví soud po slyšení účastníků znalce. Soud znalce vyslechne; znalci může také uložit, aby posudek vypracoval písemně. Je-li ustanoveno několik znalců, mohou podat společný posudek. Místo výslechu znalce může se soud v odůvodněných případech spokojit s písemným posudkem znalce.

### *3.2.2. Použití elektronických dokumentů (např. e-mailu) jako důkazního materiálu*

Email nebo jakýkoliv jiný elektronický dokument je plnohodnotný důkazní prostředek, který, pokud je v důkazním řízení navržen, může soud jako důkaz provést a nemá a priory nižší důkazní hodnotu než písemný dokument. Vlastní hodnocení důkazu provádí, jak již bylo uvedeno, soud na základě zásady volného hodnocení důkazů. V každém konkrétním případě soud tedy věrohodnost, průkaznost, správnost či úplnost emailové zprávy nebo listiny musí zkoumat zvlášť, aniž by mohl být některý důkazní prostředek již ze své povahy upřednostňován.

---

[74] §122 an. OSŘ.
[75] Srov. též Matejka, J., KDYŽ PÍŠEŠ, PODEPIŠ – současné možnosti využití elektronického podpisu, e-biz, 11/2002, s.55, ISSN 1213-063X.
[76] §125 OSŘ.

Občanský zákoník písemnou formu pozitivně nedefinuje, avšak v § 40 odst. 4 uvádí, že *písemná forma je zachována v případě, kdy je právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, které umožňují zachycení obsahu právního úkonu a určení osoby, která ho učinila.* Aby bylo tedy email nebo jiný elektronický dokument možno považovat za písemně učiněný úkon je tedy třeba naplnit následující záměry uvedeného ustanovení:

a) vyjádření obsahu právního úkonu / informační povinnosti – datová zpráva (email) musí být vyjádřen ve formě, ze které je patrný smysl a obsah předávaného sdělení, tedy typicky standardní text, vyjádřený v českém jazyce a to technickým formátem zprávy, která je pro příjemce zprávy přístupná a dostupná;

b) uchování obsahu právního úkonu / informační povinnosti – datová zpráva musí být zachycena na nosiči, které může vzhledem k obvyklým okolnostem zajistit jeho zachycení po přiměřenou dobu. Tuto podmínku by nemusela splňovat datová zpráva zaslaná klientovi prostřednictvím portálu, který neumožní příjem a uložení dat na koncovém počítači klienta;

c) určení osoby, která právní úkon činí.

Splnění prvních dvou podmínek v případě emailu (elektronické pošty), tedy vyjádření a zachycení obsahu, by v praxi nemělo být výrazně problematické, a proto se teď zaměříme především na splnění poslední podmínky, tedy na určení osoby, která email poslala, resp. učinila tento právní úkon. To může v praxi představovat již jisté komplikace, protože není problém si založit emailovou schránku zdarma a představovat se libovolným jménem. Takových emailových schránek navíc mohu mít v zásadě neomezený počet. K řešení daného problému - určení osoby, která učinila právní úkon (poslala email), poslouží v praxi elektronický podpis, resp. zaručený elektronický podpis.[77]

Stejně je také důležité upozornit na skutečnost, že zákon č. 227/2000 Sb., o elektronickém podpisu stejně tak jako Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy byly přijaty právě proto, aby elektronické komunikaci, tedy např. právě emailu, byla dána stejná váha jako komunikaci písemné. Jinými slovy, aby nedocházelo k neodůvodnitelné diskriminaci na úkor elektronické komunikace. Právě proto i z hlediska teleologického (smyslu zákona) by celá nová legislativa v rámci informační společnosti (zákon o elektronickém podpisu atd.) neměla smyslu, pokud by elektronické komunikační prostředky měly mít i nadále nižší průkazní váhu a obecně nesplňovali požadavek písemné formy.

Další problém, který může nastat v případě použití elektronických dokumentů a elektronicky podepsaných dokumentů bude prokazování platnosti takto podepsaného dokumentu s určitým časovým odstupem, tj. i v případě, kdy např. platnost certifikátu (zjednodušeně řečeno platnost elektronického podpisu) již vypršela. Řešením bude např. využití tzv. „důvěryhodné

[77] Okrajově lze také upozornit na skutečnost, že i Evropský soudní dvůr, jehož rozhodnutí mají precedenční povahu a jsou nadřízena rozhodnutím soudů členských států Evropské unie, v jednom ze svých rozhodnutí č. C-170/00 judikoval, že elektronická komunikace splňuje požadavek písemné formy.

archivy elektronických dokumentů" (TAA - Trusted Archiving Autority),[78] které zajišťuji integritu uložených dokumentů a poskytují důkazy o jejich autenticitě jak vůči uživateli, tak vůči třetím osobám. Takový archiv např. dlouhodobě „ošetřuje" elektronické podpisy dokumentů a garantuje platnost podepsaných dokumentů po celou dobu archivace, o čemž při jejich vydaní archiv poskytuje také nezpochybnitelné důkazy. Dlouhodobě také zabezpečuje obnovu platnosti časových razítek.

### 3.2.3. *Prokázání doručení elektronické (datové) zprávy*

V českém právním řadu existuji více než tři desítky odlišných právních úprav základních procesních úkonů, jako jsou podáváni, doručovaní, předvoláváni apod.[79] Na rozdíl od doporučené pošty, která poskytuje velkou míru jistoty, že tvrzení o odeslání zprávy bude prokázáno předložením příslušného potvrzení, běžná poštovní přeprava, stejně tak jako elektronická pošta (ať běžná, tak vybavena elektronickým podpisem) standardně neumožňuje jednoduché prokázání doručení zprávy.

Skutečnost, že zpráva byla odeslána nebo doručena by bylo nutné prokazovat podpůrnými technickými prostředky, popř. si vyžádat stanovisko znalce z příslušného oboru.

Obdobně potvrzení o doručení lze u písemné zásilky získat jen u doporučené zásilky, zatímco u emailu lze kromě obvyklého potvrzení (přímo z emailového software, případně i jinak z mail serverů), získat i tzv. kvalifikované časové razítko,[80] tj. důkaz o existenci toho určitého emailu v určitém časovém okamžiku.

Z důvodu průkaznosti elektronické pošty, zejména ve vztahu k otázce doručení, se proto doporučuje dodržovat následující pravidla:

a) provádět pravidelné zálohování veškeré příchozí a odchozí emailové komunikace na médiu neumožňujícím modifikaci či smazání s použitím tzv. časového razítka;

b) u důležitých zpráv (nabídky, vyžádané informace) vyžadovat potvrzení, zda elektronická zpráva byla klientovi doručena (email bude obsahovat ustanovením např.: *„Prosíme potvrďte obratem, že jste tuto zprávu společně se všemi přílohami obdržel."*);[81]

c) složitější sdělení (např. texty obsahující tabulky, číselná porovnání apod.) budou

---

[78] Důvěryhodný archiv elektronických dokumentů svým uživatelům zaručuje, že se předaný dokument nezmění, neztratí a případně nedostane do nepovolaných rukou. Důvěryhodný archiv tak zajišťuje integritu uložených dokumentů, čas archivace a důkaz o jejich autenticitě jak vůči uživateli, tak vůči orgánům státní správy. Dlouhodobě také zabezpečuje obnovu platnosti elektronického podpisu a časových razítek.

[79] Např. občansky soudní řád (zakon č. 99/1963 Sb.), soudní řád správní (zákon č. 150/2002 Sb.), trestní řád (zákon č. 141/1961 Sb.), správní řád (zákon č. 500/2004 Sb.), zákon o správě daní a poplatků (zákon č. 337/1992 Sb.) apod.

[80] §2 písm. r) zákona 227/2000 Sb., o elektronickém podpisu, v platném znění *„... datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem."*

[81] Problematiku určení okamžiku doručení datové zprávy řeší ve vztahu k veřejné správě vyhláška č.496/2004 Sb., o elektronických podatelnách - datová zpráva je považována za doručenou orgánu veřejné moci v okamžiku, kdy je dostupná elektronické podatelně provozované podle zvláštního právního předpisu.

zasílána v příloze ve formátu spolehlivěji zaručujícím přesné zachování obsahu (např. PDF);

d) upravení emailové komunikace v smluvním vztahu s klientem, např. ustanovení *„Smluvní strany považují emailovou komunikaci za dostatečně průkaznou"*.

e) v interních předpisech je možno specifikovat nejzávažnější dokumenty (např. výběr nabídky klientem), které budete požadovat v písemné podobě podepsané klientem.

f) lze rovněž jednoznačně doporučit používání tzv. uznávaného elektronického podpisu, který lze svou průkazností přirovnat k doporučené poštovní zásilce.

### *3.2.4 Elektronické vedení a archivování soudních spisů a jiných dokumentů (důkazů)*

Postupně s rozvojem elektronizace justice lze uvažovat o výlučném elektronickém vedení a archivaci spisu a přepisování záznamu do písemné podoby jen k žádosti účastníka za přiměřený poplatek (jak je tomu dnes např. u kopírování listin ze spisu). Uvedené by platilo např. s výhradou doručování žalob a rozsudků (podle současných procesních předpisů musí být doručeny). Účastník by měl ale vždy nárok na obratem vyhotovenou elektronickou kopii zvukového záznamu. Takový krok by měl být přijat i do oblasti občanského soudního řízení, protože vedle zrychlení postupu řízení zvyšuje přesnost uchování důkazů i rozhodných okolností vlastního jednání. V prvé řadě však přispívá ke kontrole řádného výkonu soudnictví, když je vyloučeno vynechání určitých „kompromitujících" částí děje, jež se v soudní síni odehrály a jež se při běžné protokolaci nejednou „ztrácí" či k nepoznání „přikrášlí".[82]

V současné době lze vést výlučně elektronicky kromě např. účetní dokumentace i např. zdravotní dokumentaci.

V souladu s ust. § 67b odt. 5 zákona č. 20/1966 Sb., o péči o zdraví lidu může být zdravotnická dokumentace vedena na záznamovém nosiči ve formě textové, grafické nebo audiovizuální. Údaje ze zdravotnické dokumentace lze z listinné formy přepsat do elektronické formy pouze za podmínky, že bude zároveň uchována listinná forma. Zápis zdravotnické dokumentace na paměťové médium výpočetní techniky, který neobsahuje zaručený elektronický podpis, se převede na papírový nosič (tiskovou sestavu), opatří se datem a podpisem osoby, která zápis provedla, a zařadí se do zdravotnické dokumentace pacienta. Přitom jednotlivé tiskové sestavy se považují za samostatné části zdravotnické dokumentace.

Pokud se vede zdravotnická dokumentace pouze na paměťových médiích výpočetní techniky, lze zápis zdravotnické dokumentace provádět jen za těchto podmínek:

1) všechny samostatné části zdravotnické dokumentace obsahují zaručený elektronický podpis osoby, která zápis provedla, podle zákona o elektronickém podpisu,
2) bezpečnostní kopie datových souborů jsou prováděny nejméně jednou za pracovní den,

[82] Zdroj a podrobněji viz Martin Elger, ARS AEQUI et BONI: Tři praktické kroky k opravdové reformě soudnictví, Časopis Vaše práva, http://i-pravo.org/časopis, 10.9.2003.

3) po uplynutí doby životnosti zápisu je zajištěn opis archivních kopií, a
4) uložení archivních kopií, které jsou vytvářeny nejméně jedenkrát za rok, je provedeno způsobem znemožňujícím do nich provádět dodatečné zásahy.

Při uchovávání archivních kopií dat na paměťových médiích výpočetní techniky musí být zajištěn přístup k datům a jejich čitelnost (použitelnost) nejméně po dobu, která je předepsána pro archivaci zdravotnické dokumentace. V návaznosti na výše uvedené zákonné zakotvení je tedy možno vést zdravotnickou dokumentaci pouze v elektronické podobě, musí však být splněny čtyři výše zmíněné podmínky.[83]

Stejně tak i zákon č. 563/1991 Sb., o účetnictví v § 33 dovoluje vést účetní dokumentací v elektronické podobě.[84] Zákon výslovně stanoví, že účetní záznam může mít písemnou nebo technickou formu. Pro účely zákona se považuje za písemnou formu účetní záznam provedený rukopisem, psacím strojem, tiskařskými nebo reprografickými technikami anebo tiskovým výstupním zařízením výpočetní techniky, jehož obsah je pro fyzickou osobu čitelný. Za technickou formu účetního záznamu se potom považuje účetní záznam provedený elektronickým, optickým nebo jiným způsobem nespadajícím pod předchozí definice, který umožňuje jeho převedení do formy, v níž je jeho obsah pro fyzickou osobu čitelný. Účetní jednotka dokonce dle zákona může provést převod účetního záznamu z jedné formy do druhé.[85] V tomto případě je ale povinna zajistit, že obsah účetního záznamu v nové formě je shodný s obsahem účetního záznamu v původní formě.[86]

### *3.2.5 Obchodní věstník online*

V aplikaci obchodní věstním online se jedná o aktuální firemní informace s povahou úředního listu online.[87] Záznamy v této databázi vycházejí rovněž v tištěné podobě obchodního věstníku a jsou zcela totožné se zněním, které je možné získat prostřednictvím Portálu veřejné správy ČR. Obchodní věstník vychází každou středu ve 12 hodin. Záznamy z posledních 26 čísel jsou k dispozici zdarma. Starší čísla jsou součástí archivu OV od roku 1992, k němuž je možné získat placený přístup. Internetovou i tištěnou verzi připravuje Economia, a. s.

### *3.2.6. Nahlížení do katastru nemovitostí online*

Aplikace „Nahlížení do katastru nemovitostí"[88] umožňuje získávat některé vybrané údaje týkající se vlastnictví parcel, budov a jednotek (bytů nebo nebytových prostor), evidovaných v katastru nemovitostí a dále informace o stavu řízení založených na katastrálním pracovišti

[83] Možnost vedení zdravotnické dokumentace výlučně v elektronické podobě byla konzultována též s vrchním ředitelem úseku legislativního a právního Ministerstva zdravotnictví ČR Mgr. Martinem Plíškem, který potvrdil správnost uvedených argumentů.
[84] Srov. též Vondruška, P., Elektronická fakturace, Data Security Management, DSM 5/2006, Praha.
[85] Srov. též Štědroň, B., Jakou má elektronická fakturace oporu v zákoně?, www.lupa.cz, Lupa – server o českém internetu, 18.03.2004, ISSN 1213-0702.
[86] V případě sporu např. s finančním úřadem by se potom musel jmenovat příslušný soudní znalec, který by shodu potvrdil.
[87] Aplikace je již v provozu na internetových stránkách - http://ov.ihned.cz.
[88] Aplikace je dostupná na http://nahlizenidokn.cuzk.cz/.

pro účely zápisu vlastnických a jiných práv oprávněných subjektů k nemovitostem v České republice, nebo pro účely potvrzování geometrických plánů.

Na rozdíl od „Dálkového přístupu do KN" je „Nahlížení" volně přístupné všem uživatelům internetu, nevyžaduje žádnou registraci a je bezplatné. Možnosti výstupů jsou však proti Dálkovému přístupu omezené. Výpis z katastru nemovitostí a některé další výstupy aplikace „Nahlížení" neumožňuje.

Výstupy, které je možno v rámci „Nahlížení" zadat a spustit, jsou rozděleny do tří sekcí:

*Řízení o vkladech*
Řízení typu „Vklad" jsou zakládána pro účely zápisu práv na základě smluv o převodu nemovitostí, zástavního práva, oprávnění týkajícího se věcného břemene, předkupního práva, převodu bytu a nebytového prostoru a na základě dalších dle § 33 vyhlášky č.190/1996 Sb. Českého úřadu zeměměřického a katastrálního, ve znění pozdějších předpisů (dále jen „vyhláška"). Výstupy v této skupině mají typ řízení V (vklad) pevně nastaven a nelze jej změnit.

*Ostatní řízení*
Výstupy spouštěné odkazy této skupiny jsou analogii výstupů „Řízení o vkladech", umožňují však volit typ řízení ze dvou alternativ: záznam nebo geometrický plán. Řízení typu „Záznam" jsou zakládána pro účely zápisu právních vztahů k nemovitostem na základě rozhodnutí soudu nebo jiného státního orgánu nebo na základě jiných podkladů podle § 36 vyhlášky. Řízení typu „Geometrický plán" jsou zakládána na základě žádosti o potvrzení plánu předkládané úředně oprávněným zeměměřickým inženýrem. Až na volbu typu řízení je funkce odkazů v této sekci zcela obdobná jako u týchž odkazů v sekci „Řízení o vkladech".

*Informace z KN*
Odkazy „Parcela" a „Budova" a „Jednotka" spouštějí výstupy informací o zadaných nemovitostech obsahující zejména vlastníka nebo spoluvlastníky nemovitosti (včetně uvedení výše vlastnického podílu) a číslo listu vlastnictví, na kterém je nemovitost zapsána. Informace o parcele obsahují též výměru pozemku včetně způsobu jejího určení, druh a způsob využití pozemku a označení mapového listu. Pokud je na pozemku umístěna budova, je na ni zobrazen odkaz. Informace o budově obsahují typ budovy, způsob využití budovy a odkaz na parcelu, na které je budova umístěna. Pokud jsou v budově umístěny jednotky, je na ně zobrazen odkaz. Informace o jednotce obsahují typ jednotky, způsob využití jednotky, podíl jednotky na společných částech domu a odkaz na budovu, ve které je jednotka umístěna.

### *3.2.7. Dálkový přístup k údajům katastru nemovitostí ČR*

Dálkový přístup (DP)[89] je placená služba, která umožňuje registrovaným uživatelům on-line přístup k údajům katastru nemovitostí (KN). Přístup k údajům je umožněn prostřednictvím webové aplikace, dostupné na adrese: https://katastr.cuzk.cz. Podrobnější informace o této službě, poskytovaných výstupech a technických předpokladech použití aplikace naleznete na stránkách přístupných níže uvedenými odkazy. Zájemci o tuto službu se s ní mohou seznámit bezplatně, prostřednictvím funkční ukázky DP na zkoušku. Postup a použitelná vstupní data

[89] Služba je již plně funkční viz. https://katastr.cuzk.cz/uvod.

jsou uvedena pod odkazem „Informace o DP na zkoušku". Uživatelská příručka pro práci s aplikací DP je pod odkazem „Návod pro ovládání funkcí DP". Pro práci se skutečnou databází KN je třeba registrace a přidělení přístupových kódů. Postup včetně formuláře žádosti je k dispozici na stránkách „Založení zákaznického účtu".

### *3.2.8. Elektronický návrh na zápis do katastru nemovitostí*

Elektronický návrh na zápis (dále jen ENZ) je bezplatná služba, která umožňuje registrovaným uživatelům podávat elektronický návrh na zápis vlastnického nebo jiného věcného práva k nemovitostem (vklad, záznam, poznámka) do katastru nemovitostí (KN).[90] Webová aplikace je dostupná na adrese https://katastr.cuzk.cz. Uživatelská příručka pro práci s aplikací ENZ je na této stránce pod odkazem „Návod pro ovládání funkcí ENZ".

Aplikace umožní uživatelům:

- zrychlení procesu podání návrhu,
- zjednodušení při vyplňování - aplikace zákazníky vede v celém procesu tím, že mu nabízí platné údaje KN (názvy katastrálních území, čísla parcel, budov...).

Aplikace slouží k výběru typu změny v KN (vklad, záznam, poznámka), výběru objektů (parcely, budovy, jednotky), které jsou obsahem návrhu na zápis, k zápisu účastníků návrhu na zápis a definování návrhu změny do KN. Vytvoření ENZ je rozčleněno do několika kroků rozdělených na jednotlivé stránky, postup na další stránku je umožněn až po správném vyplnění všech povinných polí, v každém okamžiku lze vytvoření návrhu ukončit.

Odeslané podklady, včetně vlastního textu návrhu, se vygenerují do dokumentu formátu PDF. Uživatel si jej pak může vytisknout, přiložit k němu další povinné přílohy podání (včetně originálu listiny) a doručit jej v požadované lhůtě (nejpozději pátý den) na podatelnu příslušného katastrálního pracoviště.

## 3.3. Rozhodnutí

### *3.3.1. Úvod*

Rozhodnutí je svou podstatou jedním z procesních úkonů soudu. Lze jej definovat jako výrok soudu, který má závazné právní důsledky stanovené objektivním právem.[91] Obvyklá struktura rozhodnutí se skládá ze tří částí a to (1) výroku, (2) odůvodnění a (3) poučení o opravných prostředcích. Součástí rozhodnutí jsou také tzv. formální náležitostí jako označení rozhodnutí, věci, soudu a datum.

Mezi základní formy rozhodnutí patří:

[90] Služba je již plně funkční viz. https://katastr.cuzk.cz.
[91] Viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 274 an.

- rozsudek,
- usnesení,
- platební rozkaz,
- směnečný platební rozkaz, a
- opatření (část právní teorie nepovažuje opatření za zvláštní formu rozhodnutí).[92]

Z hlediska rozhodování předmětu řízení je možno dále rozhodnutí dělit na:

- meritorní rozhodnutí, a
- procesní rozhodnutí.

Meritorním rozhodnutím (také se označuje jako rozhodnutí ve věci samé) se autoritativně a závazně řeší právní konflikt, který byl předmětem řízení. Meritorní rozhodnutí je poté možno dále dělit na tzv. konstitutivní rozhodnutí, se kterými je spojem vznik, změna nebo zánik právních skutečností, a nebo na tzv. deklaratorní rozhodnutí, která nejsou právotvorná a nezasahují do hmotněprávních vztahů.

Charakteristickým rysem procesních rozhodnutí je skutečnost, že takováto rozhodnutí nezasahují přímo do řešení dané právní věci (do tzv. merita), ale řeší určité procesní situace, které během řízení mohou nastat (např. povolání znalce k vypravování znaleckého posudku atd.).

### *3.3.2. Elektronické rozhodnutí a doručení rozhodnutí elektronickou cestou*

Z ustanovení § 157 a násl. občanského soudního řádu, které upravují náležitosti písemného vyhotovení rozsudku, výslovně nevyplývá možnost vydat toto rozhodnutí v elektronické podobě. Zákon o elektronickém podpisu oproti tomu v § 11 odst. 1 stanoví, že písemnosti orgánů veřejné moci v elektronické podobě podepsané uznávaným elektronickým podpisem mají stejné účinky jako veřejné listiny. V současné době ale chybí prováděcí předpis, který by upravil náležitosti podpisu rozhodnutí a postup při jejich odesílání adresátům v elektronické formě.[93]

Do budoucna lze v rámci elektronizace soudního procesu např. doporučit vytvoření tzv. elektronického sudiště.[94] Elektronické sudiště znamená unikátní adresu (stránku) internetu, zřízenou u věcně a místně příslušného soudu výlučně pro vedení konkrétního sporu, pro podání účastníků řízení, jakož i pro veškerá rozhodnutí soudce a uchovávání všech písemností v elektronické podobě, souvisejících se sporem. Přístup na sudiště je umožněn jen účastníkům

[92] Viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 282 an.

[93] V současné době připravuje Ministerstvo spravedlnosti novelu novelu občanského správního řádu, jejíž součástí má být i nový způsob doručování a to elektronicky. Dle plánu dostanou všechny zletilé osoby v ČR e-mailovou adresu, které bude určena pro posílání soudních obsílek. Datovou schránku, kam budou písemnosti chodit, zřídí a bude provozovat Ministerstvo vnitra ČR.

[94] Např. podobně jak je tomu u online rozhodčího řízení realizovaném Rozhodčím soudem při Hospodářské komoře ČR a Agrární komoře ČR (www.arbcourt.cz).

řízení a soudu. Rozhodnutí (např. rozsudek) soudu poté podepíše soudce v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu a uveřejní rozhodnutí na sudišti. Rozhodnutí se bude považovat za vydané dnem jeho uveřejnění na sudišti. Toto datum bude uvedeno v rozhodnutí, jakož i v oznámení o vydání rozhodnutí prostřednictvím e-mailu, zaslaného účastníkům řízení. Sudiště zůstane přístupné účastníkům řízení např. třicet kalendářních dní ode dne vydání rozhodnutí. Po uplynutí této lhůty bude sudiště znepřístupněno.

*Elektronické doručování dle návrhu zákona o elektronizaci procesních úkonů („Návrh")*

*§ 4 Návrhu*
*Zřízení datové schránky fyzické osoby a právnické osoby*

*(1) Datovou schránku zřizuje ministerstvo.*

*(2) Datovou schránku fyzické osoby zřídí ministerstvo bezodkladně po jejím narození.*

*(3) Datovou schránku fyzické osoby nebo právnické osoby, které byl přidělen identifikátor podle § 10 po nabytí účinnosti zákona, zřídí ministerstvo bezodkladně po přidělení identifikátoru.*

*(4) Datovou schránku fyzické osoby nebo právnické osoby, která má identifikátor podle § 10 ke dni účinnosti zákona, zřídí ministerstvo datovou schránku k tomuto datu.*

*§ 5 Návrhu*
*Zřízení datové schránky orgánu veřejné moci*

*(1) Datovou schránku orgánu veřejné moci zřídí ministerstvo bezodkladně po zřízení orgánu veřejné moci.*
*(2) Datovou schránku orgánu veřejné moci, který má identifikátor podle § 10 ke dni účinnosti zákona, zřídí ministerstvo datovou schránku k tomuto datu.*

*§ 6 Návrhu*
*Zřízení oprávnění přístupu do datové schránky fyzické osoby*

*(1) Ministerstvo zřídí oprávnění přístupu do datové schránky fyzické osoby do 30 dnů ode dne podání žádosti fyzické osoby o zřízení oprávnění přístupu do své datové schránky.*

*(2) Náležitosti žádosti fyzické osoby o zřízení oprávnění přístupu do datové schránky jsou*

*a) jméno, popřípadě jména a příjmení,*
*b) rodné číslo nebo datum a místo narození, nebylo-li rodné číslo přiděleno,*
*c) adresa místa trvalého pobytu nebo jiného pobytu na území České republiky anebo adresa bydliště mimo území České republiky."*

*(3) Žádost podle odstavce 1 se podává u ministerstva.*

*(4) Pro účely zřízení oprávnění přístupu do datové schránky fyzické osoby ověří ministerstvo správnost údajů uvedených v žádosti podle odstavce 2.*

*(5) Přístupové údaje pro přístup oprávněné osoby podle § 3 odst. 1 písm. a) do datové schránky doručí ministerstvo této oprávněné osobě.*

*§ 7 Návrhu*
*Zřízení oprávnění přístupu do datové schránky právnické osoby nebo orgánu veřejné moci*

*(1) Oprávnění přístupu do datové schránky právnické osoby nebo orgánu veřejné moci vzniká dnem zřízení datové schránky právnické osoby nebo orgánu veřejné moci.*

*(2) Přístupové údaje pro přístup oprávněné osoby podle § 3 odst. 1 písm. b) a c) do datové schránky doručí ministerstvo této oprávněné osobě.*

*§ 8 Návrhu*
*Přihlašování do datové schránky*

*(1) Oprávněná osoba se do datové schránky přihlašuje prostřednictvím přístupových údajů, které jí byly doručeny podle § 6 odst. 5 nebo § 7 odst. 2.*

*(2) Zvláštní zákon stanoví způsob přihlašování oprávněné osoby podle § 3 odst. 1 písm. d) do datové schránky.*

*§ 13 Návrhu*
*Doručování*

*(1) Písemnosti orgánů veřejné moci jsou fyzické osobě, které bylo zřízeno oprávnění přístupu do datové schránky, právnické osobě nebo orgánu veřejné moci doručovány do datové schránky, umožňuje-li to jejich povaha.*

*(2) Písemnost je doručena okamžikem přihlášení oprávněné osoby do datové schránky, pokud byla dodána do datové schránky.*

*(3) Pokud zvláštní zákon nestanoví jinak, považuje se písemnost orgánu veřejné moci za doručenou, neprovede-li adresát přihlášení do datové schránky ve lhůtě 10 dnů ode dne, kdy byla písemnost dodána do datové schránky.*

*(4) Doručení písemnosti podle odstavce 2 nebo 3 má stejné právní účinky jako doručení do vlastních rukou.*

### *3.3.3. Elektronický platební rozkaz*

Vláda na svém zasedání dne 18. 6. 2007 schválila novelu občanského soudního řádu. Ta navrhuje zavést do našeho práva elektronický platební rozkaz.[95] Tento nástroj má řešit spory o peněžité pohledávky, urychlit rozhodovací proces a ulehčit práci soudům.[96]

Institut elektronického platebního rozkazu navazuje na stávající rozkazní řízení a počítá se zavedením elektronického formuláře, který žalobce vyplní, podepíše zaručeným elektronickým podpisem a odešle soudu. Jedinou podmínkou pro zahájení řízení a vydání elektronického platebního rozkazu je zaplacení soudního poplatku a správné vyplnění formuláře. Při splnění všech náležitostí vydá soud automatizovaně elektronický platební rozkaz.[97]

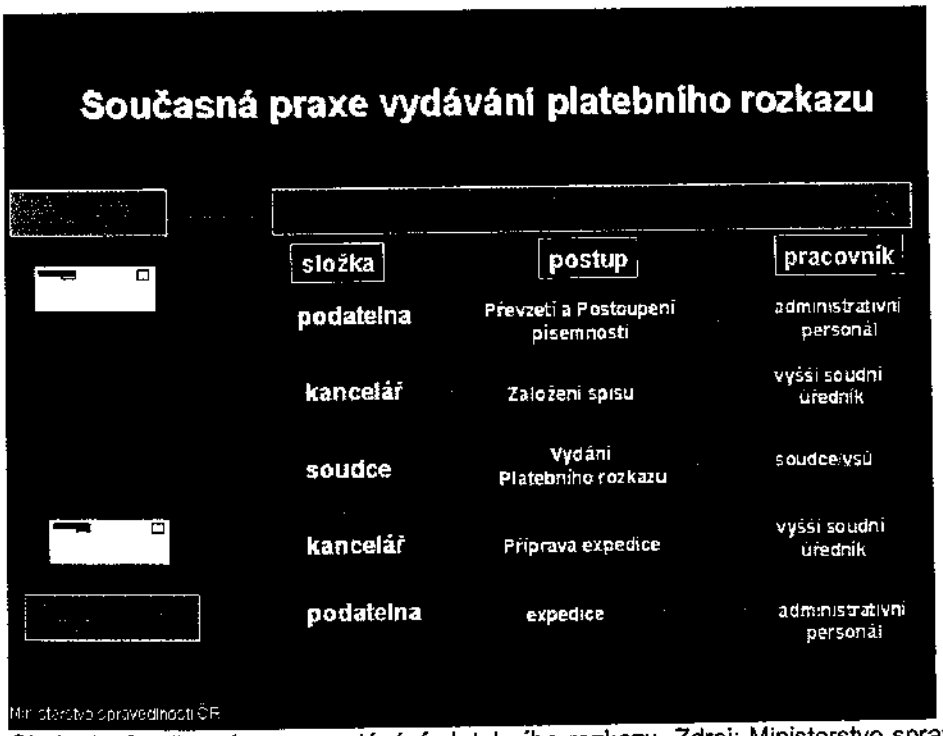
[95] Autorem návrhu na podávání platebního rozkazu elektronicky je Ministr spravedlnosti ČR Jiří Pospíšil, který mimo jiné uvedl, že se inspiroval v sousedním Německu. Elektronický platební rozkaz je dle Ministra standardní věcí ve většině zemí EU (zdroj: www.ihned.cz, 13.3.2007).
[96] Více viz. Vláda schválila elektronický platební rozkaz, C.H.Beck, www.ipravnik.cz.
[97] Více viz. Novák, F., Kdy zrychlí elektronický platební rozkaz práci soudů?, Cesko.iHNed.cz 13. 3. 2007, ISSN 1213-7693.

Řízení u soudu má být zkrácené, bez jednání, dokazování a bez slyšení žalované strany. Žalovaný ale nebude zbaven možnosti ochrany, ta se pouze přesune do stádia po rozhodnutí, kdy se může rozmyslet, zda proti rozhodnutí podá námitku či odpor nebo jej akceptuje. Žalovaný bude moci podat odpor ve lhůtě patnácti dnů ode dne doručení elektronického platebního rozkazu. V takovém případě soud platební rozkaz zruší a podobně jako v situaci, kdy se nepodaří platební rozkaz doručit, postoupí spis obecnému soudu, který nařídí jednání.

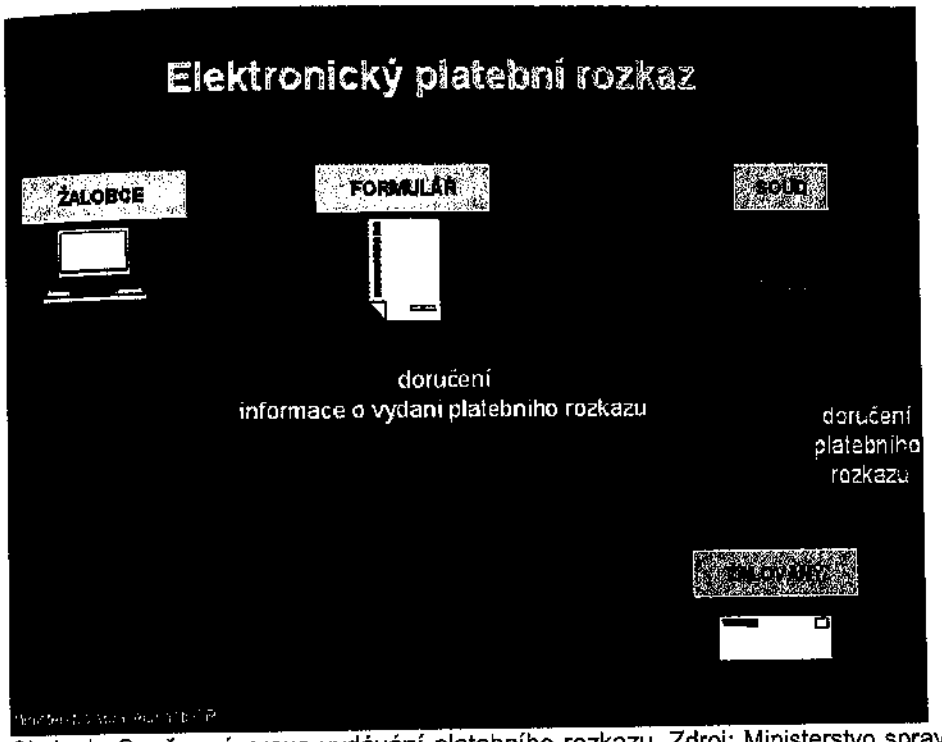
Elektronické platební rozkazy budou vydávat věcně a místně příslušné soudy. Vedle elektronického platebního rozkazu bude i nadále existovat písemný platební rozkaz a směnečný (šekový) platební rozkaz, které budou fungovat stejně jako v současnosti. Bude na volbě žalobce, který ze způsobů použije, aby se domohl svého práva.

V současné době dochází k nárůstu tzv. nesporných pohledávek a do budoucna lze očekávat další zvýšení počtu žalob. Protože nebude potřeba při vydávání elektronických platebních rozkazů zásahu soudce či jiného soudního úředníka, budou se tito lidé moci zabývat jinou agendou a soudní proces se díky tomu zrychlí.

Pokud novela občanského soudního řádu, která elektronický platební rozkaz zavádí, projde oběma komorami Parlamentu a podepíše jej prezident, začne platit od 1. 1. 2008.



Obrázek: Současná praxe vydávání platebního rozkazu. Zdroj: Ministerstvo spravedlnosti ČR, Novák František, www.ihned.cz.



Obrázek: Současná praxe vydávání platebního rozkazu. Zdroj: Ministerstvo spravedlnosti ČR, Novák František, www.ihned.cz.

## 3.4. Výkon rozhodnutí

### *3.4.1. Úvod*

Výkonem rozhodnutí se rozumí provedení výkonu rozhodnutí soudem (nebo exekutorem), které nebylo dobrovolně splněno povinným (obvykle stranou, která ve sporu prohrála). Jedná se o prostředek státního donucení, jehož cílem je (1) ochrana práv věřitelů (kterým není dovoleno vzít právo do svých rukou a zjednat si uspokojení svého práva svépomocí) a zároveň je také výkon rozhodnutí v zájmu soudní autority, aby její rozhodnutí nebyla brána na lehkou váhu.[98]

Účastníky řízení jsou při výkonu rozhodnutí oprávněný a povinný. Jsou-li nařízeným výkonem rozhodnutí postiženy majetkové hodnoty nebo práva patřící do společného jmění manželů, je účastníkem řízení, pokud jde o tyto majetkové hodnoty, i manžel povinného.[99]

Výkon rozhodnutí ukládajícího zaplacení peněžité částky lze provést srážkami ze mzdy, přikázáním pohledávky, příkazem k výplatě z účtu u peněžního ústavu, prodejem movitých věcí a nemovitostí, prodejem podniku a zřízením soudcovského zástavního práva k nemovitostem.[100]

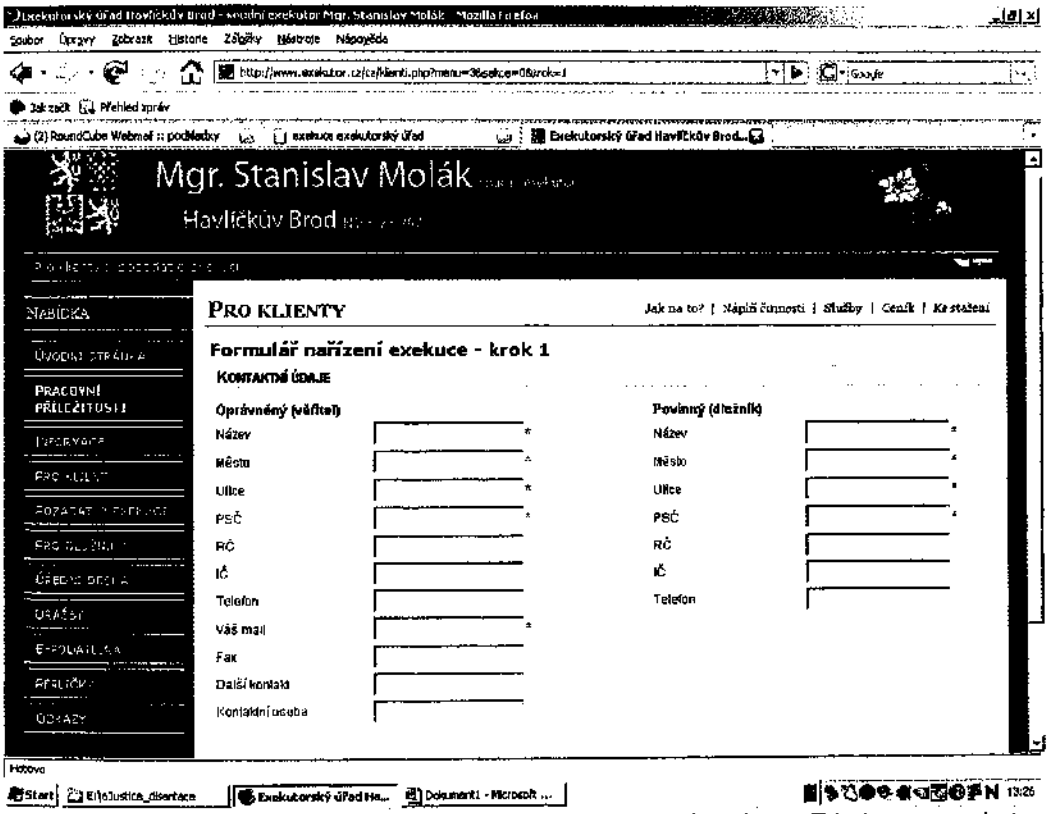
[98] Viz. Winterová, A. a kol., Civilní právo procesní, 4. vydání, Linde, Praha 2006, ISBN 80-7201-464-1, str. 490 an.
[99] §255 OSŘ.
[100] §258 OSŘ.

Výkon rozhodnutí ukládajícího jinou povinnost než zaplacení peněžité částky se řídí povahou uložené povinnosti. Lze jej provést vyklizením, odebráním věci, rozdělením společné věci, provedením prací a výkonů.

Výkon rozhodnutí prodejem zástavy lze pro zajištěnou pohledávku provést prodejem zastavených movitých a nemovitých věcí, věcí hromadných, souborů věcí a bytů nebo nebytových prostorů ve vlastnictví podle zvláštního zákona, přikázáním zastavené peněžité pohledávky a postižením zastavených jiných majetkových práv.

### *3.4.2. Elektronický formulář pro podání návrhu na exekuci*

Návrh na exekuci by mělo být také možno podávat i online (elektronicky). Někteří exekutoři již provozují elektronické aplikace, které slouží ke zjednodušení a zrychlení komunikace mezi oprávněným a exekutorem.[101]



Obrázek: Příklad elektronické aplikace – žádost o provedení exekuce. Zdroj: www.exekutor.cz.

Někteří soudní exekutoři se dále snaží zjednodušit práci oprávněným a tak na svých internetových stránkách nabízejí ke stáhnutí vzory exekučních příkazů a návrhů na výkon rozhodnutí v elektronické podobě k vyplnění.[102]

[101] Podobnou elektronickou aplikaci již provozuje např. Stanislav Molák, soudní exekutor v Havlíčkově Brodě - www.exekutor.cz.
[102] Např. Exekutorský úřad Praha 4, Roman Vytejček, soudní exekutor – www.exekuceonline.cz.

## 3.5. Další možnosti využití informačních technologií a systémů (ICT) v soudním řízení

### *3.5.1. Využití elektronického podpis a certifikátů – technický exkurs*

Zákon o elektronickém podpisu byl schválen v roce 2000 a upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. Nutnou podmínkou dle zákona pro komunikaci občanů se státní správou elektronickou cestou s využitím tzv. elektronického podpisu jsou tzv. kvalifikované certifikáty občanů.

V návaznosti na uvedený zákon o elektronickém podpisu, bývalé Ministerstvo informatiky udělilo zatím (stav v roce 2007) akreditaci třem společnostem (tzv. certifikační autority),[103] které jsou tímto oprávněny tyto tzv. kvalifikované certifikáty vydávat. Jedná se o:[104]

První certifikační autorita, a. s.
identifikační číslo 26 43 93 95,
Podvinný mlýn 2178/6,
PSČ 190 00 Praha 9

Česká pošta, s. p.
identifikační číslo 47 11 49 83,
Olšanská 38/9,
PSČ 225 99 Praha 3

eIdentity a. s.
identifikační číslo 27 11 24 89,
Vinohradská 184/2396,
PSČ 130 00 Praha 3

Výměna informací v elektronické podobě je trendem dnešní doby. Ne každá informace je však určená očím a uším každého. Jinak řečeno, data je často třeba chránit. Máme-li pak na mysli komunikaci ve sféře státní správy, financí, zdravotnictví, obchodu, dopravy a služeb aj. je nutné, aby byly stejně důvěryhodné jako klasické procedury prováděné na základě osobního styku, tedy zejména s využitím ověření totožnosti, vlastnoručních podpisů či archivaci dokumentů. Na základě této úvahy lze v souladu s mezinárodními normami definovat základní bezpečnostní cíle, jejichž plnění by měl důvěryhodný systém zajistit.[105]

Jedná se především o:[106]

- důvěrnost informací

[103] Srov. též 2] Vondruška,P., Bosáková,D., Poskytovatelé certifikačních služeb v EU a ČR, část II., Data Security Management, DSM 5/2001, Praha.
[104] Zdroj: www.micr.cz.
[105] Srov. též Vondruška,P., Elektronický podpis a PKI, Vize informační bezpečnosti 2002-2003, Data Security Management, Praha 2002.
[106] Podrobněji viz. Budiš, P., Bezpečná komunikace a certifikační autorita, DSM, č.1, 1997, ISSN 1211-8737.

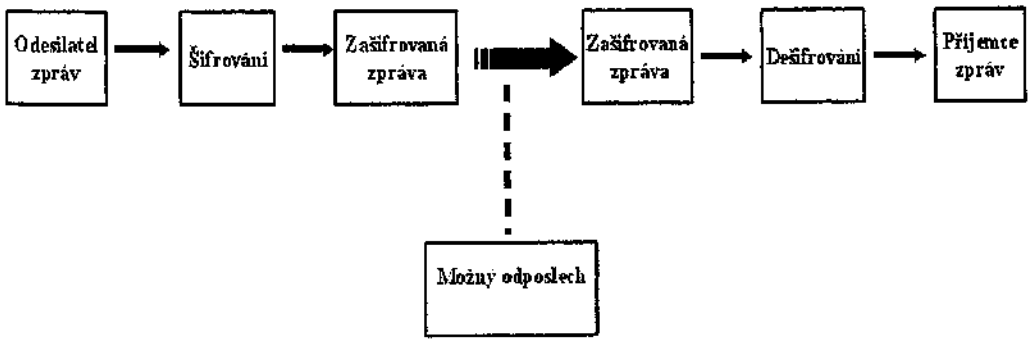
systém musí zabezpečit, že přístup k důvěrným informacím mají pouze autorizované subjekty

- integrita
  systém musí zabezpečit informace proti modifikaci

- neodmítnutelnost odpovědnosti
  systém musí mít schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, vlastnictví, odeslání, případně přijetí zprávy.

Ochranu informací lze rozdělit do dvou základních oblastí. Tou první je ochrana dat u správce či uživatele. V této fázi jsou nebo mohou být data pod výhradní kontrolou jediného subjektu. Tomu odpovídají i požadavky na zabezpečení, které může být řešeno jak fyzickou a organizační ochranou, tak i ochranou logickou, aplikací kryptografie. Pod fyzickou ochranou je možné si představit i počítač oddělený od dostupných komunikačních prostředků a sítí, ke kterému má přístup pouze jeho vlastník

Fyzická ochrana přenosu je často náročná, většinou však nemožná. Nelze si představit ochranu byť jen několik kilometrů dlouhé linky tak, aby z ní nebylo možné signál odposlechnout. Často se navíc využívá komutované linky, která na každém uzlu k odposlechu přímo vybízí. Jistou bezpečnost snad nabízí spojení pomocí optického kabelu, ale ani v tomto případě nelze mluvit o vysokém stupni ochrany. Nabízí se tedy možnost logické ochrany dat, konkrétně šifrování. Znamená to zašifrovat data na straně odesilatele, odeslat je a na straně příjemce zase dešifrovat.



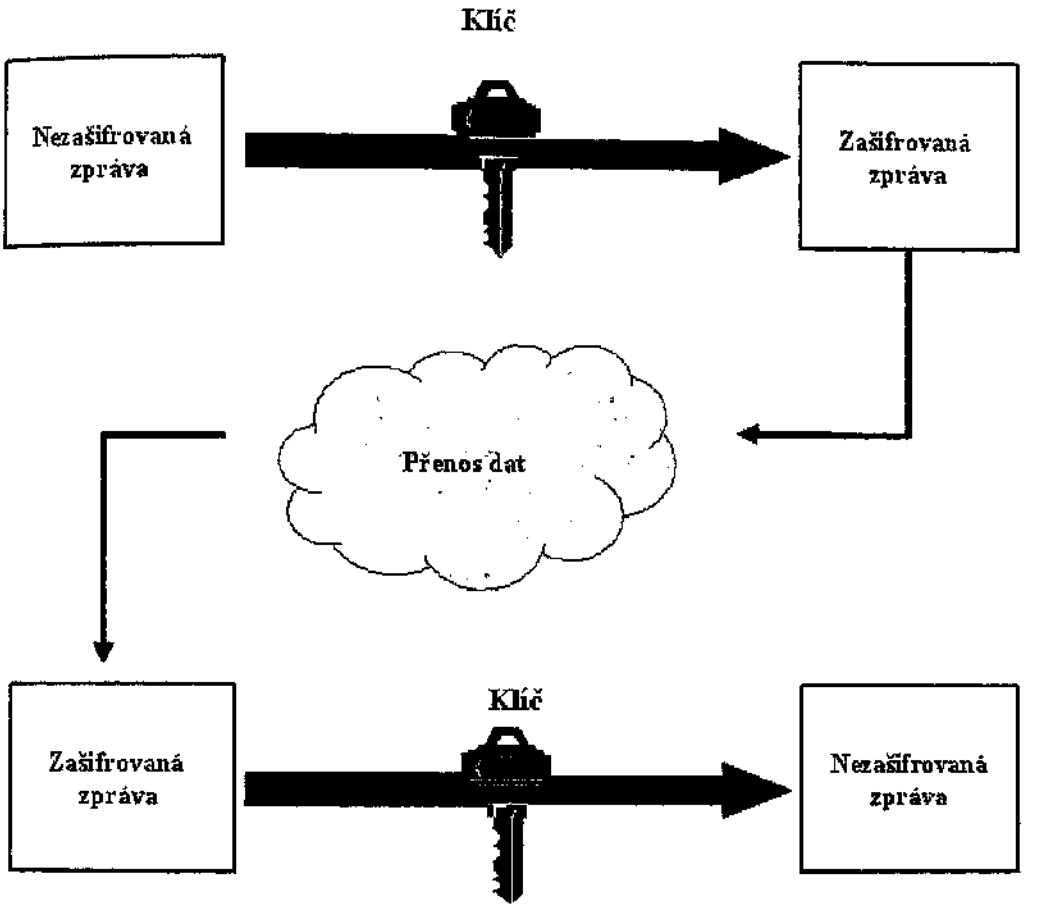

*Obrázek: Ukázka přenosu zpráv šifrovaným kanálem. Zdroj: www.ica.cz.*

Kvalita ochrany zprávy je dána šifrovací metodou, typem užitého algoritmu, jeho aplikací a délkou šifrovacího klíče. V zásadě rozlišujeme dvě šifrovací metody.[107]

První z nich je metoda symetrické šifry. Znamená to, že stejný klíč, který byl užit k zašifrování zprávy na straně odesilatele, bude užit i na straně příjemce pro dešifrování

[107] Viz. též. Matejka, J., Vondruška, P., The Basic Terms and Legal Aspects of the ESA from the Practical and Security Points of View, Sborník mezinárodní konference IDET, Brno 2001.

zprávy. Tento klíč musí být samozřejmě udržován v tajnosti. Z toho vyplývá nutnost před začátkem komunikace předat důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji (konkrétní typ algoritmu) druhé straně.

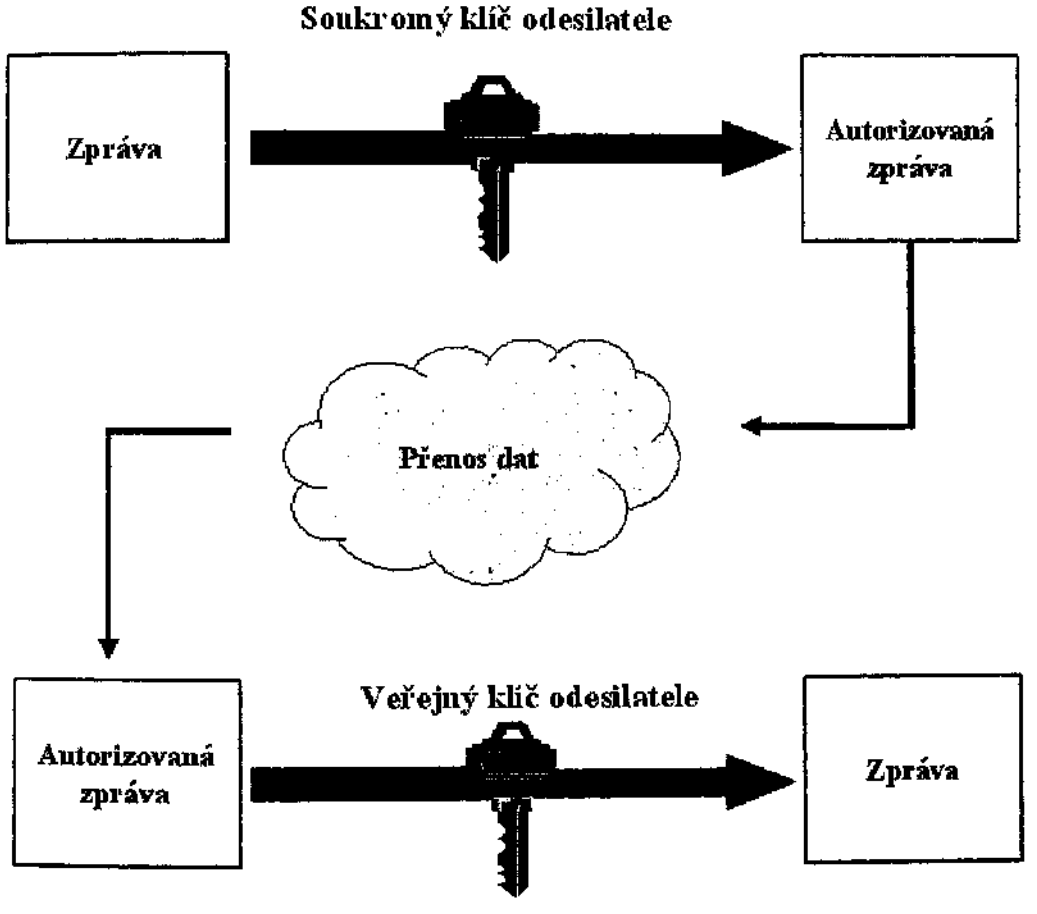



*Obrázek: Ukázka šifrování zpráv symetrickou šifrou. Zdroj: www.ica.cz.*

Současná komerčně dostupná výpočetní technika aplikuje tyto algoritmy (např. DES, TRIPLEDES, IDEA) téměř v reálném čase. Na druhé straně i nejmodernější výpočetní technika je schopna dešifrovat (resp. luštit) data bez znalosti příslušných klíčů jen za relativně dlouhé časové období a s velkými finančními náklady. Pomocí matematických metod lze poměrně přesně vyčíslit náklady a čas potřebný k dešifrování dat, která jsou šifrována definovaným algoritmem. Volbou délky klíče lze navíc tento výsledek výrazně ovlivnit. Použití symetrických algoritmů představuje způsob, jak zabezpečit důvěrnost transakcí definovaným způsobem s možností přesného stanovení hrozeb, kterým toto zabezpečení odolává. Stěžejní nevýhodou je obtížná distribuce klíčů v rozsáhlých sítích a složitá logistika klíčů.[108]

[108] Viz. též Kolektiv autorů, in Matejka, J., BEZPEČNOST DAT V POČÍTAČOVÝCH SYSTÉMECH, 2001, s.1-17, DCD Publishing.

Metoda asymetrické šifry oproti symetrické kryptografii užívá jednoznačně dané dvojice klíčů. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných SW produktů a stává se tak jejich jediným majitelem.[109] Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Jeden z nich, takzvaný privátní klíč je s maximální bezpečností ukrýván majitelem (čipové karty, disketa v trezoru, ...), zatímco druhý klíč je zveřejněn. Byla-li zpráva šifrována (autorizována) za použití privátního klíče a my známe vlastníka veřejného klíče, kterým jsme zprávu dešifrovali, známe odesilatele. Protože je veřejný klíč obecně znám všem, nelze zprávu zašifrovanou (autorizovanou) podle výše popsaného postupu považovat za zašifrovanou v plném smyslu slova (důvěrnou), ale pouze za autorizovanou.

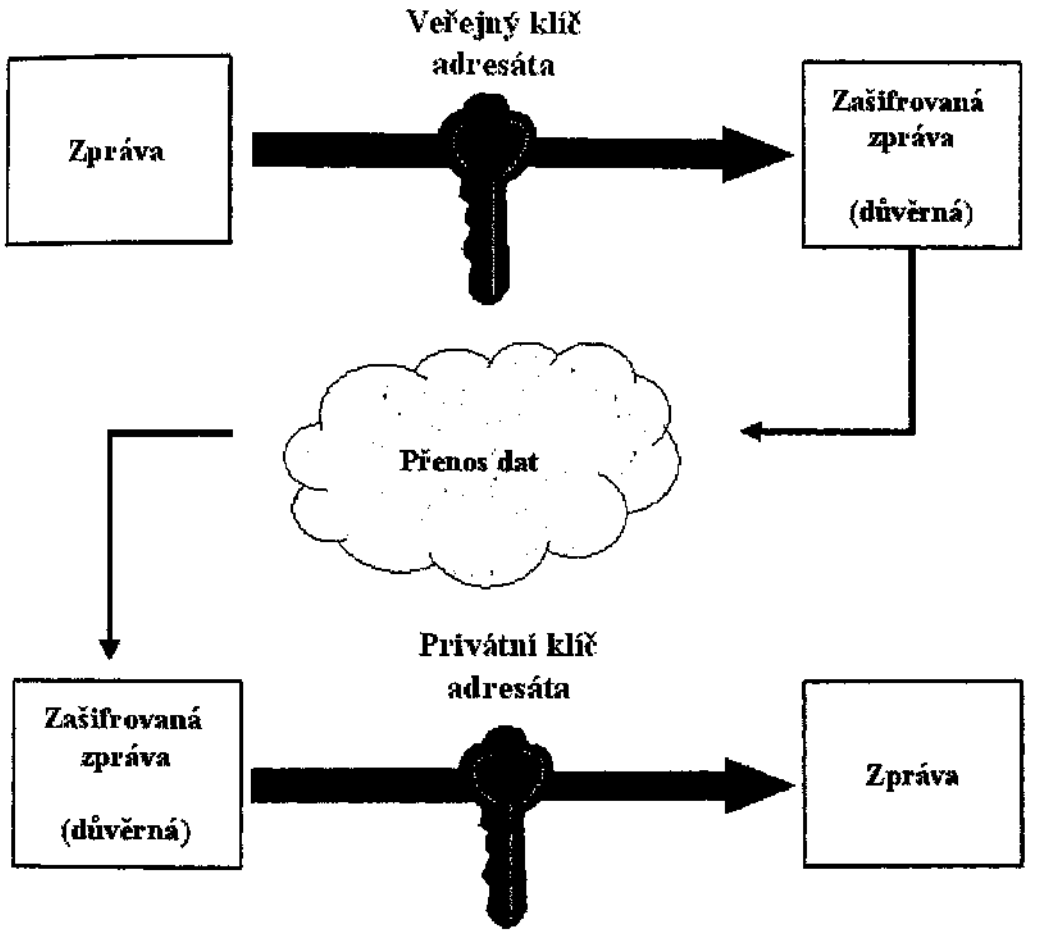



*Obrázek: Ukázka přenosu neadresované, nezašifrované (veřejné), ale podepsané (principálně) i autorizované zprávy. Zdroj: www.ica.cz*

Tímto způsobem lze za pomocí asymetrické kryptografie řešit integritu dat a neodmítnutelnost odpovědnosti na straně odesilatele. Jestliže příjemce pošle autorizované potvrzení o přijetí zprávy, je zajištěna neodmítnutelnost odpovědnosti i ze strany příjemce, který nebude moci popřít, že zprávu přijal. Výše popsaný postup neřeší požadavek důvěrnosti zpráv, tedy

[109] Viz. též Vondruška, P., Rozjímání nad PKI, Data Security Management, DSM 5/2004, Praha.

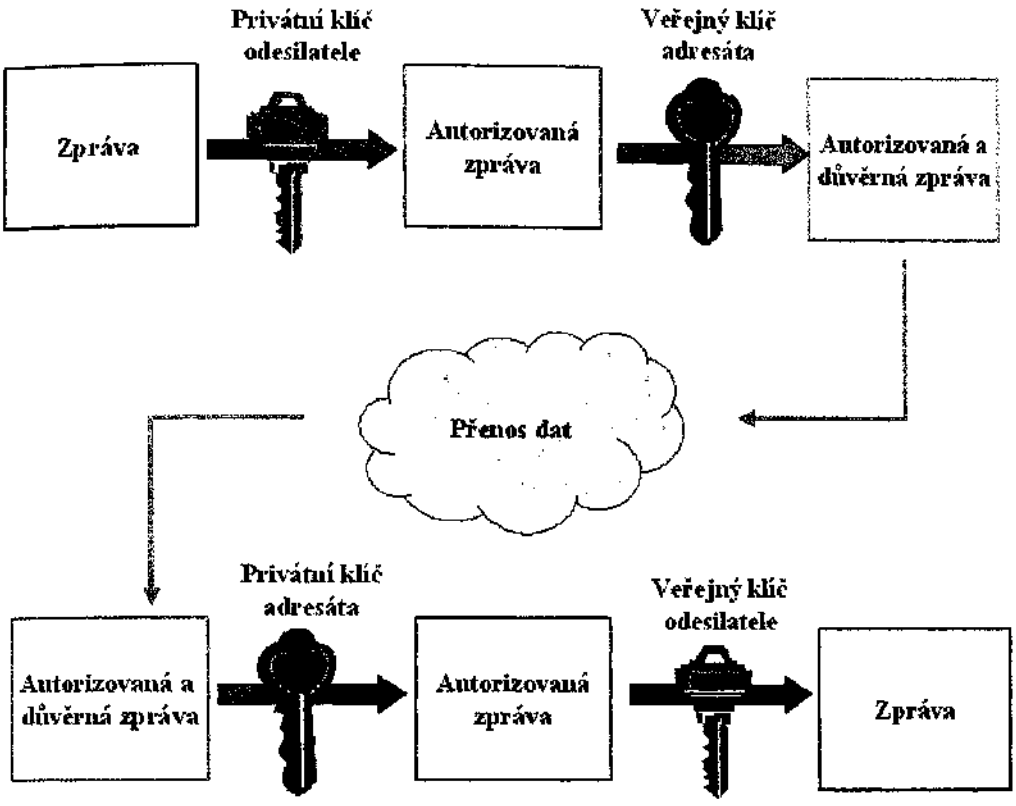
nečitelnosti pro neautorizované subjekty. K tomu lze využít šifrování zpráv pomocí veřejného klíče adresáta. Při zašifrování zprávy tímto klíčem máme jistotu, že ji přečte pouze adresát se svým privátním klíčem.[110]




*Obrázek: Ukázka přenosu adresované, zašifrované (důvěrné), ale neautorizované zprávy. Zdroj: www.ica.cz.*

Celý systém pro šifrování a podepisování zpráv pomocí asymetrické kryptografie pracuje tedy následujícím způsobem. Zpráva je obvykle na straně odesilatele nejprve autorizována, autorizován je čitelný text zprávy, a potom šifrována. Na straně příjemce je zpráva nejprve dešifrována privátním klíčem příjemce, čímž je zajištěna adresnost zprávy a teprve potom je pomocí veřejného klíče ověřena identifikace odesilatele.[111]

[110] Podrobněji viz. Budiš, P., Certifikáty a certifikační autorita, Lancom, č. 7-8, 2000, ISSN 1210-2997.
[111] Viz. též Vondruška, P., Výstavba PKI ve společnosti, Connect!, 11/2003, Praha.




*Obrázek: Ukázka přenosu* adresované, zašifrované (důvěrné) a autorizované zprávy. *Zdroj www.ica.cz.*

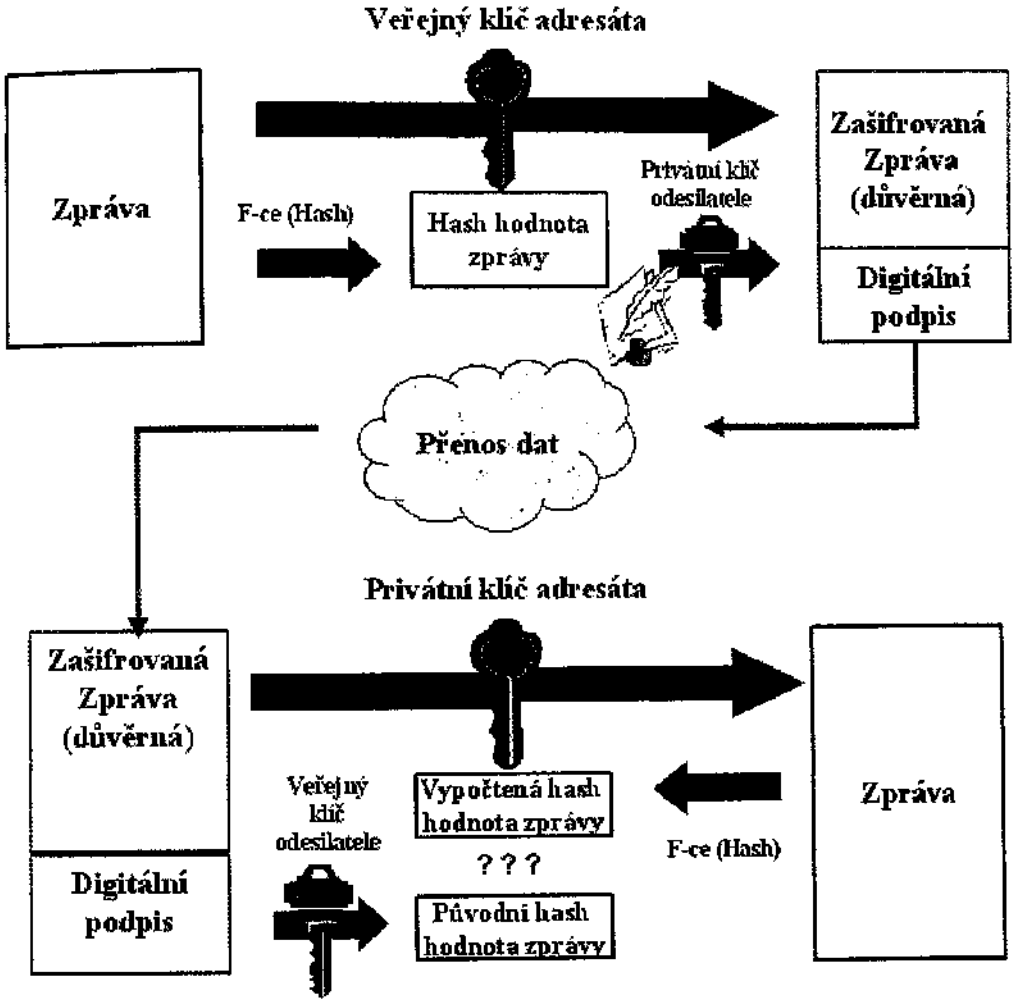
Praktické využití

Aplikace asymetrických algoritmů je výrazně pomalejší než užití algoritmů symetrických. Je to dáno matematickou podstatou asymetrických algoritmů. I proto se zpravidla při tvorbě podpisu nešifruje privátním klíčem odesilatele celá zpráva, ale nejprve se na data použije takzvaná hash funkce.[112] Hash funkce je jednosměrná transformace, která z variabilních vstupních veličin vytvoří jednoznačnou hodnotu (textový řetězec) pevné délky, který se nazývá hash hodnota. Hash hodnota představuje zhuštěnou hodnotu dlouhé zprávy, ze které byla vypočtená, ve významu „digitálního otisku prstu" (nebo „vzorku") velkého dokumentu. Opačný proces je nemožný – díky jednosměrnosti hash funkce. Výpočet hash hodnoty zprávy je velmi rychlý. Nejprve se při podpisu zprávy vypočte hash hodnota zprávy, která bývá výrazně kratší než podepisovaná zpráva, a ta se zašifruje některým asymetrickým algoritmem s použitím privátního klíče, v této souvislosti též nazývaným „data pro vytváření elektronického podpisu". Výsledkem je takzvaný digitální podpis. Ten je potom odeslán jako příloha zprávy nebo v samostatném bloku. Výhodou digitálního podpisu je, že splňuje stejná bezpečnostní kritéria jako autorizace celého dokumentu, provedení však trvá nesrovnatelně kratší dobu.

Kontrola digitálního podpisu zprávy u příjemce probíhá tak, že ke zprávě je podle dohodnutého algoritmu samostatně dopočítána nová hash hodnota a ta je potom srovnávána

[112] Podrobněji viz. Budiš, P., Certifikační autorita I.CA., DSM, č.6, 2000, ISSN 1211-8737.

s dešifrovanou (pomocí veřejného klíče předpokládaného odesilatele) hash hodnotou obsaženou v dodatku zprávy. Obě hodnoty si musí být rovny.

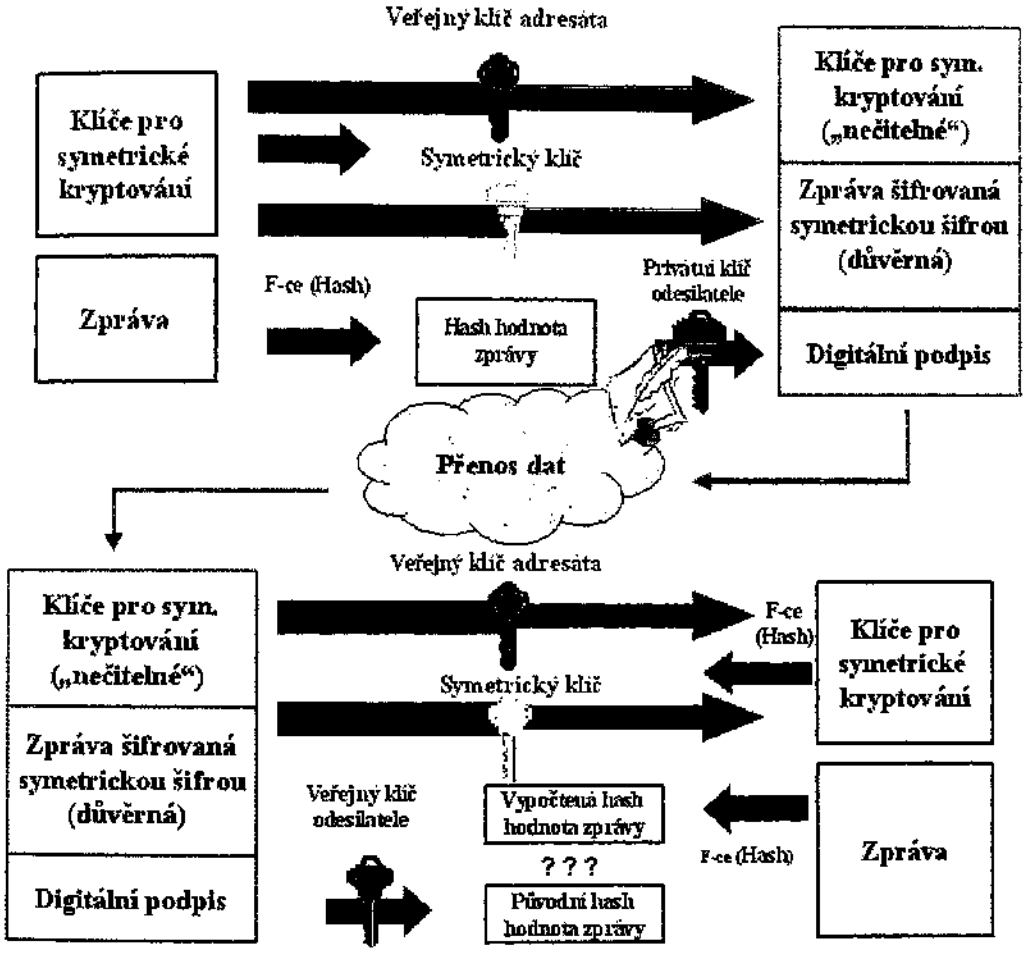



*Obrázek: Ukázka bezpečná komunikace s využitím digitálního podpisu. Zdroj www.ica.cz.*

K vytvoření digitálně podepsané a zašifrované zprávy můžeme použít níže popsaný postup. Odesilatel zprávy nejprve vypočte hash hodnotu zprávy a tu zašifruje svým privátním klíčem, čímž vznikne digitální podpis zprávy. Potom zprávu zašifruje veřejným klíčem adresáta („znečitelní" pro neautorizované subjekty). Takto upravená zpráva je spolu s digitálním podpisem předána ( zaslána po síti, předána na disketě, ...) adresátovi. Ten nejprve zprávu dešifruje za pomocí svého privátního klíče, a tím se zpráva stane čitelná. Podpis ověří výpočtem hash hodnoty zprávy a jejím srovnáním s dešifrovanou hash hodnotou z digitálního podpisu. V případě, že jsou srovnávané hash hodnoty shodné, je zřejmé, že elektronický podpis vytvořila uvažovaná osoba a zpráva navíc nebyla po jejím podepsání změněna.

Tímto způsobem lze splnit kritéria bezpečnosti z úvodu. Protože je však při tomto postupu třeba jednou zašifrovat celou zprávu pomocí asymetrického algoritmu („znečitelnění" zprávy), což by v případě delších zpráv trvalo na obou komunikujících stranách neúměrně dlouho, není toto užití v bezpečné komunikaci typické. Častěji se k šifrování zpráv používá model, ve kterém je asymetrická kryptografie použita pouze ke tvorbě digitálního podpisu a

bezpečné výměně klíčů pro symetrickou kryptografii, která je užita k vlastnímu šifrování přenášených dat. Tato komunikace vyžaduje dohodu o formátu přenášených dat a systému jejich šifrování. Pro každou přenášenou zprávu může odesilatel vygenerovat symetrický klíč, který bude použit k zašifrování (znečitelnění) zprávy. Samotný klíč je poté šifrován veřejným klíčem adresáta, čímž je zaručeno, že se k tomuto klíči dostane pouze adresát, který ho užije k dešifrování zprávy.[113]




*Obrázek: Ukázka bezpečná komunikace s využitím digitálního podpisu a šifrováním zprávy symetrickou šifrou. Zdroj www.ica.cz.*

Správa klíčů

Zřejmě nejproblematičtějším bodem bezpečné komunikace je správa a uchování klíčů.[114] Při užití symetrické kryptografie je třeba s maximální možnou mírou bezpečnosti uchovávat klíče se seznamem příslušných komunikačních partnerů. Tento požadavek je však v rozporu s nutností poměrně časté změny klíče v souvislosti s dobou potenciálního prolomení těchto algoritmů. Jednodušší situace je při užití asymetrické kryptografie. Ani v tomto případě však

[113] Srov. též Vondruška, P., Navázání vztahu důvěry mezi certifikačními autoritami, Data Security Management, DSM 5/2003, Praha.
[114] Podrobněji viz. Budiš, P., Elektronický podpis v praxi, DSM, č.3, 2002, ISSN 1211-8737.

nestačí chránit pouze soukromý klíč. Je také nutné uchovávat veřejné klíče všech komunikujících účastníků a k nim jednoznačnou identifikaci vlastníků těchto klíčů. Předání klíčů tedy je před začátkem vůbec první vzájemné komunikace bezpečným kanálem nezbytnou nutností. Při větším počtu vzájemně komunikujících subjektů to může být problém dosti závažný. Uchování těchto informací se tak stává nejslabším článkem bezpečné komunikace a může zcela znehodnotit snahy o vysoké zabezpečení přenášených dat.

Certifikační autorita a certifikáty

Řešením problému zprávy, distribuce a uchování klíčů je využití služeb poskytovatele certifikačních služeb (PCS), častěji je v praxi užíván název certifikační autorita (CA).[115] V textu dále bude zpravidla, až na výjimky, používán pojem certifikační autorita. Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako třetí nezávislý důvěryhodný subjekt, který prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu s jeho dvojicí klíčů, respektive s jeho digitálním podpisem. Certifikát se tak stává jakýmsi elektronickým průkazem totožnosti. Certifikáty obsahují ve své nejjednodušší formě veřejný klíč, jméno a další údaje zajišťující nezaměnitelnost subjektů. Běžně používané certifikáty též obsahují datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu. To je zajištěno legislativními a technickými pravidly provozu instituce certifikační autority. Splnění těchto požadavků potvrdí CA podpisem dokumentu svým privátním klíčem a následným vydáním tohoto certifikátu.[116]


*Obrázek: Ukázka certifikátu. Zdroj www.ica.cz.*

[115] Více viz. Budiš, P., Certifikáty a certifikační autorita, Lancom, č. 7-8, 2000,ISSN 1210-2997.
[116] Srov. též Vondruška, P., Bosáková, D., Kučerová, A., Peca J., Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů, ANAG 2001.

Znamená to, že certifikát je podepsaným dokumentem se všemi důsledky z toho plynoucími, tedy zejména autorizace (certifikační autorita jako garant pravosti dokumentu) a integrity dat (nelze zaměnit klíč nebo identitu klienta). Tím, že CA zaručuje správnost jí vydaného certifikátu, odstraňuje nutnost smluvní důvěryhodné výměny klíčů mezi dvěma subjekty navzájem a jejich dohoda spočívá pouze v domluvě o společně uznávané CA. Důležité je, že se utajovaná data na straně klienta redukují pouze na bezpečné uchovávání privátního klíče, protože ostatní je řešeno certifikáty. Ty si můžeme kdykoliv ověřit se znalostí veřejného klíče certifikační autority, respektive jejího certifikátu. Existence CA také umožňuje důvěryhodnou komunikaci i subjektů, jenž se navzájem fyzicky nikdy nepotkali nebo neabsolvovali složitou proceduru vzájemné důvěryhodné výměny svých klíčů.

Tvorba a životní cyklus certifikátů

Tvorba certifikátu má 6 kroků:[117]

1. *Generování klíčů.* Každý potenciální žadatel o certifikát si nejprve sám pomocí dostupného SW vybavení vygeneruje dvojici klíčů pro použití v asymetrické kryptografii. Pro tento účel není nutné počítat s nákupem nového softwaru, protože PC vybavené pro komunikaci na Internetu nutný software s největší pravděpodobností má již nainstalován. Procedura generace klíčů je zpravidla automatická nebo poloautomatická a probíhá v počítači. Aktivace procesu generace je možná buď spuštěním programu přímo na PC nebo je možné i vzdálené spuštění, například pomocí web serveru. Druhá varianta je často užívána, a to zejména pro to, že je rychlá a uživatelsky přívětivá.

2. *Příprava identifikačních dat a žádosti o certifikát.* Žadatel o certifikát shromáždí podle požadavků certifikační autority osobní identifikační materiály nutné pro vydání certifikátu, jako IČO, DIČ, resp. číslo OP, rodné číslo a podobně. Následuje vyplnění formuláře, ve kterém mohou být kromě standardních údajů, jako je například jméno a příjmení i údaje další, doplňkové. V žádosti o certifikát a následně i v certifikátu bývá často uvedena firma, pracovní zařazení, adresa atd.

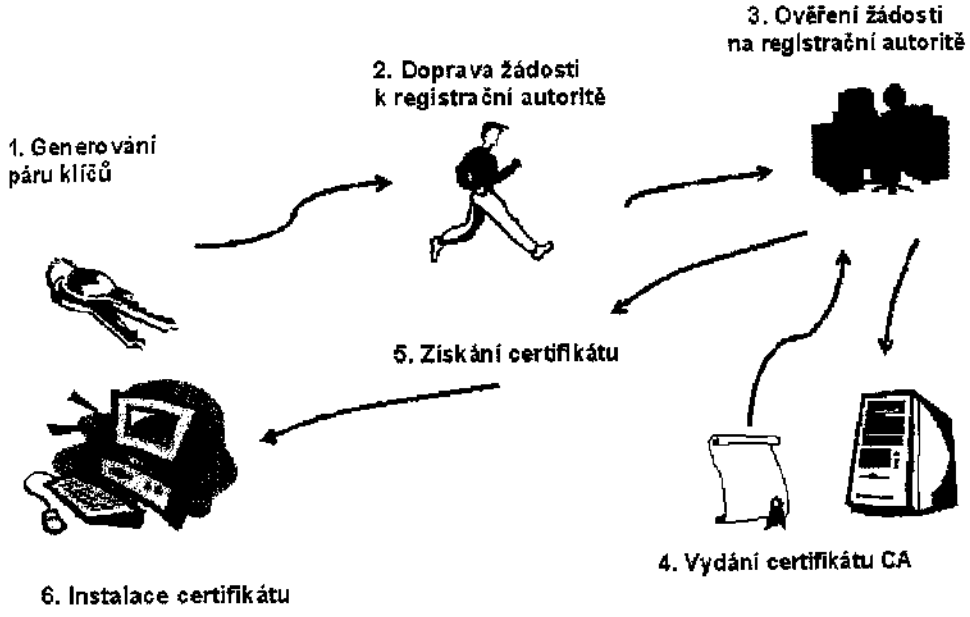
3. *Předání žádosti o certifikát autoritě.* Certifikační autority, které nabízí své služby veřejnosti, mají zpravidla kontaktní místa oddělena od centrálního systému. Důvodem není pouze vyšší bezpečnost, ale především nutnost mít kontaktní místa v mnoha lokalitách, blízko klientům. Kontaktní místa CA se nazývají registrační autority (RA). Žadatel předá na RA data nutná pro vydání certifikátu spolu s doklady o jejich pravosti. U CA vyšší úrovně bezpečnosti jsou údaje uvedené z žádosti následně kontrolovány na RA, a proto je nutné, aby bylo možné jednotlivé položky žádosti doložit příslušnými doklady a ověřit.

4. *Ověření informací.* Certifikační autorita si na příslušných místech ověří, že může vydat žadateli certifikát. Při ověření žádosti o certifikát je možné ověřit nejen doklady žadatele a informace z dostupných registrů a ostatních datových zdrojů, ale je možné ověřit i konzistenci šifrovacích klíčů a jejich jedinečnost v rámci konkrétní CA.

[117] Viz. Budiš, P., Certifikáty a certifikační autorita, Lancom, č. 7-8, 2000,ISSN 1210-2997.

5. *Tvorba certifikátu.* Certifikační autorita vytvoří digitální dokument příslušného formátu a ten poté podepíše svým privátním klíčem. U CA s vyšší úrovní bezpečnosti je certifikát vydáván off-line. Důvodem je především bezpečnost, která spočívá ve vícestupňové kontrole a možnosti oddělení centrálního systému od okolí.

6. *Předání certifikátu.* Podle dohody je certifikát žadateli předán (disketa), zaslán, nebo zveřejněn. Nezveřejnění certifikátu poskytuje pouze minimální ochranu, proto jsou certifikáty zpravidla u veřejných CA zveřejňovány. V rámci zveřejnění certifikátů CA informuje i o jeho platnosti a stavu, což naopak přispívá ke zvyšování bezpečnosti a důvěry.



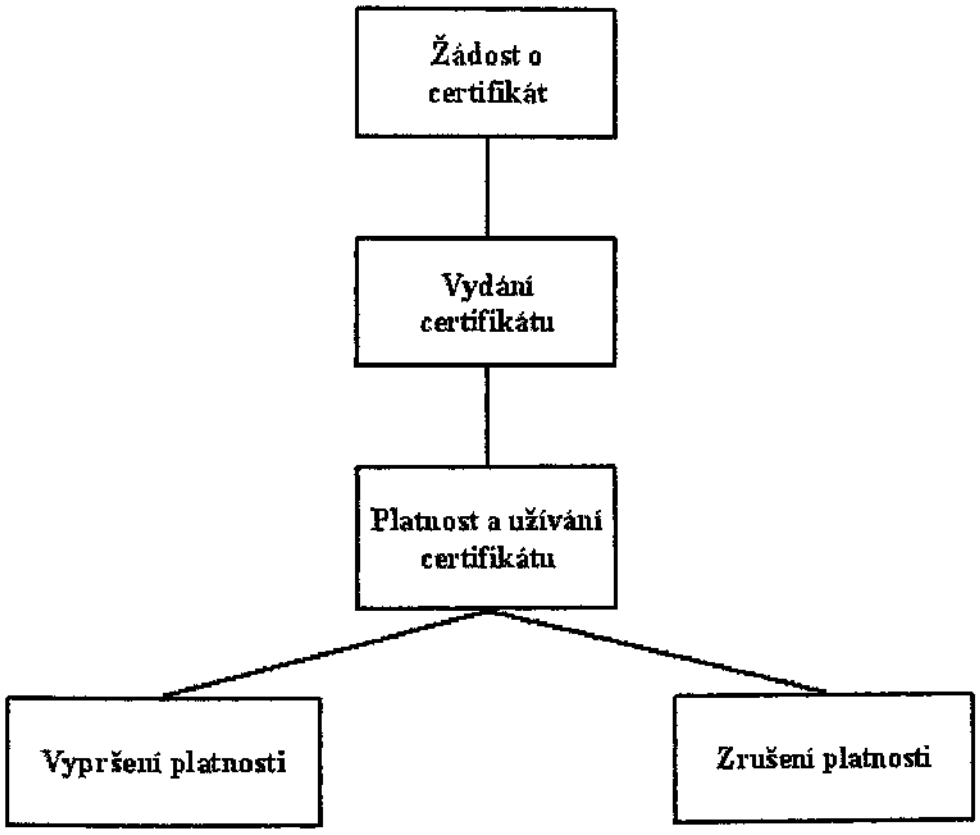

*Obrázek: Ukázka způsobu získání certifikátu. Zdroj: www.ica.cz.*

Doba platnosti certifikátů je omezená a je uvedena v každém certifikátu. Tato veličina je velmi důležitá. Pokrok ve zvyšování výkonnosti výpočetní techniky a možnost objevení mezer v protokolech nebo algoritmech by ve velkém časovém horizontu mohl způsobit, že by se certifikáty staly nespolehlivé. Běžné certifikáty jsou proto vydávány s platností 6 měsíců nebo 1 rok. I během této doby je možné zrušit platnost certifikátu. Důvodem pro toto opatření může být například vyzrazení privátního klíče. Tuto situaci je možné přirovnat ke ztrátě osobních dokladů a následných procedur s tím spojených.[118]

V praxi je možné o zneplatnění certifikátu požádat několika způsoby. Je však nutné brát v úvahu nutnost identifikace žadatele. Tím nejběžnějším způsobem zneplatnění certifikátu je osobní návštěva na RA. Zneplatnit certifikát je však často nutné i mimo pracovní dobu nebo v době a místě, kde jsou RA nedostupná. V tom případě nastupuje elektronická komunikace. K tomuto účelu umožňuje CA podat žádost o zneplatnění pomocí mailu či webu. Identifikace

[118] Viz. Budiš, P., Certifikáty a certifikační autorita, Lancom, č. 7-8, 2000,ISSN 1210-2997.

žadatele je řešena alternativně elektronickým podpisem nebo jiným identifikačním prostředkem, zpravidla jednorázovým heslem.




*Obrázek:. Ukázka životní cyklu certifikátu. Zdroj. www.ica.cz.*

Zrušený certifikát je zařazen do seznamu zneplatněných certifikátů (CRL). Seznam zneplatněných certifikátů je tedy jakási černá listina, na které jsou uvedeny neplatné certifikáty, jejichž doba platnosti ještě nevypršela Tento seznam je obdobou případu seznamu zrušených kreditních karet. Banka nemůže donutit klienta, aby neužíval svou kreditní kartu, stejně jako certifikační autorita nemůže zabránit klientovi v užívání certifikátu. Při každé transakci pomocí certifikátů je možné si pomocí této listiny certifikát ověřit. Seznam zneplatněných certifikátů je veřejně přístupná listina podepsaná certifikační autoritou a chráněná tedy stejně jako certifikát.[119]

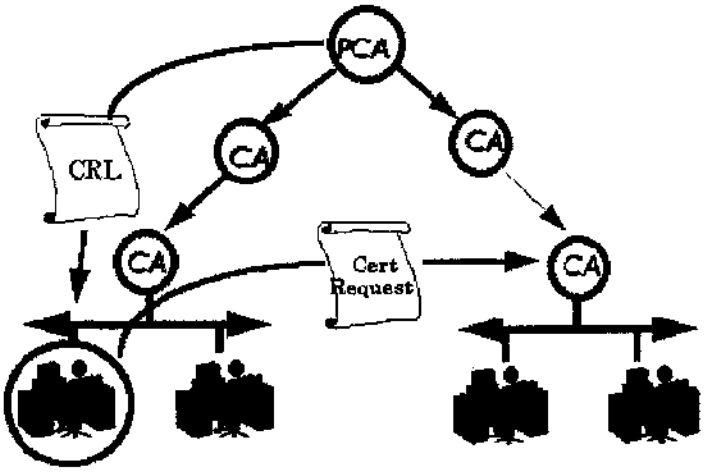
[119] Viz. Budiš, P., Elektronický podpis v praxi, DSM, č.3, 2002, ISSN 1211-8737.

Funkce certifikační autority

Funkce CA lze rozdělit do čtyř základních kategorií:

1. Autentizace a registrace ostatních certifikačních autorit a uživatelů.
2. Uložení a distribuce identifikačních informací.
3. Certifikace a certifikačně správní funkce.
4. Notářské funkce.

Bod 1. poukazuje na autentizační, identifikační a registrační funkce Certifikační autority (CA). CA nemusí existovat samostatně, jak je typické u lokálních sítí typu intranetu, kde se zpravidla jedná o účelové certifikační autority. Ve velkých sítích, zejména internet, může existovat i systém propojených CA. Každý uživatel se může registrovat u CA, kterou si sám vybere, což je výhodné s ohledem na množství uživatelů, různorodé požadavky, jejich topologii a úroveň zabezpečení.




*Obrázek: Ukázka stromové struktury certifikát. Zdroj: www.ica.cz.*

Při zařazení nové CA do stromu nebo síťové struktury CA je třeba vzájemná autentizace a registrace CA. Zpravidla stačí, jestliže nová CA vydá certifikát, a tak projeví důvěru k certifikační autoritě ve struktuře uvedené bezprostředně nad ní, případně certifikační autoritě uvedené bezprostředně pod ní. Nadřízená i podřízená certifikační autorita pak naopak vydají certifikáty této nové CA ( křížová certifikace). Při ověřování podpisu komunikačního partnera je třeba vytvořit certifikační cestu. To v praxi znamená, že první certifikát v řetězci certifikuje veřejný klíč certifikátu, který jej předcházel. Veřejný klíč posledního certifikátu náleží CA, které důvěřuje ověřovatel. Při velké složitosti stromu CA je možné vydání certifikátů i mezi nezvětvenými CA. To výrazně zjednodušuje uživateli ověřování důvěryhodnosti certifikátu komunikačního partnera, certifikovaného u vzdáleného CA, zkrácením certifikační cesty.[120]

Autentizace a registrace jednotlivých uživatelů je problém důvěryhodnosti certifikátů. Různé kvality ověřování identity uživatele určují mimo jiné i důvěru v jeho certifikát.

[120] Viz. Budiš, P., Elektronický podpis v praxi, DSM, č.3, 2002, ISSN 1211-8737.

V nejjednodušší formě zajišťuje CA pouze jedinečnost jména subjektu a nikoliv jeho identitu. Ve vyšším stupni autentizace uživatelů je nutné již zmiňované ověření totožnosti podle osobních dokladů realizované prostřednictvím registračních autorit. Vzájemná komunikace mezi RA a CA musí probíhat po bezpečném kanále (např. bezpečný e-mail).

Při chodu CA vzniká velké množství dat, které je nutno odpovídajícím způsobem zveřejnit a uchovat (bod. 2.). CA zpravidla pro tuto činnost vyžívají adresářové služby. Uložení dat CA bývá zálohováno spolehlivým způsobem. Certifikační autorita i uživatelé uchovávají i data privátního charakteru. Jsou to především privátní šifrovací klíče a certifikát nadřízené (kořenové) CA. Tato data je třeba s ohledem na důležitost a cenu těchto informací chránit před zneužitím nebo dokonce odcizením. Nejjednodušší ochranou je uložení soukromých dat na disku v zašifrované podobě chráněné přístupovým heslem. Obdobně lze tato data uchovávat na disketě, kterou po ukončení práce uložíme na bezpečném místě. V poslední době se stále více užívá k uchování citlivých dat čipová karta chráněná PINem. Odpadá pamatování složitých hesel a jediná karta může umožňovat přístup k několika zařízením. Čipová karta má navíc inteligentní logickou ochranu. Ani tato moderní technologie však zejména u CA s vysokou úrovní bezpečnosti často nestačí. Zde se užívá bezpečné řešení, které odolává jak logickým, tak i fyzickým útokům.

Obsahem bodu 3. je certifikace a certifikačně správní funkce. Certifikační autorita z hlediska uživatele pracuje jako server, který na definovaný formát žádosti odpovídá standardní odpovědí. Nezbytnou součástí žádosti je identifikace žadatele a jeho veřejný klíč. Z bezpečnostních důvodů je žádost podepsaná privátním klíčem, čímž je potvrzena pravost klíče. Opovědí CA na tuto žádost je po nezbytných procedurách vydání standardního certifikátu (X.509, EDI). Kromě standardních certifikátů umožňuje CA i vydávání tzv. rozšířených certifikátů, definovaných v X.509 v.3[121] resp. PKCS #6,[122] které mimo standardní položky obsahují navíc například položku účelu vydání certifikátu, certifikační politiku, alternativní jména a podobně.

Žádost o zneplatnění certifikátu je možné podat několika způsoby a jejich specifikace je přesně určena v příslušných dokumentech (zpravidla Certifikační politice) konkrétní CA. Opovědí na žádost o zneplatnění certifikátu je zneplatnění a vydání nového CRL, případně Delta CRL (X.509 v.3), což je seznam pouze nově zneplatněných certifikátů. Obdobně jako u certifikátů i u CRL je možné vydávat rozšířené CRL, které pak obsahuje například i důvod zneplatnění, datum a podobně.

Vydávání certifikátů se řídí tzv. Certifikační politikou. Ta určuje, za jakých podmínek bude kladně vyřízena žádost o certifikát. Certifikační politika je nedílnou součástí tzv. Bezpečnostní politiky CA, která je určující pro bezpečnost, a tím i důvěryhodnost dané CA.

Poslední 4. funkcí CA je plnění notářských funkcí. Certifikační autorita může vystupovat ve funkci elektronického notáře při ověřování podpisu dokumentů, časového cejchování, případně potvrzování celých transakcí.

Bezpečnost certifikační autority

[121] Jedná se o jeden z nejpoužívanějších typů digitálních certifikátů.
[122] Jedná se o formát, který je obvykle užíván pro zálohování certifikátů.

Bezpečnost CA, která je součástí komunikačního řetězce stejně jako komunikující strany, je velmi důležitá. Nejde však pouze o ochranu privátních dat CA, jako jsou například privátní klíče, ale o celkovou bezpečnost celého systému certifikační autority. Tento problém je složitý, a vzhledem k výše uvedeným funkcím i rozsáhlý. Vysoká úroveň bezpečnosti je na jedné straně tedy žádoucí, na straně druhé však omezuje uživatele CA restriktivními opatřeními. Úkol tedy spočívá v nalezení kompromisu.

Abychom byli schopni posoudit, zda konkrétní CA vyhovuje požadavkům na zabezpečení certifikátů pro vybraný systém, je třeba detailně prostudovat bezpečnostní dokumentaci CA. V souladu s bývalou vyhláškou Úřadu pro ochranu osobních údajů k zákonu o elektronickém podpisu[123] lze definovat základní dokumenty, které by měla mít každá CA. Každá CA by měla mít definovány a popsány tyto dokumenty:

- certifikační politika
- certifikační prováděcí směrnice
- celková bezpečnostní politika
- systémová bezpečnostní politika
- plán zvládání krizových situací a plán obnovy

Je zřejmé, že ne všechny dokumenty nutné pro činnost CA jsou veřejné. Zveřejněny musí být právě dokumenty, které nám, uživatelům, umožní rozhodnout o přijatelnosti CA pro náš účel. Mezi takové dokumenty rozhodně patří certifikační politika. Popis obsahu jednotlivých dokumentů je rozebrán v kapitole věnované legislativě. Pro první posouzení vhodnosti CA je možné vycházet i z dále popsaných kritérií, která vám umožní v krátkosti posoudit některé klíčové body hodnocení.

Deset pohledů na bezpečnost a důvěryhodnost certifikační autority

Tato kritéria jsou použita k popsání některých technických řešení, provozních procedur a úrovně důvěry pro generaci, distribuci, ověřování a použití certifikátů certifikační autority.

*1. Postupy vytváření jednoznačných jmen pro certifikační autority a uživatele*

Zjednodušeně řečeno, certifikát spojuje fyzickou totožnost subjektu s totožností elektronickou. Co to však v tomto případě je fyzická totožnost? Běžně užívané certifikáty (X.509) mají definovánu základní sadu identifikačních položek, jako například jméno, organizace, organizační jednotka, a dále rozšířené položky, jejichž použití je zpravidla nepovinné. Tyto položky se však přesně nekryjí s položkami občanského průkazu nebo obchodního rejstříku. Proto je třeba určit postup, podle kterého budou údaje z průkazů totožnosti transformovány do certifikátů tak, aby v rámci možností poskytovaly jednoznačné údaje identifikující konkrétní subjekt, včetně takových zdánlivých detailů, jako je například transkripce jmen s diakritikou. Certifikát je jednoznačně identifikován vydavatelem a číslem certifikátu. Vydavatelem certifikátu je certifikační autorita. Ta určuje postupy tvorby jednoznačných jmen svých klientů. Zákon o elektronickém podpisu popisuje dva druhy certifikátů, a to certifikát a kvalifikovaný certifikát. Certifikát jako takový není ve vztahu ke

[123] Bývalá vyhláška č.366/2001Sb., Úřadu pro ochranu osobních údajů o upřesnění podmínek stanovených v § 6 a17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu – byla zrušena vyhláškou MIČR č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. V příloze aktuální platné vyhlášky MIČR je také vzor struktury certifikační politiky a certifikační prováděcí směrnice.

konkrétním položkám jednoznačného jména zmiňován, pouze spojuje data pro ověření podpisu s podepisující osobou a umožňuje ověřit její totožnost. Zákon popisuje minimální požadavky na jednoznačné jméno uvedené v kvalifikovaném certifikátu, jméno a příjmení podepisující osoby nebo její pseudonym, případně zvláštní znaky podepisující osoby. Zvláštní kapitolou je postup vzniku jednoznačného jména certifikační autority, zejména té s obecnou působností. Jednoznačná jména certifikačních autorit bude třeba koordinovat, aby nedošlo k duplicitám, ať již úmyslným nebo náhodným. Tato situace je potenciálním bezpečnostním incidentem. Obecně je postup vytváření jednoznačných jmen popsán v dokumentu nazývaném zpravidla certifikační politika.

*2. Pravidla pro ověřování jednoznačných jmen certifikačních autorit a uživatelů*

Certifikáty lze rozdělit na dvě základní skupiny. V té první budou certifikáty, jejichž jednoznačné jméno nepodléhá žádné kontrole a ověření. To jsou především certifikáty pro testovací účely a nemají přílišného praktického využití. Druhou skupinou jsou certifikáty, jejichž položky podléhají kontrole. Tady jsou pravidla pro jednoznačná jména striktně daná. Certifikační autorita zpravidla prostřednictvím svých registračních autorit (RA) kontroluje platnost a pravdivost položek uvedených v žádosti o certifikát. Liší se však, a to mnohdy podstatně, kvalita ověřovací procedury. Mám na mysli zejména požadované doklady nutné k registraci a způsob jejich ověřování. Úroveň kontroly může být různá, od totální benevolence až k obtěžování. Vhodná úroveň tohoto atributu závisí především na účelu, ke kterému certifikáty potřebujeme. V každém případě však důvěryhodná CA musí zajistit možnost určení totožnosti vlastníka certifikátu.

*3. Ověření platnosti žádosti o certifikát*

Procedura vydání certifikátu začíná tvorbou žádosti o certifikát, potom následuje předání žádosti na vybranou certifikační autoritu. Ta žádost zpravidla ověřuje. A nejedná se pouze o ověřování položek jednoznačného jména. Je vhodné provádět pro ochranu žadatele celou řadu kontrol. Většina CA vyžaduje formát, který má obsah žádosti podepsán příslušným privátním klíčem. Tato kontrola zajistí, že žadatel má k příslušnému veřejnému klíči i klíč privátní. Je velmi důležitá a eliminuje značná bezpečnostní rizika. Příkladem dalšího typu kontroly je ověřování, je-li klíč uvedený v žádosti o certifikát jedinečný. Pravděpodobnost, že bude ať již náhodou, či úmyslně vygenerována stejná dvojice kryptografických klíčů, je minimální, přesto některé CA z důvodů vyšší bezpečnosti tuto kontrolu provádějí. Některé certifikační autority navíc zajišťují jedinečnost použitého jednoznačného jména. To sebou samozřejmě nese další kontrolu při podání žádosti a navíc potenciální obtíže při řešení a kontrole obnovovaných certifikátů. Všechny kontroly žádostí o certifikát se odráží v bezpečnostní politice CA a zárukách, které nám konkrétní CA poskytuje.

*4. Postup podepisování certifikátu a ochrana privátního klíče CA a uživatelů*

Po ověření žádosti následuje samotný akt tvorby certifikátu. To v podstatě znamená podepsat privátním klíčem CA položky získané během registrační procedury, a tím stvrdit platnost předchozích kroků. Pro CA je tento krok z bezpečnostního pohledu velice citlivý, protože znamená použití privátního klíče CA, tedy nejlépe střežených dat CA. Ztráta kontroly nad privátním klíčem je největším bezpečnostním incidentem, jaký může nastat. Proto je ochraně

privátních dat CA věnována maximální pozornost. Postup tvorby certifikátů je možný ve dvou módech. Za prvé off-line. Žádost o certifikát je pozastavena na CA a operátor musí dát souhlas k vytvoření certifikátu. Operátor aktivuje privátní klíč CA. Tento postup je obvyklý u CA vyšší úrovně zabezpečení. Jako hardwaru je použito minimálně čipových karet, častěji však zařízení vyšší bezpečnosti (black box). Privátní klíč toto zařízení nikdy neopustí a procedura podpisu probíhá přímo uvnitř tohoto zařízení. Off-line přístup sebou nese problémy v oblasti on-line služeb CA, jako například automatizované tvorby seznamu zneplatněných certifikátů (CRL) nebo služeb, jako je časové razítko. On-line služby jsou procedurálně jednodušší, a proto bývají používány zejména na jednodušších CA. Ochrana privátního klíče u uživatele je zpravidla zcela v kompetenci jeho samotného. Uložení privátního klíče na pevném disku není příliš bezpečné, i když jsou klíče zpravidla uloženy v zašifrované podobě (pomocí symetrické kryptografie). Podstatně bezpečnějším řešením je použití čipové karty se čtečkou nebo podobný systém. Takové řešení není finančně nijak náročné a rozdíl v bezpečnosti privátního klíče je diametrální. Ponecháme-li stranou uzavřené systémy, CA nemá zpravidla prostředky ke kontrole nakládání klienta se soukromým klíčem, tuto otázku však řeší svými ustanoveními přímo Zákon o elektronickém podpisu.

*5. Zneplatnění certifikátů a ověřování certifikátů*

Při potenciálním nebezpečí zneužití privátního klíče nebo i z jiných důvodů je někdy třeba, obdobně jako u platebních karet, zrušit platnost certifikátu. To se děje zpravidla on-line procedurou různými komunikačními kanály. V takovém případě je využívána identifikace heslem, které je dohodnuto již při vzniku certifikátu. Je nedostatečné požadovat pouze elektronicky podepsanou žádost, protože právě ztráta privátního klíče je často důvodem k zneplatnění certifikátu. Jestliže CA akceptuje žádost o zneplatnění, je certifikát zařazen do seznamu zneplatněných certifikátů. Ten je zveřejňován zpravidla nejméně jednou denně. Při každé transakci s použitím certifikátu bychom tedy měli zjišťovat mimo jiné i to, jestli není certifikát našeho komunikačního partnera zneplatněn a nejedná-li se tedy o potenciální útok. Kontrolu platnosti certifikátu je možné provádět dvěma způsoby. Buď kontrolujeme platnost certifikátu proti CRL a pokud tam certifikát není uveden, považujeme ho za platný, nebo se CA přímo dotazujeme na platnost konkrétního certifikátu. Oba způsoby mají své výhody i nevýhody.

*6. Ochrana báze dat a software certifikační autority*

Certifikační autorita je z určitého pohledu softwarový produkt. Po implementaci je třeba zajistit jeho bezproblémovou funkci především stabilizací jednotlivých komponent. Vzhledem k charakteru CA je důležitá minimalizace změn v primárních SW modulech, zejména v operacích s privátním klíčem CA. Případné upgrade nebo rozšíření modulů musí být upraveno vnitřními předpisy. Platí obecná bezpečnostní zásada oddělení implementace od provozu. Certifikační autorita musí uchovávat poměrně značný objem dat a dokumentů. Tato data musí předepsanou formou zveřejňovat, mnohdy po dlouhou dobu. Proto musí být základní dokumenty, jako smlouvy s klienty, identifikační údaje klientů, certifikáty, CRL a podobně chráněny nejen proti modifikaci, ale i proti ztrátě, a to kvalitním archivačním systémem. Pro akreditované certifikační autority je zákonem stanovena doba archivace na 10 let. Data v působnosti CA mají často charakter osobních údajů a jsou tedy navíc chráněna i dalšími zákony.

*7. Kontrola certifikačních autorit*

Největší hodnotou certifikační autority je její důvěryhodnost. Ta se těžko získává, ale velice lehce ztrácí. CA v začátku svého fungování veřejně vyhlásí podmínky, které nabízí svým klientům ve smluvním nebo mimosmluvním vztahu. To se děje zpravidla prostřednictvím certifikační politiky, vzorových smluv a podobně. Tyto dokumenty jsou poté pro CA závazné. Z dikce zákona byl kontrolou CA pověřen nejdříve Úřad pro ochranu osobních údajů a poté Ministerstvo informatiky ČR (dnes MVČR). Platí ale, že horší než pokuta, by pro jakoukoliv certifikační autoritu byla ztráta dobrého jména, což v tomto odvětví znamená prakticky konec.[124]

*8. Směrnice pro uživatele a systémové administrátory certifikační autority*

Součástí dokumentace CA jsou i směrnice a příručky pro uživatele i vnitřní potřebu CA. Dokumentace pro uživatele obsahuje především příručky týkající se tvorby žádosti o certifikát a operací s certifikátem obecně. Zpravidla jsou také k dispozici příručky pro instalaci certifikátu do různých prostředí. Pro bezchybné fungování CA většího rozsahu je nezbytné vytvořit kompletní dokumentaci pro operátory RA, operátory samotné CA a systémové pracovníky. Příručky jsou nezbytné i pro určení pravomocí a povinností pracovníků CA, určení odpovědnosti konkrétních pracovníků za jednotlivé operace CA. Příručky musí být přesné a detailní. Je třeba si uvědomit, že jde v neposlední řadě i o bezpečnostní atribut, protože až 80% útoků na systém je vedeno přímo z vnitřku organizace. Směrnice a příručky pro pracovníky CA jsou neveřejné.[125]

*9. Notářské úkony certifikační autority*

Certifikační autorita může kromě svého hlavního poslání, tedy vydávání certifikátů a funkcí s tím spojených, fungovat jako elektronický notář. Do těchto funkcí lze zařadit například i vydání časového razítka. CA tímto úkonem potvrzuje přesný čas konkrétní operace, například podpisu smlouvy nebo převodu peněz. CA také může nabízet služby důvěryhodné archivace citlivých elektronických dokumentů a podobně. Mnohé z těchto notářských úkonů jsou téměř nezbytné pro bezpečné využívání elektronického oběhu dokumentů v praxi. Zákon o elektronickém podpisu se o notářských funkcích CA nezmiňuje.

*10. Přístupnost služeb certifikační autority*

Dostupnost certifikační autority je jednou z veřejně deklarovaných hodnot. Nejedná se pouze o dostupnost a otevírací dobu RA, ale především o dostupnost CA jako důvěryhodného elektronického zdroje informací. Jde zejména o seznam vydaných a zneplatněných certifikátů. Tyto funkce CA mohou být pro některé operace kritické. Proto je požadována maximální, optimálně nepřetržitá dostupnost. Některé z těchto služeb jsou pro CA vydávající kvalifikované certifikáty přímo předepsány zákonem. Jedná se především o možnost „neprodleně" ukončit platnost certifikátu a dále pak o již zmiňované zveřejnění CRL. Uvedená kritéria nejsou v žádném případě vyčerpávajícím a detailním obrazem funkcí a

[124] Viz. Budiš, P., Elektronický podpis v praxi, DSM, č.3, 2002, ISSN 1211-8737.
[125] Podrobněji např. viz. Šilerová, E. . Znalostný manažment v podnikovom informačnom prostredí, 2006, ISSN 1335-2571. Acta Oeconomica et Informatica, 9, s.47 - 50.

bezpečnosti CA. Je pouze jakýmsi pohledem do problematiky. Při případném výběru konkrétní CA, ať již akreditované nebo neakreditované, vydávající kvalifikované certifikáty nebo jiné, je třeba vidět i ostatní atributy. Zajímavým atributem je počet vydaných certifikátů, počet registračních autorit nebo délka provozu CA. I tyto dílčí údaje mohou poskytnout důležité informace o celkovém postavení firmy na dynamickém trhu ICT.

### *3.5.2. Doporučení Transparency International k elektronizaci soudnictví*

#### *1. Elektronický systém přidělování a vedení případů (Court Management System)*

Předpokladem zavedení je jednak vybavení soudů odpovídající výpočetní technikou, jednak finanční rezervy na zakoupení a zavedení tohoto systému a vyškolení příslušných pracovníků k jeho obsluze.

Jako hlavní výhody zavedení tohoto systému se uvádí zejména[126] 1) výrazné zefektivnění příjmu nového nápadu (slovenské zdroje uvádějí, že zaevidování nového případu trvá soudnímu úředníkovi cca 3 min.) a 2) vyloučení voluntaristického přidělování případů jednotlivým soudcům (současný systém přidělování případů podle schváleného rozvrhu práce by sice takovou manipulaci měl vyloučit, záleží ovšem právě na kvalitě příslušného rozvrhu).

#### *2. Digitalizace vedení soudní agendy jako kontrola nakládání s důkazy*

Digitální nahrávání průběhu všech jednání. Pro úsporu v souvislosti s aktuálními problémy trestního řízení lze uvažovat o přepisování záznamu do písemné podoby pouze na žádost účastníka a za poplatek (jak je tomu např. u kopírování listin ze spisu). Naopak by účastník vždy měl nárok na obratem pořízenou elektronickou kopii zvukového záznamu. Takový krok např. v oblasti občanského soudního řízení by především zvýšil přesnost uchování důkazů i rozhodných okolností vlastního jednání a především znovu vedl ke kontrole, že to, co se odehrálo v soudní síni, je prokazatelně uchováváno. Konečně by v rámci do důsledku dovedeného institutu veřejnosti soudního jednání bylo veřejnosti dáno právo vyžádat si elektronický zvukový záznam jednání.[127]

#### *3. Hodnocení práce soudců (státních zástupců) a jejich veřejná kontrola prostřednictvím podrobných soudních statistik přístupných elektronicky*

Zveřejňovat podrobné soudní statistiky, a to tak, aby nejen orgán dohledu (ministerstvo), ale i veřejnost mohly na základě sledovaných údajů alespoň přibližně poměřovat (s výhradou, že každý případ je samozřejmě jiný) výkonnost jednotlivých soudů a soudců, a to především z hlediska délky určitých typů řízení a procenta vyššími instancemi rušených rozhodnutí.

[126] Zdroj a podrobněji viz. www.transparency.cz (Transparency International Česká republika), Vybrané obecné protikorupční nástroje v soudnictví.
[127] Zdroj a podrobněji viz. www.transparency.cz (Transparency International Česká republika), Vybrané obecné protikorupční nástroje v soudnictví.

Veřejnost statistik bude především motivovat dotčené osoby k vystříhání se zbytečným průtahům a nestandardním postupům všude tam, kde to je možné.[128]

### *3.5.3. Elektronický evropský soudní atlas ve věcech občanských*

Atlas poskytuje snadný přístup k informacím důležitým pro soudní spolupráci ve věcech občanských. Díky Atlasu je možno snadno najít příslušné soudy nebo orgány, ke kterým v některých záležitostech můžete podávat své žádosti. Dále můžete rovněž vyplňovat formuláře, které jsou za tímto účelem připraveny on-line, měnit jazykovou verzi formuláře poté, kdy jste jej vyplnili a než jej vytisknete (tak, aby osoba, která formulář přijme, byla schopna jej přečíst ve svém vlastním jazyce), a formuláře elektronickou cestou zasílat.

Atlas je k dispozici v české jazykové verzi zde:

*http://ec.europa.eu/justice_home/judicialatlascivil/html/index_cs.htm*

### *3.5.4. Elektronická evropská soudní síť v občansko-právních a obchodních záležitostech*

Tyto stránky spravuje Evropská komise a jsou pravidelně aktualizovány v úzké spolupráci s členskými státy Evropské unie. Najdete zde velké množství informací o členských státech, o právu Společenství, evropském právu a různých tématech občanského a obchodního práva.

Stránky jsou k dispozici v českém jazyce zde:

*http://ec.europa.eu/civiljustice/index_cs.htm*

### *3.5.5. Rozhodčí řízení online (mimosoudní způsob řešení sporů)*

#### *1. Obecně*

Rozhodčí řízení v České republice je upraveno zákonem č. 216/1994 Sb., o rozhodčím řízení a o výkonu rozhodčích nálezů. S přijetím zákona o rozhodčím řízení se značně rozšířila oblast možného rozhodování sporů touto cestou mimo státní soudy, neboť současná právní úprava umožňuje rozhodovat v rozhodčím řízení veškeré spory majetkové povahy s výjimkou sporů vzniklých v souvislosti s výkonem rozhodnutí a sporů vyvolaných prováděním konkurzu nebo vyrovnání, pokud se strany těchto sporů na tom dohodnou.

Tradiční oblastí rozhodování sporů cestou rozhodčího řízení však zůstává především obchodní oblast. Rozhodčí řízení může probíhat jako řízení před jedním nebo více rozhodci jmenovanými stranami sporu pro tento konkrétní spor (řízení „ad hoc") nebo může mít

[128] Zdroj a podrobněji viz. www.transparency.cz (Transparency International Česká republika), Vybrané obecné protikorupční nástroje v soudnictví.

podobu řízení před institucionálním rozhodčím soudem založeným na základě zákona (rozhodčí řízení institucionální).

Výhody rozhodčího řízení spočívají také v tom, že rozhodčí nález je snáze vykonatelný,[129] protože Newyorská úmluva z roku 1958 umožňuje uznání a výkon rozhodčích nálezů ve více než 130 státech světa.[130]

### 2. *Online rozhodčí řízení (Česká asociace pro arbitráž)*

Při této formě rozhodčího řízení většina písemného styku mezi rozhodcem a stranami probíhá prostřednictvím internetu. Česká asociace pro arbitráž zřizuje pro každý konkrétní spor elektronické sudiště, které je unikátní adresou, přičemž do sudiště mají přístup pouze rozhodce a strany sporu, podobně jako je tomu u soudního spisu. Přístup do sudiště je šifrován, čímž je zajištěn bezpečný přístup všech účastníků do sudiště. Výhody online rozhodčího řízení jsou především v tom, že veškeré dokumenty jsou doručovány v zásadě pouze elektronickou cestou do e-mailových schránek stran sporu a dále zveřejněny /vyvěšeny/ v sudišti. Rozhodnutí arbitra se doručují podepsané zaručeným elektronickým podpisem a zveřejňují v sudišti, přičemž jeho umístěním do elektronického sudiště a uplynutím stanovené lhůty se stávají pravomocnými a vykonatelnými. Podrobná pravidla Online rozhodčího řízení naleznete v Článku IX. Rozhodčího řádu.[131]

### 3. *Online rozhodčí řízení (Rozhodčí soud při HK ČR a AK ČR)*

Rozhodčí řízení online u Rozhodčího soudu při HK ČR a AK ČR umožňuje, aby všechna podání stran byla činěna elektronickou formou, aby řízení bylo vedeno elektronickou formou a aby rozhodčí nález byl vydán elektronickou formou, prostřednictvím Internetu.[132] Administračním místem se rozumí adresa Rozhodčího soudu pro rozhodčí řízení on-line na adrese (stránce) Internetu www.arbcourtonline.cz, prostřednictvím kterého mohou účastníci rozhodčího řízení zahájit rozhodčí řízení podle rozhodčího řádu on-line[133] a hradit veškeré poplatky, spojené s vedením rozhodčího řízení on-line u Rozhodčího soudu. Administrační místo zveřejňuje rovněž pravidla o nákladech rozhodčího řízení on-line; vydává pokyny o formátech podání, jakož i další důležité informace pro postup v rozhodčím řízení podle řádu on-line. Úkony administračního místa jsou úkony tajemníka Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky.

Sudiště potom znamená unikátní adresu (stránku) Internetu, zřízenou u administračního místa výlučně pro vedení konkrétního sporu, pro podání účastníků řízení, jakož i pro veškerá rozhodnutí rozhodce a uchovávání všech písemností v elektronické podobě, souvisejících se sporem. Přístup na sudiště je umožněn jen účastníkům řízení a Rozhodčímu soudu.

---

[129] Rozhodčí nález je současně exekučním titulem využitelným pro zahájení exekučního řízení podle zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) v případě, že povinná strana rozhodnutí rozhodčího soudu nerespektuje a neplní.

[130] Text úmluvy a signatářské státy jsou k dispozici na stránkách Rozhodčího soudu při HK ČR a AK ČR – www.arbcourt.cz.

[131] http://www.spory-online.cz/?article=pravidla-rizeni.

[132] Rozhodčí řády a pravidla jsou k dispozici zde: www.arbcourt.cz.

[133] Zvláštní dodatek Řádu pro rozhodčí řízení on-line (Řád on-line) - www.arbcourt.cz.

V souladu s rozhodčím řádem online se za písemnou formu nepovažují jen písemnosti ve své listinné podobě, ale též forma „elektronického záznamu" jakožto formy písemností, které zahrnují jakoukoli formu záznamu včetně datové zprávy.

Řád on-line omezuje účastníky řízení i rozhodčí soud využít výhradně komunikačních prostředků Internetu. Veškerá podání a písemnosti v řízení musí být doručovány touto formou. Není-li to technicky možné, může rozhodce připustit jinou formu. Rozhodčí soud je ale oprávněn rozhodnout, že rozhodčí řízení nebude vedeno podle řádu on-line v případech, kdy účastník řízení není, zejména po technické stránce, zjevně schopen účastnit se rozhodčího řízení podle řádu on-line, jakož i ve všech ostatních případech, kdy rozhodčí soud dojde k závěru, že rozhodčí řízení nemůže být podle řádu on-line vedeno. Rozhodčí soud o tom vydá usnesení. Dnem vydání tohoto usnesení je rozhodčí řízení dále vedeno podle řádu ve své klasické (neelektronické) podobě. Všechny dosud řádně učiněné úkony ale zůstávají v platnosti. Do ustavení rozhodce je oprávněn k vydání tohoto usnesení předseda Rozhodčího soudu.

Žalobce zahajuje rozhodčí řízení on-line podáním žaloby na administrační místo. Žaloba má náležitostí podle § 17 Řádu a musí obsahovat:

- odkaz na sjednanou rozhodčí smlouvu o vedení sporu elektronickou cestou;
- označení důkazů;
- e-mailovou adresu žalobce, pro komunikaci s Rozhodčím soudem pro účely rozhodčího řízení;
- poslední známou platnou e-mailovou adresu žalovaného; a
- poštovní adresy, telefonní a faxová čísla účastníků řízení (žalobce i žalovaného).

Po zaplacení poplatku za rozhodčí řízení posoudí rozhodčí soud, zda žaloba splňuje podmínky řádu on-line. Poté rozhodčí soud vytvoří do pěti pracovních dnů sudiště a zpřístupní tak žalobu účastníkům řízení. Rozhodčí soud současně sdělí účastníkům řízení e-mailovou adresu sudiště, jakož i přístupové parametry (login a heslo) k sudišti. Ve lhůtě deseti dnů ode dne vyrozumění žalovaného o vytvoření sudiště má žalovaný právo vyjádřit se k žalobě v žalobní odpovědi.

Rozhodčí nález podepisuje rozhodce v souladu s § 2 pís. b), § 3 a § 4 zákona č. 227/2000 Sb., o elektronickém podpisu. Rozhodčí soud vydá rozhodčí nález jeho uveřejněním na sudišti. Rozhodčí nález se považuje za vydaný dnem jeho uveřejnění na sudišti. Toto datum musí být uvedeno v rozhodčím nálezu, jakož i v oznámení o vydání rozhodčího nálezu prostřednictvím e-mailu, zaslaného účastníkům řízení. Sudiště musí zůstat přístupné účastníkům řízení třicet kalendářních dní ode dne vydání rozhodčího nálezu. Po uplynutí této lhůty bude sudiště znepřístupněno. Na žádost účastníka mu rozhodčí soud vydá rozhodčí nález také v listinné podobě. Podpis tajemníka na rozhodčím nálezu v listinné podobě ověřuje jeho pravost, jakož i podpis rozhodce.

### *3.5.5. Elektronický formulář pro evropský zatýkací rozkaz (trestní řízení)*

Dle Rámcového rozhodnutí o evropském zatýkacím rozkazu („EZR") a postupech předávání mezi členskými státy je EZR „soudní rozhodnutí, které vydal některý členský stát proto, aby

jiný členský stát zatkl a předal hledanou osobu za účelem trestního stíhání, výkonu trestu odnětí svobody nebo ochranného opatření" (čl. 1 odst. 1 Rámcového rozhodnutí). Smyslem EZR je maximálně zjednodušit a zrychlit proceduru předávání hledaných osob mezi členskými státy a kompenzovat tak neomezený pohyb přes vnitřní hranice. Je třeba zdůraznit, že EZR zcela nahrazuje dosavadní multilaterální úmluvy o vydávání.

EZR byl přijat Rámcovým rozhodnutím o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy (2002/582/5VV) OJ No.L 190/1-18, které bylo přijato Radou EU dne 13. 6. 2002 a které vstoupilo v platnost 7. 8. 2002. V ČR bylo Rámcové rozhodnutí do právního řádu implementováno novelou trestního řádu zákonem č. 539/2004 Sb., s účinností od 1. 11. 2004 (zák. č. novelizující trestní řád).

Přínos EZR ve srovnání s mezinárodním zatýkacím rozkazem:[134]

- proces vydávání (extradice) z jednoho státu druhému (na úrovni výkonné moci) je nahrazen předáváním (surrender) mezi justičními orgány - je tedy vyloučena účast výkonné moci (ministra spravedlnosti) na rozhodování o předání (kromě střetu evropského a mezinárodního zatýkacího rozkazu, kde rozhoduje příslušný orgán, tj. zpravidla ministr spravedlnosti);
- uplatňuje se zásada vzájemného uznávání, tj. dožádaný orgán nezkoumá trestní řízení vedené dožadujícím státem - pouze posuzuje splnění podmínek pro realizaci EZR;
- dochází k významnému omezení zásady oboustranné trestnosti - u vyjmenovaných 32 druhů trestných činů (Čl. 2 odst. 2 Rámcového rozhodnutí popř. §412 odst. 2 trestního řádu) s horní hranicí sazby nejméně 3 roky dožádaný stát neposuzuje trestnost podle vlastního práva - toto opatření má v praxi zásadní význam především z hlediska promlčení trestného činu (loupež či vražda je trestná ve všech členských státech, promlčecí lhůty se zásadním způsobem liší);
- za stanovených podmínek je možno k trestnímu stíhání předat i vlastního občana - není tedy již možné se před spravedlností skrývat v domovském státě, výrazně se zjednodušuje stíhání nadnárodních organizovaných skupin zločinců (trestní řízení je možno vést proti všem pachatelům v jednom státě);
- jsou stanoveny pevné lhůty pro justiční orgány k rozhodnutí o předání (60 dní od zadržení - s možností prodloužit až o 30 dní; 10 dní, souhlasí-li předávaná osoba) i k samotné realizaci (10 dní od právní moci rozhodnutí o předání) - dochází tak k výraznému zkrácení předávací procedury i k redukci předběžné a předávací vazby, což znamená menší zásah do práv předávané osoby (při nedodržení lhůty na předání musí být osoba propuštěna)
- zavedení jednotného jednoduchého formuláře - zásadně se zjednodušuje administrativní a překladatelská složka (veškeré oficiální jazykové mutace formuláře jsou soudům dostupné v elektronické podobě)
- využití Schengenského informačního systému (SIS) k šíření EZR s tím, že záznam v SIS je roven originálu EZR.

Rychlost přijetí Rámcového rozhodnutí bohužel způsobila, že řada jeho nedostatků nebyla odstraněna a praxe se s nimi nyní nepříjemně potýká. Z těchto nedostatků je možno například uvést:[135]

- nejednotné lhůty pro doručení originálu EZR v rozpětí 24 hodin - 40 dní

[134] Zdroj: Ministerstvo vnitra ČR. www.mvcr.cz.
[135] Zdroj: Ministerstvo vnitra ČR, www.mvcr.cz.

- nejednotný jazykový režim
- nemožnost zadržet osobu bez předchozího zaslání originálu EZR v některých státech
- problémy s předáváním vlastních občanů v některých státech

## 3.6. Elektronizace soudních agend a ochrana osobních údajů

### *3.6.1. Právní kvalifikace pojmu osobní údaj*

Osobním údajem je laicky řečeno jakákoliv informace o fyzické osobě, která ji umožňuje identifikovat. Zákon č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ) se vztahuje pouze na údaje o žijících fyzických osobách.[136]

ZOOÚ definuje v § 4 písmeno a) pojem osobní údaj takto: *„osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu".*

Důležité je upozornit na to, že nelze zaměňovat pojem „osobní údaj" a pojem „projev osobní povahy", jak je upraven v § 11 a dalších občanského zákoníku. Jde o dva samostatné právní instituty, přičemž však projev osobní povahy může za určité situace obsahovat osobní údaj (např. podobizna, písemnost osobní povahy nebo zvukový projev) a za takové situace dochází k jejich překrývání.

Podle výše uvedené definice tedy lze odvodit, že pokud fyzická osoba může být přímo ze shromážděných údajů nebo na jejich základě jiným způsobem identifikována, pak tyto údaje jsou údaji osobními. Znakem osobního údaje tedy je, že vypovídá o subjektu údajů,[137] který nelze zaměnit s jiným subjektem údajů. Definice osobního údaje je velmi široká, což ostatně vyplývá z rozmanitosti zpracovávání osobních údajů v praktickém životě, a bezpochyby se nevyhne aplikačním obtížím. Definice je však zásadní pro správce,[138] aby vyhověli požadavkům zákona a základním principům ochrany osobních údajů. Na definici osobních údajů není možné pohlížet izolovaně, bez znalosti dalších okolností zpracování osobních údajů.[139]

Při zpracování údajů o právnických osobách se nepostupuje podle ZOOÚ, ale údaje o právnické osobě jsou chráněny podle příslušných ustanovení obchodního zákoníku (např.

[136] Podrobněji viz Úřad pro ochranu osobních údajů k problémům z praxe - č. 1/2001.
[137] Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují (§4 ZOOÚ).
[138] Správcem je dle zákonné definice každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak (§4 ZOOÚ).
[139] Zpracováním osobních údajů se rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace (§4 ZOOÚ).

obchodní jméno-firma, obchodní tajemství), popřípadě občanského zákoníku (§ 18 a související - obecná právní úprava právnických osob). ZOOÚ se vztahuje pouze na údaje o žijících fyzických osobách.

### *3.6.2. Používání rodného čísla v elektronických databázích*

Rodná čísla se často používají jako základní identifikátor v rámci nejrůznějších elektronických aplikací.[140] Je to totiž jedinečný identifikátor, jeden z mála osobních údajů, které člověk během svého života nemění. Z toho důvodu bylo ostatně před lety zavedeno a používáno především pro účely sociálního zabezpečení. Postupně se rodné číslo stalo vhodným identifikátorem i pro jiné oblasti státní správy. Jeho výhody vyniknou zejména v souvislosti s přechodem manuálně vedených evidencí do počítačových informačních systémů. Většina z nich je totiž nastavena tak, aby se po zadání vstupního prvku – a bývá jím právě rodné číslo – zobrazila celá složka konkrétního subjektu údajů (chcete-li, konkrétní osoby). Otázka používání rodného čísla není ZOOÚ (101/2000 Sb.) speciálně upravena. V tomto ohledu se nejedná dokonce ani o citlivý údaj podle § 4 písmeno b) ZOOÚ. Přesto je svým způsobem rodné číslo osobním údajem do jisté míry výjimečným.[141]

Z výše uvedeného je však také zřejmé, jaké jsou nevýhody rodného čísla jako jednoznačného identifikátoru. Vzhledem ke značnému množství evidencí, do kterých je jedinec v moderním informačním světě zařazen, hrozí potenciální nebezpečí, že nesprávným nebo naopak záměrným užitím rodného čísla budou neoprávněným osobám zpřístupněny informace, ke kterým by se za jiných okolností dostat neměly a nemohly.

Vzhledem k tomu, že informační systémy dnes kromě státních institucí provozují i veřejnoprávní či zcela soukromé organizace je evidentní, že s nabízenou výhodou rodného čísla ve vztahu k uloženým souborům osobních údajů se tito správci chtějí jen těžko loučit. S postupující harmonizací českého právního řádu s právem Evropské unie však budou do nových právních předpisů (a do novel stávajících) upravujících zpracování osobních údajů implementována ustanovení důsledně upravující jak kategorie, tak rozsah osobních údajů. Dokud tento proces neskončí, je třeba vycházet z obecné právní úpravy – zákona č.101/2000 Sb., ve znění pozdějších předpisů. Stěžejním ustanovením pro tento účel je § 5, který stanoví povinnosti správce. Odpověď na otázku užívání rodného čísla je třeba hledat v negativním vymezení v odstavci 1, písmeno d) – správce je povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Většina správců by podle výše uvedené zákonné definice nezbytnost shromažďovat rodná čísla pravděpodobně neobhájila.

[140] Pro základní identifikaci občanů - obyvatel České republiky v rámci informačních systémů veřejné správy se dosud v převážné míře využívá rodné číslo. Není však bezvýznamovým identifikátorem (obsahuje datum narození, pohlaví a v některých ročnících lze dokonce odvodit i informaci o místu narození) a platnost jeho stávající struktury je omezena datem 31. prosince 2053. Do 1. ledna 1954 za lomítkem u rodného čísla následovaly jen tři cifry, poté přibyla čtvrtá číslice, která slouží ke kontrole platnosti, jako kontrolní číslice. Jelikož je rok narození v rodném čísle uveden pouze dvoumístně, rodné číslo přestane být roku 2054 jednoznačné (do té doby lze starší rodná čísla poznat podle jejich délky).

[141] Podrobněji viz Úřad pro ochranu osobních údajů k problémům z praxe č. 4/2002 - používání rodného čísla.

### *3.6.3. Elektronické zpracování osobních údajů zemřelých osob*

Zákon o ochraně osobních údajů nestanoví přechod práv subjektu údajů po jeho úmrtí na jiné osoby. Z toho vyplývá, že po úmrtí subjektu údajů pozbývají platnosti ta ustanovení ZOOÚ, v nichž subjekt údajů vystupuje jako účastník občanskoprávních vztahů, tedy ustanovení o právech subjektu údajů a povinnostech správce ve vztahu k subjektu údajů. Konkrétně jde především o ustanovení § 5 odst. 2 a 5 (souhlas se zpracováním osobních údajů), § 9 a) (souhlas se zpracováním citlivých údajů), § 11 a § 12 (informační povinnost správce) a § 21 – § 24 (ochrana práv subjektu údajů a náprava nemajetkové újmy), kde právo požadovat nápravu při porušení povinností správcem nebo zpracovatelem dává zákon pouze subjektu údajů.[142]

Naproti tomu při zpracování osobních údajů zemřelých osob zůstávají v platnosti ta ustanovení ZOOÚ, v nichž subjekt údajů jako účastník občanskoprávních vztahů nevystupuje a jejichž působnost je relativně nezávislá na skutečnosti, zda subjektem údajů je žijící nebo již zemřelá osoba. Jedná se především o některé povinnosti správce osobních údajů.

V prvé řadě jde o ustanovení § 5 odst. 1, v němž jsou stanoveny náležitosti účelu zpracování osobních údajů. V praxi zde mohou nastat dva případy:

(1) V prvém případě správce zpracovává údaje žijící osoby. Podle písm. a) cit. ustanovení je povinen stanovit účel zpracování. Dojde-li k úmrtí tohoto subjektu údajů a nedostane-li správce tuto informaci ihned, zjistí ji po určitém čase sám, protože je podle písm. c) povinen ověřovat, zda jsou údaje pravdivé a přesné s ohledem na stanovený účel. Podle písm. e) je pak povinen uchovávat údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Tento účel mohl, ale nemusel, smrtí subjektu údajů pominout. Nepomíjí zpravidla v tom případě, že z charakteru zpracování vyplývá zákonný přechod práv a povinností na jiné osoby (například osobní údaje klienta banky zpracovávané podle § 41c odst. 3 písm. a) zákona č. 21/1992 Sb.), nebo jde o uplatnění zákonných práv či plnění zákonných povinností samotného správce (např. uchování účetních dokladů). Pokud účel zpracování smrtí subjektu údajů pominul (např. nabízení obchodu a služeb), je podle § 20 odst. 1 zákona o ochraně osobních údajů správce povinen provést likvidaci osobních údajů.

(2) V druhém případě jsou shromažďovány osobní údaje již zemřelé osoby. I v tomto případě je nutno stanovit účel jejich zpracování a dodržovat další ustanovení § 5 odst. 1. Podle písm. f) je možno tyto údaje zpracovávat pouze v souladu s účelem, k němuž byly shromážděny. Tedy např. pohřební službou pro účely zajištění pohřbu zemřelého, krematoriem pro evidenci lidských pozůstatků a ostatků podle § 15 odst. 2 zákona č. 256/2001 Sb., o pohřebnictví, nebo pro evidenci související s provozováním veřejného pohřebiště podle § 21 zákona č. 256/2001 Sb.

V nesouladu se stanoveným účelem, a tedy v rozporu se zákonem, by bylo, kdyby tito správci volně předali osobní údaje zemřelých osob například někomu, kdo by chtěl získat kontakt na pozůstalé a využít jejich duševního rozpoložení po ztrátě blízké osoby k vlastnímu obohacení, nebo se chtěl nezákonným způsobem obohatit na úkor dědiců.

---

[142] Podrobněji viz Úřad pro ochranu osobních údajů k problémům z praxe 7/2002 - zpracování osobních údajů zemřelých osob.

V platnosti zůstávají pro zpracování osobních údajů zemřelých i další ustanovení zákona o ochraně osobních údajů, v nichž subjekt údajů nevystupuje jako účastník občanskoprávních vztahů, tedy povinnosti osob při zabezpečení osobních údajů podle § 13 – 15.

Subjekt údajů není účastníkem občanskoprávního vztahu ani při plnění oznamovací povinnosti správcem podle § 16, teoreticky tedy i toto ustanovení zůstává v platnosti pro zpracování osobních údajů zemřelých. V praxi však u takového zpracování lze téměř vždy uplatnit některé z liberačních ustanovení podle § 18. Buď jde o zpracování uložené zákonem (např. zákonem č. 256/2001 Sb., o pohřebnictví, zákonem č. 97/1974 Sb., o archivnictví, ve znění pozdějších předpisů, uchovávání účetních dokladů podle § 11 zákona č. 563/1991, o účetnictví, ve znění pozdějších předpisů) nebo je zpracování třeba k uplatnění práv vyplývajících ze zvláštních zákonů (řada zákonů, z nichž vyplývá právo či povinnost archivovat dokumenty s osobními údaji) nebo jde v souladu s § 5 (1) e) o uchování osobních údajů pro archivní či statistické účely subjektů uvedených v § 18 c). Zákon č. 101/2000 Sb. se samozřejmě podle ustanovení § 3 (3) nevztahuje na zpracování osobních údajů zemřelých osob, které provádí fyzická osoba výlučně pro osobní potřebu.

### *3.6.4. Kontrola práce zaměstnance prostřednictvím telekomunikační techniky, ochrana soukromí a osobních údajů zaměstnance*

#### *1. Právo na soukromí v pracovněprávních vztazích*[143]

Pracovně právní předpisy otázku ochrany soukromí zaměstnance, popř. ochranu osobnostních práv zaměstnance v podstatě neřeší. Zákoník práce[144] obsahuje pouze kusovitou úpravu a stanoví, že zaměstnavatelé jsou povinni zajišťovat rovné zacházení se všemi zaměstnanci, pokud jde o jejich pracovní podmínky včetně odměňování za práci a jiných peněžitých plnění a plnění peněžité hodnoty, odbornou přípravu a příležitost dosáhnout funkčního nebo jiného postupu v zaměstnání. Tedy zákaz diskriminace a ponižování a stanovení principu rovnosti zacházení se všemi zaměstnanci. Dále zákoník práce v obecné rovině stanoví, že příslušné odborové orgány mají právo vykonávat u zaměstnavatelů kontrolu nad dodržováním pracovněprávních předpisů, vnitřních předpisů a závazků vyplývajících z kolektivních smluv. Přitom jsou obvykle oprávněny zejména:

- vstupovat na pracoviště zaměstnavatelů,
- vyžadovat od vedoucích zaměstnanců potřebné informace a podklady,
- podávat návrhy ke zlepšování pracovních podmínek,
- vyžadovat od zaměstnavatelů a orgánů jim nadřízených, aby dali pokyn k odstranění zjištěných závad,
- navrhovat zaměstnavatelům, orgánům jim nadřízeným a jiným orgánům pověřeným kontrolou dodržování zákonnosti v pracovněprávních vztazích, aby podle příslušných předpisů použili vhodných opatření vůči vedoucím

[143] *„Předpokládalo se, že sledují každého neustále. A rozhodně mohli zapnout Vaše zařízení, kdy se jim chtělo. Člověk musel žít – a žil, ze zvyku, který se stal pudovým v předpokladu, že každý zvuk, který vydá, je zaslechnut, a každý pohyb, pokud není tma, zaznamenán.“*, Goerge Orwell, citát z románu 1984.

[144] Upozorňuji, že byl přijat nový zákoník práce (zákon č. 262/2006 Sb. s účinností od 1.1.2007) a jsou možné změny ve výkladu relevantních ustanovení. Na stránkách Ministerstva práce a sociálních věcí ČR je k dispozici „Příručka pro personální a platovou agendu“ - www.mpsv.cz/ppropo.php.

zaměstnancům, kteří porušují pracovněprávní předpisy nebo povinnosti vyplývající pro ně z kolektivních smluv,

- vyžadovat od zaměstnavatelů, popřípadě od orgánů jim nadřízených zprávy o tom, jaká opatření byla učiněna k odstranění závad zjištěných při výkonu kontroly nebo k provedení návrhů, které podaly odborové orgány vykonávající tuto kontrolu.

Takováto úprava je nedostatečná a proto je třeba podpůrně použít úpravu z jiných zákonů (tzv. analogie legis nebo analogie iuris). Zde půjde především o občanský zákoník (ObčZ), který upravuje ochranu osobnosti fyzických osob. Zákon říká, že každý má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.[145] Stejně tak je dále stanovena zákonem zásada, že písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.[146] Svolení ale není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona.[147] Tato úprava se vztahuje i na pracovněprávní vztahy, jak již bylo řečeno, protože i na pracovišti musí být chráněna osobnostní práva zaměstnance.

### 2. *Ochrana osobních údajů*

Z hlediska pracovněprávních vztahů je dále významný zákon o ochraně osobních údajů.[148]

Mezi základní povinnosti zaměstnavatele ve vztahu k zákonu o ochraně osobních údajů bude patřit:[149]

- shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,
- uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné.
- zpracovávat pouze přesné osobní údaje, které jsou získané v souladu se zákonem. Je-li to nezbytné, je třeba osobní údaje aktualizovat.
- až na zákonné výjimky zpracovávat osobní údaje pouze se souhlasem zaměstnance[150]
- přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

---

[145] § 11 ObčZ
[146] § 12 ObčZ
[147] § 12, odst. 2, tzv. zákonná úřední licence
[148] zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „ZOOÚ")
[149] § 5, odst. 1 ZOOÚ
[150] Takovou výjimkou by např. byl případ, kdy by šlo o zpracování výlučně pro účely archivnictví podle zvláštního zákona

Novela zákona o ochraně osobních údajů č. 439/2004 dále zasáhla i do znění § 11 (informační povinnosti správce osobních údajů) a zejména § 12, kde je nově stanoveno, že pokud požádá subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.

### 3. *Svobodný přístup k informacím*

Dalším zákonem, který se použije při stanovení meze ochrany soukromí v pracovněprávních vztazích, je zákon o svobodném přístupu k informacím.[151] Tento zákon upravuje podmínky práva svobodného přístupu k informacím a stanoví základní podmínky, za nichž jsou informace poskytovány. V souvislosti s tímto zákonem se např. v minulosti zaměstnanci domáhali informace o výši mzdy svého nadřízeného. K tomuto problému se ve svém stanovisku[152] vyjádřil i Úřad pro ochranu osobních údajů a stanovil, že zaměstnavatel má pro plnění svých úkolů právo používat a případně i jiným osobám sdělovat ty osobní údaje zaměstnance, které se týkají výlučně jeho pracovních aktivit a zjevně nevypovídají o jeho soukromém životě, za podmínky, že zaměstnavatel dodrží všechny povinnosti, uložené mu zákony (např. zákoník práce). Zaměstnavatel tak může, pokud je to potřebné k plnění jeho úkolů, např. bez souhlasu zaměstnance sdělit jeho jméno a příjmení, akademický titul, funkční zařazení, kontaktní údaje zaměstnance na jeho pracoviště (číslo telefonu, faxu, adresu elektronické pošty). Jinak je tomu však, pokud jde o přesnou výši platu, mzdy a odměny. Finanční částka, kterou zaměstnanec při výplatě obdrží, je osobním údajem, jehož zveřejnění je třeba plně podřídit režimu zákona o ochraně osobních údajů. Zaměstnavatel však bez souhlasu jednotlivých zaměstnanců může zveřejnit např. informaci o celkové výši odměn vyplacených v organizaci nebo jejím úseku. Pokud z této informace není určitelné, jaké konkrétní částky byly vyplaceny jednotlivým pracovníkům, není tento údaj údajem osobním a zákon o ochraně osobních údajů se tak na něj samozřejmě nevztahuje.

Zaměstnavatel tedy je na jednu stranu povinen chránit osobní údaje a soukromí zaměstnanců (zákon o ochraně osobních údajů), na druhé straně ale nemůže svévolným výkladem zákona bránit veřejnosti získat údaje, na které má veřejnost právo. Zákon se vztahuje především na stát jako zaměstnavatele. Konkrétně povinnost informace poskytnout, které se k jejich působnosti vztahují, mají státní orgány, orgány územní samosprávy a veřejné instituce hospodařící s veřejnými prostředky.

### 4. *Právo kontrolovat korespondenci zaměstnance obecně*

V některých velkých (nadnárodních) společnostech je takřka pravidlem, že pošta – korespondence zaměstnanců je kontrolována. Takovýto postup je právně mimořádně sporný a může být spatřen protiprávním, resp. dokonce může dojít i k naplnění skutkové podstaty některého z trestných činů (viz dále). První otázkou, na kterou je nezbytné odpovědět, je ,jak má zaměstnavatel poznat, jestli pošta, která dojde na adresu úřadu nebo firemní adresu je určena pouze konkrétnímu zaměstnanci (fyzické osobě) nebo zaměstnavateli (osobě právnické). Uvedený problém řeší v celku uspokojivě zákon o poštovních službách[153] a

[151] zákon č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen „ZPI")
[152] stanovisko k problémům z praxe č. 6/2002 – Poskytování osobních údajů o zaměstnancích (k dispozici na http://www.uoou.cz/stan_praxe_6_2002.php3)
[153] zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů

prováděcí vyhláška k tomuto zákonu.[154] Prováděcí vyhláška stanoví následující pravidlo, jak poznat komu je dopis určen.[155] Je-li v adrese uvedena na prvém místě právnická osoba a na druhém místě fyzická osoba, za adresáta se považuje právnická osoba. Je-li v adrese uvedeno na prvém místě jméno a příjmení fyzické osoby a na druhém místě označení právnické osoby, za adresáta se považuje fyzická osoba s tím, že poštovní zásilka nebo poštovní poukaz má být dodán prostřednictvím této právnické osoby. Je-li v adrese namísto jména a příjmení určité fyzické osoby uvedena pouze její funkce v právnické osobě, za adresáta se považuje právnická osoba. Pokud by zaměstnavatel toto pravidlo ignoroval, nelze jinak než upozornit na možné páchání trestního činu dle § 239 trestního zákona,[156] tedy trestného činu porušování tajemství dopravovaných zpráv. Zákon říká, že kdo úmyslně poruší tajemství uzavřeného listu nebo jiné písemnosti, při poskytování poštovní služby nebo jiným dopravním zařízením, nebo zprávy podávané telefonem, telegrafem nebo jiným takovým veřejným zařízením, bude potrestán odnětím svobody až na šest měsíců. V úvahu je třeba vzít i skutkovou podstatu dle § 240 trestního zákona, v němž stojí, že kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu nebo telefonního hovoru, které nebyly určeny jemu, nebo takového tajemství využije, bude potrestán odnětím svobody až na jeden rok.

### 5. *Právo kontrolovat a monitorovat elektronickou poštu (e-mail) zaměstnanců*

Podstatně složitější problém může nastat ale ohledně kontroly elektronické pošty – emailů, které používají zaměstnanci při práci. Podotýkám, že mluvím především o emailu ve tvaru jméno.příjmení@firma.cz (resp. jméno.příjmení@úřad.cz), tedy kdy je evidentní, že email byl dán k dispozici zaměstnanci zaměstnavatelem k plnění jeho pracovních úkolů. K dané problematice se ve svém stanovisku k problémům z praxe[157] vyjádřil také Úřad pro ochranu osobních údajů (dále jen ÚOOÚ). Názory se ale velmi liší, jak u laické tak i u odborné veřejnosti.

Jaké jsou vlastně argumenty pro a proti takovéto praxi, kdy zaměstnavatel kontroluje, případně čte emaily zaměstnancům. Znovu podotýkám, že se jedná o elektronickou poštu (email) ve tvaru jméno.příjmení@firma.cz (resp. jméno.příjmení@úřad.cz). Jinými slovy, kdy zaměstnanec používá email, který „dostal" k dispozici od svého zaměstnavatele a který „zní" na jeho firmu, resp. případy obdobné.

Nejdříve je asi nutné setřídit jednotlivé argumenty. Základním argumentem v daném „sporu", proč zaměstnanci nemají právo a nesmí číst poštu svých zaměstnanců, je čl. 13 Listiny základních práv a svobod,[158] který stanoví, že nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením. Asi nebude větších sporů o tom, že daná úprava platí i pro elektronickou poštu. Dále bude nutné zmínit i čl. 8., odst. 1) Evropské úmluvy o ochraně

[154] vyhláška Ministerstva dopravy a spojů č. 28/2001 Sb., kterou se stanoví poštovní podmínky základních služeb a základní požadavky kvality při jejich zajišťování držitelem poštovní licence (dále jen „vyhláška")
[155] § 5, odst. 7 vyhlášky
[156] zákon č. 140/1961 Sb., trestní zákon
[157] stanovisko k problémům z praxe č. 1/2003 – Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců (k dispozici na http://www.uoou.cz/stan_praxe_1_2003.php3)
[158] usnesení předsednictva ČNR č. 2/1993 o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku ČR

lidských práv a základních svobod,[159] pod kterým je uvedeno, že každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

Samotný Úřad pro ochranu osobních údajů (dle již výše zmíněného stanoviska) doporučuje následující zásady ohledně monitorování elektronické pošty:[160]

- Zaměstnanec má právo na soukromí na pracovišti. Na tomto právu nic nemění skutečnost, že zaměstnanec používá komunikační či jiná zařízení zaměstnavatele. Lokalita a vlastnictví elektronického zařízení nemůže vyloučit právo na důvěrnost komunikace a korespondence stanovené v Ústavě a v dalších právních předpisech.

- Všeobecná zásada důvěrnosti korespondence zahrnuje komunikaci na pracovišti. Tato komunikace zahrnuje elektronickou poštu (e-mail) a k ní připojené soubory.

- Respektování soukromí také zahrnuje určitou míru práva vytvářet a rozvíjet vztahy mezi jedinci. Toto právo je, mimo jiné, nutno vzít v úvahu při posouzení oprávnění zaměstnavatele použít metody sledování zaměstnanců.

V neposlední řadě je třeba upozornit i na směrnici o ochraně soukromí a elektronických komunikacích,[161] kde se v úvodních ustanoveních stanoví následující: „... *koncové zařízení uživatelů elektronických telekomunikačních sítí a jakékoliv informace uchovávané na takovém zařízení tvoří součást soukromí uživatelů, které je chráněno v souladu s Evropskou úmluvou na ochranu lidských práv a základních svobod. Tzv. špehovací software, webové štěnice, skryté identifikátory nebo podobné nástroje, které pronikají do terminálu uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele, mohou vážně narušit soukromí těchto uživatelů. Použití takových nástrojů je možné pouze ze zákonných důvodů s vědomím uživatelů, kterých se dotýká.*"

Co se týče argumentů obhajujících praxi shromažďování a archivaci elektronické pošty včetně její „kontroly a čtení" ze strany zaměstnavatele, tak se zejména argumentuje ustanoveními zákoníku práce (dále jen „ZP"), která umožňují kontrolu práce zaměstnanců. Jde o ustanovení, které vesměs stanoví, že zaměstnavatel nebo vedoucí zaměstnanci jsou oprávněni stanovit a ukládat podřízeným zaměstnancům pracovní úkoly, organizovat, řídit a kontrolovat jejich práci a dávat jim k tomu účelu závazné pokyny. Tato „kontrola" ze strany zaměstnavatele (tedy čtení elektronické pošty) by mohlo směřovat především k zjištění, zda zaměstnanec řádně hospodaří s prostředky svěřenými jim zaměstnavatelem, střeží a ochraňuje majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejedná v rozporu s oprávněnými zájmy zaměstnavatele. Dalším častým argumentem je skutečnost, že náklady na provoz emailové schrány, stejně jako náklady za připojení k internetu (např. telefonní poplatky či fixní sazba) nese zaměstnavatel. Z těchto skutečností a z faktu, že email má tvar jméno@firma.cz (resp. jméno@úřad.cz) je usuzováno, že pošta je vlastně určena zaměstnavateli, který si ji pouze vybírá prostřednictvím svého zaměstnance. Také se často poukazuje na skutečnost, že v případě, kdy je např. zaměstnanec na služební cestě, dovolené nebo dlouhodobě nemocný, musí mít zaměstnavatel právo k přístupu do

[159] ve sbírce zákonů publikována pod č. 209/1992 Sb., sdělení federálního Ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod

[160] Nutno ale upozornit, že stanoviskem vyjadřuje Úřad pro ochranu osobních údajů svůj názor, který ale není obecně závazný.

[161] Směrnice č. 2002/58/EC Evropského parlamentu a Rady týkající se zpracovávání osobních údajů a ochrany soukromí v oblasti elektronických komunikací.

emailu zaměstnance. Tedy zkontrolovat, zda není třeba něco urgentně vyřídit (např. obstarat dodávku zboží, vyřídit reklamaci v zákonné lhůtě, zabránit nebezpečí promlčení atd.).

Autor této publikace je toho názoru, že pokud je dané vhodným způsobem upraveno v pracovní smlouvě nebo v pracovním řádu, se kterým byl zaměstnanec řádně seznámen, je možné a přípustné, aby zaměstnavatelé poštu zaměstnanců vybírali a četli (tedy poštu ve tvaru jméno.příjmení@firma.cz). Zaměstnavatel má také právo v přiměřeném rozsahu sledovat, kolik času zaměstnanec stráví na internetu nebo jaké typy webových stránek navštěvuje. Proto si také někteří zaměstnavatelé, kteří chtějí mít větší kontrolu nad emaily svých zaměstnanců, zřizují různé hromadné emailové schránky typu podatelna@firma.cz (resp. podatelna@úřad.cz). Uvedením osobních údajů v emailu typu podatelna@.., sekretariát@..., sklad@..., který zjevně není spojen s konkrétní osobou, se přesouvá odpovědnost za případné neoprávněné zpracovávání osobních údajů na zasilatele emailu. Obvykle totiž nelze předpokládat, že s takovým emailem pracuje pouze jedna osoba, jejichž práva na ochranu soukromí by mohla být při nakládání s hromadnou emailovou schránkou v plné míře respektována. [162]

### 6. *Právo zaměstnavatele sledovat zaměstnance odposlechem, pomocí kamery a podobnými způsoby*

Současná právní úprava reguluje používání kamerových a odposlechových systému pouze pro potřeby státních orgánů, resp. především v případech trestního stíhání.[163] Pokud se zaměstnavatel rozhodne k takovémuto postupu, musí samozřejmě dbát na ochranu zaměstnancovi osobnosti, důstojnosti a soukromí. Obecně lze takovýto způsob kontroly práce zaměstnanců spíše nedoporučit. Dále lze konstatovat, že do jisté míry je v ČR na užívání kamer možné aplikovat zákon o ochraně osobních údajů, kde je uvedeno, že správce osobních údajů musí jasně stanovit účel jejich shromažďování (zpracování). Důležité je mít na zřeteli, že uchovávané záznamy kamer mohou obsahovat osobní údaje a jako s takovými je s nimi nutno nakládat. Pokud by je někdo zneužil, může být podle zákona o ochraně osobních údajů sankcionován.[164]

Pokud ale zaměstnavatel takovouto činnost provádět chce, potom je třeba dle názoru autora této publikace na toto zaměstnance výslovně upozornit, popř. vyžádat si jeho souhlas (např. ustanovením v pracovní smlouvě).[165] Velmi citlivou otázkou potom bude nakládání s takovýmito záznamy nebo dokonce zveřejnění. Pokud by takovýto záznam byl použit v rozporu s právy zaměstnance (ochrana důstojnosti, osobnosti, soukromí atd.), potom se zaměstnavatel vystavuje vysokému nebezpečí sankce ze strany státu, včetně možnosti žaloby ze strany zaměstnance. Pokud by na druhou stranu ale kamerový systém např. zachytil zaměstnance jak poškozuje majetek zaměstnavatele nebo porušuje své pracovní povinnosti, potom je takovýto záznam možné použít např. v případném soudním sporu. Shrneme-li právě uvedené, platí, že žádný předpis použití takovýchto kamerových a odposlechových systému

[162] Podrobněji viz. též Štědroň, B., Čtení emailové pošty zaměstnavatelem a ochrana soukromí, Bulletin advokacie, 10/2004, Česká advokátní komora, str.46-51, ISSN 1210-6348.

[163] Podrobná studie ohledně odposlechu a záznamu telekomunikačního provozu od autora Jána Matejky je k dispozici na serveru www.itpravo.cz (Odposlech a záznam telekomunikačního provozu, díl I., vyšlo 6.5.2003 a Odposlech a záznam telekomunikačního provozu, díl II., vyšlo 13.5.2004)

[164] Podrobněji viz Informační bulletin ÚOOÚ 2/2004

[165] Otázkou samozřejmě ale může být i legálnost, resp. morálnost tohoto postupu, protože, pokud zaměstnanec do práce nastoupit chce, tak pracovní smlouvu raději podepíše – ustanovení je mu tedy vlastně vnuceno. Dále bude třeba odkázat na informační povinnosti dle zákona o ochraně osobních údajů, zejména § 5/4 a §11.

výslovně nezakazuje, nicméně, jak již bylo upozorněno, je třeba brát ohled na předpisy, které chrání práva na soukromí zaměstnance.[166]

### 7. *Závěrečné doporučení*

Zaměstnanec, jak je patrné z výše uvedeného, má i na pracovišti právo na respektování svého soukromí, právo na ochranu své osobnosti a je třeba respektovat i právo na listovní tajemství (včetně pošty elektronické). Zaměstnavatelé nemohou zaměstnance těchto práv jednostranným prohlášením nebo úkonem zbavit. Vždy ale záleží na dohodě zaměstnance a zaměstnavatele, tedy v nejčastějším případě na obsahu pracovní smlouvy. Obě strany se mohou dohodnout např. na právu zaměstnavatele kontrolovat poštu (včetně elektronické) během zaměstnancovi nepřítomnosti (např. při nemoci nebo služební cestě). Stejně tak je možné i v rozumné míře, která nesnižuje zaměstnancovu důstojnost, sledovat práci zaměstnanců pomocí kamerových systémů. Takovéto způsoby kontroly by ale měly být upraveny také v pracovních řádech zaměstnavatele, které jsou pro obě strany závazné. Zaměstnanec ale musí být s obsahem pracovního řádu seznámen, pracovní řád musí být vyhlášen a přístupný všem zaměstnancům.[167]

## *3.6.5. Poskytnutí informací a získání souhlasu subjektu údajů v elektronické komunikaci*

V červenci roku 2002 přijal Evropský parlament novou Směrnici o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice).[168] Směrnice výrazným způsobem omezuje dosavadní zvyklosti při zasílání reklam a obchodních nabídek prostřednictvím elektronických zařízení (e-mailem, faxem, telefonem, SMS či MMS zprávou, Internetem). V souvislosti s implementací této Směrnice do českého právního řádu, ale zejména s jejím prováděním v praxi, musely reklamní a obchodní společnosti podstatným způsobem změnit své chování k uživatelům elektronické komunikace a také ke klientům a zákazníkům. K čestnému způsobu komunikace patří také povinnost poskytnout mu řadu informací o zamýšleném či prováděném zpracování osobních údajů.[169]

V této souvislosti dostává Úřad pro ochranu osobních údajů stále více stížností občanů na nečestnou či dokonce nezákonnou praxi obchodních či reklamních společností při poskytování informací o ochraně osobních údajů při jejich zpracování a při získávání souhlasu subjektu údajů.

---

[166] Srov. též Štědroň, B., Kontrola práce zaměstnance prostřednictvím telekomunikační techniky, Právní rádce, 12/2004, Měsíčník HN, Economia, a.s., str. 39-42, ISSN 1210-4817.

[167] Štědroň, B., Elektronická kontrola zaměstnanců a právo, Convergence 10/2004, CNG, s.r.o., str. 12-15, ISSN 1214-5785.

[168] Podrobněji viz. Štědroň, B., Evropské právo informačních a telekomunikačních systémů, Systémová integrace, říjen 2004, Česká společnost pro systémovou integraci, str.123-141, ISSN 1210-9479.

[169] Viz. též Plíšek, M., Štědroň, B., Služby a právní aspekty informační společnosti, Právní rádce, 7/2004, Měsíčník HN, Economia, a.s., str. 19-21, ISSN 1210-4817.

Pro sblížení dosavadních postupů při zpracování osobních údajů je nezbytné připomenout některé principy, které Úřad pro ochranu osobních údajů prosazuje.[170]

1. Nezbytné informace o zpracování osobních údajů musejí být subjektu údajů poskytnuty čestným a neskrytým způsobem. Protože poskytnuté informace mají pomoci při rozhodování subjektu údajů, zda osobní údaje o sobě organizaci poskytne či nikoliv, měly by tyto informace být jednotlivci poskytnuty předtím, než jsou osobní údaje o něm získány pro další zpracování.

2. Souhlas subjektu údajů musí být po celou dobu zpracování prokazatelný a je možné jej získat také elektronicky.[171] Jedním ze zásadních problémů v elektronické komunikaci je získání souhlasu subjektu ke zpracování osobních údajů, pokud ho správce pro zpracování musí mít. Stávající ustanovení zákona o ochraně osobních údajů již nevyžaduje písemnou formu souhlasu u tzv. „běžných" osobních údajů.

3. Informace související s vyžádáním souhlasu subjektu údajů k legitimnímu zpracování jeho osobních údajů by měly být odděleny od ostatních informací poskytnutých subjektu údajů. Takové informace by měly být umístěny bezprostředně za přehledem požadovaných osobních údajů. Nesmějí být součástí jiného informativního textu. Při vyžádání souhlasu subjektu údajů při elektronické komunikaci (e-mail, www stránky správce/zpracovatele) musí příslušný formulář (např. objednávka) obsahovat samostatné políčko, které subjekt údajů vyplní.

### *3.6.6. Elektronická spisová služba u Policie ČR a ochrana osobních údajů*[172]

*1. Obecně*

Spisová služba se prolíná napříč plněním všech úkolů Policie ČR. Jako taková vychází z interního aktu řízení, který představuje Nařízení Ministerstva vnitra č. 95/2000, kterým se vydává spisový řád u Ministerstva vnitra a Policie ČR. Doplňují jej další interní normativní akty, ať již z úrovně Ministerstva vnitra, tak i Policie ČR. Vyskytnou-li se v rámci plnění úkolů Policie ČR v těchto činnostech osobní údaje, musí zpracovatel (i příjemce) postupovat v souladu s obecnou právní úpravou na tomto úseku, zejména zákonem č.101/2000 Sb., v platném znění.

Ochrana skutečností, se kterými se policista seznámil při plnění úkolů Policie ČR (tím i zpracovávaných osobních údajů), je garantována obecnou povinností všech policistů zachovávat mlčenlivost (§ 52 zákona o policii), která trvá i po skončení služebního poměru. Dále je vymezena jako základní povinnost příslušníka v § 45 odst. 1 písm. c) a § 214 zákona č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, v platném znění. Pokud jde o zaměstnance, vyplývá mlčenlivost z ustanovení § 303 odst. 2 písm. b) zák. č. 262/2006 Sb. zákoník práce, v platném znění.

---

[170] Podrobněji viz. stanovisko ÚOOÚ č. 1/2004 - Poskytnutí informací a získání souhlasu subjektu údajů v elektronické komunikaci (k dispozici na www.uoou.cz).

[171] Srov. též Štědroň, B., Plíšek, M., Nový zákon proti spamu a odpovědnost poskytovatelů služeb, Convergence 9/2004, CNG, s.r.o., str. 6-7, ISSN 1214-5785.

[172] Zdroj: Policejní prezidium ČR, Úřad služby kriminální policie a vyšetřování, Analýza úkonů dle § 88 odst. 1, 3 a § 158d odst. 2, 3, 6 trestního řádu za rok 2006 (upraveno autorem), www.mvcr.cz.

## 2. *Trestní řízení – oprávnění policejních orgánů k vyžádání odposlechu a záznamu telekomunikačního provozu*

Spisová služba se projevuje i v rámci trestního řízení, kde se vedle norem trestního práva (trestní zákon + trestní řád) uplatňují další právní předpisy a interní akty. Interním aktem řízení je upraven i postup při výkonu spisové služby na úseku trestního řízení u služby kriminální policie a vyšetřování; připravuje se novela tohoto závazného pokynu zdůrazňující povinnost policejních orgánů činit opatření na ochranu osobních údajů v průběhu trestního řízení, která se nachází v současné době ve fázi připomínkového řízení.

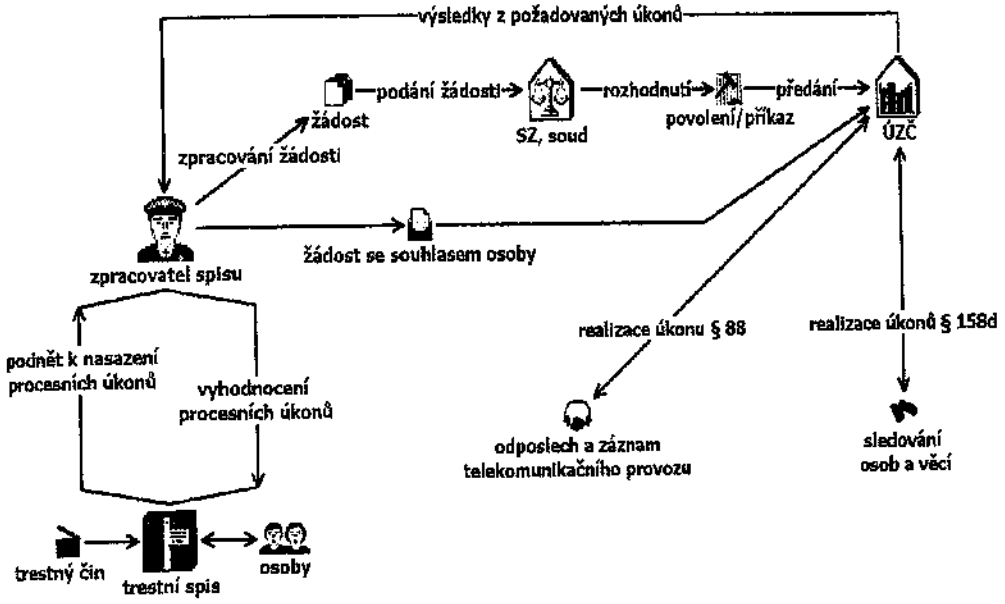
Zatímco procesní postup je stanoven taxativně trestním řádem, formy některých jednotlivých procesních úkonů jsou sjednocovány v rámci trestního řízení v podobě protokolů, formulářů a tiskopisů. Postup policejních orgánů je upraven v rámci trestního řízení pro policisty z pořádkové a železniční policie, dopravní policie, cizinecké a pohraniční policie podílející se na některých úkonech trestního řízení, tak zejména policistů SKPV[173] (ať již z teritoriálních nebo celorepublikových útvarů).

Z této velké skupiny policejních orgánů (pořádkové a železniční policie, dopravní policie, cizinecké a pohraniční policie a policistů SKPV teritoriálních i celorepublikových útvarů) podílejících se na přípravném trestním řízení, mohou použít operativně pátrací prostředky a úkon „odposlech a záznam telekomunikačního provozu" v rámci Policie ČR pouze policejní orgány zařazené u SKPV za podmínky, jsou-li současně držiteli „osvědčení fyzické osoby" (dále jen „osvědčení") o právu seznamovat se s utajovaným informacemi ve stupni „Vyhrazené", popř. vyšším (podle zákona č. 412/2005 Sb.). Pouze tyto policejní orgány jsou oprávněny, za podmínek stanovených v trestním zákoně (§ 41/2) a trestním řádě (§ 88/1), navrhnout odposlech a záznam telekomunikačního provozu. Je v praxi vyloučeno, aby mělo přístup k jednomu konkrétnímu odposlechu více policejních orgánů než je nezbytně nutné, resp. více než na případu fakticky pracují (a to i v rámci jednoho útvaru, byť jsou držiteli příslušných „osvědčení"), výjimku mohou tvořit specializované pracovní týmy (i zde jde však o omezený počet přístupů). Je tak v praxi dodržován princip zákona na ochranu utajovaných informací ve směru seznamování se s utajovanými informacemi u policejních orgánů, kteří je nezbytně nutně potřebují k výkonu své funkce (§ 6, resp. § 11 zákona č. 412/2005 Sb.). Jde-li v praxi o vyžadování odposlechu a záznamu telekomunikačního provozu ve stupni utajení „Důvěrné" tento okruh „oprávněných policejních orgánů" se ještě mnohonásobně zúží (stav vyjadřují systemizovaná služební místa), neboť uvedeným „osvědčením" v praxi zpravidla disponují toliko policejní orgány – „specialisté" SKPV na závažnou trestnou činnost (zejména na úrovni správ krajů a správy hl. m Prahy, ÚSKPV a celorepublikových útvarů). Ne všichni policisté v těchto útvarech se však podílí na prověřování a vyšetřování trestné činnosti, kde jsou splněny podmínky pro vyžádání a nasazení tohoto úkonu (hmotně-právní i procesně-právní).

Pokud jde o postup při vyžadování odposlechu a záznamu telekomunikačního provozu, je tento podrobněji upraven interním aktem řízení (je určen pro vnitřní potřebu). Stejně je tomu i v případě postupu při vyžadování sledování osob a věcí pro účely trestního řízení.

[173] SKPV je zkratka pro „služba kriminální policie a vyšetřování".

Důležitost prvků ochrany osobních údajů vyjadřuje Závazný pokyn policejního prezidenta při zpracovávání osobních údajů při plnění úkolů Policie ČR v souvislosti s trestním řízením (pro vnitřní potřebu). V současné době je přepracováván.




Obrázek: Postup při používání a nasazování úkonů dle §§ 88 odst.1,3 a 158d odst.2,3,6 trestního řádu. Zdroj: Ministerstvo vnitra ČR.

### 3. *Kontrolní činnost na úseku ochrany osobních údajů v informačních systémech*

V roce 2006 bylo skupinou správy a kontroly osobních údajů Kanceláře policejního prezidenta a zvlášť určenými pracovníky ve smyslu Závazného pokynu policejního prezidenta č. 55/2002 provedeno 658 kontrol se zaměřením zejména na oprávněnost a nutnost dotazů do informačních systémů. Bylo kontrolováno 2037 příslušníků a zaměstnanců Policie ČR. Při kontrolách bylo zjištěno 154 pochybení (pro vysvětlení např. jeden pracovník mohl mít tři i více pochybení), z toho počtu pouze 43 závažnějších pochybení.

Předmětem kontroly bylo dodržování povinností stanovených Policií ČR (dále jen „kontrolované") a osobám zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, při zabezpečení osobních údajů při jejich zpracování Policií ČR v rámci probíhajícího trestního řízení.

Kontrola se týkala podnětů, kterými bylo napadáno zveřejňování údajů z probíhajícího trestního řízení. Kontrolovanou byla Policie ČR jako celek, na některých útvarech bylo prováděno místní šetření.

Podněty shodně napadly zveřejňování údajů z probíhajícího trestního řízení v hromadných sdělovacích prostředcích, a to jednak zveřejňování obsahu odposlechů, jednak písemných informací o takovém řízení spojených vždy s identifikačními osobními údaji. Podezření směřovalo k fyzickým osobám, které přicházejí s osobními údaji u Policie ČR jako správce do styku. Úřad při předběžném posouzení stížnosti konstatoval podezření na porušení povinnosti

kontrolované podle ustanovení § 13 zákona o ochraně osobních údajů a dále podezření na porušení povinnosti kontrolované podle ustanovení § 5 odst. 3 a § 10 zákona o ochraně osobních údajů. K osobním údajům jako nedílné součásti informací o probíhajícím trestním řízení má v Policii ČR z principu přístup větší počet osob. To je dáno organizací pracovních procesů a služebního postupu v Policii ČR.

Nakládání s odposlechem a záznamy telekomunikačního provozu upravuje závazný pokyn policejního prezidenta, kterým se upravuje postup při vyžadování odposlechu a záznamu telekomunikačního provozu. Policie ČR periodicky vypracovává souhrnné dokumenty o odposlechu telekomunikačního provozu, které obsahují individuální osobní údaje, včetně údajů anonymizovaných. Zpráva pro parlamentní kontrolní orgán o použití odposlechu a sledování ve smyslu § 53a zákona o Policii ČR je vytvářena pololetně a Ministerstvu vnitra postupována jako dokument podléhající ochraně podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Parlamentní kontrolní orgán používá zprávu jako základ pro namátkovou kontrolu odposlechů. K osobním údajům jako nedílné součásti informací o probíhajícím trestním řízení má z principu přístup určený počet osob. To platí i pro řízení zahrnující odposlech a záznam telekomunikačního provozu. V rámci Policie ČR to je vždy několik fyzických osob: oprávněný žadatel, bezprostředně nadřízení služební funkcionáři oprávněného žadatele, pracovníci specializovaného pracoviště a zpracovatelé záznamů telekomunikačního provozu.

### 4. *Zjištění týkající se nakládání příjemců s osobními údaji o probíhajícím trestním řízení*

Operace s osobními údaji provádí Policie ČR jako subjekt plnící úkoly podle trestního řádu a zákona o Policii ČR a dalších věcně příslušných předpisů, zejména zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Zpracováním osobních údajů v rámci probíhajícího trestního řízení Policií ČR je např. již jejich shromažďování nebo předávání jiným příjemcům, uvedené jako operace v definici zpracování v ustanovení § 4 písm. e) zákona o ochraně osobních údajů. Policie ČR odpovídá za zpracování osobních údajů v rámci probíhajícího trestního řízení výlučně pouze do okamžiku jejich předání jinému příjemci; po tomto okamžiku za ně odpovídá společně s jiným příjemcem, pokud jím není fyzická osoba, která s osobními údaji nakládá výlučně pro osobní potřebu. Za další nakládání s osobními údaji shromážděnými převzetím od Policie ČR odpovídají přiměřeně jejich příjemci. Stanovená odpovědnost za zpracování osobních údajů o probíhajícím trestním řízení v Policii ČR je vymáhána. To bylo zjišťováno pomocí prosazované odpovědnosti (působnost) a provádění vnitřní kontroly. Při kontrole nebyly zjištěny známky popsanému stavu odporující. Policie ČR stanovila v návaznosti na věcně příslušné předpisy vnitřními akty řízení postupy likvidace osobních údajů a nosičů s osobními údaji o probíhajícím trestním řízení.

Kontrolou bylo zjištěno, že Policie ČR přijala organizační opatření a zvolila a používá technické prostředky ke splnění své povinnosti podle § 13 odst. 1 zákona o ochraně osobních údajů.[174] Rutinně používaný systém organizačních a technických bezpečnostních opatření obecně odpovídá používaným způsobům a prostředkům zpracování osobních údajů a

[174] Viz. www.mvcr.cz.

organizačním podmínkám Policie ČR. Přijatá a provedená opatření k ochraně osobních údajů reagují na základní bezpečnostní rizika.

Ze strany kontrolního úřadu při pravidelné kontrole nebylo zjištěno porušení povinnosti podle § 13 odst. 2 zákona o ochraně osobních údajů Policií ČR jako správcem osobních údajů o probíhajícím trestním řízení.[175] Nebylo zjištěno, že by u Policie ČR někdo porušil svoji povinnost podle ustanovení § 15 odst. 1 zákona o ochraně osobních údajů, ani že postupoval při zpracování osobních údajů jinak než za podmínek a rozsahu jemu stanoveném v návaznosti na věcně příslušné předpisy.

Kontrolou popsanou v tomto kontrolním protokolu nebylo zjištěno porušení povinností uložených Policii ČR v § 13 zákona o ochraně osobních údajů.[176] Z předložené a jinak shromážděné dokumentace Úřadem vyplývá, že Policie ČR přijala a provedla opatření ke splnění povinností stanovených v § 13 odst. 1 zákona o ochraně osobních údajů a že přijatá a provedená opatření podle § 13 odst. 1 zpracovává a dokumentuje.V kontrolním protokolu je konstatováno, že „Po vyhodnocení kontrolních zjištění nejsou dány důvody pro uložení opatření k nápravě".

Policii ČR bylo nicméně doporučeno, aby uvážila změnu nebo doplnění dosud užívaných technicko-organizačních opatření k ochraně osobních údajů, např.:

- vhodným způsobem omezit počet fyzických osob, které jsou současně oprávněny zpracovávat osobní údaje o probíhajícím trestním řízení v elektronických datových souborech obsahujících informace o probíhajícím trestním řízení s výjimkou údajů o pátrání po osobách,
- použitím dodatečných prvků individualizovat jednotlivé kopie dokumentů obsahujících osobní údaje shromážděné v průběhu trestního řízení, zejména pokud některá vyhotovení jsou poskytována jiným příjemcům,
- protokolovat a evidovat pořizování jakýchkoliv kopií nebo přepisů záznamů odposlechu nebo doprovodných informací o telekomunikačním provozu a další manipulaci s nimi do okamžiku předání jinému příjemci nebo likvidace; likvidaci takových záznamů provádět komisionálně,
- technickými a organizačními opatřeními omezit okruh osob, které se mohou seznamovat s účastnickými čísly uváděnými ve zprávě pro parlamentní kontrolní orgán o použití odposlechu a sledování,
- přehodnotit strukturu aktivně udržovaných datových souborů s osobními údaji, vypovídajícími o probíhajícím trestním řízení, zejména s přihlédnutím k vzájemnému obsahovému překrývání takových souborů (informačních systémů).

### 5. *Ochrana a bezpečnost před únikem informací a způsob zajištění dat*

Bezpečnostní opatření při zpracování osobních údajů jsou standardizována. Přístup k osobním údajům z informačních systémů provozovaných v uzavřeném prostředí je zprostředkován výhradně proškolenými pracovníky a vázán na uživatelské oprávnění a heslo.

[175] Viz. www.mvcr.cz.
[176] Viz. www.mvcr.cz.

Policie ČR zavedla a provádí vnitřní kontroly, které je na místě považovat za součást opatření k plnění povinnosti podle § 13 odst. 1 zákona o ochraně osobních údajů. Pořizování záznamů odposlechů a nakládání s nimi upravuje v návaznosti na trestní řád závazný pokyn policejního prezidenta, kterým se upravuje postup při vyžadování odposlechu a záznamu telekomunikačního provozu. Likvidaci záznamů odposlechů rovněž upravuje v návaznosti na trestní řád závazný pokyn policejního prezidenta.

Přes všechna přijatá opatření ze strany Policie ČR jsou úniky informací do sdělovacích prostředků z odposlechu a záznamu telekomunikačního provozu (dále jen „záznam z odposlechu") v přípravném řízení destabilizujícím prvkem v efektivnosti trestního řízení. Tento nežádoucí stav je přitom výsledkem porušování základních principů trestního řízení a co je ještě závažnější, jde o porušování zákona o ochraně osobních údajů a práv a svobod zakotvených v Listině základních práv a svobod.

Jednou ze základních zásad trestního řízení je zásada veřejnosti vyjádřená v ustanovení § 2 odst. 10 t.ř. „trestní věci se před soudem projednávají veřejně tak, aby se občané mohli projednávání zúčastnit a jednání sledovat". Tento základní princip trestního řízení vychází přímo z Ústavy ČR, čl. 96 odst. 2 („Jednání před soudem je ústní a veřejné..."), a dále z článku 38 odst. 2 Listiny základních práv a svobod („Každý má právo, aby jeho věc byla projednána veřejně, bez zbytečných průtahů a v jeho přítomnosti..."). Zásada veřejnosti tak, jak je definována zákonem, je zásadnou ústavní, požívající nejvyšší právní sílu v našem právním systému.

Pro přípravné řízení trestní z této zásady ovšem plyne opak, tj. že řízení před policejním orgánem a státním zástupcem v přípravném řízení trestním je neveřejné (analogie opaku ústavních zásad) a vyjadřuje potřebu ničím nerušeného průběhu shromažďování důkazů svědčících ve prospěch i proti podezřelému nebo obviněnému, kde kontrolu nad zákonným postupem policejních orgánů přebírá státní zástupce. Tento opak zásady veřejnosti v přípravném řízení je dán specifiky odhalování a vyšetřování trestné činnosti a má svůj zásadní význam pro následující stadium trestního řízení, a to řízení před soudem.

K úniku informací a tedy k porušování uvedených zákonných norem dochází téměř výhradně v přípravném řízení trestním, kdy informace shromážděné o odhalovaném a vyšetřovaném trestnému činu jsou nejcitlivější vzhledem k tomu, že jejich vypovídací hodnota pro účely trestního řízení je předmětem vyšetřování a jejich zveřejněním je v podstatě předjímán jejich kriminální význam, aniž tomu tak ve skutečnosti musí být. V řadě případů je tak porušena i presumpce neviny, kdy na základě těchto informací sdělených veřejnosti dochází k nezákonné kriminalizaci osob, které jsou aktéry sdělené informace.

Přesto, že dosavadní zjištění napovídají spíše tomu, že k únikům citlivých informací dochází mimo Policii ČR a že jsou stanoveny v Policii ČR standardy na ochranu těchto citlivých údajů, Policie ČR připravuje některá technicko-organizační opatření k zajištění větší bezpečnosti a ochrany těchto údajů a to jak v Policii ČR, tak směrem vně Policie ČR. V současné době jsou tato opatření ve stádiu návrhů a posuzování s cílem vytvoření nového interního aktu řízení.

V souvislosti s tím bylo řediteli ÚZČ[177] uloženo , aby v době co nejkratší byla posouzena, resp. navržena k zavedení technická preventivní opatření.

[177] ÚZČ je zkratka pro „Útvar zvláštních činností služby kriminální policie a vyšetřování".

Konkrétně se jedná o:

- ztížení kopírování archivních nosičů záznamu,
- zašifrovaný přenos,
- zabezpečení záznamů před možností jejich přehrání běžným softwarem,
- kopie vytvářet výhradně na specializovaném pracovišti za předem stanovených podmínek
- ke každému úkonu zavést evidenci o jakékoliv manipulaci s ním (kontrolní listy)
- zavedení centrální evidence každého přístupu ke každému záznamu,
- zpřísnění zásad přístupu oprávněných žadatelů do komunikačních počítačů,
- užívání komunikačních počítačů zablokovaných proti přepisu na nosiče záznamu.

### *3.6.7. Zveřejňování jmen dlužníků na internetu*

Úřad pro ochranu osobních údajů (Úřad) se k této věci vyjádřil ve svém stanovisku[178] ve věci zveřejnění jmen fyzických nebo právnických osob, které nezaplatily poplatky nebo pokuty, uložené na základě pravomocných správních rozhodnutí, ve vztahu k zákonu č. 101/2000 Sb., o ochraně osobních údajů. Úřad se k uvedené problematice vyjádřil mimo jiné i v souvislosti s probíhajícím soudním řízením, kdy se občan domáhá ochrany svého práva před neoprávněným zveřejňováním.

Úřad vychází ve svém přístupu k této problematice zejména z článku 10 odst. 3 Listiny základních práv a svobod, která zakotvila právo každého subjektu údajů na ochranu před neoprávněným zveřejňováním údajů o své osobě. Úřad došel k závěru, že ke zveřejnění osobních údajů může dojít pouze se souhlasem subjektu údajů, přičemž tento názor opřel zejména o tato zákonná ustanovení:

1. Definice pojmu „zveřejněný osobní údaj", uvedená v ustanovení § 4 písm. l) zákona, obsahuje současně výčet prostředků, kterými může dojít k tomuto úkonu, aniž by byly porušeny zásady ochrany osobních údajů uvedené v zákoně.

2. Ačkoliv zákon neobsahuje žádné konkrétní ustanovení, které by správci nebo zpracovateli osobních údajů umožňovalo tyto údaje zveřejňovat, je z dikce ustanovení § 4 písm. e) zákona patrné, že i zveřejňování osobních údajů je považováno za zpracování osobních údajů.

3. Dále citovaný zákon obsahuje zejména v ustanovení § 5 úpravu práv a povinností správce při zpracovávání osobních údajů. V této souvislosti zákon klade před správce osobních údajů řadu povinností, a to zejména v odstavci 2, kde je obsažena zásada, že zpracovávat osobní údaje lze pouze se souhlasem subjektu údajů. V tomtéž ustanovení jsou sice obsaženy výjimky z této zásady, ale žádná z nich se na uvedený případ podle našeho názoru nevztahuje.

Obecně lze dále k této problematice uvést, že Úřad považuje takové jednání za jednání nátlakové, kterým jsou porušována i další ustanovení článku 10 Listiny základních práv a

[178] Podrobněji viz Stanovisko ÚOOÚ č. 1/2001, zveřejňování jmen dlužníků, www.uoou.cz.

svobod. Zveřejňování osobních údajů v souvislosti se vznikem pohledávek považuje Úřad za nepřípustné zasahování do soukromí osob, neboť zpřístupněním takového údaje, který byl získán na základě soukromoprávního vztahu, může dojít k poškození dobrého jména takové osoby v mnoha dalších vztazích, a to jak soukromoprávních, tak i veřejnoprávních.

# 4. Vybrané statistické ukazatele (rychlost rozhodování soudů a vývoj elektronizace veřejné správy v ČR)

## 4.1. Úvod

Elektronizace justice a vedení spisu v elektronické podobě může dosáhnout sledovaných cílů (zrychlení rozhodování sporů, zajištění bezpečnosti spisu pro vykrádání atd.) pouze za předpokladu, že občané budou mít přístup k moderním informačních technologiím a k prostředkům komunikace elektronicky na dálku (typicky internetu). Cílem této kapitoly je upozornit na konkrétní (nelichotivé) statistické údaje týkající se rychlosti rozhodovací činnosti soudů a postupné elektronizace „domácností" v ČR (např. schopnosti práce s počítačem, dostupnost připojení na internet atd.)

## 4.2. Přehled o průběhů řízení – občanskoprávní agenda[179]

**Krajské + okresní soudy** **Kraje (zkratky)** **1. pololetí 2007**

| | | Praha | StČ | JČ | ZČ | SČ | VČ | JM | SM | ČR |
|---|---|---|---|---|---|---|---|---|---|---|
| Řízení bylo zahájeno | návrhem (bez návrhu) | 41667 | 14432 | 8088 | 12373 | 20811 | 13617 | 24407 | 25167 | **160562** |
| | po zrušení rozhodnutí pro zmatečnost | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | **1** |
| | povolení obnovy | 8 | 4 | 2 | 0 | 1 | 1 | 2 | 3 | **21** |
| | po zrušení rozhodnutí nálezem ústavního soudu | 4 | 1 | 1 | 2 | 2 | 0 | 1 | 7 | **18** |
| | po vyhovění dovolání | 19 | 4 | 9 | 10 | 4 | 16 | 2 | 9 | **73** |
| | po zrušení rozhodnutí po kasační stížnosti | 177 | 0 | 17 | 9 | 59 | 20 | 97 | 26 | **405** |
| Odvolání podal | žalobce | 1148 | 414 | 260 | 404 | 479 | 542 | 906 | 971 | **5124** |
| | žalovaný | 1370 | 651 | 348 | 568 | 728 | 763 | 1282 | 1232 | **6942** |
| | oba | 87 | 22 | 15 | 38 | 28 | 35 | 81 | 109 | **415** |
| | jiná osoba | 17 | 8 | 2 | 4 | 5 | 33 | 8 | 48 | **125** |
| | nebylo podáno | 39253 | 13346 | 7492 | 11380 | 19637 | 12281 | 22232 | 22853 | **148474** |
| Výsledek odvolacího řízení | rozhodnutí bylo potvrzeno | 1287 | 482 | 290 | 492 | 510 | 621 | 848 | 1143 | **5673** |
| | rozhodnutí bylo změněno | 478 | 227 | 145 | 231 | 222 | 259 | 534 | 448 | **2544** |
| | jiný výsledek | 857 | 386 | 190 | 291 | 508 | 493 | 895 | 769 | **4389** |
| Věc skončena vyhověním konečného návrhu | zcela | 25687 | 6106 | 4108 | 5570 | 9151 | 5093 | 10562 | 10766 | **77043** |
| | zčásti | 1059 | 567 | 317 | 428 | 629 | 560 | 1085 | 1232 | **5877** |
| | smírem | 671 | 471 | 285 | 425 | 530 | 467 | 637 | 579 | **4065** |
| | zamítnutím návrhu | 2051 | 809 | 419 | 561 | 943 | 828 | 1468 | 1902 | **8981** |
| | platebním rozkazem | 3932 | 3699 | 1397 | 2681 | 4106 | 3385 | 3416 | 3493 | **26109** |
| | jinak | 8475 | 2789 | 1591 | 2729 | 5518 | 3321 | 7341 | 7241 | **39005** |
| **Celkem věci** | | **41875** | **14441** | **8117** | **12394** | **20877** | **13654** | **24509** | **25213** | **161080** |

[179] Zdroj: Ministerstvo spravedlnosti ČR (upraveno autorem).

## 4.3. Přehled o průměrných délkách řízení ode dne nápadu do dne právní moci ve dnech – náhrada škody[180]

Krajské + okresní soudy | Kraje (zkratky) | 1. pololetí 2007

| | | Praha | StČ | JČ | ZČ | SČ | VČ | JM | SM | ČR |
|---|---|---|---|---|---|---|---|---|---|---|
| Náhrada škody podle občanského zákoníku | náhrada škody způsobená nezletilým | 1267 | 4381 | 0 | 177 | 1191 | 638 | 959 | 615 | 1877 |
| | náhrada škody způsobená osobou postiženou duševní poruchou | 0 | 0 | 0 | 0 | 0 | 130 | 0 | 0 | 130 |
| | náhrada škody způsobená osobou vlastní vinou v nekontrolovaném stavu | 204 | 132 | 136 | 253 | 0 | 1038 | 183 | 214 | 240 |
| | náhrada škody vzniklá úmyslným jednáním proti dobrým mravům | 962 | 467 | 224 | 547 | 1323 | 377 | 543 | 365 | 524 |
| | náhrada škody vzniklé nesplněním povinnosti k jejímu odvrácení | 931 | 584 | 616 | 500 | 446 | 756 | 1038 | 833 | 854 |
| | náhrada škody vzniklá v dopravě – při provozu silničního motorového vozidla | 688 | 541 | 313 | 440 | 1021 | 522 | 809 | 541 | 636 |
| | náhrada škody vzniklá v dopravě – při provozu železnice a jiné kolejové dopravy | 627 | 0 | 115 | 80 | 429 | 0 | 597 | 138 | 398 |
| | náhrada škody vzniklá v dopravě – letecká doprava | 198 | 0 | 0 | 0 | 0 | 0 | 1863 | 0 | 475 |
| | náhrada škody vzniklá v jiné dopravě | 860 | 0 | 0 | 0 | 0 | 0 | 368 | 878 | 483 |
| | náhrada jízdného a pokuta v hromadné dopravě | 309 | 355 | 174 | 260 | 642 | 229 | 340 | 351 | 344 |
| | náhrada škody vzniklá zvlášť nebezpečným provozem | 0 | 0 | 1345 | 0 | 0 | 0 | 415 | 576 | 698 |
| | škoda způsobená provozní činností | 674 | 1270 | 0 | 1864 | 1529 | 624 | 1296 | 1018 | 1142 |
| | náhrada škody vzniklá na vnesených nebo odložených věcech | 569 | 287 | 214 | 238 | 497 | 1320 | 1305 | 296 | 641 |
| | náhrada škody vzniklá trestným činem | 545 | 378 | 284 | 433 | 776 | 420 | 665 | 483 | 527 |
| | odpovědnost za škodu v ostatních případech | 630 | 661 | 446 | 407 | 928 | 535 | 934 | 649 | 685 |
| | bezdůvodné obohacení | 640 | 581 | 430 | 473 | 870 | 615 | 901 | 725 | 702 |
| | ***Průměr*** | 331 | 426 | 213 | 308 | 676 | 304 | 481 | 428 | 394 |

## 4.4. Přehled o průměrných délkách řízení ode dne nápadu do dne právní moci ve dnech – vlastnické vztahy[181]

Krajské + okresní soudy | Kraje (zkratky) | 1. pololetí 2007

| | | Praha | StČ | JČ | ZČ | SČ | VČ | JM | SM | ČR |
|---|---|---|---|---|---|---|---|---|---|---|
| Obč. zákoník - vlastnické vztahy | vydání nebo vrácení věci | 922 | 506 | 224 | 286 | 868 | 879 | 1082 | 689 | 741 |
| | určení vlastnictví | 886 | 659 | 551 | 599 | 1116 | 829 | 1113 | 793 | 870 |
| | sousedské spory | 683 | 503 | 1398 | 1783 | 2130 | 582 | 1336 | 978 | 1050 |
| | zásahy do vlastnických práv | 682 | 898 | 301 | 357 | 598 | 408 | 855 | 718 | 625 |
| | ochrana držby | 84 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 84 |
| | vydržení vlastnického práva k movitým i nemovitým věcem nebo věcného břemene | 1644 | 335 | 1011 | 587 | 2805 | 572 | 1873 | 1085 | 1265 |
| | spory z věcných břemen (kromě vydržení) | 594 | 727 | 372 | 856 | 833 | 692 | 1341 | 1168 | 871 |
| | zrušení nebo rozdělení spoluvlastnictví podílového | 1016 | 695 | 572 | 688 | 1426 | 662 | 1213 | 944 | 902 |
| | ostatní spory ze spoluvlastnictví podílového | 819 | 461 | 676 | 741 | 1156 | 608 | 1023 | 777 | 786 |
| | práva a povinnosti vyplývající ze společného jmění manželů | 545 | 236 | 615 | 145 | 620 | 183 | 793 | 709 | 532 |
| | zúžení společného jmění manželů | 249 | 94 | 67 | 74 | 259 | 114 | 139 | 137 | 150 |
| | vypořádání společného jmění po zániku manželství | 976 | 712 | 463 | 448 | 970 | 635 | 1037 | 790 | 797 |
| | ostatní spory ze společného jmění manželů | 586 | 501 | 221 | 392 | 875 | 362 | 788 | 565 | 595 |
| | neoprávněná stavba (§ 135 písm.c.) o.z.) | 837 | 2192 | 596 | 586 | 1524 | 252 | 1264 | 778 | 1003 |
| | zástavní a podzástavní právo | 692 | 520 | 530 | 780 | 844 | 456 | 889 | 690 | 694 |
| | spory z práva zadržovacího | 682 | 0 | 426 | 0 | 223 | 184 | 547 | 0 | 284 |
| | ostatní spory z vlastnictví podle občanského zákoníku | 560 | 500 | 279 | 422 | 858 | 579 | 745 | 395 | 537 |
| | ***Průměr*** | 747 | 621 | 446 | 504 | 969 | 614 | 988 | 631 | 721 |

[180] Zdroj: Ministerstvo spravedlnosti ČR (upraveno autorem).
[181] Zdroj: Ministerstvo spravedlnosti ČR (upraveno autorem).

## 4.5. Stížnost pro porušení zákona – rychlost vyřizování podnětů ze strany státního zastupitelství[182]

**Krajská státní zastupitelství** **I. pololetí 2007**

| Délka | Praha | StČ | JČ | ZČ | SČ | VČ | JM | SM |
|---|---|---|---|---|---|---|---|---|
| <1Měsíc | 6 | 8 | 7 | 9 | 10 | 4 | 7 | 9 |
| 1-2M. | 8 | 5 | 6 | 4 | 9 | 3 | 12 | 7 |
| 2-3M. | 1 | 1 | 0 | 7 | 6 | 2 | 5 | 5 |
| 3-4M. | 2 | 3 | 0 | 0 | 6 | 2 | 2 | 2 |
| 4-5M. | 3 | 0 | 0 | 0 | 1 | 4 | 0 | 2 |
| 5-6M. | 1 | 0 | 0 | 0 | 1 | 3 | 0 | 1 |
| 6-12M. | 3 | 0 | 0 | 0 | 3 | 12 | 0 | 1 |
| 1-2Rok | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| >2R. | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 |
| Celkem | 27 | 17 | 14 | 20 | 36 | 31 | 28 | 27 |
| Prům.délka ve dnech | 166 | 45 | 55 | 46 | 77 | 167 | 131 | 61 |

## 4.6. Rychlost vyřizování podnětů ze strany státního zastupitelství u ostatních řízení[183]

[182] Zdroj: Ministerstvo spravedlnosti ČR (upraveno autorem).
[183] Zdroj: Ministerstvo spravedlnosti ČR (upraveno autorem).

Ostatní

I. pololetí 2007

| Délka | NSZ-Brno | VSZ-Praha | VSZ-Olomouc | ČR |
|---|---|---|---|---|
| <1Měsíc | 29 | 59 | 44 | 192 |
| 1-2M. | 9 | 40 | 19 | 122 |
| 2-3M. | 8 | 39 | 6 | 80 |
| 3-4M. | 17 | 20 | 5 | 59 |
| 4-5M. | 9 | 10 | 9 | 38 |
| 5-6M. | 7 | 10 | 6 | 29 |
| 6-12M. | 26 | 63 | 20 | 128 |
| 1-2Rok | 9 | 16 | 10 | 38 |
| >2R. | 1 | 0 | 0 | 5 |
| Celkem | 115 | 257 | 119 | 691 |
| Prům.délka ve dnech | 148 | 129 | 128 | 124 |

## 4.7. Státní zastupitelství – rychlost vyřizování netrestních věcí[184]

I. pololetí 2007

| DÉLKA | KSZ (MSZ) a OSZ | | | | | | | | NSZ | VSZ | | ČR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Praha | StČ | JČ | ZČ | SČ | VČ | JM | SM | Brno | Praha | Olomouc | |
| < 1 Měsíc | 662 | 706 | 672 | 573 | 723 | 815 | 1134 | 1029 | 514 | 10 | 1 | 6839 |
| 1 - 2 M. | 284 | 53 | 16 | 44 | 33 | 120 | 104 | 76 | 75 | 2 | 1 | 808 |
| 2 - 3 M. | 78 | 14 | 5 | 17 | 35 | 13 | 37 | 15 | 18 | 0 | 0 | 232 |
| 3 - 4 M. | 23 | 6 | 1 | 14 | 21 | 5 | 14 | 8 | 34 | 0 | 0 | 126 |
| 4 - 5 M. | 26 | 2 | 0 | 5 | 16 | 4 | 19 | 2 | 30 | 0 | 0 | 104 |
| 5 - 6 M. | 12 | 1 | 0 | 6 | 1 | 2 | 3 | 2 | 19 | 0 | 0 | 46 |
| 6 - 12 M. | 31 | 7 | 0 | 9 | 1 | 2 | 13 | 2 | 48 | 0 | 0 | 113 |
| 1 - 2 Rok | 12 | 2 | 0 | 0 | 1 | 1 | 6 | 1 | 12 | 0 | 0 | 35 |
| > 2 R. | 0 | 1 | 0 | 0 | 0 | 0 | 4 | 1 | 0 | 0 | 0 | 6 |
| CELKEM | 1128 | 792 | 694 | 668 | 831 | 962 | 1334 | 1136 | 750 | 12 | 2 | 8309 |
| Prům. délka ve dnech | 41 | 15 | 5 | 18 | 16 | 13 | 22 | 12 | 51 | 9 | 27 | 22 |

[184] Zdroj: Ministerstvo spravedlnosti ČR (upraveno autorem).

## 4.8. Státní zastupitelství – rychlost vyřizování odvolání[185]

| Česká republika<br>Období: 1 - 6 / 2007 | |
|---|---|
| Rychlost vyřizování věcí dovolání | |
| DÉLKA | NSZ<br>1000 |
| < 1 M. | 576 |
| 1 - 2 M. | 184 |
| 2 - 3 M. | 47 |
| 3 - 4 M. | 5 |
| 4 - 5 M. | 2 |
| 5 - 6 M. | 1 |
| 6 - 12 M. | 8 |
| 1 - 2 R. | 0 |
| > 2 R. | 0 |
| CELKEM | 823 |
| Prům. délka ve dnech | 29 |

## 4.9. Využívání IT, internetu a počítačů v domácnostech (ČSÚ)

Základním předpokladem úspěšnosti projektu elektronizace českého soudnictví je schopnost úředníků veřejné správy a občanů pracovat s moderními informačními technologiemi (tedy zejména s počítačem a internetem). Český statistický úřad uskutečnil ve 2. čtvrtletí 2006 šetření o využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci. Ze statistik např. vyplývá, že přes 40% uživatelů internetu má zájem o služby eGovernmentu (E-Justice pojmově spadá pod eGovernment, je jeho součástí). Pouze 30% uživatelů internetu ale tyto služby využívá (v Praze dokonce jenom 25%). Česká republika výrazně zaostává ve využívání služeb eGovernmentu (Praha jako hlavní a nejbohatší region je navíc pod průměrem ČR). Zájem občanů ČR o využívání služeb eGovernmentu je značný. Přes 60% občanů chce tyto služby využívat např. při vyřizování osobních dokumentů, přes 50% občanů chce registrovat automobil přes internet a více než 40% občanů chce podávat své daňové přiznání přes internet. I přes takto velký zájem nemá více než polovina obyvatel žádné zkušenosti s využíváním internetu a méně než 30% populace má základní znalost práce s internetem. Pokročilou znalost práce s internetem má potom pouhých 3,6% populace. Jako jeden z hlavních důvod nevyužívání internetu doma uvádějí občané předraženou cenu internetového připojení, a to včetně nízkorychlostního – narrowband. Navíc skoro 400 tisíc domácností má osobní počítač, ale nemají připojení k internetu.

[185] Zdroj: Ministerstvo spravedlnosti ČR (upraveno autorem).

## Vybavenost domácností osobním počítačem - ve 2.čtvrtletí 2006 (zdroj: www.czso.cz)

***Households´ access to personal computer in the 2nd quarter 2006***

*(více možností volby / multiple choice)*

| | Domácnosti vybavené / Households equipped with | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Osobním počítačem [1] / PC [1] | | z toho domácností vybavené / *In which households equipped* | | | | | |
| | | | Stolním počítačem / *Desktop computer* | | Přenosným počítačem (notebook) / Portable computer | | Počítačem do dlaně / Handheld computer | |
| | v tis. / in thous. | %* | v tis. / in thous. | %** | v tis. / in thous. | %** | v tis. / in thous. | %** |
| **Celkem ČR/*Czech Republic - total*** | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |
| Typ domácnosti/ Type of household | | | | | | | | |
| jeden dospělý bez závislých dětí / one adult without dependent children | 143,3 | 13,2% | 115,7 | 80,7% | 43,8 | 30,6% | . | . |
| dva dospělí bez závislých dětí / two adults without dependent children | 267,0 | 21,9% | 246,3 | 92,2% | 55,2 | 20,7% | . | . |
| tři nebo více dospělých bez závislých dětí / three or more adults without dependent children | 148,6 | 39,7% | 141,6 | 95,3% | 27,7 | 18,6% | . | . |
| jeden dospělý se závislými dětmi / single adult with dependent child (ren) | 111,2 | 47,3% | 107,2 | 96,4% | 10,8 | 9,7% | - | - |
| dva dospělí se závislými dětmi / two adults with dependent children | 696,1 | 64,7% | 680,2 | 97,7% | 124,4 | 17,9% | . | . |
| tři nebo více dospělých se závislými dětmi / 3 or more adults with dependent children | 133,2 | 61,9% | 130,6 | 98,0% | 23,7 | 17,8% | . | . |
| Typ lokality / Type of locality | | | | | | | | |
| vysoká hustota populace / densely-populated area | 571,9 | 38,5% | 525,1 | 91,8% | 160,2 | 28,0% | 13,1 | 2,3% |
| střední hustota populace / intermediate area | 345,6 | 35,0% | 334,2 | 96,7% | 61,1 | 17,7% | . | . |
| malá hustota populace / thinly-populated area | 581,9 | 33,6% | 562,1 | 96,6% | 64,3 | 11,1% | . | . |
| Kraj / Region | | | | | | | | |
| Hl.m. Praha | 230,8 | 42,4% | 202,2 | 87,6% | 85,4 | 37,0% | . | . |
| Středočeský | 167,0 | 36,5% | 156,3 | 93,6% | 39,8 | 23,8% | . | . |
| Jihočeský | 86,3 | 32,9% | 85,7 | 99,2% | . | . | . | . |
| Plzeňský | 88,7 | 39,1% | 86,8 | 97,6% | 14,5 | 16,3% | . | . |
| Karlovarský | 50,3 | 38,7% | 49,6 | 98,5% | 6,8 | 13,4% | - | - |
| Ústecký | 89,4 | 24,9% | 86,5 | 96,8% | . | . | - | - |
| Liberecký | 55,3 | 32,4% | 53,7 | 97,1% | . | . | - | - |
| Královéhradecký | 73,3 | 34,4% | 72,4 | 98,8% | . | . | . | . |
| Pardubický | 77,0 | 38,7% | 71,4 | 92,7% | 13,6 | 17,7% | - | - |
| Vysočina | 74,9 | 37,1% | 71,5 | 95,5% | . | . | - | - |
| Jihomoravský | 157,7 | 37,3% | 150,9 | 95,7% | 31,8 | 20,2% | . | . |
| Olomoucký | 79,5 | 30,5% | 75,1 | 94,4% | 16,9 | 21,3% | - | - |
| Zlínský | 76,7 | 32,3% | 75,8 | 98,8% | . | . | - | - |
| Moravskoslezský | 192,5 | 37,5% | 183,9 | 95,5% | 29,9 | 15,5% | . | . |

* Hodnota je procentem z celkového počtu domácností v dané socio-demografické skupině / *As a % of total number of households in given socio-demographic group*

** Hodnota je procentem z domácností (v dané socio-demografické skupině), které jsou vybavené osobním počítačem / As a % of households (in given socio-demographic group) which are equipped by PC

1) Osobní počítač zahrnuje stolní počítač, přenosný počítač a počítač do dlaně / Personal computer = desktop, portable and handheld computer

**Připojení domácností k internetu - ve 2.čtvrtletí 2006 (zdroj: www.czso.cz)**
***Households´ access to the internet in the 2nd quarter 2006***

| | Domácnosti s připojením k internetu / *Households with internet access* | | |
|---|---|---|---|
| | v tis. *in thous.* | %* | %** |
| **Celkem ČR/*Czech Republic - total*** | 1 23 | | |
| Typ domácnosti/ Type of household | | | |
| jeden dospělý bez závislých dětí / one adult without dependent children | 111,8 | 10,3% | 78,0% |
| dva dospělí bez závislých dětí / two adults without dependent children | 205,0 | 16,8% | 76,8% |
| tři nebo více dospělých bez závislých dětí / three or more adults without dependent children | 114,8 | 30,6% | 77,2% |
| jeden dospělý se závislými dětmi / single adult with dependent child (ren) | 71,3 | 30,3% | 64,1% |
| dva dospělí se závislými dětmi / two adults with dependent children | 521,5 | 48,5% | 74,9% |
| tři nebo více dospělých se závislými dětmi / 3 or more adults with dependent children | 98,8 | 45,9% | 74,2% |
| Typ lokality / Type of locality | | | |
| vysoká hustota populace / densely-populated area | 466,1 | 31,4% | 81,5% |
| střední hustota populace / intermediate area | 255,6 | 25,9% | 74,0% |
| malá hustota populace / thinly-populated area | 401,5 | 23,2% | 69,0% |
| Kraj / *Region* | | | |
| Hl.m. Praha | 199,8 | 36,7% | 86,6% |
| Středočeský | 131,3 | 28,7% | 78,6% |
| Jihočeský | 64,5 | 24,6% | 74,7% |
| Plzeňský | 62,4 | 27,5% | 70,3% |
| Karlovarský | 33,9 | 26,1% | 67,4% |
| Ústecký | 69,5 | 19,3% | 77,8% |
| Liberecký | 40,8 | 23,9% | 73,8% |
| Královéhradecký | 59,3 | 27,8% | 80,8% |
| Pardubický | 52,5 | 26,3% | 68,1% |
| Vysočina | 49,6 | 24,6% | 66,2% |
| Jihomoravský | 119,3 | 28,2% | 75,7% |
| Olomoucký | 62,3 | 23,9% | 78,3% |
| Zlínský | 45,6 | 19,2% | 59,4% |
| Moravskoslezský | 132,5 | 25,8% | 68,8% |

* Hodnota je procentem z celkového počtu domácností v dané socio-demografické skupině / *As a % of total number of households in given socio-demographic group*

** Hodnota je procentem z počtu domácností (v dané socio-demografické skupině), které mají osobní počítač / *As a % of households (in given socio-demographic group) which have personal computer*

## Zájem uživatelů internetu o e-government (zdroj: www.czso.cz)

*Interest of the internet users in e-government*

| | Uživatelé internetu, kteří mají zájem o využívání internetu k vyřizování na úřadech / Internet users who are interested in usage of e-government | | Z toho / in which | | | |
|---|---|---|---|---|---|---|
| | | | už někdy využili internet k vyřizování na úřadech / have ever used e-government services | | ještě nikdy nevyužili internet k vyřizování na úřadech / have never used e-government services | |
| | v tis. *in thous.* | %* | v tis. *in thous.* | %** | v tis. *in thous.* | %** |
| **Celkem 16+ / *Total 16+*** | 1 602 | 45,5% | 490 | 30,6% | 1 112 | 69,4% |
| **Pohlaví/ *Gender*** | | | | | | |
| Muži/ *Males* | 840,4 | 45,6% | 279,6 | 33,3% | 560,8 | 66,7% |
| Ženy/ *Females* | 762,3 | 44,8% | 205,4 | 26,9% | 556,9 | 73,1% |
| **Věková skupina/ *Age group*** | | | | | | |
| 16 - 24 let | 362,2 | 38,3% | 70,5 | 19,5% | 291,7 | 80,5% |
| 25 - 34 let | 476,6 | 51,1% | 166,7 | 35,0% | 309,9 | 65,0% |
| 35 - 44 let | 365,6 | 48,9% | 113,8 | 31,1% | 251,8 | 68,9% |
| 45 - 54 let | 256,2 | 44,5% | 84,1 | 32,8% | 172,1 | 67,2% |
| 55 - 64 let | 114,4 | 39,5% | 38,2 | 33,4% | 76,2 | 66,6% |
| 65 - 74 let | 26,0 | 61,0% | 10,9 | 42,1% | 15,0 | 57,9% |
| 75+ | . | . | . | . | . | . |
| **Vzdělání/ *Education*** | | | | | | |
| Základní/ *Primary* | 147,0 | 29,0% | 16,4 | 11,2% | 130,6 | 88,8% |
| Střední bez maturity / Secondary without GCE | 217,6 | 32,9% | 51,3 | 23,6% | 166,3 | 76,4% |
| Střední s maturitou / Secondary with GCE | 817,0 | 49,1% | 236,0 | 28,9% | 581,0 | 71,1% |
| Vysokoškolské/ *Tertiary* | 421,1 | 59,3% | 181,3 | 43,0% | 239,8 | 57,0% |
| **Zaměstnanecký status/ Employment status** | | | | | | |
| Zaměstnaní/ *Employed* | 1 182,2 | 47,3% | 384,1 | 32,5% | 798,1 | 67,5% |
| Nezaměstnaní/ *Unemployed* | 48,4 | 52,5% | 13,0 | 26,9% | 35,4 | 73,1% |
| Neaktivní/ *Inactive* | 372,0 | 39,1% | 87,8 | 23,6% | 284,2 | 76,4% |
| **Typ lokality / Type of locality** | | | | | | |
| vysoká hustota populace / densely-populated area | 671,7 | 50,5% | 212,3 | 31,6% | 459,4 | 68,4% |
| střední hustota populace / intermediate area | 369,4 | 43,2% | 100,7 | 27,3% | 268,7 | 72,7% |
| malá hustota populace / thinly-populated area | 561,6 | 41,4% | 172,0 | 30,6% | 389,6 | 69,4% |
| Kraj / *Region* | | | | | | |
| Hl.m. Praha | 275,3 | 49,9% | 71,0 | 25,8% | 204,3 | 74,2% |
| Středočeský | 230,8 | 55,4% | 78,0 | 33,8% | 152,8 | 66,2% |
| Jihočeský | 82,5 | 42,2% | 25,8 | 31,3% | 56,7 | 68,7% |
| Plzeňský | 81,6 | 43,3% | 21,8 | 26,7% | 59,8 | 73,3% |
| Karlovarský | 27,3 | 28,0% | 11,4 | 41,8% | 15,9 | 58,2% |
| Ústecký | 117,5 | 51,6% | 42,6 | 36,3% | 74,9 | 63,7% |
| Liberecký | 37,2 | 29,2% | . | . | 30,3 | 81,5% |
| Královéhradecký | 85,3 | 44,5% | 35,0 | 41,1% | 50,3 | 58,9% |
| Pardubický | 67,5 | 36,3% | 12,5 | 18,6% | 54,9 | 81,4% |
| Vysočina | 86,0 | 50,6% | 20,3 | 23,6% | 65,7 | 76,4% |
| Jihomoravský | 193,7 | 47,6% | 74,1 | 38,3% | 119,6 | 61,7% |
| Olomoucký | 59,3 | 30,3% | 30,4 | 51,2% | 28,9 | 48,8% |
| Zlínský | 76,7 | 42,9% | . | . | 68,3 | 89,0% |
| Moravskoslezský | 182,0 | 44,5% | 46,7 | 25,7% | 135,2 | 74,3% |

* Hodnota je procentem z uživatelů internetu v dané socio-demografické skupině / *As a % of the internet users in given socio-demographic group*

** Hodnota je procentem z uživatelů internetu (v dané socio-demografické skupině), kteří mají zájem využívat internet k vyřizování na úřadech / *As a % of the internet users (in given socio-demographic group) who are interested in usage of e-government*

Pozn. : šetření proběhlo ve 2.čtvrtletí 2006 / Note : survey period - 2nd quarter 2006

**Způsob připojení domácností k internetu - ve 2.čtvrtletí 2006 (zdroj: www.czso.cz)**
***Type of the internet connection used by households - in the 2nd quarter 2006***

| Způsob připojení / *Type of connection* | Domácnosti / Households | | |
|---|---|---|---|
| | v tis. / in thous. | %* | %** |
| Standardní telefonní linka / *Standart telephone line (dial-up)* | 391,3 | 34,8% | 9,3% |
| ISDN linka / *ISDN line* | 76,6 | 6,8% | 1,8% |
| Nízkorychlostní mobilní připojení (GPRS, HSCSD) / Narrowband *mobile connection* | 38,9 | 3,5% | 0,9% |
| Kabelová televize / *Cable TV* | 215,1 | 19,2% | 5,1% |
| ADSL nebo jiné DSL technologie / *ADSL or other DSL technologies* | 151,9 | 13,5% | 3,6% |
| Bezdrátové připojení (WLAN, Wi-Fi, WiMAX) / Wireless connection | 204,1 | 18,2% | 4,9% |
| Připojení přes mobilní telefon - vysokorychlostní / Broadband mobile connection | 50,7 | 4,5% | 1,2% |
| Jiný typ vysokorychlostního připojení / Other broadband connection | 28,4 | 2,5% | 0,7% |
| Vysokorychlostní připojení celkem / *Broadband connection total* | 636,3 | 56,7% | 15,1% |

* Hodnota je procentem z počtu domácností, které mají připojení k internetu / *As a % of number of households with the internet access*

** Hodnota je procentem z celkového počtu domácností / *As a % of total number of households*

# 5. Výhody open source řešení a otevřených formátů při elektronizaci justice

## 5.1. Otevřené formáty ve veřejné správě

Otevřený formát je publikovaná specifikace pro uchovávání digitálních údajů, obvykle udržovaná neproprietární standardizační organizací, bez právních omezení ohledně používaní. Primárním cílem otevřených formátů je garantovat dlouhodobý přístup k údajům bez současné nebo budoucí nejistoty ohledně (autorských) práv nebo technické specifikace. Běžným sekundárním cílem otevřených formátů je umožnit konkurenci, aby se konkrétnímu komerčnímu dodavateli nedovolila kontrola nad proprietárním formátem, a tím likvidovat konkurenční produkty.

Všechny počítače ukládají a přenášejí informace v kódované formě. Bývaly to např. velmi jednoduché reprezentace, kde určité číselné hodnoty představovaly určitý znak. Jejich složitost rovnoměrně narůstá s výkonem a složitostí počítačů, ale vždy se uplatňují určitá základní pravidla. Prvním důležitým pravidlem je, že jakákoliv taková volba kódování je svévolná (arbitrární) a ne přirozená volba. Číslo 33 může představovat písmeno „a" nebo „z" v závislosti na konvenci tohoto standardu. Není zde jeden správný způsob, pouze možné způsoby. Druhým důležitým pravidlem je, že jakmile byla data zakódována do určitého formátu, mohou být přečtena softwarem, který implementuje tento formát a implementuje ho přesně. Dokonce malá odchylka od konvencí formátu jednoduše způsobí obrovskou deformaci dat čili absolutní znečitelnění zprávy. Běžnou a nejvíce šetrnou podobou tohoto je ztracené nebo nepřesné formátování v softwaru pro zpracování textu. V nejhorším případě se stanou data neobnovitelnými. Z tržního pohledu tato situace obecně znamená selhání trhu. Zákazníci, kteří uložili svá data v jednom formátu, se mohou dostat do situace, kdy si nemohou vybrat jiného výrobce, protože tento nebyl schopen implementovat ten samý formát, nebo ho implementoval nedostatečně.

## 5.2. Otevřený standard pro elektronizaci soudnictví – pravidla a doporučení[186]

### *5.2.1. Doporučení*[187]

1. Otevřené standardy by měly být definovány ve smyslu požadovaného ekonomického efektu: podpory plné konkurence na trhu dodavatelů technologie a souvisejících produktů a služeb, i kdyby měl vzniknout přirozený monopol v samotné technologii.
2. Otevřené standardy pro trhy softwaru by měly být definovány s cílem kompatibility s FLOSS (Free/Open Source Software) licencemi, aby se dosáhlo tohoto požadovaného ekonomického efektu.
3. Kompatibilita s proprietárními technologiemi by měla být výslovně vyloučena z kritérií veřejných zakázek a nahrazena interoperabilitou s produkty několika výrobců.

[186] Srov. též Vondruška, P., Standard pro kategorizaci bezpečnosti vládních informací a informačních systémů - FIPS PUB 199, Data Security Management, DSM 4/2003, Praha.
[187] Zdroj a podrobněji viz. program Evropské komise Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizen – http://ec.europa.eu/idabc

4. Otevřené standardy by měly být povinné pro služby e-governmentu a upřednostňovány u všech dalších veřejných zakázek softwaru a softwarových služeb.

Možnost svobodně a jednoduše sdílet data s ostatními v síti je zásadní pro růst a stabilitu informační společnosti. Síťový efekt hraje v tomto rozhodující úlohu: více hodnoty připadne spotřebiteli, pokud používá tu samou technologii využívanou mnohými dalšími.

V roce 2002 několik společností a jedinců spolupracovalo na vytvoření alternativního a otevřeného datového formátu nazývaného OpenDocument Format (ODF). Tento formát souboru dokumentu založený na XML umožňuje spotřebitelům ukládat a vyměňovat si upravitelné (editovatelné) kancelářské dokumenty (vč. zápisků, zpráv a knih), tabulky, grafy a prezentace. ODF byl vyvinut pod standardizačním konzorciem Organization for the Advancement of Structured Information Standards (OASIS) a schválen Mezinárodní organizací pro normalizaci (ISO) v květnu 2006. Jeho licenční podmínky jsou bez „háčků." Kdokoliv má volnost s ním pracovat. Ve skutečnosti je ODF jediným standardem pro upravitelné kancelářské dokumenty, který byl prozkoumán nezávislým uznávaným normalizačním úřadem, je implementován několika výrobci a může být implementován kýmkoliv, kdo je ochoten vynaložit úsilí, vč. výrobců proprietárního softwaru, a také vývojářů využívajících open-source software licence, jako např. GNU LGPL nebo GNU GPL.

### *5.2.2. Pravidla pro otevřený IT standard v resortu justice*[188]

Dvě oblasti jsou rovnocenně důležité pro určení, zda je technická specifikace skutečně otevřeným standardem: jak je vytvořen a spravován a jak může být užíván.

1. Tvorba a správa otevřeného standardu

- Proces vývoje a správy musí být formou spolupráce a musí být demokratický.
- Účast musí být přístupná všem, kdo si přejí se zúčastnit a mohou splnit spravedlivá a přiměřená kritéria uvalená organizací, pod kterou je vyvíjen a spravován.
- Procesy musí být zdokumentovány a pomocí známé metody mohou být změněny díky vkladu (vstupu) od všech zúčastněných.
- Proces musí být založen na formálních a povinných závazcích pro odhalení a licencování práv duševního vlastnictví.
- Vývoj a správa musí usilovat o konsenzus a odvolací proces musí být jasně navržen (dán).
- Specifikace standardu musí být otevřena rozsáhlému veřejnému prozkoumání (revizi) alespoň jednou během životního cyklu, s úplnou diskuzí připomínek a při potřebě musí být podle nich postupováno.

2. Užití a licencování otevřeného standardu

- Standard musí popsat rozhraní, ne implementaci, a průmysl musí být schopen vytvořit vícero konkurenčních implementací rozhraní popsaného ve standardu bez nepřiměřených a omezujících překážek. Rozhraní zahrnuje API, protokoly, schémata, datové formáty a jejich kódování.

[188] Zdroj a podrobněji viz. program Evropské komise Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizen – http://ec.europa.eu/idabc.

- Standard nesmí obsahovat žádné majetkové „háčky", které vytváří technickou nebo ekonomickou bariéru.
- Svědomité implementace standardu musí vzájemně spolupracovat (interoperate). Interoperabilita znamená schopnost počítačového programu komunikovat a vyměňovat informace s jinými počítačovými programy a vzájemně užívat informace, které si vyměnily. To zahrnuje schopnost použít, převést (konvertovat) nebo vyměnit si souborové formáty, protokoly, schémata, informace a konvence rozhraní tak, aby se povolilo počítačovému programu pracovat s jinými počítačovými programy a uživateli všemi způsoby, kterými se zamýšlí jejich fungování.
- Musí být dovolené každému kopírovat, distribuovat a číst standard za nominální poplatek nebo dokonce bez něj. Pokud je poplatek stanoven, musí být dostatečně nízký, aby se nevyloučilo široké používání.
- Musí být možné pro každého obdržet bezplatné (bez honoráře nebo poplatku; také známé pod „royalty free"), celosvětové, neexkluzívní a trvalé licence na všechny nezbytné patentové nároky pro výrobu, užití a prodej produktů založených na standardu. Jedinými výjimkami jsou ukončení pro vzájemnost (terminations per reciprocity) a ustanovení obranného odvolání (defensive suspension terms). Nezbytné patentové nároky zahrnují probíhající, nezveřejněné i zveřejněné patenty a patentové žádosti. Licence je pouze pro přesný rozsah (působnost) daného standardu.
- Může být podmíněna pouze na vzájemnou licenci kteréhokoliv patentového nároku nabyvatelů licence, nezbytného pro praktické použití standardu (také jako vzájemné ujednání - reciprocity clause).
- Může být ukončena kterémukoliv nabyvateli licence, který žaluje poskytovatele licence nebo kteréhokoliv dalšího nabyvatele licence za porušení patentového nároku, nezbytného k praktickému užití standardu (také jako ustanovení obranného odvolání - defensive suspension clause).
- Stejné licenční podmínky (ustanovení) jsou k dispozici každému potenciálnímu poskytovateli licence.
- Licenční podmínky otevřených standardů nesmí (předem) vyloučit implementace standardu pod licenčními podmínky open-source nebo omezujícími licenčními podmínkami.

## 5.3. Nasazení Open Source software v justici

### *5.3.1. Pojem Open Source software*

Za Open Source[189] se pokládají takové aplikace, které jsou šířeny se zachováním určitých práv a svobod pro jejich koncového uživatele (tedy nabyvatele licence). Jde o práva spouštět program za jakýmkoliv účelem, studovat, jak program pracuje a přizpůsobit ho svým potřebám (předpokladem k tomu je přístup ke zdrojovému kódu), redistribuovat kopie dle svobodné vůle, vylepšovat program a zveřejňovat tato zlepšení.

[189] Viz. též Štědroň, B., LinuxBizWorld, O právo a Open Source, IDG, 24.4.2006, ISSN 1801-2906.

### 5.3.2. *Zdrojový a objektový kód*

Jako zdrojový kód či zdrojový text se označuje text počítačového programu zapsaný v některém (obvykle vyšším) programovacím jazyce. Tento text je poté předlohou (zdrojem) pro jiný počítačový program, který ho buď přímo provádí (tzv. interpretuje, viz interpret), nebo z něj vytvoří samostatně spustitelný soubor (viz kompilátor). Objektový kód pak vytváří kompilátor ze zdrojového kódu programu.

### 5.3.3. *Vztah mezi Open Source a Free Software (svobodným software)*

Oba pojmy, tedy Open Source a svobodný software (angl. Free Software), je možno používat jako synonyma. Rozdíl mezi oběma pojmy je spíš ideologický, resp. filozofický, ale základní idea sdílení souborů (zdrojového kódu) je stejná. V praxi tedy oba pojmy mají v zásadě shodný obsah, tedy jde o distribuci softwaru takovým způsobem, že koncový uživatel má vždy právo na získaní zdrojového kódu programu a dále má právo tento zdrojový kód upravovat a distribuovat.

Ani v zahraniční literatuře není často mezi oběma pojmy rozlišováno. Podrobný vývoj obou pojmů je k dispozici na stránkách encyklopedie Wikipedie.[190] Navíc v angličtině se obecně dává přednost pojmu Open Source před pojmem Free Software. Anglické slovo „free" má totiž dva významy a to „zdarma" a „svobodný". Svobodný software je ale svobodný v tom smyslu, že vždy musí být distribuován se zdrojovým kódem, tedy jedná se o svobodu program jakkoliv upravovat a dále redistribuovat. Společnosti, které prodávají komerční software, obvykle zdrojový kód programu tají a nedávají jej k dispozici. To je také důvod, proč může být komerční software často chybový, protože existuje malá kontrola nad vývojem softwaru. Open Source ale neznamená, že tento software musí být nutně distribuován zdarma. Open Source je možné prodávat, ale vždy musí být k dispozici zdrojový kód, který si potom může uživatel sám upravovat a dále software svobodně distribuovat. Proto se právě před dvojsmyslným pojmem Free Software (svobodný software nikoliv software zdarma) dává přednost pojmu Open Source (tedy otevřený software ve smyslu, že je k dispozici zdrojový kód). Pro více informací k oběma pojmům je možno se podívat na stránky Free Software Foundation[191] nebo Open Source Initiative.[192]

A jeden důvod navíc, proč by se mezi oběma pojmy nemělo rozlišovat: Open Source (svobodný software) není nic, co by se mělo týkat uzavřeně skupiny lidí, ale cílem je open source masově rozšířit, aby představoval významnou konkurenci proprietárnímu (komerčnímu) software (což přinese i výrazné snížení ceny komerčního software). A proto není důvod do jisté míry mást laiky a lpět na rozlišování této terminologie. Zjednodušeně platí Open Source rovná se rovná Free Software (svobodný software). Kompromisně je možné používat zkratku OSS/FS (tedy Open Source Software and Free Software).

[190] Viz. www.wikipedia.org.
[191] Viz. www.fsf.org.
[192] Viz. www.opensource.org.

### *5.3.4. Pojem licence (licenční ujednání)*

Jakým způsobem lze právně se softwarem (programem) zacházet určuje právní dokument tzv. licence, která je připojená k počítačovému programu a ve které jsou uvedena práva a povinnosti smluvních stran (ve většině případů spíše práva a povinnosti nabyvatele licence). A právě podle druhu licencí, resp. podle způsobu a rozsahu užití počítačového programu lze pak počítačové programy (software) rozdělovat na Open Source, Shareware, Freeware, tzv. proprietární software a jiné. Protože ale hranice mezi jednotlivými typy licencí (typy software) nejsou často ostré, vždy platí, že uživatel by se měl důkladně seznámit s licenční smlouvou a ne ji jenom „odkliknout", jak se pravidelně stává.

### *5.3.5. K některým dalším pojmům*

Public domain (pojem se používá v anglosaském světě) je software bez vyhrazených práv, tzn. že není nijak chráněný. Jinými slovy je možné jej libovolně používat, kopírovat, popř. měnit. Laicky řečeno u Public Domain se jedná o software, se kterým můžeme libovolně nakládat, aniž bychom se museli strachovat, že porušujeme autorská práva. Příkladem z praxe mohou být počítačové programy, kterým uplynula doba trvání majetkových práv (doba majetkových práv trvá 70 let od smrti autora a po uplynutí této doby je možno software volně používat).

Copyleftovaný software (software opatřený doložkou Copyleft) je svobodný software bez všech dalších omezení při rozšiřování nebo jeho změně. Copyleftovaný software je typ svobodného software, který nedovoluje přidávat nějaká další omezení, pokud někdo programový kód modifikuje či dále distribuuje. Znamená to, že každá další kopie, dokonce i když byla změněna, musí zůstat svobodným softwarem. To představuje určité nebezpečí pro softwarové společnosti, které využijí při vývoji svého programu copyleftovaný software, protože potom celý nově vyvinutý program musí zůstat svobodný (tedy musí být zveřejněn zdrojový kód). Hovoří se o tzv. infikování proprietárního software.

Proprietární (komerční) software jsou všechny počítačové programy, k jejichž zdrojovému kódu nemá uživatel přístup (zdrojový kód nelze tedy studovat) a počítačové programy, které uživatel nemůže měnit, z čehož vyplývá, že uživatel proprietárního software nemůže ovlivnit jeho funkčnost. Takovýto software tedy není z pohledu Open Source svobodný. Jeho svobodné užívání, změna či šíření jsou zakázány nebo je třeba zažádat o povolení. Typickým příkladem proprietárního software je MS Windows.

Shareware je software s povolením šířit kopie, ale každý, kdo se rozhodne jej trvale používat, má povinnost zaplatit licenční poplatek. Poskytování počítačového programu jako shareware je dnes již běžným ekonomickým modelem, který je využíván velkým počtem softwarových společností. Ve většině případů je sharewarový počítačový program zpřístupňován koncovým uživatelům prostřednictvím sítě internet, což umožňuje obejít tradiční nákladnější modely propagace a distribuce software. Často bývají tyto počítačové programy umisťovány na CD-ROM či DVD-ROM, jako příloha nejrůznějších specializovaných periodik. Potencionálním zákazníkům přináší shareware tu výhodu, že si počítačový program mohou vyzkoušet ještě předtím, než za jeho užívaní zaplatí. Po zaplacení obdrží uživatel heslo, kterým program „oživí", nebo celý nový program v poslední verzi s neomezenou dobou užívání.

Freeware je software, který je šířen zdarma, například na internetu nebo na různých CD. Program je možno provozovat zdarma po neomezenou dobu a je možno jej i zdarma šířit dále.

Není však dovoleno (stejně jako u shareware) šířit jej za úplatu. Z původní definice freeware také plyne, že autorská práva k takovému programu drží jeho autor a není tedy dovoleno bez jeho souhlasu program jakkoliv měnit či upravovat pro komerční účely. Typickým příkladem freeware je dnes velmi rozšířená Java od Sun Microsystems.

Při tzv. licenci OEM (Original Equipment Manufacture) se jedná o software, který je předinstalovaný na počítači a zákazník jej získá již s koupí počítače. Např. společnost Microsoft tímto způsobem často distribuuje svůj software (typicky MS Windows). Licence pořízená touto formou je vázaná na počítač, na kterém byl software nainstalován. Jinými slovy software nelze nainstalovat na žádný jiný počítač a v případě ztráty nebo zničení počítače, kde je software nainstalován, zaniká i tato licence a program již není dovoleno dále používat. Pokud dojte k prodeji počítače, potom nabyvatel získává automaticky i tuto licenci a oprávnění software požívat. Všechny produkty pod licencí OEM jsou tak vlastně vázány na hardware a není možné je koupit samostatně.

Adware je program (druh licence), který můžete užívat zdarma. V programu se ale objevuje placená reklama, za kterou získává autor peníze. Stejně tak program nesmí být měněn a zejména nesmí být odstraněna reklama, která se během používání programu objevuje (obvykle je stahována z internetu).

### 5.4. Důvody pro využívání Open Source software v justici

Hlavní důvody pro využívání Open Source software a otevřených formátu ve veřejné správě jsou tyto:[193]

(1) ekonomická výhodnost a úspory při využívání Open Source software a otevřených formátů
Většina Open Source produktů (kancelářský software, webový prohlížeč atd.) jsou k dispozici zdarma včetně aktualizací, tedy odpadá placení licenčních poplatků.

(2) Zvýšení bezpečnosti při komunikaci ve veřejné správě
Při využívání proprietárního (komerčního) softwaru neexistuje přístup ke zdrojovým kódům aplikace a tedy není možnost kontroly činnosti aplikace (softwaru). Organizace se tedy může vystavovat riziku např. průmyslové špionáže nebo odposlechu bezpečnostních složek, protože během práce s textovým souborem může proprietární (komerční) aplikace posílat soubory z počítače organizace (úřadu) konkurenci.

(3) Snížení softwarového pirátství
Většina nejčastěji užívaných open source aplikací (software) jsou k dispozici zdarma a je možno je neomezeně kopírovat. Open Source software tedy díky své povaze minimalizuje porušování autorských práv a softwarové pirátství.

(4) Elektronická archivace dokumentů
Pokud dnes chcete pracovat s daty (soubory), které jste vytvořili a uložili např. před 5 lety, potom to může pro Vaší organizaci představovat velký problém, protože např. dnešní novější verze softwaru již problematicky pracují se soubory

[193] Srov. též Štědroň, B., O politice státu v oblasti informačních a komunikačních technologií. Společná příloha Ekonomu a Hospodářských novin, 22.6.2006, ISSN 1210-4817.

uloženými ve starších nebo jiných verzích softwaru. Otevřené formáty (Open Document Format) pracují v standardu schváleném jako ISO norma, a tedy máte jistotu, že i za 100 let budete moci s daty pracovat.

(5) Podpora tržního prostředí a konkurenceschopnosti na trhu s kancelářským softwarem
Využíváním otevřených formátů ve veřejném a soukromém sektoru se umožní, že jakákoliv společnost, která vyvíjí kancelářský software (typicky textový a tabulkový procesor) bude moci zajistit 100% kompatibilitu svého softwaru se softwarem jiné společnosti. Laicky řečeno, vytvoříte-li datový soubor v jakémkoliv softwaru a pošlete jej třetí osobě, tato třetí osoba s ním vždy bude moc bez problému pracovat. Tímto bude prolomeno monopolní postavení některých softwarových firem a dán nový impuls trhu pro rozvoj kancelářského softwaru. Navíc tím bude naplněno heslo, že e-government nesmí občany nic stát, protože díky otevřeným formátům bude mít každý občan nebo podnikatel volbu, zda si koupit proprietární software nebo použít zdarma např. kancelářský balík OpenOffice.org.

## 5.5. Příklady nejčastěji užívaných Open Source aplikací[194]

| Název softwaru | Charakteristika | Plně nahradí tento placený software |
|---|---|---|
| 1) *OpenOffice.org Writer* | textový editor | náhrada za MS Word |
| 2) *OpenOffice.org Calc* | tabulkový procesor | náhrada za MS Excel |
| 3) *OpenOffice.org Impress* | prezentační nástroj | náhrada za MS PowerPoint |
| 4) *OpenOffice.org* | Base - databázový systém | náhrada za MS Access |
| 5) *Gimp* | grafický editor | náhrada za Adobe Photoshop |
| 6) *OpenXchange* | groupwarový nástroj, kalendář, e-mailový server, vedení projektů apod. | náhrada za MS Exchange, Lotus Notes či Novell GroupWise |
| 7) *Mozilla Firefox* | internetový prohlížeč | náhrada za Internet Expolorer |
| 8) *Mozilla Thunderbird* | e-mailový klient | náhrada za MS Outlook |
| 9) *Apache Web Server* | nástroj pro provoz internetových stránek a portálů | |
| 10) *Drupal* | redakční systém pro provoz zpravodajských portálů, intranetů apod. | |

[194] Podrobněji viz. internetové stránky Společnosti pro výzkum a podporu Open Source (www.oss.cz), jejímž jedním ze zakladatelů je i autor této publikace.

# 6. Příklady komerčních řešení informačních systémů vhodných k využití v resortu justice

## 6.1. Úvod

V rámci elektronizace justice musí existovat dva komplexní informační systémy, a to systém spisové služby (elektronický oběh dokumentů v rámci resortu justice) a systém elektronického soudního řízení, jehož základním kamenem bude elektronický spis, do kterého budou mít účastníci řízení přístup dálkově prostřednictvím sítě internet.

Nemá vůbec smysl, aby si stát tyto systémy budoval vlastními silami a v rámci jednotlivých resortů, protože komerční společnosti takovéto aplikace (software) již dávno mají vyvinuté a trhem prověřené. Důležité je tedy vybrat pouze ten správný informační systém a přizpůsobit jej na míru konkrétním požadavkům a potřebám resortu. Stejně tak je i extrémně důležité precizně upravit právní vztahy s dodavatelem takového systémů a to především s ohledem na odpovědnost a náhradu škody při chybovosti systémů (možno řešit např. tak, že dodavatel bude muset uzavřít vysokou pojistku z profesní odpovědnosti atd.).

Dále je třeba sjednotit standardy ministerstev a způsob identifikace a popisu dokumentu. Veškeré informační systémy ve veřejné správě by měly být založeny na otevřených formátech a ideálně by měly také vycházet z Open Source Softwaru, který je zdarma (resp. z těch aplikací open source, které jsou k dispozici zdarma).[195]

V této kapitola jsou popsána řešení soukromých společností, která jsou již úspěšně využívána jak ve veřejné správě, tak v soukromém sektoru (např. v bankovnictví nebo na městských úřadech).

## 6.2. Informační systém Gordic GINIS

### *6.2.1. Obecně*

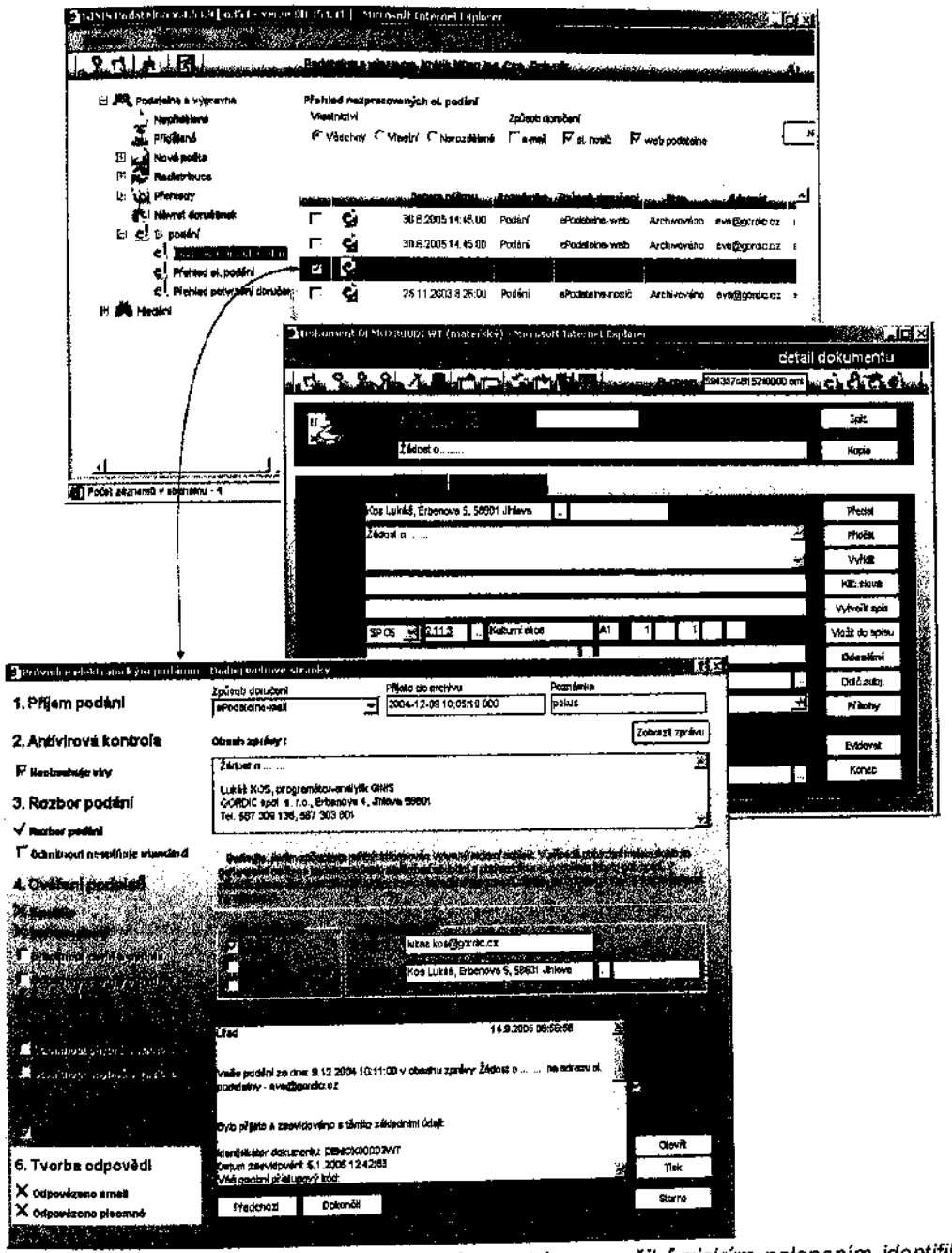
Systém Spisové služby ("SSL") plní roli evidenci veškerých údajů o dokumentech i spisech a jejich pohybu v organizaci. Oběh jednotlivých dokumentů mezi moduly SSL je závislý na vykonávaném procesu (předání k vyřízení, stornování, vrácení k doplnění, předání do předarchivní péče atd.), který je řízen metodikou SSL a interními normami organizace (zejména Spisovým a skartačním řádem).[196]

[195] Podrobněji viz Štědroň, B., Open source best option for e-gov't, Czech Business Weekly, 24.7.2006, ISSN 1214-8415.
[196] Podrobněji viz. www.gordic.cz.


*Obrázek: Základní moduly systému Spisové služby GINIS SSL. Zdroj: Gordic.*

### *6.2.2. Podatelna (POD)*

Modul POD slouží pro hromadný příjem, označování, evidenci a roztřiďování dokumentů. Modul Podatelna kromě příjmu „klasických" (analogových) podání také kompletně řeší problematiku elektronické podatelny - umožňuje příjem podání dokumentů v digitální podobě, tj. dle vyhlášky 496/2004 Sb., o elektronických podatelnách a zákona 227/2000Sb. o elektronickém podpisu. Dále zajišťuje vnitroorganizační tok dokumentů. Uživateli je k dispozici i podpora hromadného návratu dodejek do organizace. Dokument vstupující do systému podléhá přísné evidenci a je tedy označen jednoznačným Prvotním identifikátorem (PID). Dokument lze označit fyzickým nalepením identifikátoru, nebo pouhým vygenerováním tohoto identifikátoru uvnitř modulu.

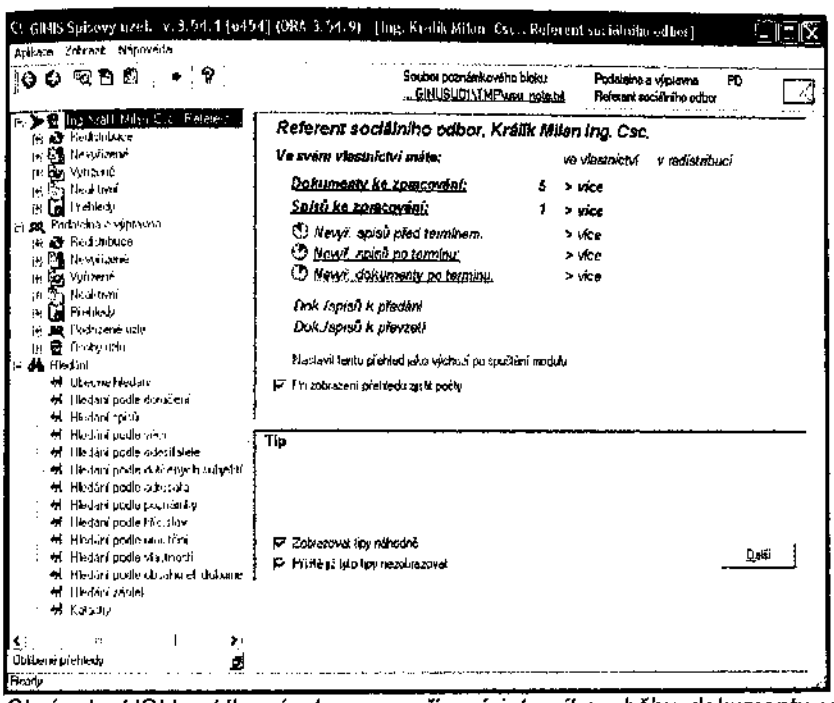



*Obrázek: POD - Elektronické podání: dokument lze označit fyzickým nalepením identifikátoru, nebo pouhým vygenerováním tohoto identifikátoru uvnitř modulu. Zdroj: Gordic.*

### 6.2.3. *Univerzální spisový uzel (USU)*

Modul Univerzální spisový uzel umožňuje evidovat veškeré údaje o dokumentech i spisech včetně sledování jejich pohybu v organizaci. Modul umožňuje podání došlých i vlastních dokumentů, kde jako základní evidenční prvek používá prvotní identifikátor (PID) u dokumentů evidovaných v podacím deníku prvotní identifikátor a číslo jednací. Modul dále sleduje profilové i pomocné údaje o dokumentu (věc, odesilatel, klíčová slova, typ dokumentu, úroveň přístupu...), vytváří spis, umožňuje zadání údajů o stornu, ztrátě, nalezení, způsobu vyřízení, přerušení a obnově vyřizování, nabytí právní moci, zadání spisových a

skartačních znaků a skartačních lhůt, ukládání dokumentů do operativních úložných míst, zadání údajů o odeslání dokumentu mimo organizaci a následné zpracování doručenek.



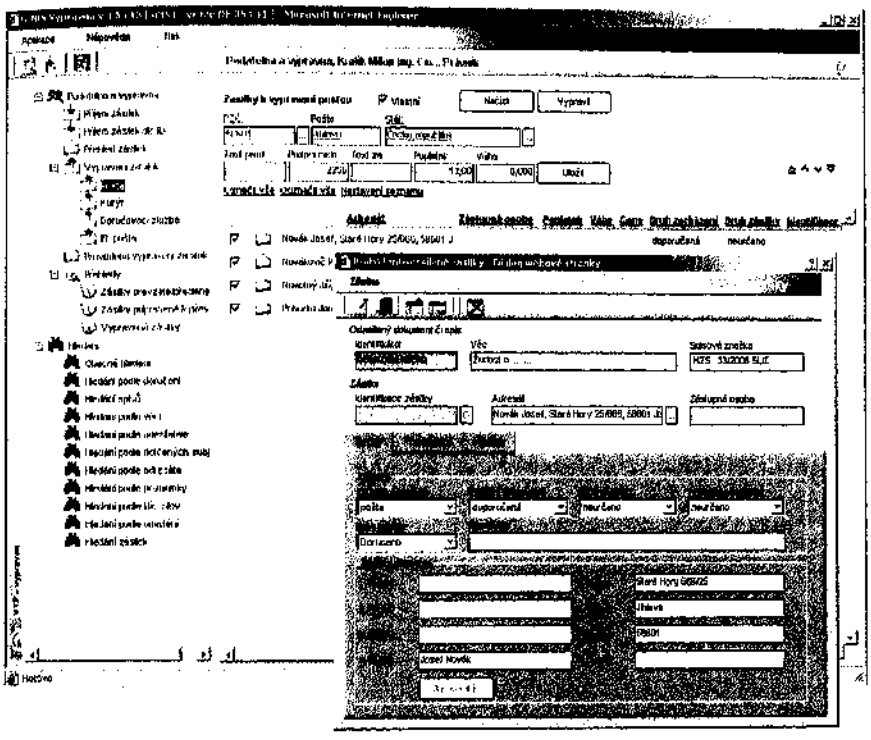

*Obrázek: USU - Hlavní okno: pro řízení interního oběhu dokumentu v organizaci slouží důsledné předávání a převzetí včetně sledování osobní zodpovědnosti. Zdroj: Gordic.*

### *6.2.4. Vedoucí (VED)*

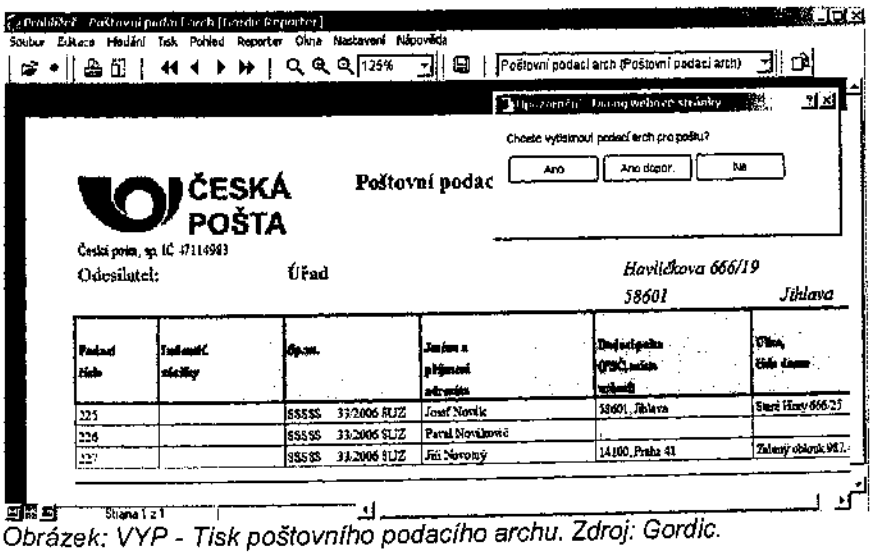
Modul Vedoucí slouží pro manažerské a controllingové činnosti příslušející vedoucím a pro prohlížení záznamů o evidovaných dokumentech. Modul předpokládá součinnost s ostatními moduly Spisové služby, pomocí nichž se provádí operace evidenčního charakteru. Modul přináší přehledy o podaných, evidovaných a vyřizovaných dokumentech systému GINIS příslušné organizační jednotky nebo celé organizace. Umožňuje realizovat vybrané činnosti příslušející vedoucím a slouží pro prohlížení záznamů o evidovaných dokumentech, neumožňuje tedy pořizování nových záznamů.

### *6.2.5. Výpravna (VYP)*

Modul VYP slouží především k vypravení zásilek mimo organizaci. Zpracovává zásilky vznikající v modulu USU při odeslání dokumentů. Hlavní funkčnost modulu Výpravna spočívá v příjmu odesílaných zásilek od jednotlivých spisových uzlů, jejich evidenci, následném třídění a vypravení odesílaných zásilek mimo organizaci (poštou, doručovací službou, atd.). Uživatel má k dispozici obecné přehledové a vyhledávací funkce, pomocí kterých lze téměř libovolně vytvořit požadovaný přehled zásilek či dokumentů podle potřebných kritérií.



*Obrázek: VYP - Detail odesílané zásilky. Zdroj: Gordic.*




*Obrázek: VYP - Tisk poštovního podacího archu. Zdroj: Gordic.*

## E-Výpravna

Výhody e-Výpravny:

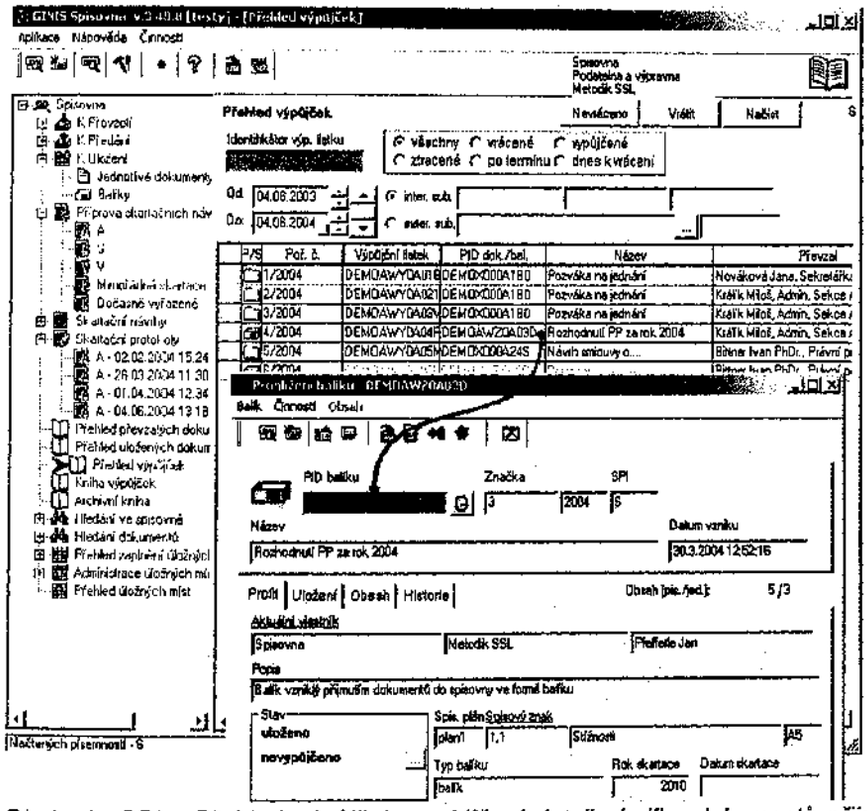
- bezpečnost - jediný styčný bod s internetem
- jedna e-mailová adresa
- jediný elektronický podpis

S ohledem na stále rostoucí potřebu komunikace elektronickou poštou, možnost využití elektronického podpisu či značky a zároveň na nutnost zachování vysokého stupně bezpečnosti byl systém GINIS rozšířen o možnost odesílat elektronické zprávy z jednoho

místa organizace, tzv. Elektronické výpravny. Toto místo bude z důvodu bezpečnosti jediným výstupním bodem úřadu pro elektronickou komunikaci směrem ven (napojeno na internet).

### *6.2.6. Spisovna (SPI)*

Modul je určen pro správu centrálních i odborových spisoven a evidenci dokumentů v předarchivní péči. Modul Spisovna umožňuje přijímat dokumenty do spisovny, sledovat a kontrolovat kapacitu úložných míst, sledovat a evidovat zápůjčky. Modul dále vytváří skartační návrhy a skartační protokoly. Takto uložené dokumenty již nevstupují do „běžného života". K základním evidenčním údajům se přidávají informace o lokaci (místě uložení) a případných výpůjčkách. Modul spolupracuje s ostatními moduly subsystému Spisové služby, především s modulem USU.




*Obrázek: SPI - Přehled výpůjček: prohlížení detailu balíku dokumentů přijatých do spisovny. Zdroj: Gordic.*

### *6.2.7. Generátor podacích deníků (TPD)*

Modul TPG slouží především pro tisk podacího deníku za dané období. Modul Generátor podacích deníků umožňuje načítat data z databáze, která již byla do systému Spisové služby zadána některým z ostatních modulů Spisové služby. Sestavy Podacího deníku pro celou organizaci, které modul generuje, jsou pro archivní účely legislativně povinné a jejich tisk je nutno provádět v pravidelných intervalech.

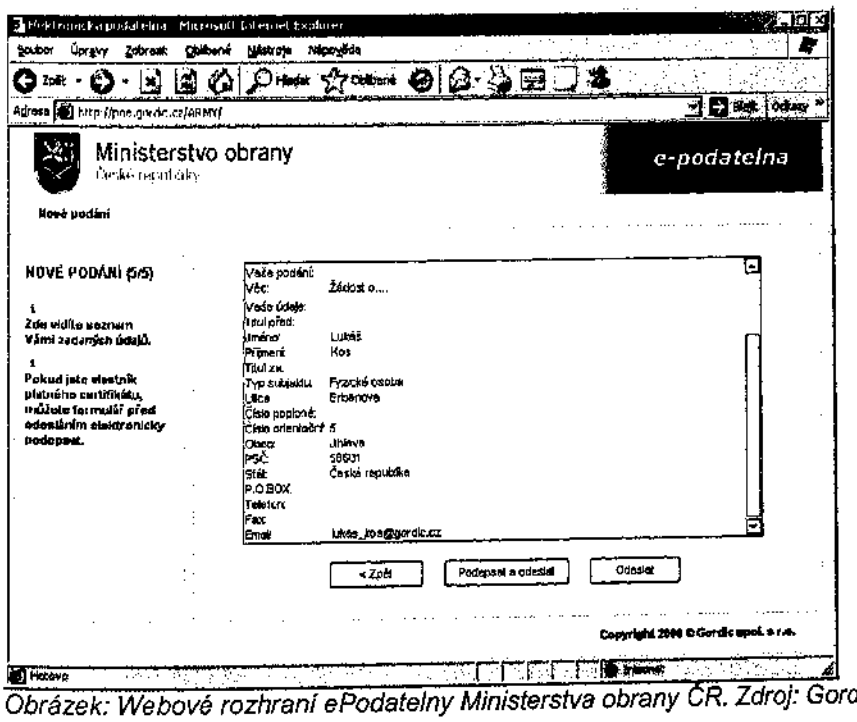
### 6.2.8. *Úkoly (UKO) a Usnesení a porady (USN)*

Modul UKO řeší komplexním způsobem agendu úkolů, jež je agendou sdílenou. Úkoly jsou chápány jako evidované činnosti vyvolané písemným zadáním s termíny splnění a s povinností hlásit splnění, případně i průběh, anebo ohrožení splnění úkolu. V rámci jednoho úkolu je jeden konkrétní nositel odpovědný za splnění celého zadání jednomu konkrétnímu zadavateli. Nositel může přenášet část, anebo celé zadání na další pracovníky (nezbavuje se tak ale výše uvedené zodpovědnosti za splnění jemu zadanému úkolu). Stává se tak zadavatelem dalších (podřízených) úkolů. Každý úkol může být navázán na zdrojový dokument, evidovaný ve Spisové službě.

Modul USN řeší komplexním způsobem agendu usnesení a porad. Modul Usnesení umožňuje vytváření a sběr podkladů pro jednání, přípravu textace a výroků k jednotlivým bodům. Výsledný zápis z jednání včetně prezenční listiny je automaticky evidován ve Spisové službě a je možné jej publikovat např. na portálu organizace.

### 6.2.9. *Užití digitálních dokumentů a převod dokumentů do digitální podoby*

Webové rozhraní (POE) příjemnou uživatelskou formou umožňuje vnějšímu uživateli zaslat své podání v elektronické formě a elektronicky podání podepsat. Takto vzniklá e-podání jsou dále řádně zpracována modulem POD plně v souladu se souvisejícími legislativními požadavky a dle zákona o elektronickém podpisu. Vnější uživatel získá jednoznačnou identifikaci podaného dokumentu i osobní přístupový klíč, pomocí kterého má možnost se v budoucnu pomocí POE dotazovat na aktuální stav vyřizování svého podání.



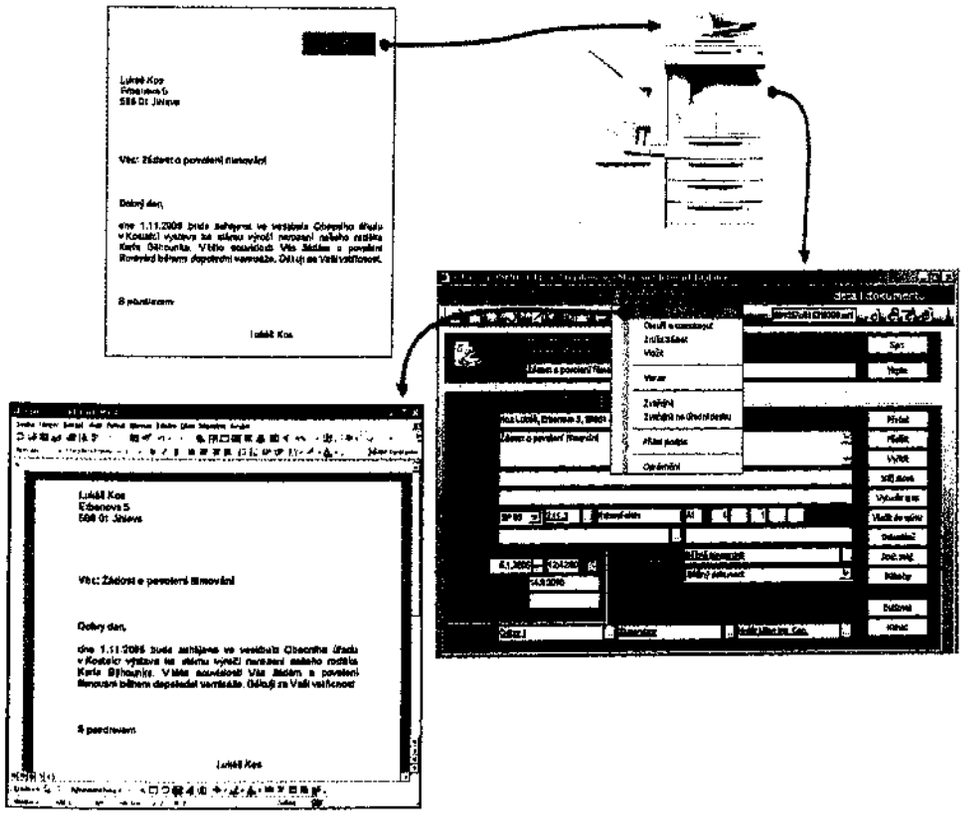
*Obrázek: Webové rozhraní ePodatelny Ministerstva obrany ČR. Zdroj: Gordic.*

## Elektronický podpis

Elektronický podpis je možné využít v SSL jak interně pro jednoznačnou autorizaci dokumentů vznikajících uvnitř organizace (např. pro jednotlivé verze postupně vznikajícího dokumentu), tak především pro autorizovanou a případně i šifrovanou komunikaci s jinými subjekty.

## Skenovací linka

Skenovací linka je řešena jako součást integrovaného informačního systému GINIS. Originální analogové dokumenty je možné ihned po skenování uložit do spisovny. Podle velikosti organizace a podle technické a technologické úrovně vybavení je možné tímto způsobem zpracovávat buď všechny analogové dokumenty, nebo jen vybrané, např. s vyšší očekávanou zátěží na rozkopírovávání a předávání. Výhodou tohoto řešení je snížení objemu předávaných analogových dokumentů, zmenšení množství rozkopírovaných dokumentů, minimalizace rizika ztráty dokumentů, výrazně vyšší dohledatelnost dokumentů a možnost provázanosti na plnotextové prohledávání obsahu dokumentů.



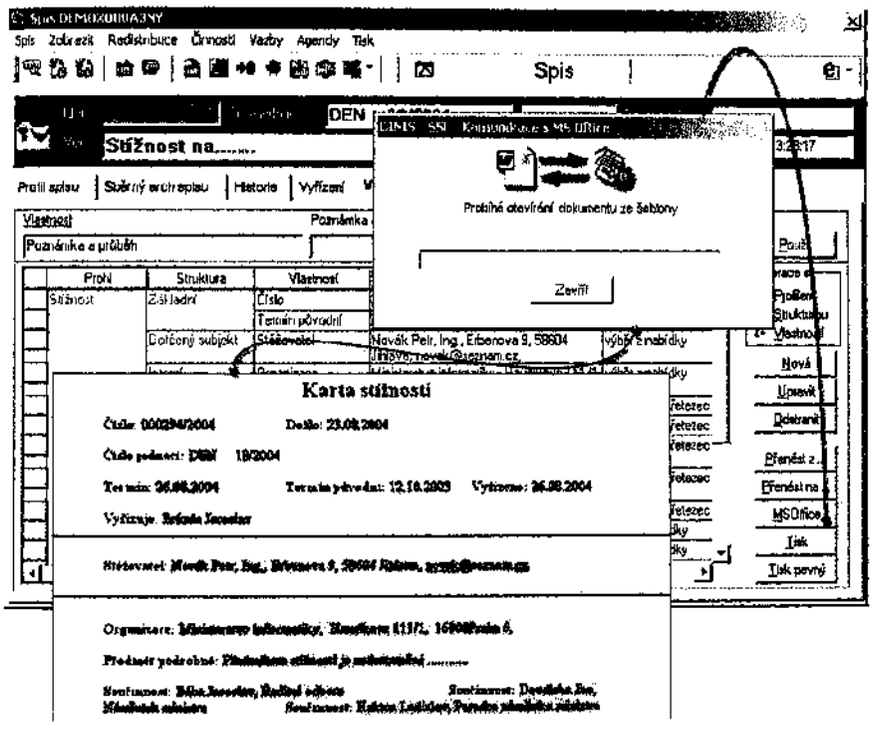
Obrázek: Skenovací linka - s naskenovanými dokumenty může uživatel dále pracovat již výhradně v elektronickém tvaru.

## Frankovací stroje

Spisová služby GINIS umožňuje prostřednictvím aplikace Výpravna propojení s některými typy moderních frankovacích strojů. Tím lze přes vydefinovaný interface automaticky načítat z frankovacího stroje do systému GINIS údaje o poplatku a váze k jednotlivým zásilkám.

### Integrace MS Office

Systém je oboustranně integrován s běžnými kancelářskými systémy. Systém Spisové služby GINIS umožňuje např. přímou tvorbu strukturovaných dokumentů prostřednictvím šablon či automatizovaný příjem i odesílání e-mailů ze systému. A to vše velice jednoduše pro obsluhu (drag-drop).




Obrázek: Integrace směrem ven. Zdroj: Gordic.

Spisová služba představuje jeden z klíčových subsystémů IS GINIS. Subsystémy jsou dále členěny na specializované komponenty (agendy a programové moduly), které svojí funkčností umožňují komfortní, průkazné, přehledné a výkonné vedení podvojného účetnictví, rozpočtování, spisové služby atp. Za účelem komunikace systému GINIS s externími systémy je systém vybaven vrstvou společných rozhraní (interface).


*Obrázek: Schéma IS GINIS - komplexní řešení informačního systému. Zdroj: Gordic.*

## 6.3. Objentis Software Integration

### *6.3.1. DM Systémy dnes*

Pod pojmem Dokument Management (DM) rozumíme v Evropě správu systémů původně papírových dokumentů v elektronických systémech. Pro lepší odlišení od obyčejné správy papírových dokumentů se také používá označení ECM - ELECTRONIC CONTENT MANAGEMENT jako nejvyšší možná organizace elektronických obsahů. Zkratka DMS znamená Dokument-Management-System a je v rozšířeném smyslu používána pro celkové zpracovávání jak elektronických, tak papírových dokumentů.[197]

OBJENTIS rozumí pod pojmem Document Management systém s následujícími znaky:

- DM-systém slouží správě méně strukturovaných informací v institucích (nejde o správu databází)
- Způsob práce s daty umožní přehledné ukládání a znovuvyvolání dokumentu
- Metadata (ID, Verze, Status tec.) jsou vytvářena a používána jako základní funkcionalita
- Robustní vyhledávací funkce umožňují libovolné prohledávání obsahů
- Existuje rozvětvený a bezpečný systém oprávnění pro zákonem nebo jinak definovaný přístup k informacím
- Systém disponuje Groupware- a Workflow funkcemi pro řízení Business procesů a Output Managementu

[197] Podrobněji viz. www.objentis.at.

### *6.3.2. Co je DMSs?*

DMSs je inteligentní řešení založené na platformě IBM LOTUS NOTES, slouží správě a uchovávání dokumentů nejrůznějšího typu. DMSs umožňuje integraci dat a psaných informací do jedné databanky. Informace jsou seskupeny v přehledné formě dle příslušných datových vztahů.

Díky použití RELACÍ je zajištěna přehlednost a minimalizovány redundantní vstupy. Kategorizované náhledy umožňují rychlé hledání v dokumentech a jejich verzích dle zadaných kriterií. Od fulltextového hledání v databázích až po texty uložených dokumentů.

DMSs využívá funkcionální přednosti Lotus Notes, ale v mnohém je daleko předčí. Díky hlavnímu konfiguračnímu modulu je takřka libovolně adaptovatelný. Adaptace a vývoj nových funkcionalit uvnitř DMSs probíhá prostřednictvím zcela nového IDE KENTUMI, nástroje firmy Objentis. Viz bod 11.2. Tím je zajištěna vysoká kvalita, průběžné verzování, relační chování, modelování a tvorba GUI.

DMSs Objentis obsahuje dva variabilní moduly:

DM Classic: klasická správa dokumentů

Doporučuje se zejména pro menší správní jednotky, menší firmy, obce, krajské úřady, malá zdravotnická zařízení, atd.

DM + : Enterprise Content Management System

Systém správy dokumentů s vysokým stupněm komplexity, doporučuje se pro velké útvary státní správy, nemocnice a kliniky, banky, telekomunikační a dopravní operátory, firmy a instituce, které musí denně zacházet s velkým množstvím dokumentů.

Využíváním DMSs získáte:[198]

- Snadné vyhledávání dokumentů a objektů v systému
- Obslužnost PLNĚ v českém jazyce, angličtině, slovenštině a němčině a mezi jazykovými verzemi lze přepínat za běhu programu
- Verzování všech informačních entit
- Snadná tvorba dokumentů – tvorba šablon
- Synchronizace práce mezi mnoha uživateli
- Snadné a bezpečné řízení přístupů a oprávnění
- Nejrůznější druhy Workflow, snadno a rychle nastavitelné
- Replikace dat a datových modulů včetně procesů je velmi rychlá
- Systém protokoluje informace o manipulaci se sebou samým, uchovává data o historii změn v dokumentech, objektech i systémových komponentách. Odpovídá mezinárodním standardům SOX, Basel II a Solvency – tzv. Audit Trail.
- Nese informace o právním statutu informace a o její zákonné či smluvní přístupnosti

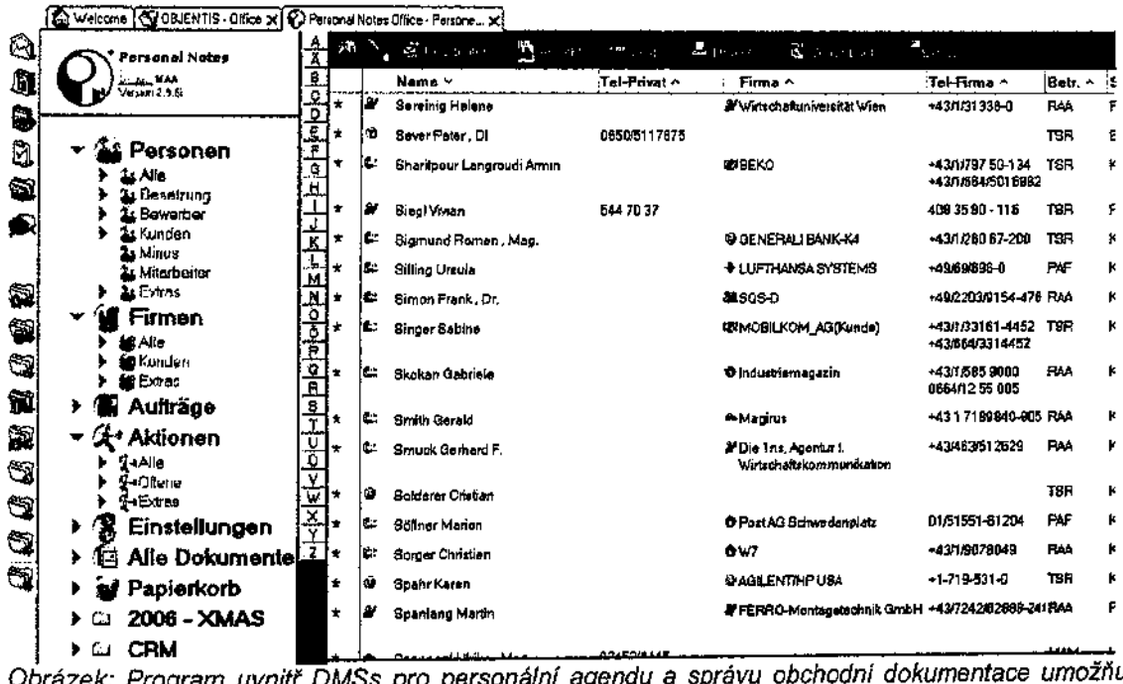
[198] Srov. též Matejka, J., Zálešák, M., Nové možnosti e-demokracie, Business World, 10/2002, s.39 - 45, ISSN 1213-063X.

- Minimalizuje nejasnosti o původu, statutu a změnách dokumentů
- Šetří práci a místo tím, že znemožní paralelní zpracování či uložení.

### *6.3.3. Použití DMSs*

#### *a) Obchodní dokumenty*

DMSs je určen pro obchodní korespondenci, účetnictví, daňovou dokumentaci, smlouvy, personální řízení a příbuzné druhy spravovaných dat. Obchodní korespondence může být po naskenování skartována, jestliže je informace plně, za pomocí indexů a v nezměněné podobě archivována elektronicky. Obchodní dokumentaci představují také emaily a záznamy z porad a jednání, projektové archivy, standardy, normy, odborná literatura, katalogy, atp.




*Obrázek: Program uvnitř DMSs pro personální agendu a správu obchodní dokumentace umožňuje mnoho variant, jak pracovat s těmito typy dokumentů. Na obrázku ukázka německé jazykové verze. Zdroj: Objentis.*

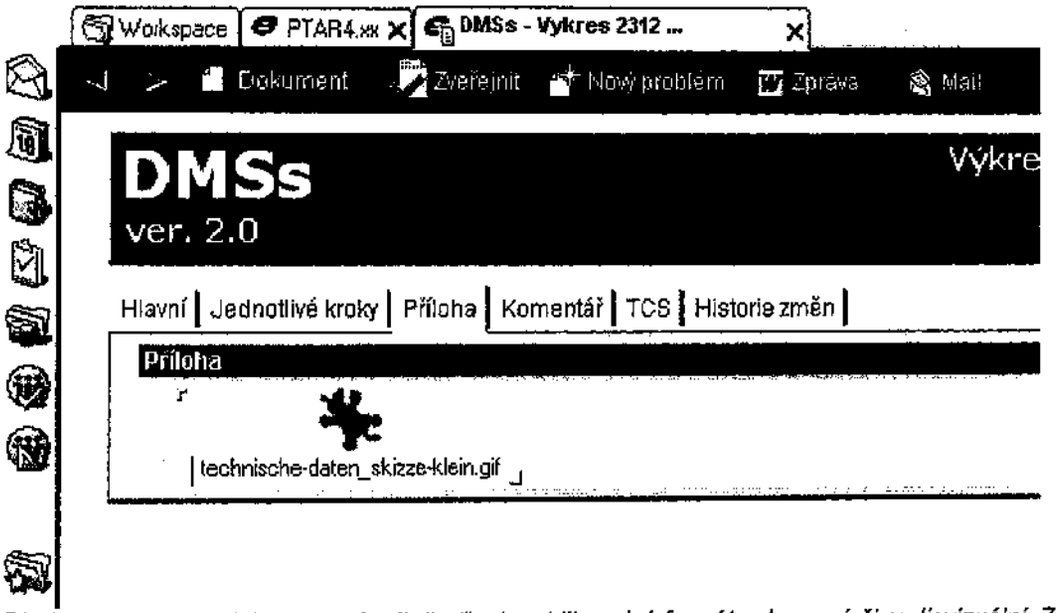
#### *b) Veřejná správa - eGovernment*

Ke klasickému DMS zde přistupuje ještě nutnost vytvořit řešení z oblasti EAI – Enterprise Application Integration. Tato řešení se dnes užívají hlavně při fúzích velkých telekomunikačních a bankovních firem, kde je třeba sjednotit nejrůznější systémy provozované na různých platformách. Do systému navíc spadá nutnost integrovat dokumenty z oblasti E-government, tedy formuláře, záznamy mailové komunikace, komunikační statistiky a archivy nejrůznějších elektronických akt s elektronickým podpisem. Systém

DMSs nabízí velkou kompetitivní výhodu, a sice svou kompatibilitu a snadnou rozšiřitelnost díky univerzální programovací bázi, ve které je vytvořen.

*c) Technické výkresy a mapy*

V konstrukčních a projektových kancelářích, strojírenských závodech, v kartografii, a na obdobných pracovištích musí být spravovány technické výkresy, mapy nebo obrazová dokumentace. Může se přitom jednat o tisíce či desetitisíce velkoformátových informačních souborů. Technický dokument management dovoluje v tomto případě vyhledávání podle druhu výkresu, podle zadavatele, autora, čísla zařazení, data vytvoření a dalších běžných příznaků. Výkresy jsou většinou skladovány podle formátů, ve kterých jsou uloženy.




*Obrázek: Ve formulářích lze pohodlně připojovat libovolné formáty obrazové či audiovizuální. Zdroj: Objentis.*

*d) Knihovny*

Knihovny jsou typickým příkladem skladování statických informací, s jejichž obsahy se dále nepracuje a u kterých je třeba třídit doprovodná data tak, aby byla přístupna v jednoduché formě vyhledávání jakémukoliv uživateli.

*Modul DM Classic*

DM Classic spravuje dokumenty s personálními daty, smlouvami nebo informacemi o klientech firem či úřadů. Tyto informace obsahují jednotlivé typy dokumentů (Scan, elektronický text – až po audio-soubory) a jejich metadata (ID, Kategorizace atd.).

Data jsou vyprodukována a centrálně uložena, mohou být libovolně replikována a hromadně zálohována, (na různých decentralizovaných částech systému). Takto spravované dokumenty podléhají možnostem rešerše dle nejrůznějších kriterií. Tím překonávají klasické identifikační znaky v běžných databázích.

V DMSs jsou k dispozici nejrůznější vyhledávací a řadící identifikátory jako např.: autor, editor, poslední editor, data vytvoření, data a sledování všech změn, verze, typ souboru, přílohy v nejrůznějších formátech, aktivní linky, html, klíčová slova, stupeň nutných oprávnění pro práci s dokumentem, administrátor sekce, doba platnosti dokumentu, třída a zařazení v sekci, komentáře k dokumentu atd.

*Modul DM+*

Modul je rozšířen o další základní funkcionality a naplňuje tak již většinu požadavků ECM-Enterprise Content Managementu. Kromě klasických kategorií DM zde přicházejí ke slovu kategorie navíc:

- Kancelářská komunikace
- Scan a Document Imaging
- Groupware (kategorie pro stanovení pravidel spolupráce ve skupině)
- Archiv
- Modul Virtuálních elektronických akt –VMEA
- Prohlížeč méně obvyklých formátů Focus
- XML Break

*a) SCAN*

Modul Document Imaging řídí vytvoření, zformátování a publikování skenovaných dokumentů, které je propojeno s možností textového rozpoznávání. To dovoluje propojit tento modul se správou metadat a indexů a organicky jej začlenit do systému správy aktivních dokumentů nebo elektronického archivu.

*b) VMEA*

Důležitým modulem je virtuální modul elektronických akt-VMEA, který je definován těmito funkcionalitami: autentizace a autorizace, správa statutů, vyhodnocování atributů dokumentu a dokumentačních tříd. Slouží k práci s netextovými formáty a jejich dalšímu řízení. Pracuje s nejrůznějšími formáty včetně audiovizuálních souborů. Navazuje na Scan a Document Imaging.

*c) XML Spider a XML Break*

Nasazení každé nové komponenty nebo její přiřazení z již existujícího DM systému je podmíněno organickým přístupem k ostatním komponentám. Vzájemná kompatibilita komponent je nejsložitější a zároveň nejžádanější vlastností systému DM +. Systém Kentumi umožňuje napojení DMSs a jeho libovolných modulů na jakýkoli stávající již užívaný systém, který dovoluje Export a Import dat skrze modul XML Spider od IBM nebo XML Break Objentis.

*Společné vlastnosti*

*a) 'S' jako SECURE*

DMSs znamená Document Management System secure. Důraz na zabezpečení a řízení oprávněných vstupů není náhodný. Tato bezpečnostní funkcionalita je nezbytnou konsekvencí požadavku zabezpečit užívání dokumentů pro co nejširší počet uživatelů. Odpovídající informace musí být ihned k dispozici všem pověřeným spolupracovníkům. Příslušné akce informačního toku musí být přitom řízeny v časové a organizační souslednosti – v tzv. Workflow. DMSs klade velký důraz na procesy bezpečného řízení autorizace a autentizace uživatelů.

Ve stávajícím systému existuje trojí systém oprávnění:

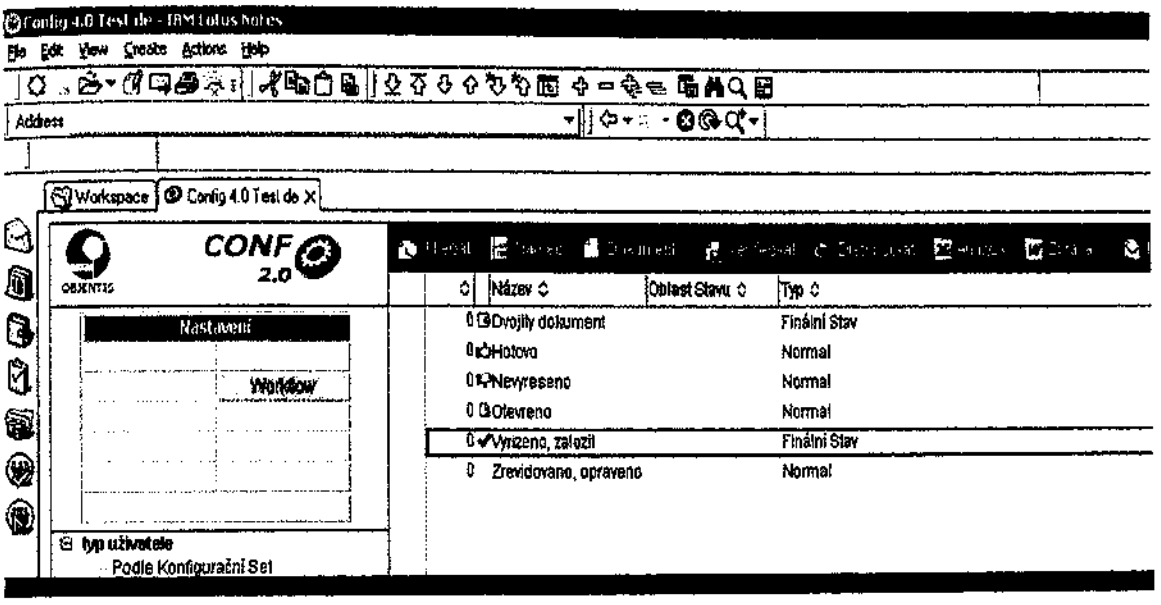
- Autorizace a autentizace
- Access Control List – administrátorem řízený seznam operací s dokumenty, ke kterým je jmenovitě nebo v obecné roli ten který uživatel přiřazen
- Stupňovaná oprávnění ve Workflow – administrátor entity (projektu, archivu, mailové komunikace) konfiguruje práva dle pracovních toků a příslušných operací, které mohou role vykonávat. Práva jsou vázána na anonymní roli, takže tuto roli může přebrat libovolný pracovník, aniž by se musela měnit konfigurace.

To je také jeden z nejdůležitějších důvodů, proč tolik bank a telekomunikačních operátorů používá Lotus Notes a příbuzná řešení - jde zejména o obsáhlý systém oprávnění a silný bezpečnostní koncept.

*b) WORKFLOW*

Modul řízení Workflow je jedním z nejstarších a nejpropracovanějších v celém systému. Workflow je rychle a snadno nastavitelné od jednoduchých schémat, která si předem načrtnete do bloku a hned je můžete v systému realizovat až po mnohočlenné vrstvy oprávnění a činností, pro projekty a práce, které vyžadují zapojení velkého množství lidí či skupin s ekvivalentním oprávněním.

Workflow je variabilní co do počtu uživatelů a oprávnění k činnostem a systém verifikuje sám správnost jeho nastavení. V případě, že Workflow není nastaveno úplně nebo správně, dostane příslušný tvůrce workflow ihned upozornění na část chybějící definice. Nastavení je časově nenáročné a zvládne jej úplně každý uživatel.

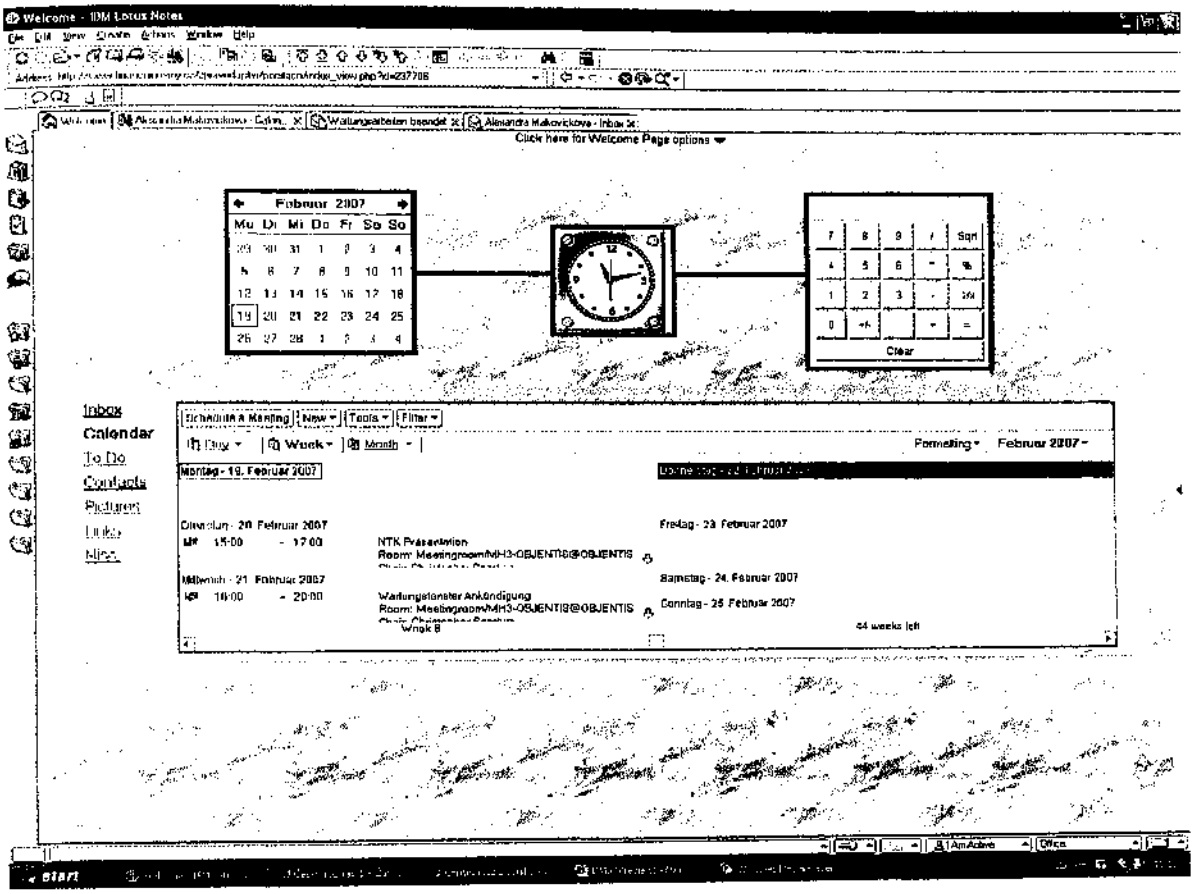



*Obrázek: Příklady možných jednoduchých workflow konfigurací DMSs. Zdroj: Objentis.*

*c) Další vlastnosti*

Společné znaky DM Classic a DM+:

- Integrovaný e-MAIL a Instant Messenger
- Diář s aktivním připomínáním
- Úkolovník
- Zasílání automatických zpráv o projektech a úkolech
- Grafické reporty o stavu dokumentů či jiných entit
- Integrace různých formátů v jednom prostředí
- Webový přístup
- Vytváření a ukládání šablon pro rychlou tvorbu nových dokumentů




*Obrázek: Aktivní diář je propojen s různými úlohami Workflow a dovoluje uživateli nechat si zasílat mailem upozornění na aktuální pracovní kroky ve správný čas. Na obrázku jeden z mnoha volitelných layoutů. Zdroj: Objentis.*

### *6.3.4. Dokument v DMSs*

Dokument má v DMSs tyto vlastnosti:

- Fyzický nosič (papír, soubor),
- Formální vlastnosti (stavba, způsob vytvoření, formát, linky, atd.),
- Zařazení (oborová příslušnost, pořadí, verze),
- Obsah (klíčový výtah obsahu),
- Charakter (schopnost rychlé aktivace, dosažitelnost, povinnost skladování),
- Právní status, (povolené možnosti zpracování a řízení),
- Čas (datum a čas vytvoření, datum ztráty platnosti, poslední editace),
- Tvůrce (odesilatel, autor),
- Uživatel (příjemce, oprávněný editor, čtenář, poslední editor).

Tyto znaky tvoří klíčové třídy pro architekturu byznys procesů v systému. K nim náleží ještě znaky vedlejší, které vznikají až dle místních potřeb klienta a dle charakteristik jeho procesů.

Dokument jako takový se může ale skládat i z mnoha objektů, například

- Zpracovaný text, tabulkový výpočet nebo grafika,

- Obrázky, například Scany a Fotografie,
- Formuláře,
- COLD-Dokumenty (Computer Output to Laser Disk),
- ASCII- nebo XML -textové soubory,
- Video-klipy, nebo
- Nahrávky živé řeči, rozhlasové záznamy, záznamy z porad, atd.

Technika OCR - u dokumentů, které měly svůj původní nosič v podobě papíru nebo např. mluvené řeči a nejsou vázány na jiný datový tok, mluvíme o NCI „Non Coded Information". U dokumentů, které mohou být hned vyhodnoceny za základě přímého datového přístupu hovoříme o CI „Coded Information". Díky technice OCR zde dochází k převodu NCI na CI dokumenty.

Doba skladování - pro správu dokumentů a systémy skladování je rozhodující také další kriterium: Zda se jedná o dynamické, v krátkodobém horizontu dvou až čtyř let používané dokumenty nebo systémy skladování dlouhodobě uzavřených či dokonce neměnných dokumentů. Systém DMSs firmy Objentis je zaměřen především na dynamické operace s užitými dokumenty a v tomto kratším časovém horizontu. Systémy dlouhodobé archivace vyvíjí v ČR např. firma ICZ.

Compound a Container Dokumenty - podle stupně komplexity pak systém DMSs rozlišuje:

- Elementární Dokumenty, které se skládají z jednoho objektu, obsahují data jednoho typu, žádné vložené grafiky nebo volání jiných objektů.
- Compound Dokumenty – sestávají se z více objektů. Smíšené soubory, text, formátové informace, obrázky, tabulky, hyperlinky nebo odkazy na jiné systémové komponenty, atd.
- Kontejnery - komplexní objekty, odkazové informace, linky, metadata a interní správní data.

### *6.3.5. Samopopisné Objekty*

Kontejner dokument může být vytvořen pouze v řídícím programovacím prostředí, kde je také zobrazen a interpretován. Jestliže je třeba využít dokument složený z mnoha příloh nebo dokonce mnoha komponent, musí Kontejner dokument obsahovat všechny identifikační struktury a správní informace a nést je s sebou. Jsou-li tyto podmínky splněny, mluvíme o samopopisném objektu (Self-description Object).

Samopopisný objekt se sestává z metadat, která dovolují přístup k jiným dokumentům a jejich katalogizaci. Skládá se z libovolné obsahové komponenty a záhlaví (Header). Samotný Header je složen z několika informací:

- Informace o formátu,
- Jednoznačná identifikace objektu - Unique Identifier,
- Kód sebedeklarace,
- Informace o druhu, počtu a struktuře komponent Obsahu,
- Informace o užití a uživatelích,

- Bezpečnostní a přístupová informace,
- Reference,
- Obsah.

Tyto atributy mohou být vyhodnoceny, i když spravovaná databáze není momentálně připojena nebo se nachází vně systému.

## 6.4. Unicorn Enterprise System

### *6.4.1. Co je systém UES*

Unicorn Enterprise System (UES) je kontinuálně vyvíjeným řešením pro on-line řízení úřadu na bázi ECM (Enterprise Content Management). Korporátní informační systém UES je určen zejména pro podporu velkých duševně pracujících týmů, podporuje zejména procesy v oblasti řízení, komunikace a sdílení informací. Mezi hlavní součásti systému patří správa obsahu, workflow, správa zdrojů, správa znalostí, správa požadavků a podpora rozhodování. UES efektivně slučuje dostupné technologie do jednotného sdíleného systému, harmonizuje podnikové systémy, procesy komunikace a předávání korporátních informací, to vše za účelem maximální podpory úspěšného řízení firemních procesů.[199]

*Základní vlastnosti*
Systém nabízí řadu nástrojů, které podporují celkové zrychlení a zefektivnění veškeré komunikace uvnitř příslušného úřadu. Převedení administrativních agend do elektronické podoby šetří čas a peníze. UES významně podporuje sofistikované sdílení znalostí a informací (knowledge management).

1. *Bohatá nabídka funkcí*
   Správa obsahu, workflow, diář, úkolovník, připomínkovací aparát, vlastní editor podporující pluginy, správa zdrojů, správa znalostí, správa požadavků a podpora rozhodování, evidence docházky zaměstnanců.

2. *Rozšiřitelnost*
   O další funkce je možné systém rozšířit prostřednictvím skriptovacího jazyka. Skripty je možné také využít pro automatické provádění hromadných operací.

3. *Flexibilita*
   Všechny funkce systému jsou přístupné z jakéhokoli počítače připojeného k internetu/intranetu prostřednictvím webového prohlížeče 24 hodin denně.

4. *Vysoký stupeň zabezpečení*
   Veškerá práce se systémem probíhá prostřednictvím šifrovaného spojení (protokol https). Data jsou uložená v zabezpečených prostorách provozovatele.

5. *Spolehlivost uložení dat*

[199] Podrobněji viz. www.unicorn.cz.

Veškerá systémové soubory a data uživatelů jsou uloženy na serveru, který je pravidelně zálohován. Používání systému eliminuje hrozbu finančních nákladů spojených se ztrátou cenných dat uložených na lokálních discích uživatelů z důvodu hardwarové poruchy nebo napadení viry či jiným škodlivým softwarem.

6. *Použitelnost a ergonomie*
Systém UES disponuje jednoduchým a uživatelsky přívětivým rozhraním. Rozvržení pracovní plochy, ovládání a navigace prostřednictvím ikon, jednoduché a všeobecně známe pojmosloví – to jsou hlavní prvky, které přispívají ke spokojenosti uživatelů každodenně pracujících se systémem. Při návrhu grafického rozhraní systému bylo využito nejmodernějších poznatků v oblasti ergonomie a použitelnosti webových aplikací.

7. *Přizpusobivost grafického a jazykového rozhraní*
Systém prostřednictvím tzv. skinů nabízí možnost kompletních změn grafického rozhraní. Grafických motivů lze v rámci jedné instalace systému využívat neomezený počet. Např. každá organizační jednotka firmy pak může používat vlastní grafický motiv. Dále systém umožňuje využívat různých jazykových prostředí. Uživatel si může jednoduše nastavit jazyk, podle svých preferencí. Architektura systému umožňuje jednoduše přidávat další jazykové verze.

8. *Vysoký výkon*
Systém díky použitým technologiím disponuje vysokým výkonem. Architektura systému využívá možnosti odkládat zpracování časově náročných úloh na sekundární server.

9. *Použité technologie*
Oracle10g, J2EE, Java 1.4/1.5, XML, XSL, JSP, HTML, CSS, JS, JMS, Apache, Tomcat, JBOSS, CVS, Eclipse, ANT, JUNIT

10. *Neustálý vývoj a zdokonalování systému*
Systém prochází neustálým dalším vývojem, prostřednictvím kterého je dále obohacován o další funkce. Aktualizace jsou k dispozici všem uživatelům okamžitě. Aktualizace systému probíhá pouze na serveru, nikoli na počítačích jednotlivých uživatelů. Není tedy nutné provádět časově i finančně náročné aktualizace na jednotlivých počítačích jako u běžného softwaru.

### *6.4.2. Klíčové funkční oblasti*

*Správa firemního obsahu (Content Management)*
Systém UES nabízí výkonné nástroje pro pružnou organizaci resortních a vnitropodnikových informací a jejich řízení v úrovni vzájemných vazeb i workflow. UES umožňuje vkládání a revize různých typů dokumentů do systému, udržování historie verzí po celý život vložené informace, nastavení schvalovacích a distribučních workflow mezi jednotlivými uživateli nebo skupinami uživatelů.

*Řízení organizační struktury*

Systém UES plně podporuje správu pružné organizační struktury, a to od nejvyšších vrstev až po jednotlivé zaměstnance. Jednotliví uživatelé v systému nevystupují přímo, nýbrž pod tzv. rolemi, na které jsou vázána přístupová práva k jednotlivým funkcím systému, dokumentům a dalšímu obsahu. UES důsledně odděluje uživatele systému od rolí, ve kterých v systému vystupují. Veškerá práva a kompetence jsou spojené s rolemi, nikoliv s fyzickými osobami. Role je tedy možné jednoduše přenášet mezi uživateli. Systém umožňuje vytváření libovolně složité hierarchie organizačních struktur a s nimi spojených informací, a to s možností flexibilních následných změn a úprav.

*Uživatelská a přístupová práva*
Systém UES uplatňuje bezpečnostní politiku, založenou na uživatelských a přístupových právech, a to na všechny činnosti, které v systému lze provádět a na veškerý informační obsah.

*Workflow management*
Systém UES podporuje různé typy workflow. Na základě resortních, vnitropodnikových a nebo oborových standardů, metodiky, procesů a metrik je možné jednoduše vytvářet vlastní unifikovaná workflow pro různé typy informací a aktivit. Workflow se automaticky promítá do životního cyklu jakékoliv informace, jejímuž typu dané workflow odpovídá. Informace o workflow jsou u každé entity snadno dostupné a zobrazitelné. Umožňují dodatečné změny, monitoring stavu a okamžitou komunikaci nad jednotlivými událostmi.

*Verzování obsahu*
Systém automaticky verzuje obsah dokumentů a příloh. Uživatel se může jednoduchým způsobem vrátit k jakékoli předchozí verzi (rollback).

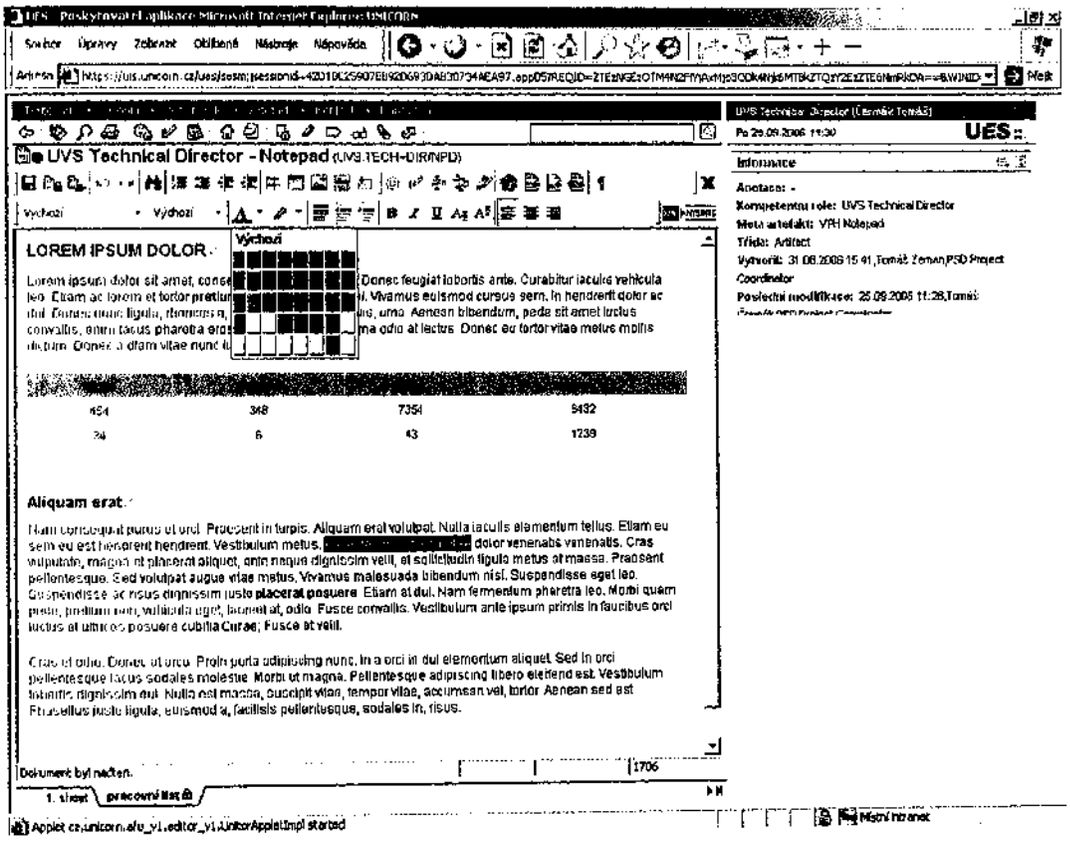
*Agregace informací a vztahů*
UES podporuje sdružování a agregaci dat z různých zdrojů. Data je možné spojovat do logických celků, bloků komponent a informačních přehledů. Obsah jednotlivých informací je možné rozdělit do více listů, každý z těchto listů reprezentuje určitý pohled. Každému z listů je přidělena zvláštní skupina uživatelských práv. Informace je tedy možné členit podle stupně důvěrnosti anebo určení.

*Společná komunikační platforma*
UES poskytuje uživatelům jednotnou komunikační platformu. Podporuje výměnu, sdílení a distribuci informací ve firmě, a to jak mezi jednotkami, tak mezi jednotlivci. Umožňuje vytvoření komunikačního řetězce na základě workflow, podporuje kvalitu informace, ke které mají možnost se vyjádřit všichni zainteresovaní. Díky integraci s kalendářem a úkolovníkem každého uživatele (viz dále) komunikace probíhá také v podobě zadávání a kontroly úkolů, plánování událostí apod. Systém UES umožňuje přímou komunikaci nad věcnými informacemi (dokumenty, úkoly, záznamy v kalendáři...). Tato komunikace je zaznamenávána do workflow každé informace či objektu, kde je uložena a dohledatelná po celý životní cyklus informace.

*Knowledge Management*
Systém UES podporuje veškeré procesy spojené s tvorbou, uchováváním a distribucí informací.V systému UES je možné udržovat obsáhlé databáze znalostí, informace o lidských zdrojích úřadu, podniku apod.

*Editor*

K vytváření a následným úpravám obsahu slouží editor, který je nedílnou součástí systému UES. Prostřednictvím tohoto editoru, který běží stejně jako ostatní komponenty systému UES v internetovém prohlížeči, je možné psát a formátovat texty, vytvářet tabulky, vkládat obrázky, hypertextové odkazy atd. Editor, který je naprogramovaný v jazyce Java (pro jeho spuštění je nezbytné mít na počítači nainstalovanou Javu), poskytuje funkce a komfort srovnatelný s běžnými desktopovými aplikacemi. Práce v editoru je velmi podobná vytváření dokumentů např. v textovém editoru Microsoft Word. Editor se ovládá prostřednictvím ikon, klávesových zkratek a kontextových menu přístupných přes pravé tlačítko myši.



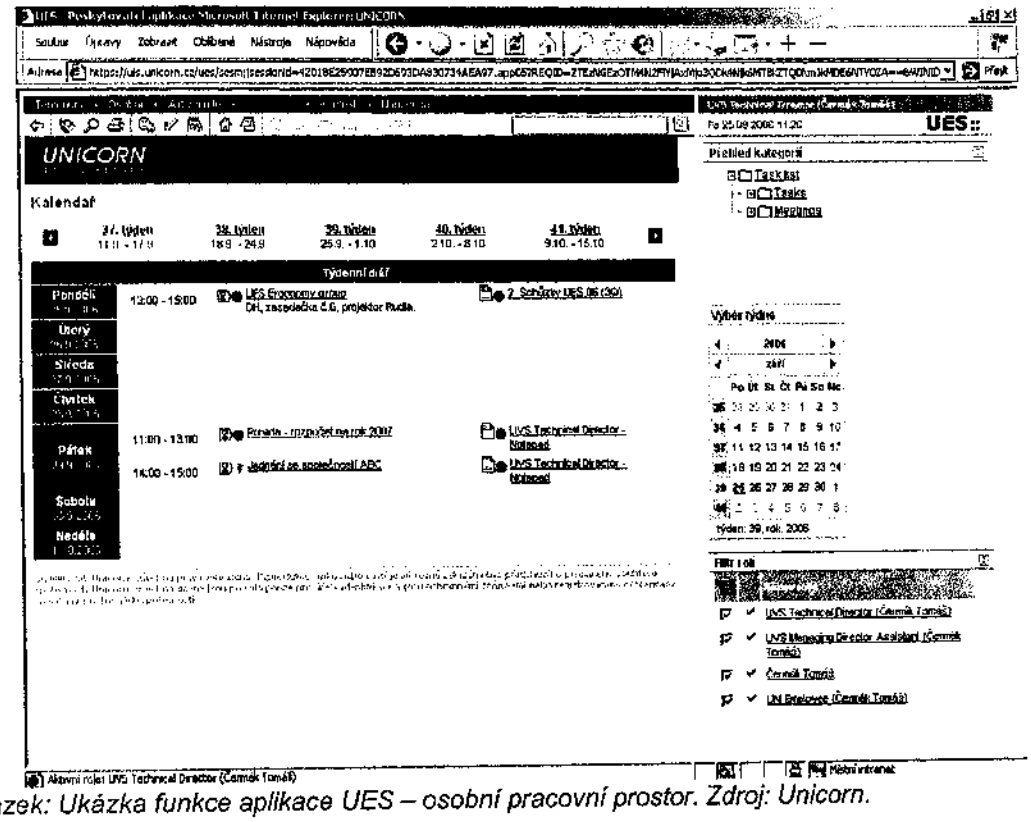

*Obrázek: Ukázka rozhraní editoru UES. Zdroj: Unicorn.*

Editor nabízí bohaté možnosti formátování textu. Je možné používat předdefinované styly, různé úrovně nadpisů, typy písma, barvy atd. Samozřejmostí jsou odrážky, číslované nadpisy. Součástí editoru je i bohatá a konfigurovatelná sada ikon a emotikon (smajlíků). Obsah dokumentů je možné členit do listů. Jednotlivé obsahové prvky (kapitoly, odstavce nebo jakékoli jiné části dokumentu) je možné označit a pojmenovat jako tzv. logický blok, který je možné například vložit do jiného dokumentu. Veškeré změny v původním zdrojovém bloku se pak automaticky promítnou i do dokumentu, kde byl vložen odkaz na zdrojový blok. Dokumenty jsou v systému UES ukládány na server v podobě strukturovaných XML souborů. Soubory jsou ukládány v pravidelných časových intervalech, nehrozí tedy ztráta provedených úprav například v případě náhlého výpadku el. proudu.

*Osobní digitální pracovní prostor*

Nedílnou součástí systému UES jsou nástroje pro plánování času, evidenci a zadávání úkolů a dále nástroj pro ukládání osobních poznámek a souborů. Systém rovněž slouží jako aktivní komunikační nástroj, prostřednictvím kterého je možné jednotlivcům i skupinám například

posílat návrhy termínů konání schůzek. Návrhy je možné přijmout, zamítnout nebo o nich dále komunikovat, vše v přehledné formě v rámci systému UES bez nutností používat e-mail nebo telefon. Samozřejmostí je možnost zadávání a následného sledování plnění úkolů.




*Obrázek: Ukázka funkce aplikace UES – osobní pracovní prostor. Zdroj: Unicorn.*

*Diář*

Diář slouží k plánování času. K dispozici je řada pohledů: denní, týdenní, měsíční a speciální pohled formou časové osy. Systém umožňuje zobrazit diář jiného uživatele. Je tak možné velmi jednoduše ověřit časovou dostupnost osoby například při plánování schůzek. Ke každé události se kromě data a času konání může vázat řada informací: související artefakt, poznámky, zúčastněné osoby a poznámky. Upozornění na blížící se termíny událostí se v nastaveném časovém předstihu zobrazují v úkolovníku.

*Úkolovník*

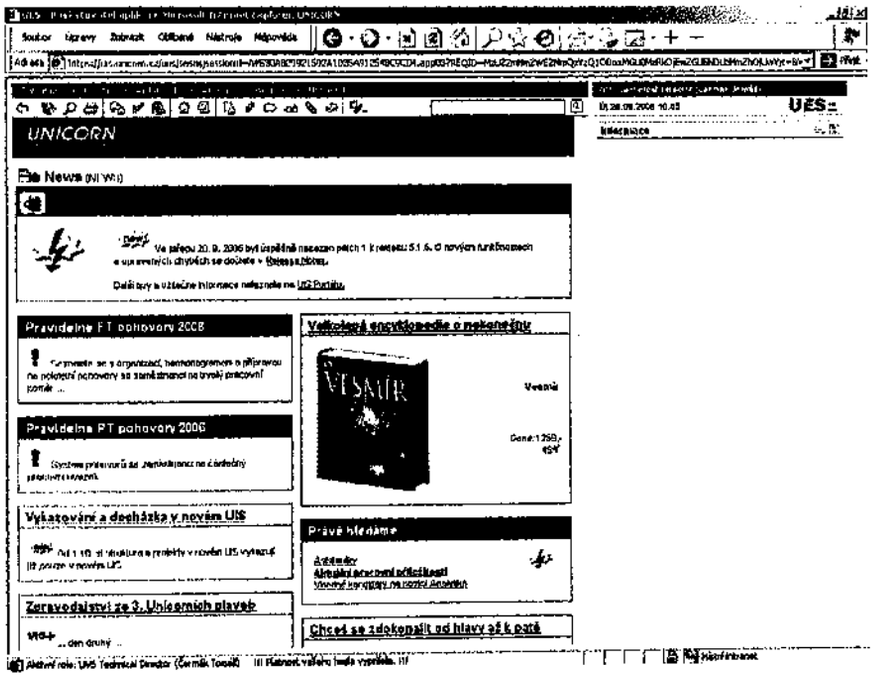
Úkolovník je určen k přehlednému evidování úkolů. Ke každému úkolu je možné přiřadit termín splnění, prioritu, artefakt se souvisejícími informacemi a poznámky. Úkoly je možné zadávat také jiným uživatelům (obvykle ve vztahu nadřízený/podřízený). Takto zadané úkoly může úkolovaná osoba předat k vyřízení jiným uživatelům. Úkoly je možné zadávat jednotlivcům nebo skupinám uživatelů. Nadřízení mohou jednoduchým způsobem kontrolovat průběh plnění zadaných úkolů.

*Poznámkový blok*

Každý uživatel má k dispozici speciální prostor, který může sloužit k zapisování poznámek nebo například jako soukromý, plně personalizovaný rozcestník. K poznámkovému bloku je možné přidávat neomezené množství příloh. Uživatel si zde může ukládat soubory jakéhokoli typu.

*Rezortní a podnikové portály*

Portály systému UES slouží k prezentaci informací uvnitř firmy formou intranetu. Na portálu mohou být zveřejněny strukturované informace týkající se celé firmy nebo určité divize. Informace o významném projektu pak mohou být soustřeďovány na portále projektu. Jednotlivé portály jsou propojeny prostřednictvím hypertextových odkazů, tvoří hierarchickou strukturu. Portály jsou běžnými dokumenty systému UES – je tedy velmi jednoduché je vytvářet, editovat, aktualizovat. Vše probíhá v editoru UES v prostředí webového prohlížeče. Struktura komponent portálů je formalizovaná, je možné ji měnit prostřednictvím předem připravených šablon, sad grafických prvků a barevných schémat. Přístupová práva k prohlížení obsahu jednotlivých portálů se mohou lišit. Hlavní portál s aktualitami z prostředí firmy může být přístupný všem zaměstnancům, portál určitého projektu je určen pouze pracovníkům daného projektového týmu a nadřízeným, na portál s finančními ukazateli by naopak mohl být přístupný jen zodpovědným osobám z finančního oddělení a členům vedení resortu, popř. top managementu.




*Obrázek: Ukázka vnitroresortního portálu aplikace UES. Zdroj: Unicorn.*

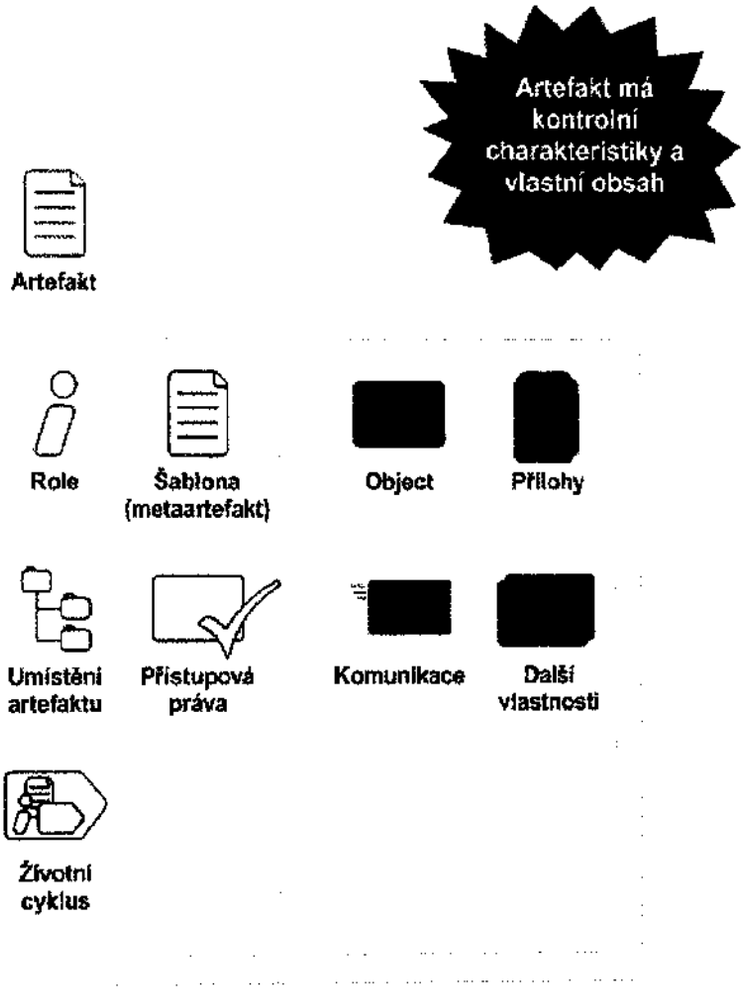
*Skriptovací jazyk*

Systém UES je možné prostřednictvím skriptovacího jazyka rozšířit o další funkce. Pomocí skriptů lze také elegantně řešit provádění hromadných úloh. Aplikace vytvořené skriptovacím jazykem nad jádrem UES lze využít v prakticky neomezené řadě oblastí – od jednoduchých rozhraní pro import a export dat z účetního software přes zpracování rozsáhlých databází až po řízení komplexních procesů.

### *6.4.3. Artefakt*

*Co je artefakt?*

Nositeli všech informací uložených v systému UES jsou tzv. „chytré dokumenty", které se v rámci systému nazývají artefakty. Artefakt je komplexním dokumentem, který je kromě vlastního obsahu nositelem řady dalších objektů a charakteristik.




*Obrázek: Schéma tzv. artefaktu (chytrého dokumentu). Zdroj: Unicorn.*

*Charakteristické znaky artefaktu:*

1. Obsah
   V každodenním pracovním životě pracujeme s celou řadou druhů dat – texty, tabulky, obrázky... To vše může být součástí obsahu artefaktu. V rámci artefaktů je možné pracovat také s jednoduchými vzorci a s odkazy na webové stránky nebo jiné artefakty. Vlastní obsah artefaktu je možné pro pohodlnější práci a větší přehlednost rozdělit na více listů (podobně jako např. v programu pro práci s tabulkami MS Excel).

2. Přílohy
   Součástí artefaktu mohou být také přílohy jakéhokoli druhu (textové dokumenty, tabulky, obrázky, hudba, video atd.). Na tyto přílohy lze odkazovat přímo z textu artefaktu.

3. Komunikace

„Nad artefaktem" lze také komunikovat. Taková komunikace se velmi podobá e-mailové korespondenci, je však spojená přímo s daným artefaktem a probíhá přímo v rámci systému UES.

4. Další vlastnosti
V tzv. dalších vlastnostech artefaktu lze ukládat strukturovaná data (typicky textová nebo numerická data), se kterými je možné dále pracovat například prostřednictvím vzorců (výhodné např. pro zpracování finančních dat) nebo je možné tvořit databáze prostřednictvím formulářů atd.

5. Role
Za obsah a další charakteristiky každého artefaktu je zodpovědný konkrétní uživatel systému UES. Uživatelé v systému nevystupují přímo, ale výhradně pod tzv. rolemi (např. Marketingový ředitel, Asistentka generálního ředitele apod.). Každý uživatel může v rámci systému vystupovat v jedné či více rolích. Systém rolí umožňuje například v případě změny zaměstnance na určité pozici jednoduše přeobsadit uvolněnou roli jiným uživatelem, který pak přebírá veškerá práva k artefaktům náležejícím k dané pracovní roli. Tento princip lze využívat například i při dočasné nepřítomnosti pracovníka v průběhu nemoci nebo čerpání dovolené. Systém dále nabízí možnost obsazení uživatele do tzv. skupinové role. Tato funkce bývá využívána například za účelem hromadného úkolování nebo k udělování přístupových práv k artefaktům pracovním týmům nebo jiným skupinám uživatelů.

6. Šablony
Nové artefakty uživatelé v systému vytvářejí výhradně ze šablon – tzv. metodických artefaktů (meta artefaktů). Metodické artefakty definují nejen základní prvky layoutu artefaktu, nýbrž také veškeré další charakteristiky (přístupová práva, vzorový životní cyklus artefaktu, umístění do určité složky atd.).

7. Umístění artefaktu
Artefakty jsou ukládány do systému tzv. organizačních jednotek a složek. Obrovské množství informací umístěných v jednotlivých artefaktech tak dostává řád a pevnou logickou strukturu, která odráží skutečné organizační schéma firmy nebo instituce, která systém UES používá. V určitých situacích je výhodné k artefaktům vytvářet tzv. zástupce. Zástupce - neboli odkazy na artefakty – umisťujeme podle potřeby do různých složek. K jednomu artefaktu je možné vytvořit prakticky neomezené množství zástupců.

8. Přístupová práva
Přístupová práva jsou nedílnou součástí práce s artefakty. Artefakt může konkrétní uživatel (resp. role) pouze prohlížet, nebo jej může také editovat. Práva lze přiřazovat konkrétním rolím nebo celým skupinám. Základní soubor přístupových práv je dán již samotnou šablonou, ze které byl daný artefakt vytvořen. Tato tzv. implicitní práva může uživatel dále rozšířit o další role či skupinové role - zde pak hovoříme o tzv. explicitních právech.

9. Životní cyklus
Nedílnou součástí každého artefaktu je tzv. životní cyklus, který je dán šablonou, ze které byl vytvořen. Životní cyklus určuje posloupnost stavů, kterými artefakt během svého „života" projde. Jedná se o jeden ze základních manažerských nástrojů, které

systém UES nabízí. Například artefakt se zápisem z porady může postupně procházet následujícími stavy: „založeno", „zapsáno", „schváleno", „rozesláno", „archivováno". Do jednotlivých stavů se artefakt dostane prostřednictvím aktivit. Tyto aktivity vykonávají uživatelé, kteří jsou zodpovědní za určité části životního cyklu artefaktu. Asistentka ředitele je např. zodpovědná za vytvoření zápisu z porady, její nadřízený pak za jeho schválení apod. Vše postupně probíhá automaticky na základě předem nastaveného životního cyklu na šabloně „Zápis z porady". Jednotlivé aktivity, jako například schválení zápisu, se příslušným uživatelům (v tomto případě řediteli, který řídil poradu své divize) automaticky objeví v jejich diáři a úkolovníku.

## 7. Závěr

Ministerstvo spravedlnosti ČR plánuje elektronizaci české justice, což je jednoznačně správný vývoj, který je plně v souladu s vývoje justice v nejvyspělejších státech EU. Stále více občanů a úředníků veřejné správy využívá prostředky elektronické komunikace na dálku, zejména internet (email a web), a proto je zcela nepochybné, že možnost komunikovat se soudy pomocí sítě internet by ocenili a to včetně možnosti nahlížet do „svého" (elektronického) spisu.

Významných úkolem vlády a příslušných resortů (tedy zejména Ministerstva spravedlnosti ČR a Ministerstva vnitra ČR) by měla být snaha, aby projekt E-Justice nezůstal pouze na papíře, ale aby se začal systematicky realizovat. Základní ideou projektu bude myšlenka, že v dnešní době už nemají úřady a soudy obíhat občané a podnikatelé, ale pouze data v elektronické podobě. Proto musejí být postupně vytvářeny soustavy registrů veřejné správy, které se stanou základními zdroji údajů pro veřejnou správu a soudnictví. Tím bude také mimo jiné umožněno fyzickým a právnickým osobám neprokazovat se nadále soudu a policii skutečnosti, které jsou vedeny v některém informačním systému justice, příp. veřejné správy. Úprava sdílení dat v elektronické podobě přispěje k lepšímu a kvalitnějšímu chodu justice a veřejné správy jako celku, čehož výsledkem bude zvýšení rychlosti a efektivity soudní činnosti ve vztahu k občanům.

Dále je třeba vytvořit kvalitní aplikace elektronické spisové služby, která se bude moci využívat v rámci celé veřejné správy. Je tedy třeba sjednotit standardy ministerstev a způsob identifikace a popisu dokumentů. Spisová služba musí být založena na otevřených formátech a ideálně by měla také vycházet z Open Source Softwaru, který je často k dispozici zdarma.

Na postupnou elektronizaci má také stále větší vliv evropské právo (právo ES), v souladu s kterým musíme náš právní řád pravidelně harmonizovat.[200] Do budoucna lze potom předpokládat, že v rámci elektronizace justice budou více využívány nové technologie a poznatky jako např. RFID čipy, soudní expertní systémy atd.[201,202]

[200] Srov. též Štědroň, B., ECJ's jurisprudence and its vital influence on European legal system, www.vsehrd.info, Všehrd Online - časopis Spolku českých právníku Všehrd, 12.01.2005, ISSN 1801-3678.
[201] Podrobněji viz. např. Stedron, B., Forecast for Artificial Intelligence, FUTURIST (USA), March-April 2004, pp.24-25, ISSN 0016-3317.
[202] Srov. též Štědroň, B., Law and Artificial Inteligence, Cyberspace 2003: Normative framework, Spisy Právnické fakulty Masarykovy univerzity v Brně, řada teoretická 273, 2004,str. 9-11, ISBN 80-210-3387-8.

# 8. Použitá a doporučená literatura

## 8.1. Psaná literatura


- Cejpek, J., *Úvod do právní informatiky*, Karolinum, Praha 1997, ISBN 80-7184-336-9
- Bělohlávek J.A., *Zákon o rozhodčím řízení a výkonu rozhodčích nálezů*, C.H.Beck, 2004, ISBN 80-7179-629-8
- Bělohlávek, J.A., Štědroň, B., *Budoucnost již začala*, Sdělovací technika, 2003, ISBN 80-86645-06-1
- Bureš, J., Drápal L., Krčmář Z., Mazanec M., a kol., *Občanský soudní řád - Beckova edice komentované zákony*, 7 vydání, C.H.Beck, 2006, 80-7179-378-7
- Cowart, R., *Počítač – kompletní počítačová gramotnost*, SoftPress, Brno 2001, ISBN 80-86497-05-4
- Curtain, G., *The World of E-Government*, Haworth Press, 2004, ISBN 978-0789023063
- Gálc, L., Pour, J., Toman, P., *Podniková informatika*, Grada, Praha 2006, ISBN 80-247-1278-4
- Gerloch, A. a kolektiv, *Ústavní systém České republiky – základy českého ústavního práva*, Prospektrum, Praha 2002, ISBN 80-7175-077-8
- Gerloch, A., *Teorie práva*, Nakladatelství Čeněk, Plzeň 2004, ISBN 80-86473-85-6
- Fountain, J., *Building the Virtual State: Information Technology and Institutional Change*, Brookings Institution Press, Washington D.C. 2001, ISBN 978-0815700777
- Frimmel, M., *Elektronický obchod – právní úprava*, Prospektrum, Praha 2002, ISBN 80-7175-114-6
- Hendrych D. a kolektiv, *Právnický slovník*, C.H.Beck, Praha 2003, ISBN 80-7179-740-5
- Chuděra, O., *Občan v soudním řízení*, C.H.Beck, Praha 2001, ISBN 80-7179-542-9
- Jehlička, O., Švestka J., Škárová M., Spáčil J., *Občanský zákoník - Beckova edice komentované zákony*, 10. vydání, C.H.Beck, 2006, ISBN 80-7179-486-4
- Korbel, F., a kol., *Právo na informace*, Linde, 2005, ISBN 80-7201-532-X
- Knapp – Gerloch, *Logika v právním myšlení*, Eurolex Bohemia, Praha 2000, ISBN 80-86432-02-5
- Kubů, L. a kolektiv, *Teorie práva*, Linde, Praha 2007, ISBN 978-80-7201-637-2
- Lipinski, K., *Lexikon der Datenkomunikation*, mitp-Verlag, Bonn 2001, ISBN 3-8286-4089-6
- Macková, A., *Právní pomoc advokátů a její dostupnost*, C.H.Beck, Praha 2001, ISBN 80-7179-457-0
- Macková, A., *Nezávislost soudců*, Ediční středisko PF UK, Praha, 1998, ISBN 8085889196
- Madar, Z. a kolektiv, *Slovník českého práva – 1 a 2 díl*, Linde, Praha 2002, ISBN 80-7201377-7
- Mates, P., *Ochrana soukromí ve správním právu*, Linde, 2006, ISBN 80-7201-589-3
- Mates, P., Smejkal, V., *E-government v českém právu*, Linde Praha, Praha 2006, ISBN 80-7201-614-8
- Pecinovský, J., Smejkal, V., *Internet v kanceláři - typické činnosti krok za krokem*, Grada, 2003, ISBN 80-247-0660-1
- Pour, J. a kol., *Informační systémy a elektronické podnikání*, VŠE, 2003, ISBN 80-245-0227-5
- Požár, J., *Informační bezpečnost*, Aleš Čeněk, Plzeň 2005, ISBN 80-86898-38-5

- Pužmanová, R., *Moderní komunikační sítě od A až do Z*, Computer Press, Brno 1998, ISBN 80-7226-098-7
- Plecitý, V. a kolektiv, *Základy občanského práva*, Nakladatelství Čeněk, Plzeň 2005, ISBN 80-86898-25-3
- Schelleová, I. a kolektiv, *Organizace soudnictví a právní služby*, Alfa Publishing, Brno 2006, ISBN 80-86575-40-7
- Schelleová I., *Civilní proces*, Nakladatelství Čeněk, Praha, 2006, ISBN 80-86861-09-0
- Sklenák V., a kol., *Data, informace, znalosti a Internet*, C. H. Beck pro praxi, 2001, ISBN 80-7179-409-0
- Smejkal, V., *Právo informačních a telekomunikačních systémů*, C.H.Beck, Praha 2001, ISBN 80-7179-552-6
- Smejkal, V., Rais, K., *Řízení rizik ve firmách a jiných organizacích*, Grada, 2006, ISBN 80-247-1667-4
- Sodomka, P., *Informační systémy v podnikové praxi*, Computer Press, Brno 2006, ISBN 80-251-1200-4
- Spirit, M., *Základy právní vědy a veřejného práva*, Prospektrum, Praha 1998, ISBN 80-7175-070-0
- Šín, Z., et al., *Metodika tvorby předpisů – příručka pro hospodářské a správní instituce*, Prospektrum, Praha 1993, ISBN 80-85431-34-3.
- Štědroň, B., *Úvod do eGovernmentu v České republice - právní a technický průvodce*, Úřad vlády České republiky, 2007, ISBN 978-80-87041-25-3
- Štědroň, B., *Notion and Obligations of Undertakings with Significant Market Power in the Law of Electronic Communications*, Schulthess Juristische Medien, Curych 2007, ISBN 978-3-7255-5353-2
- Štědroň, B., *Manažerské řízení a informační technologie*, Grada, Praha 2007, ISBN 978-80-247-2052-4
- Štědroň, Beneš, Potůček a kol., *Svět 2050*, Sdělovací technika 2005, ISBN 80-86645-10-X
- Varvařovský, P., *Základy práva – o právu, státě a moci*, ASPI, Praha 2004, ISBN 80-7357-038-6
- Veber, J., a kol., *Řízení jakosti a ochrana spotřebitele*, Grada, Praha 2002, ISBN 80-247-0194-4
- Voříšek J., *Strategické řízení informačního systému a systémová integrace*, Management Press, Praha 1997, ISBN 80–85943–40–9
- Winterová, A. a kol., *Civilní právo procesní*, 4. vydání, Linde, Praha 2006, ISBN 80-7201-595-8
- Zelenka, J., a kol., *Ochrana dat - kryptologie*, Gaudeamus, Hradec Králové 2003, ISBN 80-7041-737-4

## 8.2. Online veřejně přístupná literatura a zdroje

- Projekt rakouské vlády „E-Recht" (elektronické právo)
  *www.cio.gv.at/ikt-board/beratungen/e-law/info*
- Ministerstvo informatiky ČR (dnes již zrušeno)
  *www.micr.cz*
- Ministerstvo vnitra ČR (nástupce MIČR pro oblast eGovernmentu)
  *www.mvcr.cz*

- Ministerstvo spravedlnosti ČR
  *www.justice.cz*
- Zákazníci české justice – spotřebitelská organizace
  *www.ejustice.cz*
- VAŠE PRÁVA - Časopis pro uživatelsky přátelské právo
  *i-pravo.org/casopis*
- eGovernment in the European Countries
  *http://ec.europa.eu/idabc/en/document/5094/5671*
- Estonian Information Society Strategy 2013
  *http://ec.europa.eu/idabc/en/document/6811/5677*
- Sdružení Efektivní stát
  *www.estat.cz*
- Společnost pro výzkum a podporu Open Source (OSS Alliance)
  *www.oss.cz*
- Bez korupce – pilotní projekt nevládní organizace Oživení
  *http://www.bezkorupce.cz*
- Lupa – server o českém internetu
  *www.lupa.cz*
- eArchiv – archív článků a přednášek Jiřího Peterky
  *www.earchiv.cz*
- Internet ve státní správě a samosprávě (k dispozici přednášky a referáty z konference)
  *www.isss.cz*
- IT právo - Server o internetovém a počítačovém právu
  *www.itpravo.cz*
- První certifikační autorita, a.s.
  *www.ica.cz*
- European Commission Group for Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens
  *http://ec.europa.eu/idabc*
- Wikipedie, otevřená encyklopedie
  *www.wikipedia.cz*

## 8.3. Metodiky, předkládací zprávy, studie proveditelnosti a návrhy zákonů

- Návrh zákona o elektronizaci některých procesních úkonů včetně důvodové zprávy
- Metodický pokyn pro popis datových prvků
- Metodický pokyn pro popis elektronických informačních zdrojů
- Best practice - pravidla pro vyřizování elektronické pošty
- Best practice - Pravidla pro tvorbu přístupného webu
- Předkládací zpráva „Provázanost informačního systému elektronické justice se systémem eGovernment v celé veřejné správě", Ministerstvo spravedlnosti ČR, 2007, č.j. 67/2007 OIS SP
- Ministerstvo spravedlnosti ČR, Popis modulární struktury včetně jejich vazeb a návazností a harmonogram vybudování elektronické justice - studie proveditelnosti