Jihočeská univerzita v Českých Budějovicích
Zdravotně sociální fakulta

# Historie vývoje vztahu POLICIE České republiky k ochraně dat obsahujících osobní údaje v policejních informačních systémech v období (1990 -2007)

Bakalářská práce

Autor práce: Pavel Sufčák
Vedoucí práce: PaedDr. Bc. Jaroslav Pangl

15. srpna 2011

**Abstrakt**

Tématem bakalářské práce je historie vývoje vztahu POLICIE České republiky k ochraně dat obsahujících osobní údaje v policejních informačních systémech v období (1990 -2007).

Cílem práce je provedení analýzy vývoje ochrany osobních údajů od roku 1990 do roku 2007 a to ve vztahu k denní praxi policejních orgánů POLICIE ČR, Správy Jihočeského kraje. Dalším pak provedení rozboru vývoje výpočetní techniky v policejní praxi (zabezpečování, ochrana, provoz, zálohování, antivirová ochrana, kazuistika).

Teoretická část práce rozebírá pojem soukromí, vývoj práva na soukromí, vývoj práva na ochranu osobních údajů v měřítku celosvětovém, evropském, českém, veřejnoprávním, trestněprávním a policejním. Je poukázáno na možné druhy hrozícího nebezpečí v oblasti ohrožení datových fondů za použití nejzávažnějších metod kybernality.

Součástí práce je provedení rozboru kvantitativního vývoje nápadu trestných činů dle § 178 Neoprávněné nakládání s osobními údaji, §§ 239, 240 Porušování tajemství doručovaných zpráv, § 257a Poškození a zneužití záznamu na nosiči informací, vycházejícího z informačního systému ESSK (evidenčně statistický systém kriminality) vedeného Centrálou informatiky a analytických procesů služby kriminální policie a vyšetřování Policejního prezidia České republiky v letech 1990 - 2007.

Druhý rozbor hodnotí úroveň činnosti pověřených kontrolních pracovníků, kteří na základě zákona o Policii ČR vykonávají přímý dohled nad dodržováním legislativních norem zákonných i rezortně vnitřně závazných v podmínkách policejního sboru, včetně poukázání na nejčastější pochybení.

## Abstract

The subject of this bachelor's work is a history of development process of relation and attitude of the POLICE of the CZECH REPUBLIC to the protection of the data containing personal data in police information systems covering time period from the year 1990 to the year 2007.

The goal of this bachelor's work is performance of analysis of the development of personal data protection in the time period from the year 1990 until the year 2007 with special emphasis on everyday work and practise of police organisms and police bodies within Management of the South Bohemia Region, POLICE of the CZECH REPUBLIC. Next successive goal of this bachelor's work is the performance of analysis of the development of computer technology applied and used in police practice (safeguarding, protection, operation, back-up and archiving, anti-virus protection, case reporting).

Theoretical part of this bachelor's work deals with and analyses the concept of privacy, the development of the right of privacy, the development of the right to protection of personal data in terms of global, European, the Czech Republic, public-law, criminal-law and police. This bachelor's points out the possibility of various types of imminent danger in the area of data funds being exposed to danger while using the most important relevant methods of cybernetics and cybernality.

The integral part of this bachelor's work is performance of quantitative analysis of the development of occurrence and incidence of criminal acts according to § 178 Unlawful/wrongful treatment of personal data, §§ 239, 240 Breach of secrecy of delivered messages, § 257a Damage and misuse/ill-use of a record on information carrier, arising out of the ESSK (Monitoring, Evidence Statistical System of Criminality) information system, which is run by the Centre (Headquarter Centre) of Informatics and Analytical Processes of the Service of Criminal Investigation Police Headquarters of the Czech Republic in the time period from the year 1990 until the year 2007.

The second analysis assesses and evaluates the level of activities of appointed/ authorized policemen, who on the basis of the Act On Police of the Czech Republic perform direct supervision and inspection regarding observance of legislative standards of both having their basis in laws and falling and being obligatory within the Ministry of Interior under the conditions of Police Force in the Czech Republic, including pointing out the most frequent slight mistakes.

***Prohlášení:***

Prohlašuji, že jsem bakalářskou práci na téma „**Historie vývoje vztahu POLICIE České republiky k ochraně dat obsahujících osobní údaje v policejních informačních systémech v období (1990 -2007)“** vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. V souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v nezkrácené podobě fakultou elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

Souhlasím dále, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 15. srpna 2011 ……

podpis studenta

Poděkování

Chci touto cestou poděkovat panu PaedDr. Bc. Jaroslavu Panglovi, za odborné vedení při zpracování této bakalářské práce a své rodině, za projevenou trpělivost k mé osobě v období celého studia vysoké školy.

**Pavel Sufčák**

**Obsah**

## Úvod

Práce mapuje dostupné informace týkající se problematiky ochrany soukromí a zejména pak ochrany osobních údajů v dnešním přetechnizovaném světě. Alespoň částečně nastiňuje zásady jak předcházet hrozícímu nebezpečí a minimalizování vzniklých a nevratných škod při provozování rozsáhlého datového fondu.

Jednotlivé kapitoly práce popisují historický vývoj, zejména právní úpravy ochrany osobních údajů v evropském a celosvětovém měřítku. Mechanizmy chránící tuto problematiku jsou zde popisovány chronologicky i na našem území a to od dob vlády Josefa II. po současnost.

Následuje přehled legislativních úprav, které navazují a konkretizují zásady uvedené v zákoně č. 101/2000 Sb., o ochraně osobních údajů, včetně úpravy pro instituce veřejnoprávní, zejména pak uplatňované v podmínkách Policie České republiky.

Nastínění procesu budování policejní informatiky v letech 1990 až 2007 nemá za cíl zveřejňování či poodhalování metod Policie České republiky v ochraně citlivého datového fondu. Ochrana informací zpracovávaných u policejních složek je pro společnost bezesporu zásadní. Je zde plně na místě vysoká míra obezřetnosti při dodržování bezpečnostních směrnic, postupů a uplatňování kontrolních mechanizmů. Obecně lze uvést, že se v zásadě bezpečnostní metody nijak neliší od standardních doporučení a metod užívaných v civilním a veřejném sektoru.

## 1. Soukromí

Definice soukromí je obtížná, poněvadž soukromí je o naší existenci a o kvalitě života jedince – kdo jsme, jací jsme, co umíme, co si myslíme, co máme rádi, co jsme udělali či co dělat chceme. Ochrana soukromí je tedy ochrana jedince, ochrana jeho způsobu života vycházejícího z jeho osobnostních práv.[1]

„Soukromí má i své prostorové vyjádření, je to místo, kam se vracíme“[2]

Právní institut soukromí je regulován a chráněn jak hmotně-právními, tak procesně-právními normami, které jsou součástí systémů různých právních odvětví. Ústavního, občanského, pracovního, správního i trestního.[3] Právo na ochranu osobních údajů je nedílnou součástí práva na soukromí.

## 2. Vývoj práva na soukromí

### *2.1 Celosvětové zakotvení práva na soukromí*

Již Aristotelovo rozlišení mezi sférou veřejné politiky, *polis,* a domácí soukromou sférou rodiny, *oikos,* jakožto dvou odlišných sfér života, naznačuje odkaz na určitý stav soukromí. Nelze ho však z historického hlediska co do jeho smyslu, hodnoty a rozsahu pokládat za klasický odkaz na soukromí.[4]

**Právo na soukromí** jako pojem pochází z USA. Jeho formulace má původ v článku z roku 1890 nazvaném **The Right to Privacy**.[5] Tehdy bylo toto právo chápáno ve smyslu „*zaručuje se každému jednotlivému právo na určení, do jaké míry své myšlenky, city a emoce sdělí ostatním*“. Nejznámějším katalogem lidských práv je **Všeobecná deklarace lidských práv** (1948),[6] která byla schválena Valným shromážděním Organizace spojených národů jako nezávazný dokument.

---

[1] KUČEROVÁ, A. BÁRTÍK, V. PECA, J. NEUWIRT, K. NEJEDLÝ, J. *Zákon o ochraně osobních údajů:* Komentář. 1. vydání. Praha: C. H. Beck, 2003. 406 s. ISBN 80-7179-762-6. s. 23.

[2] PORTÁL KOSTROŇ. KOSTROŇ, L. *Soukromí,* [datový soubor] 2003, [online], [cit. 2010-03-02]. Dostupný z <http://www.kostron.cz/soukromi.doc>.

[3] MATES, P. *Ochrana soukromí ve správním právu.* Praha: Linde Praha a.s., 2004, 307 s. ISBN 80-7201-458-7. s. 26.

[4] PORTÁL Stanford Enciklopedia Of Philosophy. *Ochrana osobních údajů*. [webová stránka], [online], [cit. 2010-03-02]. Dostupný z <http://plato.stanford.edu/entries/privacy>.

[5] PORTÁL BRANDEIS UNIVERSITY OF LOUISVILLE. *The Right to Privacy.*[webová stránka], [online], [cit. 2010-03-02]. Dostupný z <http://www.law.louisville.edu/library/collections/brandeis/node/225>.

[6] PORTÁL UN - Organizace spojených národů. *The Universal Declaration of Human Rights.*[webová stránka], [online], [cit. 2010-03-02]. Dostupné z <http://www.un.org/en/documents/udhr>.

Článek 12 Deklarace hovoří:

*„Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“*

Následuje:[7]

- Deklarace práv dítěte (1959),[8]
- Mezinárodní pakt o občanských a politických právech (1966),[9]
- Mezinárodní pakt o hospodářských, sociálních a kulturních právech (1966).[10]

Podle Opčního protokolu k Mezinárodnímu paktu o občanských a politických právech může např. jednotlivec po vyčerpání vnitrostátních prostředků k ochraně svých práv podat stížnost k Výboru pro lidská práva.[11] Výbor nemůže rozhodovat ve věci a jeho rozhodnutí končí sdělením názoru stěžovateli a výzvou státu, proti němuž stížnost směřovala, k zaujetí stanoviska. Své výsledky a šetření výbor uveřejní a shrne ve své výroční zprávě.[12]

### *2.2 Evropské zakotvení práva na soukromí*

Evropská Úmluva o ochraně lidských práv a základních svobod (sjednána v rámci Rady Evropy v Římě roku 1950), ve svém 8 článku věnovaném právu na respektování soukromého a rodinného života uvádí: [13]

- Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence,

---

[7] KUČEROVÁ, A. BÁRTÍK, V. PECA, J. NEUWIRT, K. NEJEDLÝ, J. *Zákon o ochraně osobních údajů: Komentář. 1. vydání.* Praha: C. H. Beck, 2003. 406 s. ISBN 80-7179-762-6. s. 24.

[8] PORTÁL OSN. *Deklarace práv dítěte.* [datový soubor], [online], [cit. 2010-03-02]. Dostupný z <http://www.osn.cz/dokumenty-osn/soubory/deklarace-prav-ditete.pdf>.

[9] PORTÁL OSN. *Mezinárodní pakt o občanských a politických právech.* [datový soubor], [online] [cit. 2010-03-02]. Dostupný z <http://www.osn.cz/dokumenty-osn/soubory/mezinar.pakt-obc.a.polit.prava.pdf>.

[10] PORTÁL OSN. *Mezinárodní pakt o hospodářských, sociální a kulturních právech.* [počítačový soubor], [online], [cit. 2010-03-02]. Dostupný z <http://www.osn.cz/dokumenty-osn/soubory/mezinarodni-pakt-o-hospodarskych-socialnich-a-kulturnich-pravech.pdf>.

[11] MALENOVSKÝ, J. *Mezinárodní právo veřejné:* jeho obecná část a poměr k vnitrostátnímu právu, zvláště právu českému. 4. opravené a doplněné vydání. Brno: Nakladatelství Doplněk, 2004, 468 s. ISBN 80-7239-160-7. s. 139.

[12] MATES, P. *Ochrana soukromí ve správním právu.* Praha: Linde Praha a.s., 2004, 307 s. ISBN 80-7201-458-7. s. 12.

[13] U nás vyhlášena sdělením federálního ministerstva zahraničních věcí č. 209/1992 Sb.

- Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

### *2.3 Zakotvení práva na soukromí na našem území*

„Únorová ústava - Schmerlingova"(1861)[14] zřizuje říšský zákonodárný sbor, který přijímá zákon o ochraně svobody osobní (č. 87/1862 ř. z.) a zákon na ochranu svobody domovní (č. 88/1862 ř. z.), ve kterém vymezuje podmínky vstupu policejních a finančních orgánů do obydlí. Prvorepubliková ústava z roku 1920 a ostatní zákony navazující pojem právo na soukromí výslovně neochraňují. V roce 1964 je schválen občanský zákoník,[15] který je neustále novelizován. § 7 odst. 1 zákona 40/1964 Sb. uvádí, že právo na ochranu své osobnosti má každý občan včetně nezletilce.[16]

**Listina základních práv a svobod** (1993),[17] jako součást ústavního pořádku České republiky vedle Ústavy České republiky, je nejvyšší právní silou, od které se odvíjejí ostatní zákonné normy právního státu. Článkem 7 Listiny je zaručena nedotknutelnost osoby a jejího soukromí jako široký, obecný právní pojem.

## 3. Vývoj práva na ochranu osobních údajů

### *3.1 Mezinárodní zakotvení ochrany osobních údajů*

Na základě zkušeností z USA z konce 60. let v souvislosti s realizací projektu na vytvoření národního informačního centra (NIC),[18] dochází v důsledku rostoucího rozvoje informačních technologií v demokratických zemích k postupnému přijímání zákonů na ochranu osobních údajů.

---

[14] MATES, P. *Ochrana soukromí ve správním právu.* Praha: Linde Praha a.s., 2004, 307 s. ISBN 80-7201-458-7. s. 9.
[15] Zákon č. 40/1964 Sb., občanský zákoník.
[16] DOLEŽÍLEK, J. *Přehled judikatury ve věcech ochrany osobnosti.* Praha: ASPI a.s., 2008, 216 s. ISBN978-80-7357-313-3. s. 62.
[17] Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.
[18] PORTÁL FEDERAL FINANCIAL INSTITUCIONS EXAMINATION COUNCIL. *National Information Center*. [webová stránka], [online], [cit. 2010-03-02]. Dostupný z <http://www.ffiec.gov/nicpubweb/nicweb/NicHome.aspx>.

## *3.2 Evropské zakotvení ochrany osobních údajů*[19]

### *3.2.1 Rezoluce Rady Evropy*

Rezoluce Rady Evropy č. 22 (1973)[20] o ochraně osob vzhledem k elektronickým bankám dat v soukromém sektoru a Rezoluce č. 29 (1974)[21] o ochraně osob vzhledem k elektronickým bankám dat ve veřejném sektoru jsou mezi prvními na evropské půdě.

### *3.2.2 Úmluva č. 108*

Úmluvu Rady Evropy č. 108 (1981)[22] na ochranu osob se zřetelem na automatizované zpracování osobních údajů následuje dodatkový protokol č. 181[23] k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat a o orgánech dozoru a toku dat přes hranice. Pro Českou republiku vstoupila Úmluva č. 108 v platnost v roce 2001[24] a dodatkový protokol v roce 2004.[25]

### *3.2.3 Doporučení Rady Evropy*

Postupně přijímaná Doporučení Rady Evropy, rozvíjejí v Úmluvě č. 108 zakotvené principy v jednotlivých oblastech:

- Doporučení č. 1 (1981) o omezeních pro automatizované zdravotní banky dat - nahrazeno doporučením č. 5 (1997).
- Doporučení č. 10 (1983) o ochraně osobních údajů používaných pro vědecký výzkum a statistiku - nahrazeno doporučením č. 18 (1997).
- Doporučení č. 20 (1985) o ochraně osobních údajů používaných pro účely přímého marketingu.

---

[19] ZEHLOVÁ, V. *Správněprávní aspekty ochrany osobních údajů.* Brno: Masarykova univerzita, Právnická fakulta, Katedra správní vědy, správního práva a finančního práva, 2008. 63 s. Vedoucí práce: doc. JUDr. Soňa Skulová, Ph.D.

[20] PORTÁL COUNCIL OF EUROPE. *Usnesení (1973) 22*. [datový soubor], [online], [citováno 2010-03-02]. Dostupný z <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%2520legal%2520instruments/1Resolution%2873%2922_EN.pdf>.

[21] PORTÁL COUNCIL OF EUROPE. *Usnesení (1974) 29.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%2520legal%2520instruments/1Resolution%2874%2929_EN.pdf>.

[22] PORTÁL COUNCIL OF EUROPE. *Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm>.

[23] PORTÁL COUNCIL OF EUROPE. *Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat, o orgánech dozoru a toku dat přes hranice.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>.

[24] PORTÁL MVČR. *Sbírka mezinárodních smluv.* [datový soubor], [online], [cit. 2010-03-29]. Dostupné z <http://aplikace.mvcr.cz/archiv2008/sbirka/2001/sb052-01m.pdf>.

[25] PORTÁL MVČR. *Sbírka mezinárodních smluv.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://aplikace.mvcr.cz/archiv2008/sbirka/2005/sb015-05m.pdf>.

- Doporučení č. 1 (1986) o ochraně osobních údajů pro účely sociálního zabezpečení.
- Doporučení č. 15 (1987) o úpravě používání osobních dat v policejním sektoru.
- Doporučení č. 2 (1989) o ochraně osobních údajů používaných pro účely nezaměstnanosti.
- Doporučení č. 19 (1990) o ochraně osobních dat používaných pro platební a další operace.
- Doporučení č. 4 (1995) o ochraně osobních údajů v oblasti telekomunikačních služeb zvláště s ohledem na telefonní služby.
- Doporučení č. 5 (1997) o ochraně zdravotních dat.
- Doporučení č. 18 (1997) o ochraně osobních údajů shromažďovaných a zpracovaných pro statistické účely.
- Doporučení č. 5 (1999) o ochraně soukromí na internetu.
- Doporučení č. 9 (2002) o ochraně osobních údajů shromažďovaných a zpracovávaných pro účely pojišťovnictví.

### *3.2.4 Směrnice č. 95/46/ES (1995)*

- Směrnice 95/46/ES[26] určuje požadavky na technickou bezpečnost zpracovávaných dat. Ukládá povinnost oznamovat zpracování osobních dat nezávislému dozoru nad dodržováním přijatých zásad.
- Směrnice 95/46/ES, článek 3, poskytuje ochranu i osobním údajům, které nejsou zpracovávány strojově za podmínky kartotékového uspořádání a vhodnosti k dalšímu zpracování.
- Směrnice 95/46/ES zahrnuje ochranu osobních údajů, které jsou přenášeny z Evropské unie do třetích států.[27]
- Směrnice 95/46/ES určuje přísnější regulaci nakládání s citlivými osobními údaji než nakládání s ostatními osobními údaji.[28]

### *3.2.5 Ostatní důležité směrnice*

- Směrnice č. 00/31/ES (2000)[29] o elektronickém obchodu.

---

[26] PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 1995/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.*[datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:CS:PDF>.

[27] KUČEROVÁ, A. BÁRTÍK, V. PÉCA, J. NEUWIRT, K. NEJEDLÝ, J. *Zákon o ochraně osobních údajů:* Komentář. 1. vydání. Praha: C. H. Beck, 2003, 406 s. ISBN 80-7179-762-6. s. 351.

[28] ŠALOMOUN, M. *Právní regulace nakládání s citlivými údaji.* Právní rozhledy: časopis pro všechna právní odvětví. Praha: C. H. Beck. 2006. č. 19. s. 697-705. ISSN 1210-6410.

[29] PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o*

- Směrnice č. 02/58/ES (2002)[30] o zpracování osobních údajů a ochranu soukromí v telekomunikačním sektoru. Doplňuje Směrnici 95/46/ES a postupně je sama doplňována směrnicí č. 2006/24/ES[31] a směrnicí č. 09/136/ES (2009).[32] V České republice je ochrana soukromí v telekomunikačním sektoru provedena zákonem č. 151/2000 Sb. o telekomunikacích.[33]

### *3.2.6 Úmluva o lidských právech a biomedicíně*

Úmluva o lidských právech a biomedicíně (1997) zaručuje právo jedince na ochranu soukromí ve vztahu k informacím o svém zdraví. V České Republice vstupuje v platnost roku 2001[34]. Každý má právo získat informace, které jsou shromažďovány v souvislosti s jeho zdravotním stavem. V Úmluvě o lidských právech a biomedicíně se v článku 5 objevuje institut – informovaný souhlas pacienta.

### *3.2.7 Listina základních práv Evropské Unie*

V reakci na padesáté výročí Všeobecné deklarace lidských práv z prosince roku 1948 rozhoduje zasedání Evropské rady v Kolíně nad Rýnem ve dnech 3. – 4. června 1999 o sepsání návrhu nového uceleného dokumentu, který by soustředil všechny až dosud publikované, závazné či doporučující, normy upravující oblast lidských práv, to vše s cílem zvýšení všeobecného povědomí o těchto právech.

---

*elektronickém obchodu")* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:25:32000L0031:CS:PDF>.

[30] PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:29:32002L0058:CS:PDF>.

[31] PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:CS:PDF>.

[32] PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:CS:PDF>.

[33] Zákon č. 151/2000 Sb. ze dne 16. května 2000 o telekomunikacích a o změně dalších zákonů.

[34] Vyhlášena sdělením ministerstva zahraničních věcí č. 96/2001 Sb .m.s.

Práce spojené s přípravou jsou svěřeny zvláštnímu orgánu – konventu. Navržený text je vyhlášen 7. 12. 2000 v rámci Mezivládní konference v Nice. Je přijat jako společná deklarace Evropského parlamentu, Rady Evropy a Evropské komise. Jde tedy zatím o politickou deklaraci, tj. dokument právně nezávazný. Listina základních práv Evropské Unie, která je někdy označována jako Charta základních práv občanů EU, je prvním uceleným textem v evropské historii, obsahujícím jak tradiční lidská práva, tak práva ekonomická, politická a sociální.[35] Stejný konvent navrhuje začlenění Charty do smluvního rámce ve formě Smlouvy o Ústavě pro Evropu v červnu 2004. Po neúspěchu s přijetím evropské ústavy navrhuje začlenění ve znění Lisabonské smlouvy (2007).

### *3.3 Ústavní zakotvení ochrany osobních údajů*

**Listina základních práv a svobod** (1993)[36] v článku 10, ochraňuje právo na lidskou důstojnost, osobní čest, právo před neoprávněným zásahem do soukromého a rodinného života a v odstavci 3 pak ochranu osobních údajů.

## 4. Současná právní úprava ochrany osobních údajů pro ČR

### *4.1 Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů*

V návaznosti na článek 10 Listiny zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů (dále jen ZoOOÚ) představuje podrobnou a konkrétní právní ochranu osobních údajů v rámci České republiky. Obsah ZoOOÚ je zaměřen na dosažení co největší vzájemné slučitelnosti se Směrnicí 95/46/ES a Úmluvy č. 108[37]

#### *4.1.1 Zásady zpracování osobních údajů*

- Zásada legitimity zpracování[38]
- Zásada účelovosti[39]
- Zásada časového omezení[40]
- Zásada potřebnosti a přiměřenosti[41]

[35] PORTÁL EUROPA. *Charta základních práv občanů EU.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://ec.europa.eu/ceskarepublika/information/glossary/term_46_cs.htm>.
[36] Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod.
[37] ZoOOÚ nabyl účinnosti dne 1. června 2000.
[38] § 3, odst. 6, ZoOOÚ.
[39] § 5, odst. 1, písm. f), ZoOOÚ.
[40] § 5, odst. 1, písm. e), ZoOOÚ.
[41] § 5, odst. 1, písm. d), ZoOOÚ.

- Zásada průhlednosti[42]
- Zásada bezpečnosti[43]
- Zásada práva přístupu k údajům[44]
- Zásada práva na opravu a výmaz[45]
- Zásada nezávislého dozoru[46]
- Zásada souhlasu subjektu údajů[47]
- Zásada zákazu sdružování osobních údajů[48]

### *4.1.2 Působnost ZoOOÚ:*[49]

- ZoOOÚ se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.
- ZoOOÚ se vztahuje na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.
- ZoOOÚ se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.
- ZoOOÚ se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.
- ZoOOÚ se dále vztahuje na zpracování osobních údajů:
    - Jestliže se právní řád České republiky použije přednostně na základě mezinárodního práva veřejného, i když správce není usazen na území České republiky,
    - jestliže správce, který je usazen mimo území Evropské unie, provádí zpracování na území České republiky a nejedná se pouze o předání osobních údajů přes území Evropské unie; v tomto případě je správce

[42] § 11, ZoOOÚ.
[43] § 13, ZoOOÚ.
[44] § 12, ZoOOÚ.
[45] § 21, odst. 1, písm. b), ZoOOÚ.
[46] § 2, ZoOOÚ.
[47] § 5, ZoOOÚ.
[48] § 5, ZoOOÚ.
[49] § 3, ZoOOÚ.

povinen zmocnit postupem podle § 6 na území České republiky zpracovatele.

- jestliže zpracování provádí správce prostřednictvím svých organizačních jednotek umístěných na území Evropské unie, musí zajistit, že tyto organizační jednotky budou zpracovávat osobní údaje v souladu s národním právem příslušného členského státu Evropské unie.

### *4.1.3 Výjimky z působnosti ZoOOÚ*

Výjimky[50] z působnosti ZoOOÚ jsou stanoveny zvláštními zákony k zajištění:

- bezpečnosti České republiky,[51]
- obrany České republiky,[52]
- veřejného pořádku a vnitřní bezpečnosti,[53]
- předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů,[54]
- významného hospodářského zájmu České republiky nebo Evropské unie,[55]
- významného finančního zájmu České republiky nebo Evropské unie, kterým je zejména stabilita finančního trhu a měny, fungování peněžního oběhu a platebního styku, jakož i rozpočtová a daňová opatření,[56]
- výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci v případech ochrany veřejného pořádku a vnitřní bezpečnosti, předcházení a stíhání, trestné činnosti nebo zajištění významného hospodářského či finančního zájmu České republiky nebo Evropské unie; činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti,[57]
- činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti.[58]

[50] § 3, odst. 6, ZoOOÚ.
[51] Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.
[52] Zákon č. 219/1999 Sb., o ozbrojených silách České republiky.
[53] Zákon č. 273/2008 Sb., o Policii České Republiky.
[54] Zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti.
[55] Zákon č.241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů.
[56] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů.
[57] Zákon č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, ve znění pozdějších předpisů.
[58] Zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činností bývalé Státní bezpečnosti, ve znění zákona č. 10 7/2002 Sb.

### *4.1.4 Úřad pro ochranu osobních údajů*

Úřad pro ochranu osobních údajů je nezávislým orgánem vytvořeným za účelem provádění dozoru nad zpracováním osobních údajů. Původně bylo navrhováno, aby měl postavení tzv. jiného ústředního správního úřadu, s tím, že měli být speciálně upraveny záruky jeho nezávislosti. Z podnětu Legislativní rady vlády byl koncipován jako nezávislý orgán sui genesis.[59] Z hlediska materiálního je ovšem jeho činnost typickou činností správního orgánu.[60] Podobnou koncepci má například Nejvyšší kontrolní úřad[61] nebo Česká národní banka.[62] Tato pozice mu umožňuje vydávání právních předpisů – vyhlášek, které se zveřejňují ve Sbírce zákonů. Ve státním rozpočtu má svoji zvláštní kapitolu a tím získává materiální nezávislost na jiných orgánech[63]. Mluvíme-li o nezávislosti, je třeba zdůraznit, že se nejedná o nezávislost absolutní, ale jen v mezích ZoOOÚ, případně dalších právních předpisů, které upravují jeho působnost a které jsou pro výkon působnosti Úřadu aplikovány. Relativita nezávislosti se projevuje současně i možností podat žalobu proti rozhodnutí Úřadu ve správním soudnictví, způsobem jmenování předsedy a inspektorů Úřadu, kdy tito jsou jmenováni prezidentem ČR na návrh Senátu a stanovením neslučitelnosti jejich funkcí s některými dalšími funkcemi (např. poslance, senátora, soudce atd.)[64]

### *4.1.5 Kompetence Úřadu pro ochranu osobních údajů*

ZoOOÚ přiznává Úřadu pro ochranu osobních údajů následující kompetence:

- provádění dozoru nad dodržováním povinností stanovených zákonem při zpracování osobních údajů,
- vedení registru zpracování osobních údajů,
- přijímání podnětů a stížností na porušení povinností při zpracovávání osobních údajů a informační povinnost o stavu jejich vyřízení,

[59] PORTÁL WIKIPEDIA. *Internetová encyklopedie.* [webová stránka], [online], [cit. 2010-03-02]. Dostupný z <http://cs.wikipedia.org/wiki/Sui_generis>.
[60] MATES, P., NEUWIRT, K. *Právní úprava ochrany osobních údajů v ČR*. Praha: Nakladatelství IFEC, Praha, 2000, 128. s. ISBN 80-86412-02-4. s. 37.
[61] § 2, odst. 1 zákona č. 166/1993 Sb., o Nejvyšším kontrolním úřadu.
[62] §1, zákona č. 6/1993 Sb., o České národní bance.
[63] BÁRTÍK, V. JANEČKOVÁ, E. Ochrana osobních údajů v aplikační praxi:vybrané otázky. Praha: Linde Praha a.s., 2009. 277 s. ISBN 978-80-7201-740-9. s. 234.
[64] ZEHLOVÁ, V. *Správněprávní aspekty ochrany osobních údajů.* Brno: Masarykova univerzita, Právnická fakulta, Katedra správní vědy, správního práva a finančního práva, 2008. 63 s. Vedoucí práce: doc. JUDr. Soňa Skulová, Ph.D.

- projednávání přestupků a jiných správních deliktů,
- udělování pokut
- zajištění plnění požadavků vyplývajících z mezinárodních smluv, jimiž je ČR vázána,
- zajištění plnění požadavků z přímo použitelných předpisů ES,
- poskytování konzultací v oblasti ochrany osobních údajů.

### *4.2 Trestně právní úprava do 31. 12. 2009 – zákon č. 140/1961 Sb., Trestní zákon:*

- § 257a Poškození a zneužití záznamu na nosiči informací.
    - Společnost se bránila proti tomu, kdo v úmyslu spáchat trestný čin poškodil či zneužil počítačový systém nebo nosič informací.

### *4.3 Trestně právní úprava od 1. 1. 2010 – zákon č. 40/2009 Sb., Trestní zákoník:*

- § 180 TZ Neoprávněné nakládání s osobními údaji.
    - Společnost se brání proti tomu, kdo neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracuje nebo si přisvojí osobní údaje jiného, které byly o něm shromážděny v souvislosti s výkonem veřejné moci. Podmínkou je zde způsobení vážné újmy na právech nebo oprávněných zájmech osoby, jíž se tyto údaje týkají.[65]
- § 182 TZ Porušení tajemství dopravovaných zpráv.
    - Společnost se brání proti tomu, kdo úmyslně porušuje tajemství uzavřeného listu, datové, textové, hlasové, zvukové či obrazové zprávy a tajemství neveřejného přenosu počítavých dat do počítačového systému, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková data.[66]

[65] Fryšták, M. a kol. *Trestní právo hmotné*: zvláštní část, stav k 1. 1. 2010. Ostrava: KEY Publishing s.r.o., 2009. 170 s. ISBN 978-80-7418-040-8, strana 30.
[66] Tamtéž, strana 32.

- §230 TZ - Trestný čin neoprávněný přístup k počítačovému systému a nosiči informací.
    - Společnost se brání proti tomu, kdo v úmyslu spáchat tr. čin překoná bezpečnostní opatření a tím neoprávněně získá přístup k počítačovému systému nebo takový přístup získá k nosiči informací.[67]
- §231 TZ - Trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.
    - Společnost se brání proti tomu, kdo v úmyslu spáchat tr. čin přechovává, vlastní, nebo vyrobí apod. nástroje, pomocí nichž lze získat přístup k počítačovému systému nebo jeho části.[68]
- §232 TZ - Trestný čin poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.
    - Společnost se brání proti tomu, kdo v hrubé nedbalosti způsobí na cizím majetku značnou škodu tím, že poruší mu danou povinnost[69]

### *4.4 Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů zákon o soudnictví ve věcech mládeže § 94 Uveřejnění výsledků řízení.*

- Společnost se brání proti tomu, aby nedocházelo ke zveřejňování výsledků řízení o uložení opatření dítěti mladšímu než patnáct let, které se dopustilo činu jinak trestného. Aby nedocházelo k uveřejnění ve veřejných sdělovacích prostředcích před nabytím právní moci rozhodnutí, kterým bylo řízení skončeno, a jen bez uvedení jména a příjmení dítěte, dalších účastníků řízení a jejich opatrovníků nebo jiných zástupců. Výjimky ze zákazů uveřejnění povoluje soud pro mládež.

[67] Fryšták, M. a kol. *Trestní právo hmotné*: zvláštní část, stav k 1. 1. 2010. Ostrava: KEY Publishing s.r.o., 2009. 170 s. ISBN 978-80-7418-040-8, strana 65.
[68] Tamtéž, strana 66.
[69] Tamtéž.

### *4.5 Zákon č. 52/2009 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony*

- Cílem novely je maximálně omezit okruh informací poskytovaných veřejnosti o oběti trestného činu, kterou je třeba zvýšeně chránit, a zabránit zveřejňování jejích osobních údajů, fotografií či obrazových záznamů prostřednictvím veřejných sdělovacích prostředků (tisk, rozhlas, televize), včetně veřejných počítačových sítí.[70]

### *4.6 Zákon č. 273/2008 Sb. o Policii České republiky*

- Společnost upravuje nakládání s osobními údaji v jednotlivých ustanoveních takto: [71]
  - § 39 - Rušení provozu elektronických komunikací.
  - § 40 - Vstup do obydlí, jiného prostoru nebo na pozemek.
  - § 60 - Obecná ustanovení o zpracování informací policií.
  - § 62 - Pořizování záznamů.
  - § 65 - Získávání osobních údajů pro účely budoucí identifikace.
  - § 66 - Získávání informací z evidencí.
  - § 67 - Získávání informací v souvislosti s odhalováním a šetřením přestupků.
  - § 78 - Předávání informací.
  - § 79 - Zvláštní ustanovení o zpracování osobních údajů policií.
  - § 80 - Předávání ne zpřístupňování osobních údajů.
  - § 81 - Zveřejňování osobních údajů.
  - § 82 - Prověřování potřebnosti dalšího zpracování osobních údajů.
  - § 83 - Informování o osobních údajích a oprava nepravdivých nebo nepřesných osobních údajů.

[70] PORTÁL SAGIT. *Zákon č. 52/2009 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://www.sagit.cz/pages/zpravodajtxtanot.asp?cd=166&typ=r&zdroj=../_anotace/sb09052b>.

[71] PORTÁL POLICIE ČR. *Zákon č. 273/2008 Sb., o Policii České Republiky.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://www.policie.cz/soubor/zakon-o-policii-cr-273-2008-sb.aspx>.

- § 84 - Zpracování údajů v Schengenském informačním systému.
- § 85-88 - Zpracovávání osobních údajů při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů a zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti
- § 98 Kontrola použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí, rušení provozu elektronických komunikací a kontrola činnosti Inspekce policie.
- § 115 je bez názvu a upravuje povinnost mlčenlivosti.

### *4.6.1 Sbírka interních aktů řízení policejního prezidia*

Ve svém závazném pokynu č. 215/2008 stanoví policejní prezidium některé bližší podmínky a postupy pro zpracování osobních údajů rozpracované na podmínky policejní práce.

V jednotlivých částech a oddílech a článcích předpisu popisuje (zkráceně):

- Úvodní ustanovení a vymezení pojmů.
- Členění zpracování osobních údajů:
  - Trvalá zpracování osobních údajů,
  - časově a věcně omezená zpracování.
- Subjekty zpracování osobních údajů:
  - Správce, zpracovatel, příjemce,
  - vedoucí pracovník
    - určení příjemce,
  - gestor problematiky zpracování,
  - zvlášť určený pracovník.
- Podmínky pro zahájení zpracování osobních údajů:
  - Trvalá zpracování,
    - podmínky pro zahájení zpracování osobních údajů,
  - pracovní soubory.
- Zpracování osobních údajů při zajišťování veřejného pořádku a při pátrání po osobách.

- Zpracování osobních údajů při plnění úkolů Policie ČR stanovených zvláštními zákony.
- Provozní zpracování osobních údajů:
    - Zpracování osobních údajů pracovníků při výkonu řídící, kontrolní a hodnotící činnosti vedoucími pracovníky.
- Organizační zpracování:
    - Evidence přístupů, evidence příjemců,
    - zpracování osobních údajů pracovníků prováděná vedoucími pracovníky pro účely řídící a kontrolní činnosti při plnění úkolů policie.
- Zpřístupňování (předávání) osobních údajů:
    - Zpřístupňování (předávání) osobních údajů v rámci policie,
    - zpřístupňování (předávání) osobních údajů s využitím telefonního spojení a mobilní lustrace a prostřednictvím radiostanice,
    - zpřístupňování (předávání) osobních údajů mimo rámec policie,
- Prokazování oprávněnosti a nutnosti přístupu.
- Registr evidencí a zpřístupnění informace o prováděných zpracováních osobních údajů.
- Právo přístupu subjektu údajů k informacím:
    - žádost, postup příjemce žádosti,
    - odložení žádosti, zamítnutí žádosti, postoupení žádosti,
    - postup správce a zpoplatnění poskytnuté informace.
- Kontrolní činnost.
- Opatření k zajištění ochrany osobních údajů:
    - dokumentování technicko-organizačních opatření k zajištění ochrany osobních údajů.

Ve své části „kontrolní činnost“ popisuje závazný pokyn v článku 71 až 73 metody, postupy a nakládání s výsledky kontrol dodržování pravidel. V odstavci třetím čl. 73, pak ukládá kontrolnímu pracovišti (zvlášť určenému pracovníkovi) zasílat vždy do 15. července a do 15, prosince kalendářního roku gestorovi problematiky cestou

nadřízeného služebního funkcionáře, souhrnnou informaci o provedených kontrolách za pololetí a kalendářní rok, v níž se uvádí:

- Počet provedených kontrol,
- počet kontrolovaných pracovníků,
- druhy a počet zjištěných pochybení a k nim přijatá opatření,
- přehled organizačních celků, na nichž byla kontrola provedena.

## 5. Koncepce informačních systémů veřejné správy

Novelou zákona č. 365/2000 Sb[72]., o informačních systémech veřejné správy (dále jen „zákon o ISVS“), která byla provedena zákonem č. 81/2006 Sb., se zavádí institut dlouhodobého řízení informačních systémů veřejné správy (dále jen ISVS). Dlouhodobé řízení ISVS se realizuje prostřednictvím informační koncepce orgánu veřejné správy a provozní dokumentace jím provozovaných ISVS.

Informační systémy veřejné správy představují významný nástroj výkonu veřejné správy na všech úrovních. Řízení ISVS na nejvyšší úrovni přísluší Ministerstvu vnitra (dále jen „MV“) jako úřadu veřejné správy s kompetencemi v této oblasti. MV využívá pro řízení ISVS následující nástroje:

- právní předpisy,
- metodické pokyny MV,
- koordinační, koncepční a strategické dokumenty a věstník MV,
- dohled nad investicemi do informačních technologií (IT) ve veřejné správě,
- provoz informačního systému o informačních systémech veřejné správy (IS o ISVS vyhláška č. 528/2006 Sb.)[73] a o datových prvcích (vyhláška č. 469/2006 Sb.),[74]
- výkon státní kontroly v oblasti ISVS,

[72] PORTÁL MVČR. *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.* [datový soubor], [on-line], [ cit. 2010-04-11]. Dostupný z <http://www.mvcr.cz/soubor/zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy-s-barevnym-vyznacenim-zmen-provedenych-zakonem-c-190-2009-sb.aspx>.

[73] PORTÁL MVČR. *Vyhláška č. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy*. [datový soubor], [on-line], [cit 2010-04-11]. Dostupný z <http://www.mvcr.cz/soubor/vyhlaska-c-528-2006-sb-o-informacnim-systemu-o-informacnich-systemech-verejne-spravy.aspx>.

[74] PORTÁL MVČR. *Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích*. [datový soubor], [on-line], [cit 2010-04-11]. Dostupný z <http://www.mvcr.cz/soubor/vyhlaska-c-469-2006-sb-o-informacnim-systemu-o-datovych-prvcich.aspx>.

- účast na procesech akreditace a atestace, povinnost dlouhodobého řízení ISVS pro orgány veřejné správy.

Změnu pravidel v této oblasti přinesl i zákon č. 110/2007 Sb.,[75] o zrušení Ministerstva informatiky, kterým byly kompetence v oblasti dlouhodobého řízení ISVS, původně svěřené Ministerstvu informatiky, převedeny na Ministerstvo vnitra.

### *5.1 Předmět a úprava informační koncepce*

Zákon o ISVS ukládá povinnost zpracování informační koncepce jako stěžejního nástroje dlouhodobého řízení informačních systémů veřejné správy a na jejím základě vytvoření provozní dokumentace k jednotlivým ISVS do 1. ledna 2009. Vyhláška č. 29/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy upravuje strukturu a obsah informační koncepce, postupy orgánů veřejné správy při jejím vytváření, vydávání, při vyhodnocování jejího dodržování a požadavky na řízení bezpečnosti a kvality ISVS podle § 5a odst. 1 zákona o ISVS.[76]

V příloze č.: 7 je uvedena ukázky vzorové informační koncepce obce s výkonem přenesené působnosti

### *5.2 Dlouhodobé cíle v oblasti řízení bezpečnosti*

Za účelem řízení bezpečnosti informačních systémů je nutné, stejně jako v oblasti kvality, aby orgán veřejné správy definoval dlouhodobé cíle, kterých chce v této oblasti dosáhnout.

Ve vyhlášce jsou vyjmenovány cíle, které nelze při zajišťování bezpečnosti opomenout. Jedná se o:

- bezpečnost dat (např. data není možné neoprávněně číst, měnit nebo mazat),

[75] PORTÁL MVČR. *Zákon č. 110/2007 Sb., o některých opatřeních v soustavě orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů*. [datový soubor], [on-line], [cit 2010-04-11]. Dostupný z <http://aplikace.mvcr.cz/archiv2008/micr/files/3882/zak110_sb041_07.pdf>.

[76] PORTÁL MVČR. *Komentář k vyhlášce č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy.* [datový soubor], [on-line], [cit 2010-04-11]. Dostupný z <http://www.mvcr.cz/soubor/komentar-k-vyhlasce-c-529-2006-sb-o-pozadavcich-na-strukturu-a-obsah-informacni-koncepce-a-provozni-dokumentace-a-o-pozadavcich-na-rizeni-bezpecnosti-a-kvality-informacnich-systemu-verejne-spravy.aspx>.

- bezpečnost technických a programových prostředků (např. není možné měnit zdrojový kód programu bez oprávnění, ve vytvářených programech je nutné ověřovat všechna vstupní data)
- bezpečnost služeb (např. poskytované služby musí být přístupné jen oprávněným uživatelům, o přístupu ke službám musí být pořizovány záznamy).

### *5.3 Schvalování informační koncepce*

Vyhláška vymezuje, jaké údaje je nutné do dokumentů informační koncepce uvádět; smyslem je, aby i v případě provádění změn bylo možné dohledat platné znění dokumentu a byli známi původci informační koncepce.[77]

### *5.4 Provozní dokumentace*

Provozní dokumentaci informačního systému veřejné správy tvoří tyto dokumenty:

- bezpečnostní dokumentace informačního systému veřejné správy:
  - bezpečnostní politika informačního systému veřejné správy,
  - bezpečnostní směrnice pro činnost bezpečnostního správce systému,
- systémová příručka,
- uživatelská příručka.

### *5.5 Role při správě IS VS*

Orgán veřejné správy musí vymezit role správce systému a bezpečnostního správce systému, a to včetně jejich oprávnění, která potřebují pro provádění činností umožňujících řádné a bezpečné fungování informačního systému.[78]

[77] PORTÁL MVČR. *Komentář k vyhlášce č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy.* [datový soubor], [on-line], [cit 2010-04-11]. Dostupný z <http://www.mvcr.cz/soubor/komentar-k-vyhlasce-c-529-2006-sb-o-pozadavcich-na-strukturu-a-obsah-informacni-koncepce-a-provozni-dokumentace-a-o-pozadavcich-na-rizeni-bezpecnosti-a-kvality-informacnich-systemu-verejne-spravy.aspx>.

[78] Tamtéž.

# 6. Problémy v oblasti ochrany soukromí a ochrany osobních údajů

Největší problémy v oblasti ochrany soukromí a ochrany osobních údajů se odvíjejí od pokroku moderních technologií a elektronických komunikací:[79]

- Internet. Sociální diskusní sítě. Sociální inženýrství. IP telefonie.
- Monitorovací a sledovací systémy. Kamerové systémy všech druhů.
- Pevná i bezdrátová telefonie. – globální odposlech[80]
- RFID[81] – smart cards.
- Biometrika – digitalizace lidského těla.
- Nanotechnologie[82]

## *6.1 Ohrožení datových fondů*

### *6.1.1 Požár, voda, destrukce objektu*

Počítačové technologické místnosti se budují v takových částech budovy, kde je předpoklad, že případný požár, havárie vody, plynu či sesuv půdy neohrozí provozovanou technologii. Vhodné je předem vypracovat plán zásahu při odvracení škodlivých havarijních situací. Zejména je potřeba si uvědomit, že technologické místnosti jsou pro svou důležitost vybaveny nepřerušitelným zdrojem energie (OnLine UPS[83], Diesel agregát) a že v případě zásahu nebude vždy možné odpojit elektrickou energii. V místnosti se nedoporučuje rozvod vody ani centrální vytápění. Naopak se doporučuje místnost vybavit požárním hlásičem s vysokou citlivostí detekce, případně automatizované spuštění nehořlavého zaplynování prostoru. V žádném případě se nedoporučuje v technologické místnosti skladovat archivní a instalační média. V případě havárie většinou dojde k jejich poškození.

---

[79] PORTAL IMA. NEUWIRT, K. *Ochrana soukromí – nutnost nebo překážka?* [datový soubor] 2008, [online], [cit. 2010-03-29] Dostupný z <http://www.ima.cz/download/cz/3infoday/sablonaPSPEV_prezentace_KN.pdf>.

[80] JIROVSKÝ, V. *Kybernetická kriminalita.* První vydání. PRAHA: Grada Publishing, a.s. 2007, 288 s. ISBN 978-80-247-1561-2. s. 179 – 192.

[81] PORTÁL WIKIPEDIA. *Identifikace na radiové frekvenci RFID*. [webová stránka], [online], [cit. 2010-03-02]. Dostupný z [webová stránka] [online] <http://cs.wikipedia.org/wiki/RFID>.

[82] PORTÁL TECHNISCHE UNIVERSITÄT DORTMUND. Rizika plynoucí z vojenského využití nanotechnologie. [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://e3.physik.tu-dortmund.de/P&D/Pubs/RiskMilNT_Lecce.pdf>

[83] PORTÁL WIKIPEDIA. *UPS.* [webová stránka], [online], [cit. 2010-03-29] dostupný z <http://cs.wikipedia.org/wiki/UPS>.

### *6.1.2 Přepětí nebo podpětí v elektrické síti*

Bouřky, následné výpadky a nestabilita napětí elektrické energie je nutné eliminovat používáním nepřerušitelného zdroje energie (OnLine UPS, Diesel agregát) s možností řízeného uzavření operačních systémů.

### *6.1.3 Hacking – vymezení a vývoj pojmu*

Pojmenování „hacker“ a termín „hacking“ vznikl v padesátých letech minulého století v komunitě radioamatérů.[84]

Prvními hackery byli nadšenci, kteří zásahem do programového vybavení počítače odstraňovali nedokonalý chod počítače. Nelze je spojovat s porušováním zákonů, ani získáváním dat z cizích počítačů. Zásahy jsou označovány jako „hacks“ (odtud hacking, hacker).[85] Dnes je termín hacker užíván běžně, ale často v nesprávném kontextu. Hacking tak spadl do oblasti počítačové kriminality, avšak ne vždy je postižitelný zákonem, na rozdíl od crackingu a softwarového pirátství. Cracking je „postup určité úpravy bez užití zdrojových kódů programovacího jazyka, v němž byl daný program naprogramován.“[86]

Hackeři se dělí do několika kategorií:[87]

- Skriptový amatér (Script Kiddie), útočník, užívající hotové nástroje, nebere ohled na to, zda něco zničí či překročí hackerská pravidla,
- hacker začátečník – lama, (Lamer),
- bílé klobouky (White Hats), kteří dodržují daná pravidla a chtějí být hackery v původním slova smyslu,
- černé klobouky (Black Hats), kterým jde o vlastní prospěch, nejčastěji finanční zisk,
- šedé klobouky (Gray Hats), kteří stojí na pomezí předchozích dvou kategorií.[88]

[84] JIROVSKÝ, V. *Kybernetická kriminalita.* První vydání. PRAHA: Grada Publishing, a.s. 2007, 288 s. ISBN 978-80-247-1561-2. s. 47.
[85] MATĚJKA, M. *Počítačová kriminalita.* 1. vyd. Praha : Computer Press, 2002. 108 s. ISBN 80-7226-419-2. s. 20-21.
[86] ZEMÁNEK, J. *Slabá místa Windows aneb jak se bránit hackerům*. 1. vyd. Kralice na Hané : Computer Media s. r. o., 2004. 156 s. ISBN 80-86686-11-6.s. 10-11.
[87] MATĚJKA, M. *Počítačová kriminalita.* 1. vyd. Praha : Computer Press, 2002. 108 s. ISBN 80-7226-419-2. s. 54.
[88] Morální hodnoty hackerské komunity jsou uvedeny v příloze č.: 4.

## *6.2 Metody počítačové kriminality*

### *6.2.1 Příprava před útokem*

Příprava před útokem je součástí analýzy zejména u cílených útoků. Může být představována různými činnostmi pro zjištění informací k dalšímu útoku. Pro hackera je dobré získat co nejvíce informací, které mu mohou usnadnit práci.

### *6.2.2 Zjišťování informací o cíli*

Informací o cíli lze získat z otevřených zdrojů:

- Prohledáváním odpadků vyvážených z firmy, ve kterých lze nalézt:
  - Účty za telefon, výpisy bankovních účtů, firemní manuály, staré diáře,
  - CD-ROMy, diskety, starý Hardware – pevné disky vyřazený počítačů,
- Prohledávání internetu legální cestou pomocí vyhledávačů. Kniha Google HACKING[89] popisuje nejčastěji využitelné operátory vyhledávání. Základní operátory vyhledávání jsou uvedeny v příloze č.: 5
- Prohledávání volných databází typu obchodní rejstřík, živnostenský rejstřík, katastrální úřad apod.,
- Prohledávání volných databází typu „Whois“ (informace o vlastnících doménových jmen a IP[90] adres) nebo „YellowPages“ (informace o firmách) Základní výpis pro doménové jméno jcu.cz je uveden v příloze č.: 6

### *6.2.3 Skenování*

Skenováním síťových portů[91] lze zjistit, jaké porty jsou otevřené a přijímají spojení. Podle zjištěných otevřených portů lze usuzovat, jaké služby jsou v systému spuštěny. Hacker při skenování zjišťuje bezpečnostní mezery.[92]

---

[89] LONG, J. *Google Hacking*. Miroslav Kučera; RNDr. Jan Pokorný. Brno : Zoner Press, 2005. 472 s. ISBN 80-86815-31-5.
[90] DOSTÁLEK, L., KABELOVÁ, A. a kol. *Velký průvodce protokoly TCP/IP a systémem DNS.* 3. aktualizované a rozšířené vydání, Brno: CP Books, a.s., 2005, 542 s. ISBN 80-7226-675-6. s. 163 a násl.
[91] PORTÁL WIKIPEDIA. *Síťový port.* [webová stránka], [online], [cit. 2010-03-29] Dostupný z <http://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_port>.
[92] ERICKSON, J. *Hacking : umění exploitace.* 1. vyd. Brno : Zoner Press, 2005. 263 s.ISBN 80-86815-21-8. s. 182.

### *6.2.4 Malware*

Malware (malicious software) označuje škodlivý kód, jehož úkolem je poškodit zařízení, data, vyčerpat systémové zdroje, zcizit informace apod.[93]

Malware lze rozdělit následovně: [94]

- Virus (Počítačový vir).[95]
- Worm (Červ).[96]
- Trojan Horse (Trojský kůň).[97]
- Spyware (Data Miner - informační důl)[98]
- Adware (software za reklamu).[99]
- Ostatní
    - Software Keylogger (programový zachytávač stisknutých kláves).[100]
    - Cookie (Sušenka).[101]
    - Webbug (Štěnice).[102]
    - Backdoor (Zadní vrátka).[103]
    - Password dealer (Zloděj hesel).[104] a mnoho dalších.

[93] GÁLA, L. POUR, J. TOMAN, P. *Podniková informatika*: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky. Praha: Grada Publishing a.s., 484 s. ISBN 80-247-1278-4. s. 383

[94] KRÁL, M. *Bezpečnost domácího počítače: Prakticky a názorně.* Praha : Grada Publishing a.s. 2006. 334 s. ISBN 80-247-1408-6. s. 21-22.

[95] PORTÁL SPAMFINGER. *Spam a Scam glosář*. [webová stránka] 2003-2011, [online], [cit. 2010-03-29]. Dostupný z <http://www.spamfighter.com/lang_cs/faq_glossary.asp>.

[96] Tamtéž.

[97] Tamtéž.

[98] CRAIG, P. HONICK, R. BURNETT, M. *Softwarové pirátství bez záhad.* Praha: Grada Publishing a.s., 2008. 212 s. ISBN 80-247-1765-4. s. 183.

[99] ŠTĚDROŇ, B. *Open Source software*: ve veřejné správě a soukromém sektoru. Praha: Grada Publishing a.s., 2009. 128 s. ISBN 978-80-247-3047-9. s. 21.

[100] JANCZEWSKI, L. COLARIK, A. M. *Cyber warfare and cyber terrorism.* Idea Group Inc. (IGI), 2008. 532 s. ISBN 978-1-59140-991-5. s. 310.

[101] AULDS, CH. ROUBÍČEK, L. *Linux*: administrace serveru Apache. Praha : Grada Publishing a.s. 2003. 535 s. ISBN 978-8-02470-640-5. s. 346.

[102] PORTÁL SPAMFINGER. *Spam a Scam glosář*. [webová stránka] 2003-2011, [online], [cit. 2010-03-29]. Dostupný z <http://www.spamfighter.com/lang_cs/faq_glossary.asp>

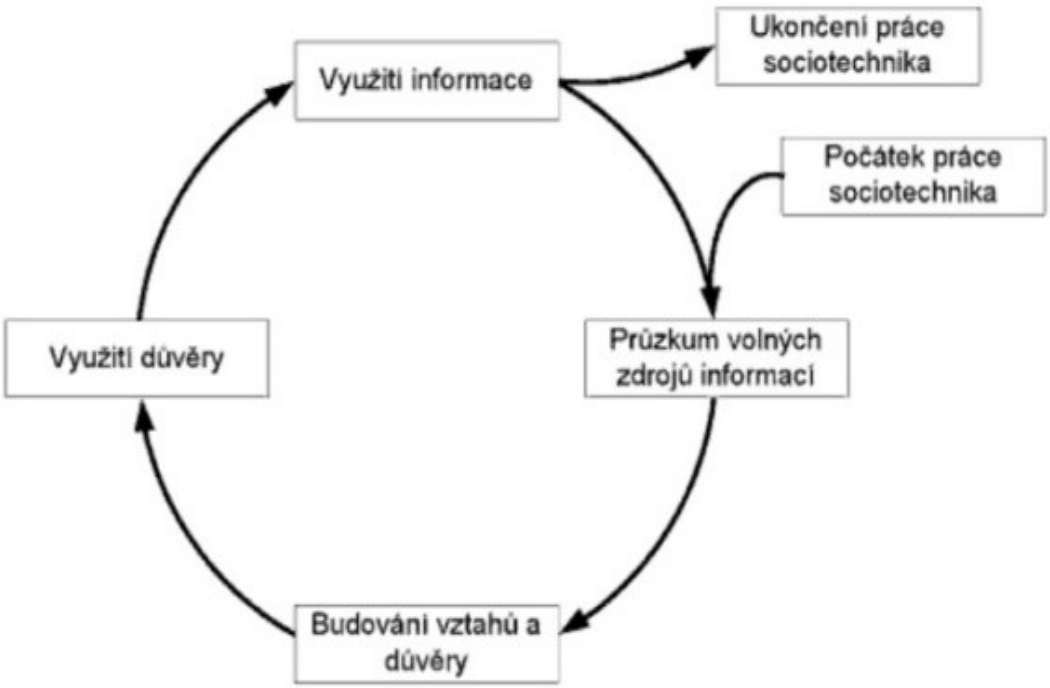
[103] Tamtéž.

[104] Tamtéž.

### *6.2.5 Sociální inženýrství - sociotechnika*

Kevin Mitnik, „Umění klamu“[105] - uvězněný autor definuje rozdíl mezi podvodníkem a sociotechnikem. „Ten kdo mámí z lidí peníze je obyčejný podvodník, ale ten kdo využívá manipulace a přesvědčování vůči firmám se záměrem získání informací je sociotechnik.“ Mitnikova aféra upozornila na jeden z nejslabších článků počítačových systémů – člověka. V případě sociálního inženýrství útočník vždy něco požaduje, mohou to být informace, peníze či činnost (např. otevření přílohy e-mailu). Nejrozšířenějším druhem podvodu spojeného se sociálním inženýrstvím, jsou tzv. nigerijské dopisy[106].

Obrázek č.: 1 Sociotechnický cyklus zneužití informace.




Zdroj Jirovský, strana 197

[105] MITNICK, K. SIMON, W. *Umění klamu*. Lazarczyk, R.; Vašta, L. 1. Vydání. Gliwice : HELION S.A., c2003. 348 s. ISBN 83-7361-210-6.

[106] PORTÁL PINA. *Nigerijské dopisy v novém.* [webová stránka], [online], [cit. 2010-04-12]. Dostupný z <http://www.pina.cz/2008/03/08/nigerijske-dopisy-v-novem/>.

### *6.2.6 Phishing - rybaření*

Základem termínu je „fish“ (resp. „phish“), což v přeneseném významu znamená úlovek. Tak byly označovány uživatelské účty, ke kterým hackeři získali přístup. Phishing se zaměřuje na finanční instituce, jako banky či spořitelny, ale lze s ním také odcizit osobní identitu. Pro hackera je nejjednodušší umístit do e-mailu formulář s požadovanými položkami a odeslat je uživateli nebo mu odeslat e-mail s odkazem na falešnou webovou stránku na které se formulář nachází s žádostí o jeho vyplnění.[107]

### *6.2.7 Brutální útok*

Brutální útok představuje metodu, kdy se útočník do počítače pokouší proniknout hrubou silou. Jedná se o přímý a cílený útok na konkrétní počítač. V převážné většině se jedná o útoky vedené za pomoci nespokojených zaměstnanců. Smazáním dat nebo software může vzniknout firmě významná škoda. Pokud chce obeznámený zaměstnanec spáchat takový čin, zničí i zálohy dat. Přitom vše může vypadat jako nehoda a ne záměrný útok. Zejména nepříjemné je, pokud se jedná o software vyvinutý „na míru“ nebo o zdrojové kódy nového programového produktu.[108] Mezi brutální útoky můžeme zařadit i použití Hardware Keylogger (technický zachytávač stisknutých kláves).

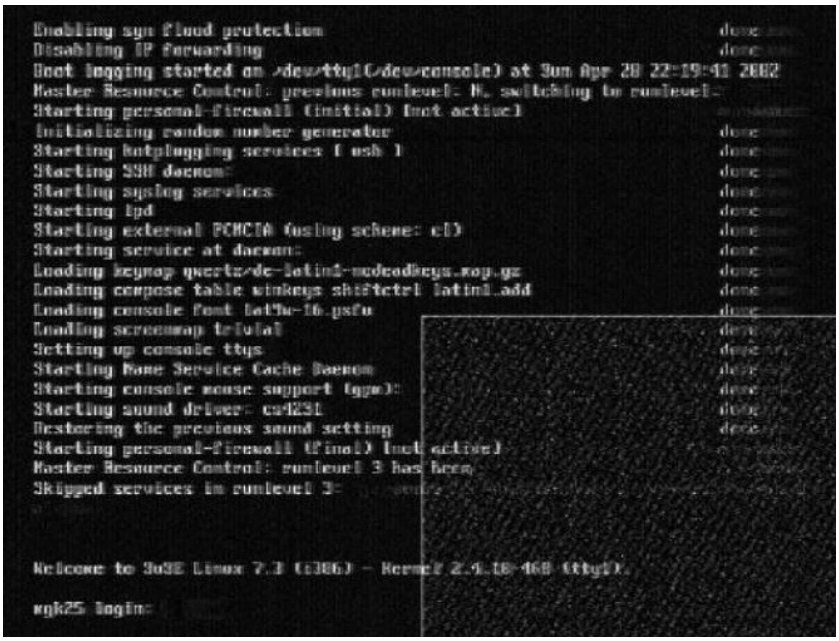
### *6.2.8 Únik informací klasickou cestou – komunikační kanál – oblast radiového spektra*

Uvádí se odposlech monitorů počítačů klasickou cestou, tedy toho co obsluha na monitoru vidí. Kmitočet horizontálního a vertikálního rozkladu obrazu se poměrně snadno šíří prostorem a jeho zachycení vhodnou anténou je možný i na několik metrů.

[107] KOVÁŘOVÁ, P. *Problematika získávání dat z cizího osobního počítače s OS Windows XP s přihlédnutím k situaci v ČR.* Brno: Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, 2006, 76 s., Vedoucí práce Mgr. Petr Škyřík.

Rekonstrukce textu digitálního monitoru při startu systému Linux

Obrázek č.: 2




Zdroj: Jirovský, strana 175

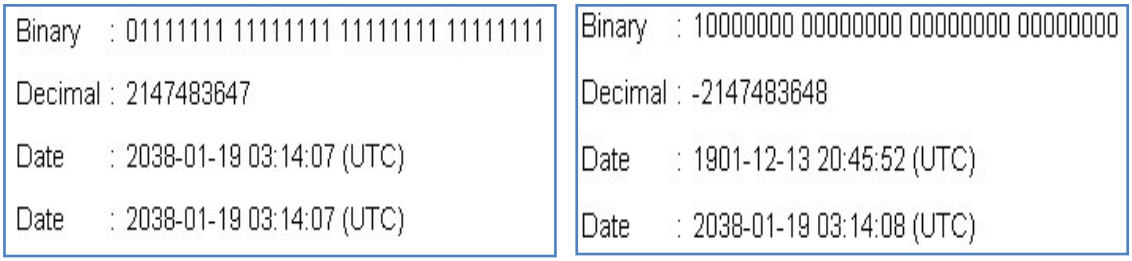
### *6.2.9 Problém Y2K38*

Na webové stránce http://www.y2k38.org/ se odečítá pomyslný čas pro všechny programátory a zejména majitele Unixových aplikací, který jim zbývá do provedení potřebných opatření na odvrácení hrozby, která podobně jako fenomén Y2K hrozila při přechodu z roku 1999 na rok 2000. Co se stane v sobotu dne 19. ledna 2038 v době mezi 3 hodinou ranní, 14 minutou, 07 a 08 sekundou? Problém může nastat v Unixových nebo podobných datovacích systémech, které reprezentují systémový čas jako počet sekund (ignorujíce přestupné sekundy) od 00:00:00 1. ledna 1970. Tato reprezentace času se díky masové rozšířenosti programovacího jazyka C vyskytuje v programech pro většinu operačních systémů. Datový typ „time_t“ je na většině 32-bitových systémech používán k ukládání vteřinového počítadla jako 32bitové celé číslo se znaménkem (32bit signed integer). Poslední čas, který takto může být zapsán, je úterý 19. ledna 2038 v 03:14:07. Čas v další sekundě „přeteče“ a bude vnitřně

[108] JIROVSKÝ, V. *Kybernetická kriminalita.* První vydání. PRAHA: Grada Publishing, a.s. 2007, 288 s. ISBN 978-80-247-1561-2. S. 121.

reprezentován jako záporné číslo, což může způsobit pád programů, jelikož neuvidí takovéto datum jako 2038, ale spíše jako 1901. Řešením je přechod na datový typ „time_t“ pracující na 64-bitových systémech. Přetečení tohoto datového typu by poté nastalo až v neděli 4. prosince roku 292277026596.[109]

Obrázek č.: 3




Zdroj: Wikipedia

## 7. Cíle práce a hypotézy

Cíle práce:

- Provedení analýzy vývoje ochrany osobních údajů od roku 1990 do roku 2007 a to ve vztahu k denní praxi policejních orgánů POLICIE ČR, Správy Jihočeského kraje.
- Provedení rozboru vývoje výpočetní techniky v policejní praxi (zabezpečování, ochrany, provoz, zálohování, antivirová ochrana, kazuistika).

Ověřované hypotézy:

- Ochrana osobních údajů – důležitý faktor fungování demokratické společnosti.
- Policejní praxe preferuje ochranu osobních údajů občanů.
- Aplikace zákona č. 213/2003 Sb. o soudnictví ve věcech mládeže v praxi policejních útvarů posílilo ochranu osobních údajů.

[109] PORTÁL WIKIPEDIA. *Problém roku 2038*. [webová stránka], [on-line], [cit. 2010-04-12]. Dostupný z <http://cs.wikipedia.org/wiki/Y2k38>.

### *7.1 Statistické zpracování nápadů trestné činnosti a dopravní nehodovosti.*

Evidenčně statistický systém kriminality je počítačově vedený systém, který registruje a zpracovává údaje o neobjasněné i objasněné trestné činnosti a jejích pachatelích v období od 1. 1. 1973 do současnosti. Databázi tohoto systému naplňují případy, které šetří policie, úřady vyšetřování. Databáze se naplňuje zpracováním formulářů (formulář trestného činu a formulář známého pachatele). Formuláře jsou vyplňovány na základě existujících číselníků, kde určité skutečnosti jsou nahrazeny kódem. [110]

### *7.2 Evidence obyvatel*

Různé formy evidencí či přehledů mají v našich zemích již dlouhodobou tradici a to od dob Josefa II., který zavádí evidenci poddanstva. Způsob vedení farních záznamů (později matričních) se víceméně zachoval i za první republiky, protektorátu, druhé republiky a převzala ho i ČSR po únoru 1948. V roce 1954, se vnikem „čtyřciferného" lomítka rodného čísla jako objektového identifikátoru fyzické osoby,[111] byla založena manuální okresní evidence občanů. Způsob mechanického fonetického vyhledávání přes příjmení a jméno byl na tehdejší dobu značně vyspělý. Přibližně v té době také začaly vznikat okresní evidence motorových vozidel. V roce 1972 rozhodla tehdejší vláda o vybudování počítačové evidence občanů za využití strojově načtených dat z formulářů sčítání lidu v r. 1980. Výsledek sehrání dat byl katastrofický – skoro 50% chybovost. V průběhu let 1980–1985 proběhla další 3 kola sehrání a čištění dat, která upravila chybovost na 15 %. Následoval pokus o vytvoření třístupňového systému okres – kraj – centrum na technice SMEP[112] (SM 5211, SM 5212) s operačním systémem DOS-RV (ОСРВ „Операционная Система Реального Времени" - operacionaja sysťéma

[110] PORTÁL VYŠŠÍ POLICEJNÍ ŠKOLA MV BRNO. JEDLIČKA, M. *Počítačová kriminalita* [webová stránka], [on-line], [cit. 2010-04-12]. Dostupný z <http://www.vpsmvbrno.cz/jedlicka/poc_krim/pocitace.html>.

[111] MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*: 2. Doplněné a aktualizované vydání. Praha: ASPI, Wolters Kluwer, 2008, 468 s. ISBN 978-80-7357-322-5. s. 60-61.

[112] PORTÁL ROOT. TIŠNOVSKÝ, P. *Unixové vykopávky*. [webová stránka], [on-line], 1998 – 2010 [cit. 2010-04-12]. Dostupný z <http://www.root.cz/clanky/pdp-11-a-smep-system-malych-elektronickych-pocitacu/>.

reálnovo vrémeni).[113] Zkušebně nasazeno v Jihočeském kraji. Pro kvalitu techniky byl experiment v r. 1990 ukončen.[114]

V témž roce byl na MV zpracován projekt JIS – „Jednotný informační systém státní správy“, který zahrnoval integraci správních evidencí (včetně evidence zbraní) a byl stavěn ve dvou stupních – okres - centrum. Realizace byla zahájena v r. 1991 na tehdy špičkové technologii WYSE 7000i[115] s operačním systémem UNIX V3.2[116] (zakoupení techniky ještě v době embarga bylo možné na základě schválení „doložky nejvyšších výhod“ mezi vládou ČSFR a USA v roce 1990).[117] Data byla z centra rozehrána na všechny okresy a byla provedena jejich oprava a doplnění z manuálních okresních evidencí. Tyto revize byly ukončeny cca v r. 1994. Přístup do systému byl řízený, jak na úrovni operačního systému UNIX, tak na úrovni databázového prostřední. Veškerá činnost uživatele byla zaznamenána v systémovém logu.

### *7.2.1 Volební seznamy pro první svobodné volby 1990*

Příprava voleb do Sněmovny národů Federálního shromáždění konaných ve dnech 8. - 9. června 1990 se v Jihočeském kraji, uskutečnila za efektivního přispění tehdy již částečně zrevidovaného fondu evidence obyvatel a došlo k vytištění sestav, podkladů pro volební seznamy. Podklady byly předány jednotlivým volebním komisím, s cílem připravit řádný průběh voleb. Podklady obsahovaly mimo jiné celá rodná čísla nejen trvale hlášených oprávněných voličů, ale i oprávněných voličů - emigrantů s uvedením jejich poslední adresy trvalého pobytu na našem území. Později se toto ukázalo jako ne zrovna šťastné řešení. V porevoluční euforii se jmenné seznamy s rodnými čísly objevovaly na nástěnkách panelových domů, nebo byly volně vyvěšeny před volebními místnostmi. U pozdějších podkladů se již rodná čísla neuváděla a pro identifikaci voliče ve volební místnosti postačuje jako identifikátor fyzické osoby jméno, příjmení, datum

[113] PORTÁL WIKIPEDIA. *RSX-11*. [webová stránka], [on-line], [cit 2010-04-11]. Dostupný z <http://en.wikipedia.org/wiki/RSX-11>.
[114] PORTÁL INTERNET STÁTNÍ SPRÁVY A SAMOSPRÁVY. MALÁTEK, J. *Celostátní správní a dopravně správní evidence.* [datový soubor], [on-line], 2010 [cit 2010-04-11]. Dostupný z <http://www.isss.cz/archiv/2001/sbornik/prednasky/malatek.doc>.
[115] PORTÁL WIKIPEDIA. *Wyse Technology*. [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://en.wikipedia.org/wiki/wyse>.
[116] PORTÁL WIKIPEDIA. *UNIX*. [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/UNIX>.
[117] PORTÁL SPOLEČNÁ ČESKO-SLOVENSKÁ DIGITÁLNÍ PARLAMENTNÍ KNIHOVNA. *Stenoprotokol 8. Společné schůze Sněmovny lidu a Sněmovny národů Federálního shromáždění ČSFR.* [webová stránka], [on-line], [cit 2010-04-11]. Dostupný z <http://www.psp.cz/eknih/1990fs/slsn/stenprot/008schuz/s008002.htm>.

narození a místo trvalého pobytu. Podklady pro volební seznamy přestala Policie ČR pro obce tisknout po odchodu dopravně správních agend pod Okresní úřady v roce 2000 na základě dříve přijatých usnesení vlády č. 338/1995,[118] 622/1997[119] a 623/1997[120]

### *7.3 Operativně taktická evidence*

Kartotéky plné děrovaných karet jednotlivých spáchaných deliktů a pachatelů trestné činnosti, ze kterých lze pomocí zvláštního napichování na jehlice a následného setřásání vytipovat možné pachatele bylo nutno nahradit efektivnější technologií zpracování. Roku 1992 dochází k náhradě karet informačním systémem NTC – Nápad trestné činnosti. Byl veden na lokálních personálních počítačích s operačním systémem MS-DOS[121] za použití databázového prostředí Fox-Pro[122]. Systém byl velmi zranitelný a nestabilní. Přistupovat k datům mohl každý, kdo měl přístup do uzamčené místnosti a mnohdy jedinou zábranou bylo heslo do BIOSu[123].

### *7.4 Pátrací systémy*

Ve stejném období vznikají informační systémy „pátrání po osobách“ (osoby pohřešované, osoby hledané pro svoji kriminální činnost, nalezené neznámé mrtvoly a kosterní nálezy) a „pátrání po motorových vozidlech“. Oba systémy byly stejně jako NTC řízeny operačním systémem MS-DOS a databází Fox-Pro. Denně modifikovaná data byla zasílána do ústředí a zpět přenosem komprimovaných, šifrovaných dávek po vnitřní telefonní sítí ministerstva vnitra neskutečně nízkou rychlostí, nejprve 2400 bps., později 9600 bps.

Dávka byla v ústředí zpracována a zpět byla zaslána aktualizační dávka z ostatních okresů. Stejnou dávkou postupně putovala data všech kriminalistických evidencí.

---

[118] PORTÁL VLÁDA ČR. *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 7. června 1995 č.338.* [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/8EDD579E0F7EB5BBC12571B6007103E4>.

[119] PORTÁL VLÁDA ČR. *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 8. října 1997 č.622.* [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/E08A091A2B26D648C12571B6006EF667>.

[120] PORTÁL VLÁDA ČR. *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 8. října 1997 č.623.* [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/02CE5D7A1B946D86C12571B6006F2E52>.

[121] PORTÁL WIKIPEDIA. *MS-DOS.* [webová stránka],[on-line], [cit 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/MS-DOS>.

[122] PORTÁL WIKIPEDIA. *FoxPro.* [webová stránka],[on-line], [cit 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/FoxPro>.

[123] PORTÁL WIKIPEDIA. *BIOS.* [webová stránka],[on-line], [cit 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/BIOS>.

### *7.5 Zákon o ochraně osobních údajů v informačních systémech*

Po schválení zákona č. 256/1992 Sb. *o ochraně osobních údajů v informačních systémech* došlo u ministerstva vnitra ČR k přijetí NMV č. 65/1994, *kterým se stanoví postup při sestavování projektových záměrů informačních systémů a počítačových sítí, při realizaci a evidenci projektů informačních systémů a počítačových sítí a při evidenci počítačových sítí a jednotek výpočetní techniky*. Jinými slovy nařízení, které zahájilo řízené evidování informačních systémů, prostředků výpočetní techniky a vznikající lokální počítačové sítě (LAN) a jejich propojování do rozsáhlých počítačových síťí (WAN). Na základě již neplatného NMV č. 68/1994, *kterým se určují pracoviště zajišťující evidenci a kontrolu informačních systémů nakládajících s osobními údaji provozovaných MV a Policií ČR*, pak došlo k přehodnocení některých informačních systému. Některé byly zakonzervovány, jiné dále podporovány.

### *7.6 Formování pracovišť garantujících profesionální přístup k informatice*

V roce 1996 došlo na celém území ke vzniku okresních OAI (oddělení analytiky a informatiky, dnešní OddIKT – oddělení informačních a komunikačních technologií). Pracovníkům těchto oddělení se společně s ÚSŘI (útvar systémového řízení a informatiky policejního prezidia, dnešní CIAP SKPV[124] – centrála informatiky a analytických procesů služby kriminální policie a vyšetřování) a krajskými pracovišti OTZ (odbor technického zajištění, dnešní OIKT – odbor informačních a komunikačních technologií) v poměrně krátké době podařilo nasadit na všechna obvodní oddělení pořádkové policie první výpočetní techniku s operačním systémem Windows NT. Technika byla pořízena z větší části z prostředků „readmisní dohody“.[125]

V tomto období dochází k:

- Vybudování počítačové sítě v budovách okresních ředitelství,

[124] PORTÁL POLICIE ČR. *CIAP SKPV*. [webová stránka],[on-line], [cit 2010-04-11] Dostupný z <http://www.policie.cz/clanek/centrala-informatiky-a-analytickych-procesu-sluzby-kriminalni-policie-a-vysetrovani.aspx>.

[125] PORTÁL VEŘEJNÉ SPRÁVY. *Dohoda o zpětném přebírání osob na společných hranicích se SRN.* [webová stránka], [on-line], [cit 2010-04-11] Dostupný z http://www.portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_l=5/1995&PC_8411_ps=10#10821>.

- propojení se směrem k centru a vybudování celorepublikové intranetové sítě MV ČR na vlastních přenosových trasách,
- propojení se směrem k základním útvarům policie – obvodním oddělením pořádkové policie na vlastních přenosových trasách včetně pracovišť pohraniční policie,
- zavedení interní elektronické pošty na všechna pracoviště,
- zavedení okresních, krajských a centrálních webových stránek jako uživatelského rozhraní pro přístup ke zmodernizovaným informačním systémům vedeným již na okresních SQL databázových strojích na serverových počítačích v doménovém prostředí Windows Server NT verze 4.

### *7.7 Příprava na vstup do evropských struktur*

Novela zákona č. 283/1991 Sb., o Policii České republiky přináší v roce 2001 v hlavě páté (§42g a následující) zvláštní ustanovení o zpracování osobních údajů. K zajištění specifické kontroly uvedených činností je na každém okresním ředitelství Policie ČR zřízeno jedno tabulkové místo. Pracovník je zařazen na již zmíněné informatické pracoviště a mimo technickou činnost vykonává pravidelné kontroly dodržování pravidel pro zpracování osobních údajů dle závazných pokynů policejního prezidia, které jsou neustále zdokonalovány a uzpůsobovány.[126]

### *7.8 Centralizace informačních systémů*

Jak se zlepšují jednotlivé technologie pracovních stanic, serverů, rychlosti připojení dochází k přehodnocení prvotního úsilí dostat VT na koncové body a probíhá snaha o centralizaci datových fondů jednotlivých informačních systémů. Postupně se jedna databáze za druhou přesouvá na centrální výkonné řídící počítače. Dochází k posilování náhradních řešení pro případné výpadky. Buduje se páteřní optická datová síť propojující všechny okresy mezi sebou, kraje a centrum navzájem.

[126] Např. ZP PPR č. 215/2008, kterým se stanoví některé bližší podmínky a postupy pro zpracování osobních údajů (o ochraně osobních údajů).

### *7.9 Posilování bezpečnosti*

Vzhledem k bezpečnostním rizikům bylo ze strany ministerstva vnitra ČR vypsáno výběrové řízení na jednotné antivirové prostředí. Bylo vybráno řešení firmy Symantec™, které svým uceleným řešením chrání všechny koncové body. Symantec™ Endpoint Protection Manager Console je zobrazena na obrázku č.: 4. a přehledně zobrazuje okamžitý stav virové nákazy, stav rizikových stavů na jednotlivých stanicích ve spravovaném segmentu počítačové sítě (většinou kopíruje okresní teritorium). Rovněž tak pravidelná instalace opravných balíčků v operačních systémech Microsoft® pomocí produktu Windows® Server Update Services[127] (WSUS) a jeho pravidelné vyhodnocování zaručuje zvýšenou ochranu proti napadení datového fondu jak zevnitř, tak zvenčí prostřednictvím externích médií i síťových hrozeb. Microsoft® WSUS Console je zobrazena na obrázku č.: 5. Důležité je pravidelné vyhodnocování bezpečnostních logovacích (kontrolních) souborů a okamžitá reakce na vzniklou situaci. Používání GPO[128] (Group Polici – zásady skupiny) umožňuje centralizovanou správu a konfiguraci operačních systémů pracovních stanic, provozovaných aplikací a nastavení systémových proměných i práv uživatelů v Active Directory[129] a dálkové instalace software package - MSI balíčků[130]. Z pohledu správce systému je velice důležité kontrolovat to, co uživatelé mohou a nemohou dělat při své práci na pracovní stanici a operativně to měnit dle potřeby. GPO má za cíl také snížení nákladů na podporu uživatelů. Obrázek Console GPO není uveřejněn záměrně.

---

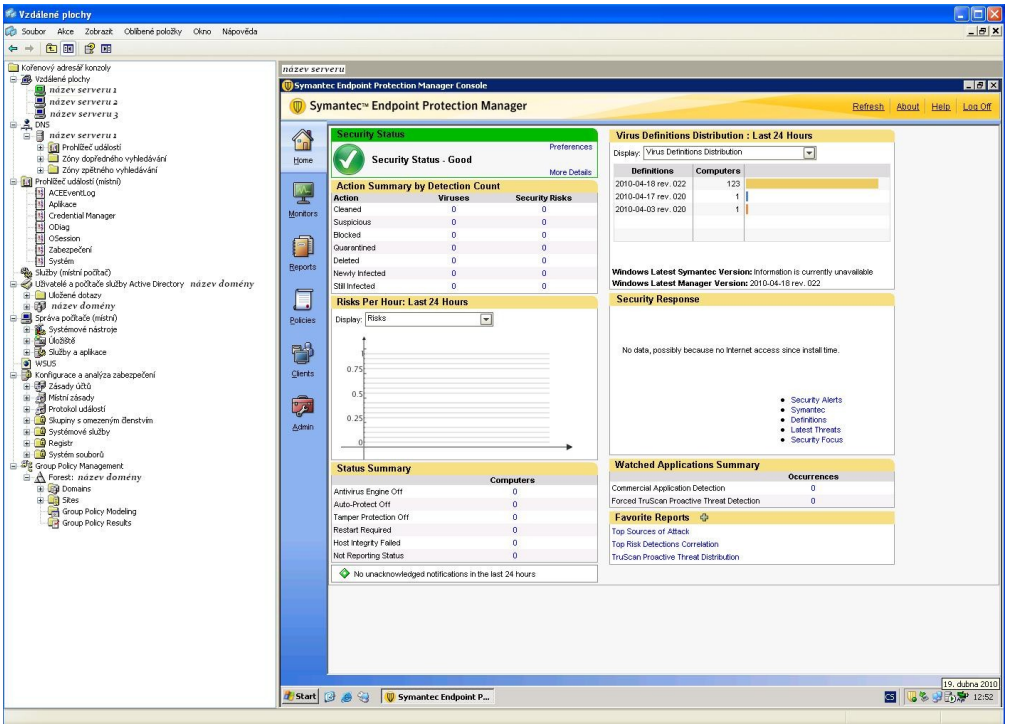
[127] PORTÁL WIKIPEDIA. *Windows Server Update Servises.* [webová stránka], [on-line], [cit. 2010-03-29] Dostupný z <http://cs.wikipedia.org/wiki/Windows_Server_Update_Services>.

[128] MAR-ELIA, D., MELBER, D., STANEK, W. R., *Microsoft Windows Group Policy Guide:* Zásady skupiny Microsoft Windows. Brno: Computer Press, a.s., 2006, 760 s. ISNB 80-251-1262-4 s. 28 a násl.

[129] RUSSEL, CH., CRAWFORD. S., GEREND, J. *Microsoft Windows Server 2003:* Velký průvodce administrátora. Brno: CP Books, a.s., 2005, 1374 s. ISNB 80-251-0579-2 s. 413 a násl.

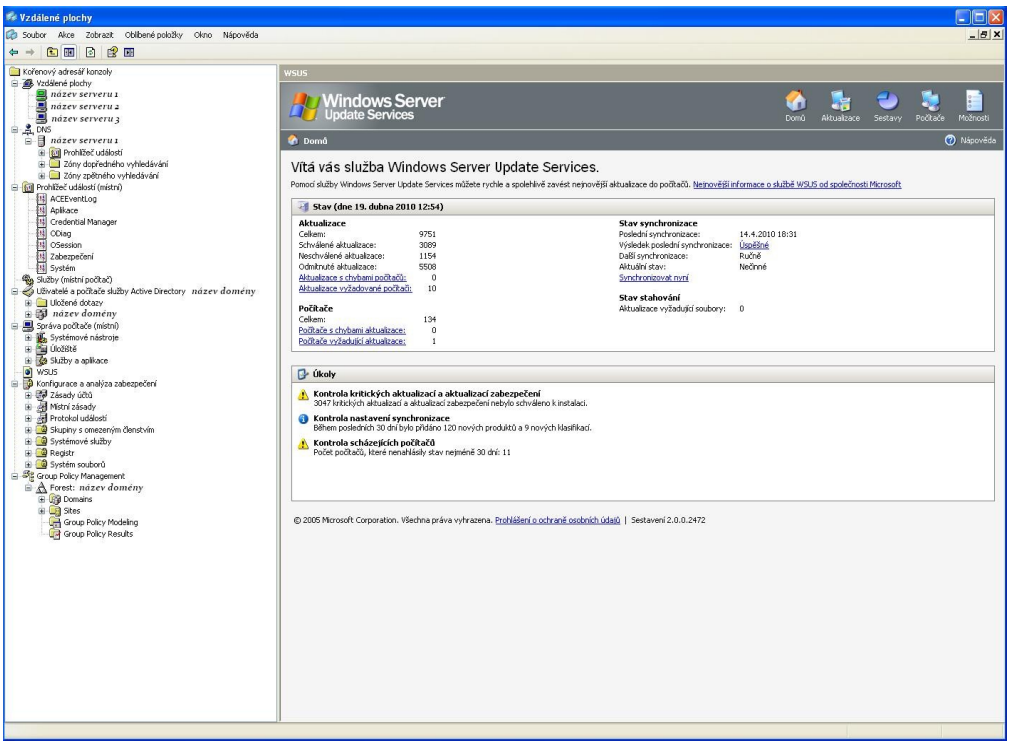
[130] HLAVELKA, J. a kol. *Výkladový slovník výpočetní techniky a komunikací.* Vydání první, Praha: Computer Press, 1997, 452 s. ISBN 80-7226-023-5. s. 380.

Obrázek č.: 4




Zdroj: vlastní

Obrázek č.: 5




Zdroj: vlastní

### *7.10 Kazuistika*

- Případ pojišťovací společnosti

„Nejvyšší správní soud rozhodl v právní věci žalobkyně …, proti žalovanému Úřadu pro ochranu osobních údajů …, o kasační stížnosti žalobkyně …. proti rozsudku Městského soudu v Praze č.j. 10 Ca 118/2003 – 61 ze dne 14. 10. 2004 takto:

I. Kasační stížnost s e z a m í t á .“

..

V roce 2004 projednával Nejvyšší správní soud kauzu, kdy jedné pojišťovací společnosti, byla v prvoinstančním rozhodnutí uložena pokuta ve výši 3 miliony korun. V této společnosti, jejíž činností dochází ke zpracovávání osobních údajů o klientech, došlo ke krádeži přenosného zálohovacího zařízení s datovým fondem v rozsahu 500-700 tisíc záznamů. Policie ČR případ odložila. Pochybení ovšem neuniklo pozornosti inspektorům Úřadu pro ochranu osobních údajů. [131]

- Případ kontrolovaného policisty

V roce 2006 prováděl pověřený pracovník OAI kontrolu policisty, který v rámci dotazu na osobní údaje konkrétní osoby uvedl jako důvod dotazu „ Dotaz na syna“. Po bližším zjištění okolností tohoto zdůvodnění bylo konstatováno, že policista svým jednáním pochybil. Jeho provedený dotaz nijak nesouvisel s jeho služební činností a byl neoprávněný. Na syna se dotazoval z důvodu toho, že potřeboval informace k řádnému vyplnění formuláře daňového přiznání.

[131] PORTÁL ÚOOÚ. *Rozsudek nejvyššího správního soudu.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://www.uoou.cz/files/judik_09.pdf>.

## 8. Metodika

K rozboru trestné činnosti byla použita statistická data Centrály informatiky a analytických procesů Policejního prezídia ČR. Na základě získaných statistických údajů z let 1992 - 2007, byl vytvořen přehled o vývoji trestné činnosti dle §§ 180 - **Neoprávněné nakládání s osobními údaji**, 182 - **Porušení tajemství dopravovaných zpráv**, 257a - **Poškození a zneužití záznamu na nosiči informací trestního zákona**.

K rozboru počtu provedených kontrol směřujících na dodržování pravidel ochrany osobních údajů pracovníky POLICIE ČR Správy Jihočeského kraje byla použita data z let 2006 – 2007 ze souhrnných hlášení, poskytovaných Policejnímu prezídiu krajským pracovištěm a jednotlivými okresními pracovišti. Hodnocení kontrol jiného časového období nebylo možno použít, jelikož plánování, hodnocení a vykazování shora uvedených kontrol bylo pracovníky jednotlivých pracovišť prováděno nesystémově, nahodile.[132]

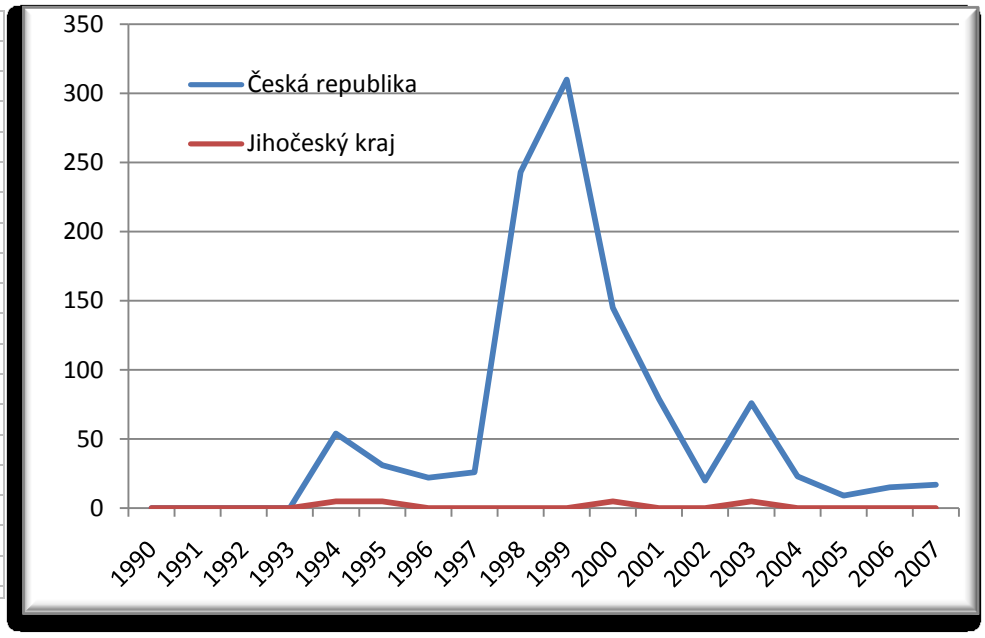
[132] V této době docházelo k formování jednotné metodiky.

## 9. Výsledky

Analýza vývoje trestné činnosti dle § 182 TZ Porušení tajemství dopravovaných zpráv za sledované období 1994 až 2007 porovnává situaci v České republice a v Jihočeském kraji. Ukazuje, že nejvyšší počet zjištěných skutků v České republice byl dosažen v roce 1999. V Jihočeském kraji byl počet skutků nulový. Ze zpracovaného grafu č. 1 je patrný nejprve prudký vzestup v letech 1998 až 1999. Následuje prudký pokles zjištěných skutků v České republice v roce 2000, 2001 a 2002. V Jihočeském kraji se počet zjištěných skutků pohybuje průměrně v jednotkách zjištěných skutků, což zobrazuje plochá křivka vývoje.

**Graf č. 1** **Počet zjištěných případů trestného činu - Porušování tajemství dopravovaných zpráv.**

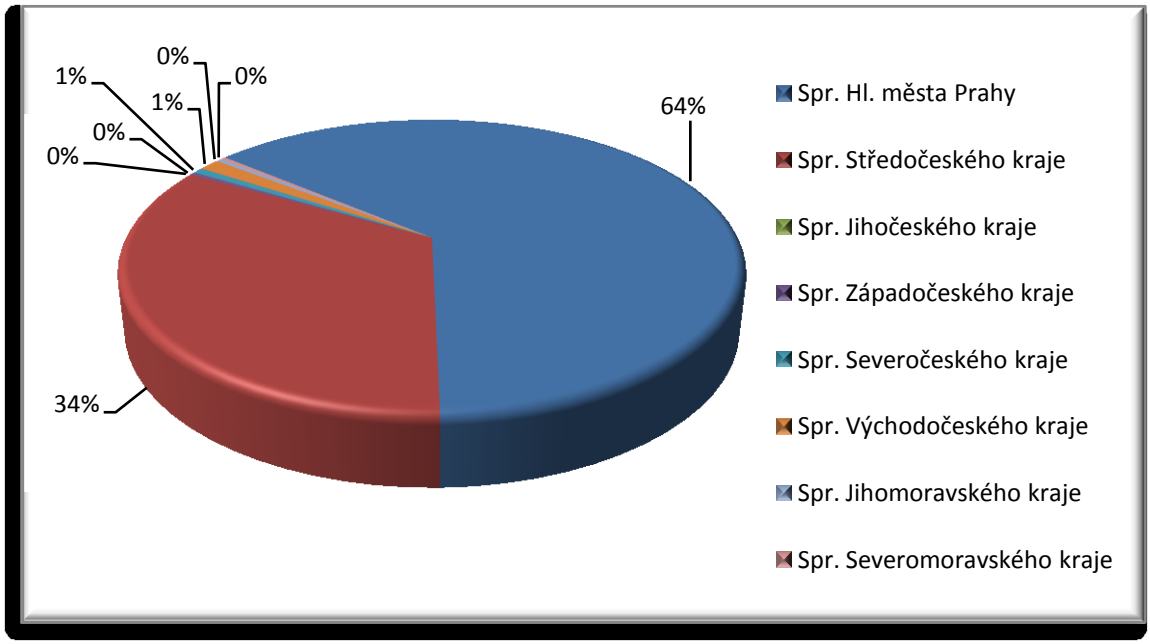
| | ČR | JČ |
|---|---|---|
| 1990 | - | - |
| 1991 | - | - |
| 1992 | - | - |
| 1993 | - | - |
| 1994 | 54 | 1 |
| 1995 | 31 | 1 |
| 1996 | 22 | 0 |
| 1997 | 26 | 0 |
| 1998 | 243 | 0 |
| 1999 | 310 | 0 |
| 2000 | 145 | 1 |
| 2001 | 79 | 0 |
| 2002 | 20 | 0 |
| 2003 | 76 | 1 |
| 2004 | 23 | 0 |
| 2005 | 9 | 0 |
| 2006 | 15 | 0 |
| 2007 | 17 | 0 |




Zdroj: PČR CIAP – ESSK

Podíl jednotlivých policejních oblastí v době největšího nápadu v roce 1999 popisuje graf č. 2. Analýza ukazuje, že největší podíl na páchání trestné činnosti dle § 182 TZ Porušení tajemství dopravovaných zpráv byl zjištěn na území Správy Hl. města Prahy. Následuje území Správy Středočeského kraje. Ostatní krajské správy se podílejí pouze nepatrně.

**Graf č. 2 Podíl jednotlivých policejních oblastí v době největšího nápadu roku 1999.**

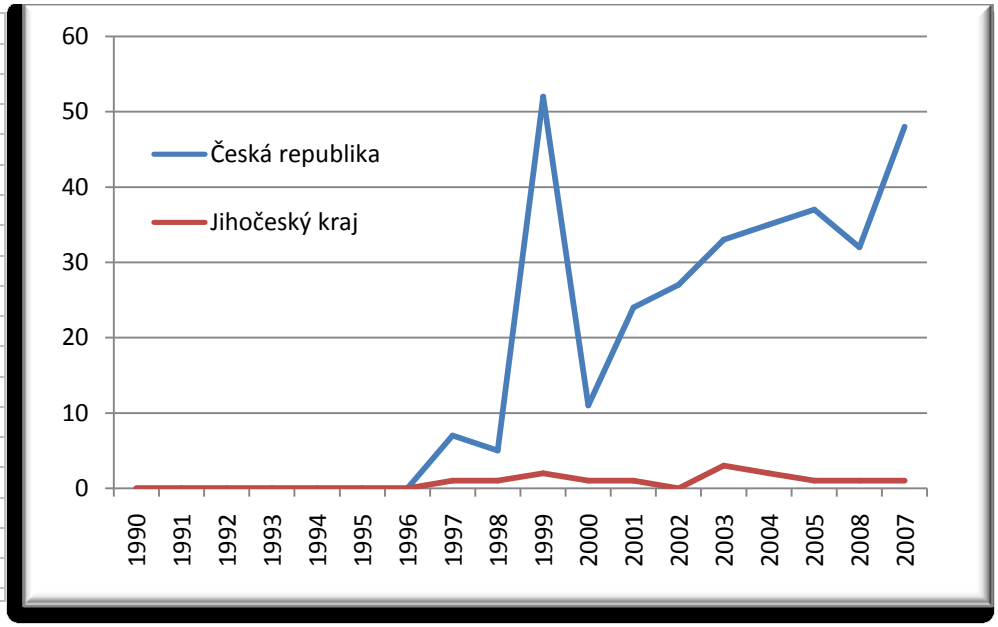



Zdroj: PČR CIAP – ESSK

Analýza vývoje trestné činnosti dle §230 TZ - Trestný čin neoprávněný přístup k počítačovému systému a nosiči informací za sledované období 1995 až 2007 porovnává situaci v České republice a v Jihočeském kraji. Ukazuje, že nejvyšší počet zjištěných skutků v České republice byl dosažen v roce 1999. V Jihočeském kraji byl počet zjištěných skutků roven 2. Ze zpracovaného grafu č. 3 je patrný nejprve prudký vzestup v roce 1999. Následuje prudký pokles zjištěných skutků v České republice v roce 2000 a postupný růst v letech 2001 až 2007. V Jihočeském kraji se počet zjištěných skutků pohybuje průměrně v jednotkách zjištěných skutků, což zobrazuje plochá křivka vývoje.

**Graf 3:** **Počet zjištěných případů trestného činu – Poškození a zneužití záznamu na nosiči informací.**

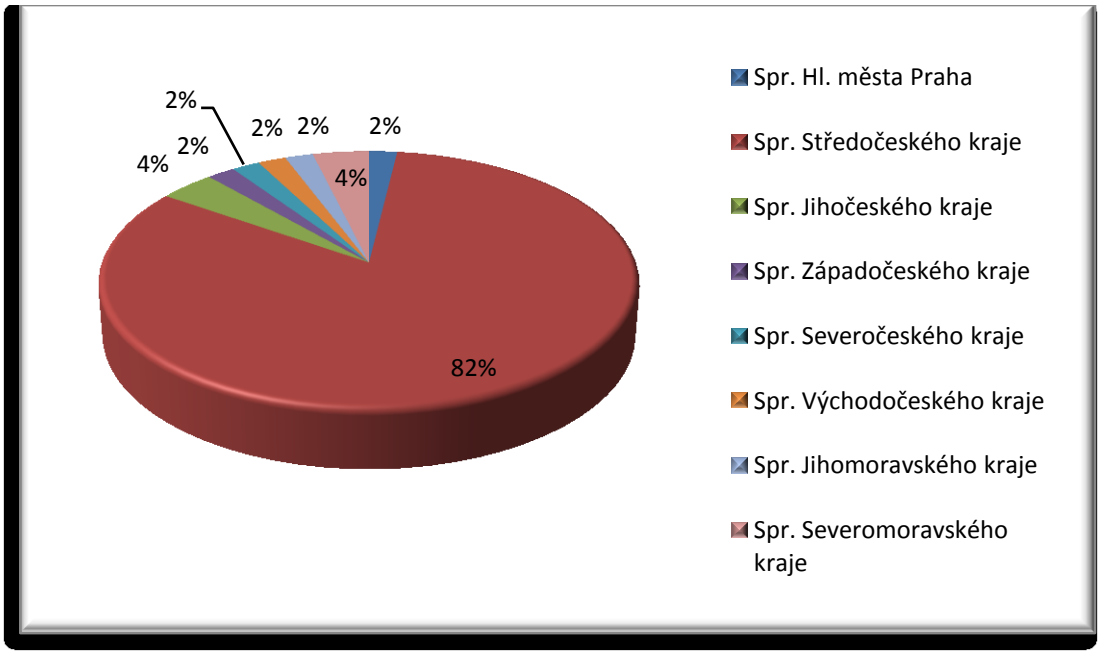
| | ČR | JČ |
|---|---|---|
| 1990 | - | - |
| 1991 | - | - |
| 1992 | - | - |
| 1993 | - | - |
| 1994 | 0 | 0 |
| 1995 | 0 | 0 |
| 1996 | 0 | 0 |
| 1997 | 7 | 1 |
| 1998 | 5 | 1 |
| 1999 | 52 | 2 |
| 2000 | 11 | 1 |
| 2001 | 24 | 1 |
| 2002 | 27 | 0 |
| 2003 | 33 | 3 |
| 2004 | 35 | 2 |
| 2005 | 37 | 1 |
| 2006 | 32 | 1 |
| 2007 | 48 | 1 |




Zdroj: PČR CIAP – ESSK

Podíl jednotlivých policejních oblastí v době největšího nápadu v roce 1999 popisuje graf č. 2. Analýza ukazuje, že největší podíl na páchání trestné činnosti dle §230 TZ - Trestný čin neoprávněný přístup k počítačovému systému a nosiči informací byl zjištěn na území Správy Středočeského kraje. Ostatní krajské správy a Správa Hl. města Prahy se podílejí pouze nepatrně.

**Graf 4: Podíl jednotlivých policejních oblastí v době největšího nápadu roku 1999.**

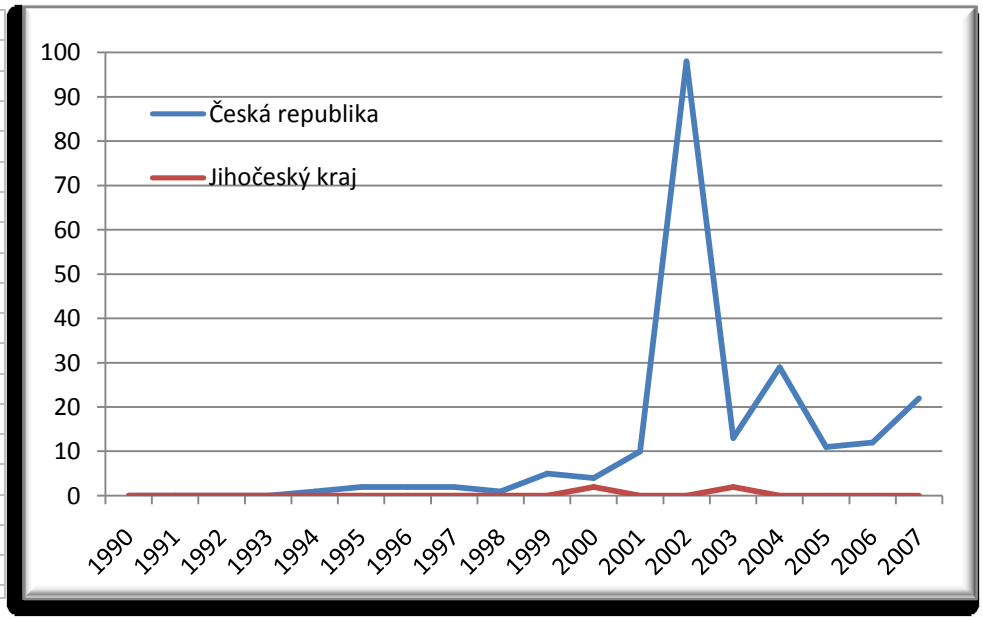



Zdroj: PČR CIAP – ESSK

Analýza vývoje trestné činnosti dle § 180 TZ Neoprávněné nakládání s osobními údaji za sledované období 1994 až 2007 porovnává situaci v České republice a v Jihočeském kraji. Ukazuje, že nejvyšší počet zjištěných skutků v České republice byl dosažen v roce 2002. V Jihočeském kraji byl počet zjištěných skutků nulový. Ze zpracovaného grafu č. 5 je patrný prudký vzestup v roce 2002. Následuje prudký pokles zjištěných skutků v České republice v roce 2003 a postupné kolísání růstu v letech 2004 až 2007. V Jihočeském kraji se počet zjištěných skutků pohybuje průměrně v jednotkách zjištěných skutků, což zobrazuje plochá křivka vývoje.

**Graf č. 5** **Počet zjištěných případů trestného činu - Neoprávněné nakládání s osobními údaji.**

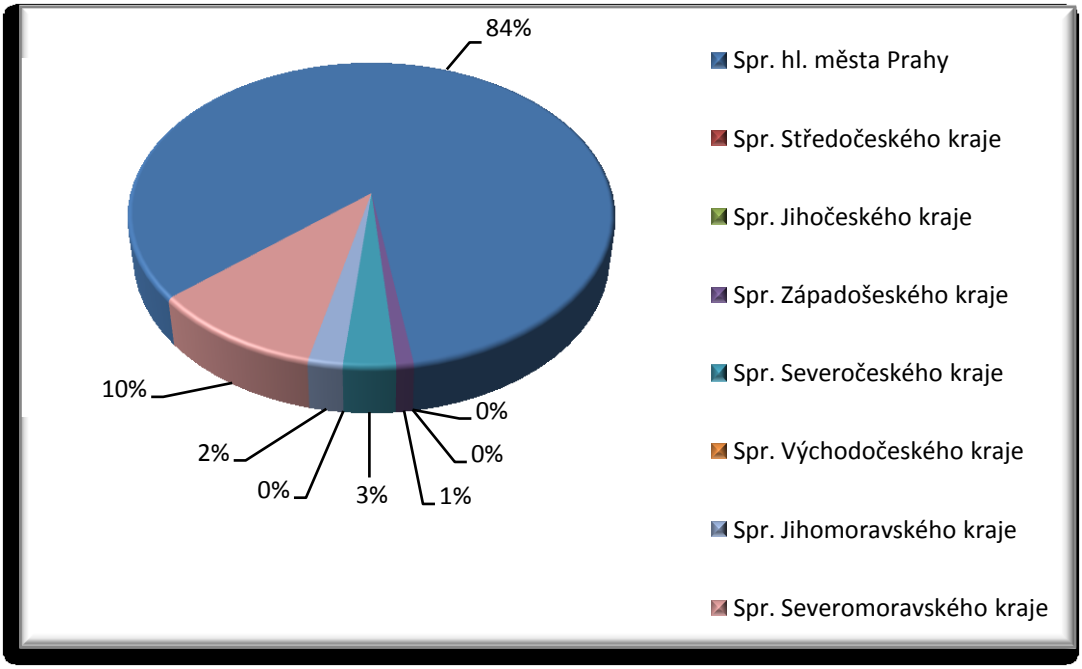
| | ČR | JČ |
|---|---|---|
| 1990 | - | - |
| 1991 | - | - |
| 1992 | - | - |
| 1993 | - | - |
| 1994 | 1 | 0 |
| 1995 | 2 | 0 |
| 1996 | 2 | 0 |
| 1997 | 2 | 0 |
| 1998 | 1 | 0 |
| 1999 | 5 | 0 |
| 2000 | 4 | 1 |
| 2001 | 10 | 0 |
| 2002 | 98 | 0 |
| 2003 | 13 | 1 |
| 2004 | 29 | 0 |
| 2005 | 11 | 0 |
| 2006 | 22 | 0 |
| 2007 | 22 | 0 |




Zdroj: PČR CIAP – ESSK

Podíl jednotlivých policejních oblastí v době největšího nápadu v roce 2002 popisuje graf č. 62. Analýza ukazuje, že největší podíl na páchání trestné činnosti dle § 180 TZ Neoprávněné nakládání s osobními údaji byl zjištěn na území Správy Hl. města Prahy. Následuje území Správy Středočeského kraje. Ostatní krajské správy a Správa Hl. města Prahy se podílejí pouze nepatrně.

**Graf č. 6 Podíl jednotlivých policejních oblastí v době největšího nápadu roku 2002.**




Zdroj: PČR CIAP – ESSK

Analýza vývoje počtu provedených kontrol cílených ze strany pověřených pracovníků OAI na dodržování pravidel pro zpracování osobních údajů dle závazných pokynů policejního prezidia je znázorněna v tabulce č. 1. Dostupné údaje vypovídají pouze o počtu provedených kontrol. Vzhledem k tomu, že jednotlivé kontroly byly cíleny na různé činnosti kontrolovaných pracovníků, nelze tato data využít k porovnání kvality jednotlivých pracovišť OAI.

**Tabulka č.:1 Počet provedených cílených kontrol ze strany pověřených pracovníků OAI**

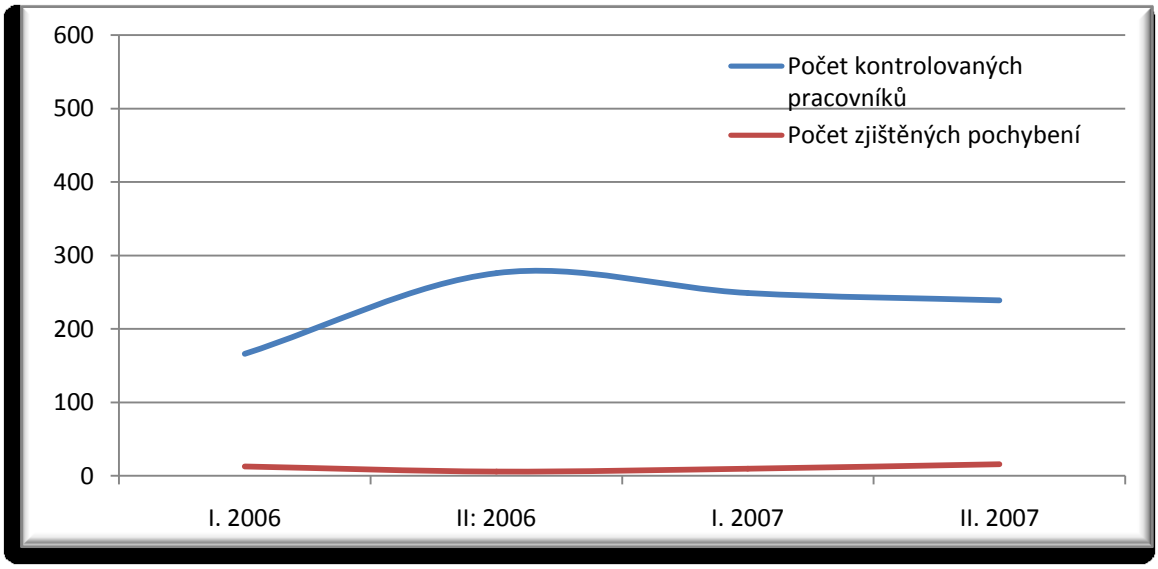
| | I. 2006 | II. 2006 | I. 2007 | II. 2007 |
|---|---|---|---|---|
| Správa Jihočeského kraje | 10 | 15 | 1 | 11 |
| Okr. ředitelství České Budějovice | 11 | 11 | 11 | 16 |
| Okr. ředitelství Český Krumlov | 6 | 5 | 8 | 7 |
| Okr. ředitelství Jindřichův Hradec | 7 | 9 | 9 | 11 |
| Okr. ředitelství Pelhřimov | 10 | 6 | 9 | 5 |
| Okr. ředitelství Písek | 7 | 12 | 11 | 11 |
| Okr. ředitelství Prachatice | 7 | 4 | 10 | 10 |
| Okr. ředitelství Strakonice | 13 | 8 | 4 | 4 |
| Okr. ředitelství Tábor | 3 | 2 | 1 | 1 |

Zdroj: PČR SJčK

Analýza vývoje počtu kontrolovaných pracovníků Správy Jihočeského kraje v letech 2006 – 2007 je znázorněno v grafu č. 8. Ukazuje postupný nárůst kontrolovaných pracovníků v roce 2006, který se v roce 2007 ustálil. V Jihočeském kraji byl ve sledovaném období počet zjištěných pochybení zanedbatelný. Zjištěná pochybení lze hodnotit jako ne příliš závažná. Ve většině případů se jednalo o nedodržování řádného zdůvodnění dotazů do datového fondu. Následným doložením oprávněnosti takového dotazu souvisejícího se služební činností a po odstranění zjištěných závad s návrhem na

přijetí preventivních opatření lze konstatovat, že dodržování zásad ochrany osobních údajů ve sledovaném období u policejních složek Správy Jihočeského kraje bylo na velmi dobré úrovni. Tuto skutečnost dokládá i fakt, že ani jeden případ porušení dle závazných pokynů policejního prezidia nemusel být posuzován z hlediska trestně-právního. Ve většině případů bylo přistoupeno k potrestání viníka v kázeňské pravomoci příslušného vedoucího pracovníka.

**Graf č. 8** **Počet kontrovaných pracovníků Správy Jč. kraje v letech 2006 – 2007 včetně neplánovaných.**




| | I. 2006 | | II. 2006 | | I. 2007 | | II. 2007 | |
|---|---|---|---|---|---|---|---|---|
| | Celkový počet kontrolovaných pracovníků | Počet pochybení | Celkový počet kontrolovaných pracovníků | Počet pochybení | Celkový počet kontrolovaných pracovníků | Počet pochybení | Celkový počet kontrolovaných pracovníků | Počet pochybení |
| Celkem | 166 | 13 | 276 | 6 | 249 | 10 | 239 | 16 |

Zdroj: PČR SJčK

## 10. Diskuse

Zpracovávané problematice – administraci datového centra se ve své praxi věnuji od počátku budování informačních technologií v rezortu ministerstva vnitra. Postupné budování elektronické evidence obyvatel, evidence občanských a cestovních průkazů, evidence motorových vozidel, evidence řidičských průkazů je považováno za velice zodpovědný úkol. V roce 1990 je datovým centrům ze strany společnosti věnována náležitá pozornost nejen po stránce ekonomické, ale i po stránce organizační. Datové centrum je budováno dle obecných standardů pro budování velkých center. Místnosti pro technologickou část jsou vybaveny dvojitou antistatickou podlahou, klimatizací dostatečné kapacity, obložením stěn absorbujícího hluk.

Rozvody elektrické energie ukončené v samostatném podružném rozvaděči zaručují spolehlivost její dodávky. Celé datové centrum je podporováno centrálním diesel agregátem a zdroji nepřerušitelného proudu UPS.

Vybudováním těchto prostor se může ministerstvo vnitra plně srovnávat s datovými centry komerčních společností.

S příchodem nových technologií dochází k postupnému zkvalitňování a využívání uložených dat. Pravidelné zálohování dat a jejich bezpečné ukládání je zorganizováno tak, aby možnost jejich zneužití nebo poškození nebyla možná. Neustále se hledají nová řešení jak zlepšit spolehlivost systému a organizaci práce.

Na pracovišti je od počátku uplatňována personální a objektová bezpečnost a povinnost dodržování zpracovaných režimových směrnic. Tyto směrnice upravují jednotlivé činnosti pracovníků pracujících přímo u řídících počítačů, tak uživatelů napojených pomocí pracovních stanic. I pro pracovníky ostrahy budovy je pro případ nestandardních situace v době nepřítomnosti administrátorů centra zpracována příslušná směrnice. Ta mimo jiné obsahuje plán zásahu hasičského záchranného sboru pro případ živelné události. Vzhledem k tomu, že při výstavbě technologických místností, došlo k odklonění všech nepotřebných elektrorozvodů, rozvodů centrálního vytápění i ostatních přípojek pitné i odpadní vody, připadá jako možný ničivý živel pouze požár.

Pro podporu protipožární ochrany je centrum opatřeno požárními hlásiči. Rovněž tak jsou technologické místnosti vybaveny pohybovými čidly.

V roce 1993 dochází ke snahám jednotlivých služeb nasazovat nové a nové informační systémy pro evidování všech možných informací. V jednotlivých informačních systémech se informace vedou duplicitně. Regulaci jednotlivých informačních systémů zavádí přijetí NMV č. 65/1994, *kterým se stanoví postup při sestavování projektových záměrů informačních systémů a počítačových sítí, při realizaci a evidenci projektů informačních systémů a počítačových sítí a při evidenci počítačových sítí a jednotek výpočetní techniky*.

S rozvojem potřeb policejních orgánů, dochází k nasazování nových služeb jako elektronické pošty, intranetovému propojení jednotlivých pracovišť – využití zejména pro jednotné informační prostředí pro vytěžování a doplňování webových aplikací klient-server.

Pracoviště OAI je několikráte nápomocno při získávání podkladů pro přípravu znění rezortních závazných předpisů upravujících postupy a doporučení pro jednotlivé informační systémy. Do uživatelských příruček, jejichž dodržování se v podmínkách POLICIE ČR uplatňuje vydáváním interních aktů řízení (rozkazy a metodické pokyny), se tak dostávají mnohdy nepopulární, ovšem vysoce bezpečnostně-organizační prvky týkající se např. podmínek pro tvorbu uživatelských přístupových hesel a jejich pravidelnou změnu. Informační systémy jsou navrhovány tak, aby bylo umožněno zpětné dohledání toho, kdo, kdy a proč konkrétní údaj vložil, měnil ho nebo se na něho dotazoval.

V části kazuistika uvádím příklad organizace, která na jedné straně ochraňuje vysoké hodnoty pojištěnců a na straně druhé hrubou nezodpovědností ohrozila soukromí svých klientů. Uvádím i příklad policisty, který datový fond využíval pro soukromé potřeby.

Práce policie je založena v převážné části na zpracování osobních údajů. Personální, objektové i organizační ochraně datových technologických center je věnována vysoká pozornost. To se ovšem nedá říci o drobných, dílčích technických prostředcích, které dnešní doba přináší. Je na každém pracovníkovi, aby zvážil, jaká bude jeho odpovědnost při případné ztrátě nebo odcizení tak nenahraditelného pomocníka dnešní doby, USB Flash disku nebo externího harddisku, byť je služební a evidovaný.

Ano, něco jiného je 500 tisíc záznamů o klientech pojišťovny, něco jiného elektronická kopie trestního spisu a něco jiného anonymizované formuláře přestupkového řízení (i vymazaný soubor lze obnovit). Ve vztahu k §13 zákona č. 101/200 Sb., o ochraně osobních údajů to však vůbec není podstatné. Podstatná bude zřejmě pouze výše uložené pokuty.

Policejní sbor vytváří veškerou možnou snahu o vybudování funkčního souboru aplikací, který i přes přísná pravidla pro nakládání s osobními údaji poskytne silnou podporu v boji proti trestné činnosti v našem demokratickém státě. Rovněž tak předávání těchto mnohdy citlivých informací v rámci mezinárodní spolupráce probíhá na základě pevně stanovených pravidel.

Je však až s podivem, jak se chováme v civilním životě v celosvětové počítačové síti – Internetu. Při pozorování dnešní nastupující mladé generace se lze oprávněně ptát, zda má vůbec nějaký smysl soukromí jednotlivce ochraňovat. Všechna ta sdělení ve "spřátelené komunitě" na společné sociální síti prozrazují mnohdy natolik choulostivé informace nejen v tištěné, ale mnohdy i fotografické či dokonce filmové, že uveřejnění osobních informací už nemůže napáchat vůči dotčené osobě žádných škod.

Bohužel takto dobrovolně jednajícího jedince není schopna ochránit žádná deklarace, evropská směrnice nebo zákon. Činí-li takto lidská bytost dobrovolně a vědoma si následků je veškerá ochrana společností marná. Zde je na řadě pouze výchovná a preventivní činnost objasňující možná rizika.

## 11. Závěr

Cílem mé práce bylo provedení analýzy vývoje ochrany osobních údajů od roku 1990 do roku 2007 a to ve vztahu k denní praxi policejních orgánů POLICIE ČR, Správy Jihočeského kraje.

Pro objasnění zpracovávané problematiky je v práci vysvětleno evropské, celosvětové, české, veřejně-správní, trestně-právní a rezortní legislativní prostředí, které upravuje a doporučuje nakládání s osobními údaji.

Je zde rozebrána i koncepce budování informačních systémů veřejné správy. Popsán je její předmět, cíle, jednotlivé role podílejících se subjektů na její tvorbě a proces schvalování informačního systému veřejné správy.

Problematika ochrany soukromí a ochrany osobní údajů popisuje možné hrozby ohrožení ochrany osobních údajů a doporučované zásady jak těmto hrozbám předcházet.

Historický exkurs do počátků budování policejní informatiky naznačuje, že již na počátku tohoto dění nebylo nic ponecháváno náhodě a vše se bralo velmi vážně. Je však také pravdou, že s rychlým nástupem dostupnosti personálních počítačů docházelo ze strany některých služeb k nesystémovému budování okrajových a z policejního hlediska úzce specializovaného pomocných databází. Zavedením vnitřně rezortních závazných předpisů se však situace dostává do již zmíněných standardních řešení.

Pro zpracování rozboru vyjadřujícího četnost případů protiprávního jednání byla použita data čerpaná ze systému ESSK provozovaného Centrálou informatiky a analytických procesů Policejního prezidia ČR. Rozbor kontrolní činnosti pověřených pracovníků vychází z údajů čerpaných z jednotlivých pracovišť okresních OddIKT a z POLICIE ČR, správy Jihočeského kraje.

Ověřovaná hypotéza – Ochrana osobních údajů jako důležitý faktor fungování demokratické společnosti je naplněna v **Listině základních práv a svobod** (1993) v článku 10. Ochraňuje právo na lidskou důstojnost, osobní čest, právo před neoprávněným zásahem do soukromého a rodinného života a v odstavci 3 pak ochranu osobních údajů. Společnost, která tato základní lidská práva nectí a nevytváří podmínky pro jejich dodržování, se nemůže nazývat demokratickou.

Ochranu osobních údajů v policejní praxi dokládá vývoj a realizace jednotlivých metod posilování bezpečnosti provozovaných informačních systémů, zákonem upravená povinnost mlčenlivosti a v neposlední řadě etický kodex příslušníka policejního sboru. Ověřovaná hypotéza je tedy naplněna.

Aplikace zákona č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů v praxi policejních útvarů posílilo ochranu osobních údajů zejména v tom, že tuto ochranu garantuje nejen osobám – pachatelům nezletilým a mladistvým, ale i jejich obětem z řad této věkové kategorie. Vynucuje si po celou dobu, jak přípravného trestního řízení, tak řízení soudního, naprostou mlčenlivost nejen ze strany policejních pracovníků, ale i ostatních subjektů.

Předpokládané využití práce vidím zejména při preventivní a metodické práci nejen ICT pracovníků, ale i jako ucelený přehled pro získání povědomí o zpracovaném tématu.

## 12. Klíčová slova

Citlivé údaje

Evidence obyvatel

Hacking

Informační systémy

Malware

Osobní údaje

Sociální inženýrství

Soukromí

Úřad pro ochranu osobních údajů

## 13. Seznam použitých zdrojů

### *Monografie*


1. AULDS, CH. ROUBÍČEK, L. *Linux*: administrace serveru Apache. Praha: Grada Publishing a.s. 2003. 535 s. ISBN 978-8-02470-640-5.

2. BÁRTÍK, V. JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*: vybrané otázky. Praha: Linde Praha a.s., 2009. 277 s. ISBN 978-80-7201-740-9.

3. CRAIG, P. HONICK, R. BURNETT, M. *Softwarové pirátství bez záhad.* Praha: Grada Publishing a.s., 2008. 212 s. ISBN 80-247-1765-4.

4. DOLEŽÍLEK, J. *Přehled judikatury ve věcech ochrany osobnosti.* Praha: ASPI a.s., 2008, 216 s. ISBN 978-80-7357-313-3.

5. DOSTÁLEK, L., KABELOVÁ, A. a kol. *Velký průvodce protokoly TCP/IP a systémem DNS.* 3. aktualizované a rozšířené vydání, Brno: CP Books, a.s., 2005, 542 s. ISBN 80-7226-675-6.

6. ERICKSON, J. *Hacking : umění exploitace.* 1. vyd. Brno : Zoner Press, 2005. 263 s. ISBN 80-86815-21-8.

7. FRYŠTÁK, M. a kol. *Trestní právo hmotné*: zvláštní část, stav k 1. 1. 2010. Ostrava: KEY Publishing s.r.o., 2009. 170 s. ISBN 978-80-7418-040-8.

8. GÁLA, L. POUR, J. TOMAN, P. *Podniková informatika*: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky. Praha: Grada Publishing a.s., 484 s. ISBN 80-247-1278-4.

9. HLAVELKA, J. a kol. *Výkladový slovník výpočetní techniky a komunikací.* Vydání první, Praha: Computer Press, 1997, 452 s. ISBN 80-7226-023-5.

10. JANCZEWSKI, L. COLARIK, A. M. *Cyber warfare and cyber terrorism.* Idea Group Inc. (IGI), 2008. 532 s. ISBN 978-1-59140-991-5.

11. JIROVSKÝ, V. *Kybernetická kriminalita.* První vydání. PRAHA: Grada Publishing, a.s. 2007, 288 s. ISBN 978-80-247-1561-2.

12. KOVÁŘOVÁ, P. *Problematika získávání dat z cizího osobního počítače s OS Windows XP s přihlédnutím k situaci v ČR.* Brno: Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, 2006, 76 s., Vedoucí práce Mgr. Petr Škyřík.

13. KRÁL, M. *Bezpečnost domácího počítače: Prakticky a názorně.* Praha : Grada Publishing a.s. 2006. 334 s. ISBN 80-247-1408-6.

14. KUČEROVÁ, A. BÁRTÍK, V. PECA, J. NEUWIRT, K. NEJEDLÝ, J. *Zákon o ochraně osobních údajů:* Komentář. 1. vydání. Praha: C. H. Beck, 2003. 406 s. ISBN 80-7179-762-6.

15. LONG, J. *Google Hacking*. Miroslav Kučera; RNDr. Jan Pokorný. Brno : Zoner Press, 2005. 472 s. ISBN 80-86815-31-5.

16. MAR-ELIA, D., MELBER, D., STANEK, W. R., *Microsoft Windows Group Policy Guide:* Zásady skupiny Microsoft Windows. Brno: Computer Press, a.s., 2006, 760 s. ISNB 80-251-1262-4.

17. MATES, P. *Ochrana soukromí ve správním právu.* Praha: Linde Praha a.s., 2004, 307 s. ISBN 80-7201-458-7.

18. MATES, P., NEUWIRT, K. *Právní úprava ochrany osobních údajů v ČR*. Praha: Nakladatelství IFEC, Praha, 2000, 128. s. ISBN 80-86412-02-4.

19. MALENOVSKÝ, J. *Mezinárodní právo veřejné:* jeho obecná část a poměr k vnitrostátnímu právu, zvláště právu českému. 4. opravené a doplněné vydání. Brno: Nakladatelství Doplněk, 2004, 468 s. ISBN 80-7239-160-7.

20. MATES, P. *Ochrana soukromí ve správním právu.* Praha: Linde Praha a.s., 2004, 307 s. ISBN 80-7201-458-7.

21. MATĚJKA, M. *Počítačová kriminalita.* 1. vyd. Praha : Computer Press, 2002. 108 s. ISBN 80-7226-419-2.

22. MATOUŠOVÁ, M. HEJLÍK, L. *Osobní údaje a jejich ochrana*: 2. Doplněné a aktualizované vydání. Praha: ASPI, Wolters Kluwer, 2008, 468 s. ISBN 978-80-7357-322-5.

23. MITNICK, K. SIMON, W. Umění klamu. Lazarczyk, R.; Vašta, L. 1. Vydání. Gliwice: HELION S. A., 2003. 348 s. ISBN 83-7361-210-6.

24. RUSSEL, CH., CRAWFORD. S., GEREND, J. *Microsoft Windows Server 2003:* Velký průvodce administrátora. Brno: CP Books, a.s., 2005, 1374 s. ISNB 80-251-0579-2.

25. ŠTĚDROŇ, B. *Open Source software*: ve veřejné správě a soukromém sektoru. Praha: Grada Publishing a.s., 2009. 128 s. ISBN 978-80-247-3047-9.

26. ZEHLOVÁ, V. *Správněprávní aspekty ochrany osobních údajů.* Brno: Masarykova univerzita, Právnická fakulta, Katedra správní vědy, správního práva a finančního práva, 2008. 63 s. Vedoucí práce: doc. JUDr. Soňa Skulová, Ph.D.

27. ZEMÁNEK, J. *Slabá místa Windows aneb jak se bránit hackerům*. 1. vyd. Kralice na Hané: Computer Media s. r. o., 2004. 156 s. ISBN 80-86686-11-6.

***Články***

28. ŠALOMOUN, M. *Právní regulace nakládání s citlivými údaji.* Právní rozhledy: časopis pro všechna právní odvětví. Praha: C. H. Beck. 2006. č. 19. ISSN 1210-6410.

***Internetové zdroje***

29. PORTÁL BRANDEIS UNIVERSITY OF LOUISVILLE. *The Right to Privacy.*[webová stránka], [online], [cit. 2010-03-02]. Dostupný z <http://www.law.louisville.edu/library/collections/brandeis/node/225>.

30. PORTÁL COUNCIL OF EUROPE. *Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat, o orgánech dozoru a toku dat přes hranice.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>.

31. PORTÁL COUNCIL OF EUROPE. *Usnesení (1973) 22*. [datový soubor], [online], [citováno 2010-03-02]. Dostupný z <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%2520legal%2520instruments/1Resolution%2873%2922_EN.pdf>.

32. PORTÁL COUNCIL OF EUROPE. *Usnesení (1974) 29.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%2520legal%2520instruments/1Resolution%2874%2929_EN.pdf>.

33. PORTÁL COUNCIL OF EUROPE. *Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm>.

34. PORTÁL DAILYTECH. *Vláda USA zakázala používání USB Flash disků*. [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://www.dailytech.com/Pentagon+Bans+USB+Drives+After+Virus+Hits+Computers/article13427.htm>.

35. PORTÁL EMAG. *Keyloggers I. díl.* [webová stránka], [on-line], [cit. 2010-04-12]. Dostupný z <http://www.emag.cz/keyloggers-i-dil/>.

36. PORTÁL EUROPA. *Charta základních práv občanů EU.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://ec.europa.eu/ceskarepublika/information/glossary/term_46_cs.htm>.

37. PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 1995/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.*[datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:CS:PDF>.

38. PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“)* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:25:32000L0031:CS:PDF>.

39. PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:29:32002L0058:CS:PDF>.

40. PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:CS:PDF>.

41. PORTÁL EUROPA. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:CS:PDF>.

42. PORTÁL FEDERAL FINANCIAL INSTITUCIONS EXAMINATION COUNCIL. *National Information Center*. [webová stránka], [online], [citováno 2010-03-02]. Dostupný z <http://www.ffiec.gov/nicpubweb/nicweb/NicHome.aspx>.

43. PORTÁL INTERNET STÁTNÍ SPRÁVY A SAMOSPRÁVY. MALÁTEK J. *Celostátní správní a dopravně správní evidence.* [datový soubor], [on-line], 2010 [cit 2010-04-11]. Dostupný z <http://www.isss.cz/archiv/2001/sbornik/prednasky/malatek.doc>.

44. PORTAL IMA. NEUWIRT, K. *Ochrana soukromí – nutnost nebo překážka?* [datový soubor] 2008, [online], [cit. 2010-03-29] Dostupný z <http://www.ima.cz/download/cz/3infoday/sablonaPSPEV_prezentace_KN.pdf>.

45. PORTÁL KOSTROŇ. KOSTROŇ, L. *Soukromí,* [datový soubor] 2003, [online], [cit. 2010-03-02]. Dostupný z <http://www.kostron.cz/soukromi.doc>.

46. PORTÁL OSN. *Deklarace práv dítěte.* [datový soubor], [online], [cit. 2010-03-02]. Dostupný z <http://www.osn.cz/dokumenty-osn/soubory/deklarace-prav-ditete.pdf>.

47. PORTÁL OSN. *Mezinárodní pakt o občanských a politických právech.* [datový soubor], [online] [cit. 2010-03-02]. Dostupný z <http://www.osn.cz/dokumenty-osn/soubory/mezinar.pakt-obc.a.polit.prava.pdf>.

48. PORTÁL OSN. *Mezinárodní pakt o hospodářských, sociální a kulturních právech.* [počítačový soubor], [online], [cit. 2010-03-02]. Dostupný z <http://www.osn.cz/dokumenty-osn/soubory/mezinarodni-pakt-o-hospodarskych-socialnich-a-kulturnich-pravech.pdf>.

49. PORTÁL ROOT. TIŠNOVSKÝ, P. *Unixové vykopávky*. [webová stránka], [on-line], 1998 – 2010 [cit. 2010-04-12]. Dostupný z <http://www.root.cz/clanky/pdp-11-a-smep-system-malych-elektronickych-pocitacu/>.

50. PORTÁL MVČR. *Sbírka mezinárodních smluv.* [datový soubor], [online], [cit. 2010-03-29]. Dostupné z <http://aplikace.mvcr.cz/archiv2008/sbirka/2001/sb052-01m.pdf>.

51. PORTÁL MVČR. *Sbírka mezinárodních smluv.* [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://aplikace.mvcr.cz/archiv2008/sbirka/2005/sb015-05m.pdf>.

52. PORTÁL MVČR. *Vyhláška č. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy*. [datový soubor], [on-line], [cit 2010-04-11] Dostupný z <http://www.mvcr.cz/soubor/vyhlaska-c-528-2006-sb-o-informacnim-systemu-o-informacnich-systemech-verejne-spravy.aspx>.

53. PORTÁL MVČR. *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.* [datový soubor], [on-line], [ cit. 2010-04-11] Dostupný z <http://www.mvcr.cz/soubor/zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy-s-barevnym-vyznacenim-zmen-provedenych-zakonem-c-190-2009-sb.aspx>.

54. PORTÁL MVČR. *Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích*. [datový soubor], [on-line], [cit 2010-04-11] Dostupný z <http://www.mvcr.cz/soubor/vyhlaska-c-469-2006-sb-o-informacnim-systemu-o-datovych-prvcich.aspx>.

55. PORTÁL MVČR. *Komentář k vyhlášce č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy.* [datový soubor], [on-line], [cit 2010-04-11] Dostupný z <http://www.mvcr.cz/soubor/komentar-k-vyhlasce-c-529-2006-sb-o-pozadavcich-na-strukturu-a-obsah-informacni-koncepce-a-provozni-dokumentace-a-o-pozadavcich-na-rizeni-bezpecnosti-a-kvality-informacnich-systemu-verejne-spravy.aspx>.

56. PORTÁL MVČR. *Zákon č. 110/2007 Sb., o některých opatřeních v soustavě orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů*. [datový soubor], [on-line], [cit 2010-04-11] Dostupný z <http://aplikace.mvcr.cz/archiv2008/micr/files/3882/zak110_sb041_07.pdf>.

57. PORTÁL VEŘEJNÉ SPRÁVY. *Dohoda o zpětném přebírání osob na společných hranicích se SRN.* [webová stránka], [on-line], [cit 2010-04-11] Dostupný z <http://www.portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_l=5/1995&PC_8411_ps=10#10821>.

58. PORTÁL PARLAMENT ČESKÉ REPUBLIKY. *Sněmovní tisk 374 - Zákon o ochraně osobních údajů.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://www.psp.cz/sqw/historie.sqw?t=374&o=3>.

59. PORTÁL POLICIE ČR. *Zákon č. 273/2008 Sb., o Policii České Republiky.* [datový soubor], [online], [cit. 2010-03-29] Dostupný z <http://www.policie.cz/soubor/zakon-o-policii-cr-273-2008-sb.aspx>.

60. PORTÁL POLICIE ČR. *CIAP SKPV*. [webová stránka],[on-line], [cit 2010-04-11] Dostupný z <http://www.policie.cz/clanek/centrala-informatiky-a-analytickych-procesu-sluzby-kriminalni-policie-a-vysetrovani.aspx>.

61. PORTÁL PUBLIC-DOMAIN-PHOTOS, *Hacker Emblem.* [počítačový soubor], [on-line], [cit. 2010-04-19]. Dostupný z <http://www.public-domain-photos.com/free-cliparts/other/games/hacker_emblem-3706.htm>.

62. PORTÁL SAGIT. *Zákon č. 52/2009 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z <http://www.sagit.cz/pages/zpravodajtxtanot.asp?cd=166&typ=r&zdroj=../_anotace/sb09052b>.

63. PORTÁL SPAMFINGER. *Spam a Scam glosář*. [webová stránka] 2003-2011, [online], [cit. 2010-03-29]. Dostupný z <http://www.spamfighter.com/lang_cs/faq_glossary.asp>.

64. PORTÁL PINA. *Nigerijské dopisy v novém.* [webová stránka], [online], [cit. 2010-04-12]. Dostupný z <http://www.pina.cz/2008/03/08/nigerijske-dopisy-v-novem/>.

65. PORTÁL SPOLEČNÁ ČESKO-SLOVENSKÁ DIGITÁLNÍ PARLAMENTNÍ KNIHOVNA. *Stenoprotokol 8. Společné schůze Sněmovny lidu a Sněmovny národů Federálního shromáždění ČSFR.* [webová stránka], [on-line], [cit 2010-04-11]. Dostupný z <http://www.psp.cz/eknih/1990fs/slsn/stenprot/008schuz/s008002.htm>.

66. PORTÁL STADFORD ENCIKLOPEDIA OF PHILOSOPHY. *Ochrana osobních údajů*. [webová stránka], [online], [cit. 2010-03-02]. Dostupný z <http://plato.stanford.edu/entries/privacy>.

67. PORTAL TECHNISCHE UNIVERSITÄT DORTMUND. Rizika plynoucí z vojenského využití nanotechnologie. [datový soubor], [online], [cit. 2010-03-29]. Dostupný z <http://e3.physik.tu-dortmund.de/P&D/Pubs/RiskMilNT_Lecce.pdf>.

68. PORTÁL UN - Organizace spojených národů. *The Universal Declaration of Human Rights.*[webová stránka], [online], [cit. 2010-03-02]. Dostupné z <http://www.un.org/en/documents/udhr>.

69. POTRÁL VIRTUÁLNÍ AKADEMIE, *Antivirová ochrana.* [webová stránka], [online], [cit. 2010-03-29]. Dostupný z http://www.e-skripta.eu/ssos/index.php?id=skripta/rocnik1/informatika/informatika-kap2>.

70. PORTÁL VLÁDA ČR. *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 7. června 1995 č.338.* [webová stránka], [on-line], [cit 2010-04-11]. Dostupný z <http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/8EDD579E0F7EB5BBC12571B6007103E4>.

71. PORTÁL VLÁDA ČR. *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 8. října 1997 č.622.* [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/E08A091A2B26D648C12571B6006EF667>.

72. PORTÁL VLÁDA ČR. *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 8. října 1997 č.623.* [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/02CE5D7A1B946D86C12571B6006F2E52>.

73. PORTÁL VYŠŠÍ POLICEJNÍ ŠKOLA MV BRNO. JEDLIČKA, M. *Počítačová kriminalita* [webová stránka], [on-line], [cit. 2010-04-12]. Dostupný z <http://www.vpsmvbrno.cz/jedlicka/poc_krim/pocitace.html>.

74. PORTÁL WIKIPEDIA. *BIOS.* [webová stránka],[on-line], [cit 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/BIOS>.

75. PORTÁL WIKIPEDIA. *FoxPro.* [webová stránka],[on-line], [cit 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/FoxPro>.

76. PORTÁL WIKIPEDIA. *Identifikace na radiové frekvenci RFID*. [webová stránka], [online], [cit. 2010-03-02]. Dostupný z [webová stránka] [online] <http://cs.wikipedia.org/wiki/RFID>.

77. PORTÁL WIKIPEDIA. *Internetová encyklopedie.* [webová stránka], [online], [cit. 2010-03-02]. Dostupný z <http://cs.wikipedia.org/wiki/Sui_generis>.

78. PORTÁL WIKIPEDIA. *MS-DOS.* [webová stránka],[on-line], [cit 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/MS-DOS>.

79. PORTÁL WIKIPEDIA. *Problém roku 2038.* [webová stránka], [on-line], [cit. 2010-04-12]. Dostupný z <http://cs.wikipedia.org/wiki/Y2k38>.

80. PORTÁL WIKIPEDIA. *RSX-11.* [webová stránka], [on-line], [cit 2010-04-11]. Dostupný z <http://en.wikipedia.org/wiki/RSX-11>.

81. PORTÁL WIKIPEDIA. *Síťový port.* [webová stránka], [online], [cit. 2010-03-29] Dostupný z <http://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_port>.

82. PORTÁL WIKIPEDIA. *UNIX*. [webová stránka], [on-line], [cit. 2010-04-11]. Dostupný z <http://cs.wikipedia.org/wiki/UNIX>.

83. PORTÁL WIKIPEDIA. *UPS*. [webová stránka], [online], [cit. 2010-03-29] dostupný z <http://cs.wikipedia.org/wiki/UPS>.

84. PORTÁL WIKIPEDIA. *Wyse Technology*. [webová stránka], [on-line], [cit 2010-04-11]. Dostupný z <http://en.wikipedia.org/wiki/wyse>.

## 14. Přílohy

Příloha č.: 1 - Zásady zpracování osobních údajů vyplývající z Úmluvy č. 108

Příloha č.: 2 - Legislativní proces přijetí zákona ÚoOOÚ

Příloha č.: 3 - Antivirové desatero

Příloha č.: 4 - Morální hodnoty hackerské komunity

Příloha č.: 5 - Pokročilé operátory používané ve vyhledávači Google

Příloha č.: 6 - Ukázka výpisu typu WHOIS - registrace domény

Příloha č.: 7 - Vzorová informační koncepce obce s výkonem přenesené působnosti

Tabulka- Dílčí odpovědnosti za splnění zákonných povinností

*Příloha č.: 1 - Zásady zpracování osobních údajů vyplývající z Úmluvy č. 108*

## Zásady zpracování osobních údajů vyplývající z Úmluvy č. 108[133]

### Zásada legitimity zpracování

Vychází ze skutečnosti, že osobní údaje, které jsou předmětem zpracování, musí být získány a dále zpracovávány poctivě a v souladu se zákonem. Je nezbytně nutné, aby při nakládání s osobními údaji byly respektovány základní práva a svobody jednotlivců, kterých by se případné zpracování mělo týkat.

### Zásada účelovosti[134]

Při respektování této zásady se údaje shromažďují pouze pro specifické, stanovené a legitimní účely. Je tedy zřejmé, že samotnému nakládání s údaji musí předcházet určení účelu, ke kterému mají být tyto použity. Pokud tato podmínka nebude splněna a účel shromažďování nebude předem stanoven, nelze s předmětnými údaji nakládat. Údaje dále nesmějí být zpracovávány k účelům, které by odporovaly původnímu, zamýšlenému účelu. Je však možné použít osobní údaje v souvislosti s opětovným právním posouzením například soudních spisů či účetních dokladů. V tomto případě pak musí být dostatečně zajištěn, aby nedošlo k použití údajů pro jiné účely. Zpracovávat údaje k jinému účelu, než k jakému byly určeny lze za podmínek, že se bude jednat o výjimky plynoucí z ustanovení § 3 odst. 6 ZoOOÚ[135] nebo pokud je k tomu získán předem souhlas subjektu údajů.

### Zásada časového omezení[136]

Osobní údaje, které jsou předmětem zpracování, se uchovávají jen po takovou dobu, která je nutná k naplnění předem stanoveného účelu. Tato zásada napomáhá zabránit nekontrolovanému archivování údajů, které by tak mohly být případně zneužity k jiným, i nezákonným účelům. Výjimky jsou připuštěny v případech dlouhodobého uchovávání údajů například pro vědecké, statistické či archivní účely, kdy můžou sloužit při výzkumu, ale je nutné tyto údaje náležitě zabezpečit proti jejich zneužití.

---

[133] ZEHLOVÁ, V. *Správněprávní aspekty ochrany osobních údajů.* Brno: Masarykova univerzita, Právnická fakulta, Katedra správní vědy, správního práva a finančního práva, 2008. 63 s. Vedoucí práce: doc. JUDr. Soňa Skulová, Ph.D.

[134] § 5, odst. 1, písm. f), ZoOOÚ.

[135] Stanovení účelu není potřeba pro zpracování osobních údajů nezbytných pro plnění povinností správce, které stanoví zvláštní zákony. Např. ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.

### Zásada potřebnosti a přiměřenosti[137]

Tato zásada souvisí se zásadou účelovosti, jelikož veškeré shromažďované údaje musí být po celou dobu, kdy jsou zpracovávány opravdu nezbytné k dosažení stanoveného účelu. Pokud by se stalo, že se během určité doby některé ze shromážděných údajů stanou již nepotřebnými vzhledem k dosažení účelu, je třeba tyto údaje vyřadit ze systému. Někdy je tato zásada nazývána zásadou minimalizace.

### Zásada průhlednosti[138]

Díky zakotvení této zásady má osoba, které se předmětné osobní údaje týkají, možnost získávat úplné a srozumitelné informace o zpracovávaných údajích. Tato informace obsahuje přehled kategorií osobních údajů, vymezený účel, ke kterému jsou shromažďovány, identifikaci správce, případně další vhodné informace. Pokud by bylo zřejmé, že osoba již nějakým jiným způsobem informovaná je či by poskytnutí informací vyžadovalo nadměrné úsilí, je možné poskytnutí informace odmítnout. V této souvislosti je vhodné zmínit článek 9 Úmluvy č. 108, který připouští neposkytnutí informace v případě, kdy je to stanoveno zákonem a zároveň by šlo o zájem ochrany bezpečnosti státu, veřejné bezpečnosti nebo potírání trestné činnosti a také pokud by to bylo v zájmu subjektu údajů.

### Zásada bezpečnosti[139]

Ze zásady bezpečnosti vyplývá potřeba učinit vhodná technická, organizační i personální opatření, které budou chránit osobní údaje v datových souborech proti jejich náhodné ztrátě nebo neoprávněnému zničení, změnám či šíření. Význam této zásady je spjat zejména s problematikou ochrany údajů vyskytujících se v internetových databázích.

---

[136] § 5, odst. 1, písm. e), ZoOOÚ.
[137] § 5, odst. 1, písm. d), ZoOOÚ.
[138] § 11, ZoOOÚ.
[139] § 13, ZoOOÚ.

### Zásada práva přístupu k údajům[140]

Zásada se týká práva osob na přístup k údajům, které se ho týkají, kdy této osobě je dána možnost získávat v jednotlivých intervalech a bez průtahů potvrzení o tom, zda jsou v souborech dat uloženy údaje o jeho osobě.

### Zásada práva na opravu a výmaz[141]

Tato zásada souvisí s povinností zpracovávat pouze pravdivé, přesné a aktuální údaje. Každá osoba má právo na opravu nepřesných a nepravdivých či zastaralých údajů nebo právo na jejich úplný výmaz v případě, pokud byly zpracovány v rozporu s vnitrostátním právním řádem státu, který uplatňuje základní zásady ochrany osobních údajů.

### Zásada nezávislého dozoru[142]

K efektivnímu fungování systému ochrany osobních údajů je třeba, aby existovala instituce, která bude dohlížet na dodržování zásad a právních norem upravujících oblast osobních údajů. Neexistence takového dozoru by mohla vést k nekontrolovatelnému nakládání a zneužívání osobních dat, což byl i případ předchůdce ZoOOÚ. Smluvní státy proto v souladu s touto zásadou zřizují nezávislé orgány, které jsou pověřené zabezpečováním dodržování zásad a vnitrostátních předpisů. Takovéto orgány existují nejen v evropských státech, ale i státech mimo Evropu. Přestože rozsah jejich působnosti není ani v rámci Evropy sjednocen, jelikož v některých státech funkce dozoru náleží jak speciálnímu dozorovému úřadu, tak i soudním institucím, jejich společným cílem je vždy ochrana osobních údajů.

---

[140] § 12, ZoOOÚ.
[141] § 21, ZoOOÚ.
[142] § 2, ZoOOÚ.

## *Příloha č.: 2 - Legislativní proces přijetí zákona ÚoOOÚ*

Legislativní proces přijetí zákona ÚoOOÚ[143]

---

***POSLANECKÁ SNĚMOVNA***
*Vláda **předložila** sněmovně návrh zákona 28. 9. 1999.*
*Zástupce navrhovatele: Mertlík Pavel.*
*Návrh zákona rozeslán poslancům jako tisk **374/0** dne 29. 9. 1999.*
***Organizační výbor** projednání návrhu zákona **doporučil** 30. 9. 1999 (usnesení č. 173). Určil zpravodaje: **JUDr. Cyril Svoboda** a navrhl přikázat k projednání výborům: **Petiční výbor***

---

***1. Čtení** proběhlo 3., 4. 11. 1999 na 17. schůzi. Návrh zákona **přikázán k projednání** výborům (usnesení č. 555).*

---

***Petiční výbor** projednal návrh zákona a vydal 30. 11. 1999 **usnesení** doručené poslancům jako tisk **374/1**.*

---

***2. Čtení***
*Návrh zákona **prošel** obecnou rozpravou 19. 1. 2000 na 21. schůzi.*
*Návrh zákona **prošel** podrobnou rozpravou 19. 1. 2000 na 21. schůzi.*
*Podané **pozměňovací návrhy** zpracovány jako tisk **374/2**, který byl rozeslán 21. 1. 2000 v 14:00.*

---

***3. Čtení** proběhlo 27. 1. 2000 na 21. schůzi. Návrh zákona **schválen** (hlasování č. 266, usnesení č. 760).*

---

***SENÁT***
*Poslanecká sněmovna **postoupila** dne 23. 10. 2002 návrh zákona Senátu jako tisk **171/0**.*
*Organizační výbor dne 19. 11. 2002 **stanovil** garančním výborem Výbor petiční, pro lidská práva, vědu, vzdělávání a kulturu (Ing. Josef Kaňa) a **přikázal** tisk k projednání: Ústavně-právní výbor, Výbor pro zahraniční věci, obranu a bezpečnost (Michael Žantovský), Výbor pro evropskou integraci (Doc.MUDr. Jaroslava Moserová, DrSc.).*

---

***Výbor pro evropskou integraci** projednal návrh dne 16. 2. 2000 a přijal usnesení č. 132, které bylo rozdáno jako tisk **171/3** (pozměňovací návrhy).*
***Ústavně-právní výbor** projednal návrh dne 16. 2. 2000 a přijal usnesení č. 155, které bylo rozdáno jako tisk **171/S** (zamítá).*
***Výbor petiční, pro lidská práva, vědu, vzdělávání a kulturu** projednal návrh dne 23. 2. 2000 a přijal usnesení č. 146, které bylo rozdáno jako tisk **171/1** (pozměňovací návrhy).*
***Výbor pro zahraniční věci, obranu a bezpečnost** projednal návrh dne 23. 2. 2000 a přijal usnesení č. 124, které bylo rozdáno jako tisk **171/4** (zamítá).*

---

***POSLANECKÁ SNĚMOVNA***
*O návrhu zákona vráceném Senátem hlasováno 4. 4. 2000 na 24. schůzi.*
*Sněmovna **setrvala** na původním návrhu zákona (hlasování č. 41, usnesení č. 908).*

---

***PREZIDENT***
*Zákon **doručen** prezidentovi k podepsání 6. 4. 2000.*
*Prezident zákon **podepsal** 17. 4. 2000.*

---

*Schválený zákon **doručen** k podpisu premiérovi 19. 4. 2000.*
*Zákon **vyhlášen** 25. 4. 2000 ve Sbírce zákonů v částce 32 pod číslem 101/2000 Sb.*

---

[143] PORTÁL PARLAMENT ČESKÉ REPUBLIKY. *Sněmovní tisk 374 - Zákon o ochraně osobních údajů.* [webová stránka], [online], [cit. 2010-03-29]. Dostupné z <http://www.psp.cz/sqw/historie.sqw?t=374&o=3>.

*Příloha č.: 3 - Antivirové desatero*

**Antivirové desatero**[144]

- **Provádějte pravidelný update svého antivirového programu!** Antivir, který obsahuje zastaralou virovou databázi nelze využívat jako prevence zachycení virové nákazy, protože každý den se objevují nové a nové viry, ze kterých navíc mohou vznikat různé mutace. U mnohých antivirů lze nastavit tzv. "live update", po připojení se k internetu program sám zjistí, zda je k dispozici aktualizace, a pokud ano, stáhne ji. Uživatel se tak nemusí starat vůbec o nic a jeho počítač je dobře chráněn proti novým přírůstkům na virové scéně.
- **Nikdy neotvírejte e-mailovou přílohu, kterou jste nepožadoval(a)!** nebo nejste-li přesvědčeni o jejím původu.
  Virus obsažený v příloze e-mailu, se nemusí pouze šířit na adresy, které najde v poštovním programu. Může obsahovat i další škodlivé rutiny, které například zlikvidují data na zasaženém počítači.
- **Mějte kontrolu nad svým počítačem a nad tím, kdo jej používá!**
  Riziko virové nákazy a ztráty dat vzrůstá úměrně s počtem lidí, kteří mají ke konkrétnímu počítači přístup. Stačí jediný nezodpovědný člověk, který přinese z domova zavirovanou disketu nebo otevře e-mailovou přílohu s virem, a práce všech ostatních přichází vniveč. V současné době se je důležité ochránit počítač pomocí programu, který zajistí přístup pouze definovaným uživatelům. Nejde pouze o zamezení virové nákazy, ale i o ochranu informací uchovávaných v počítači. Je třeba si uvědomit, že informace mají také svoji cenu. S připojením počítače na internet vyvstává potřeba chránit se i proti nežádoucím průnikům ze sítě.
- **Instalujte včas všechny „záplaty“ na používaný software!**
  Existují viry, které používají tzv. bezpečnostní díry v operačních systémech a aplikacích. Pokud je taková chyba v programu zjištěna, jeho výrobce

zpravidla připraví tzv. záplatu (patch), kterou lze na daný program aplikovat (nainstalovat), a tím chybu odstranit. Tyto soubory jsou zpravidla k dispozici ke stažení na stránkách jednotlivých výrobců software. Je v zájmu uživatele sledovat aktuální situaci a nové záplaty co nejdříve aplikovat. Toto pravidlo platí zejména pro operační systémy.

- **Vždy prověřujte diskety a CD média předtím, než je použijete!**
  Je bezpečnější vždy investovat několik minut času a vstupní médium otestovat, než se potom několik hodin trápit nad zavirovaným počítačem, případně platit specialistu.
- **S každým novým souborem (i z důvěryhodného zdroje) nakládejte s největší opatrností!**
  Uvedené pravidlo platí nejen pro pirátský software. Existují dokonce i případy, kdy instalační CD od známého výrobce tiskáren obsahovalo virus. Mnohonásobně větší je riziko v případě souborů stahovaných z internetu. Nezáleží na tom, komu stránky patří, i na stránkách renomované firmy mohou být soubory infikované viry. Připomeňme třeba případ, kdy na stránkách světově proslulého výrobce nejmenovaného operačního systému byl několik týdnů k dispozici dokument nakažený makrovirem. Inu virus si nevybírá, komu patří soubor, který napadá. Ještě větší obezřetnost by měla být dodržována při stahování hudby či filmů z P2P sítí. Pokud někdo tuto nelegální činnost provádí, měl by brát rovněž na vědomí, že stahovaná data mohou být s velkou pravděpodobností zavirována.
- **Využívejte více než jen jeden způsob antivirové ochrany!**
  Z hlediska celkové bezpečnosti není dostačující použití pouze jednoduchého antivirového programu, který umí na požádání prověřit daný soubor či adresář. Je žádoucí, aby antivirový program uměl kombinovat několik druhů ochrany.

[144] POTRÁL VIRTUÁLNÍ AKADEMIE, *Antivirová ochrana*. [webová stránka], [online], [cit. 2010-03-29]. Dostupný z http://www.e-skripta.eu/ssos/index.php?id=skripta/rocnik1/informatika/informatika-kap2>.

- **Vytvořte si zaručeně „čisté“ bootovací médium a pečlivě jej uložte na bezpečné místo!**

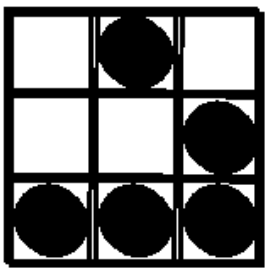
  Může nastat případ, že na počítači, který byl napaden virem, nelze spustit operační systém. Nemusí to však nutně znamenat, že by virus data na pevném disku počítače smazal. V takovém případě je vhodné mít k dispozici předem vytvořené tzv. bootovací médium (samozřejmě nezavirované), které současně obsahuje antivirový program. Pomocí tohoto média lze napadený počítač spustit a infikované soubory vyléčit či přinejhorším smazat.
- **Pravidelně zálohujte!**

  Ačkoliv toto pravidlo přímo nesouvisí s antivirovou ochranou, jeho dodržování umožňuje minimalizovat případné škody způsobené agresivním virem, nespolehlivým hardwarem apod. V porovnání s cenou ztracených dat je čas strávený zálohováním zcela zanedbatelný. Vytvořené zálohy je vhodné uložit na bezpečném místě (pro případ požáru či jiné živelné katastrofy).
- **Nepodléhejte panice!**

  Účelem těchto pravidel není strašit uživatele počítačů. Počítačové viry jsou ve své podstatě jen obyčejné programy. Jediným rozdílem, který je činí nebezpečnými, je to, že svoji činnost provozují nezávisle na vůli uživatele. Viry jsou programovány obyčejnými lidmi a nemohou tedy mít žádné přehnané schopnosti. Mnohem větší škody zpravidla napáchá nezkušený uživatel, který se v panickém strachu snaží napadený počítač „vyléčit“.

***Příloha č.: 4 - Morální hodnoty hackerské komunity[145]***

Základním vyznáním hackerů je svoboda jedince, nicméně jsou ochotni i pomáhat druhým. Elektronický svět, v němž se pohybují, je pro ně plný výzev a problémů čekajících na vyřešení. Hacker neřeší žádný problém dvakrát a k vyřešenému problému se nevrací. Morální povinností hackera je sdílení získaných informací a know-how.



Hacker logo[146]

**Hackerská pravidla a etika byly během času shrnuty do základních pravidel:**

- Přístup k počítačové technologii pro všechny bez rozdílu a zdarma,
- všechny informace zdarma,
- nedůvěřujeme vládě a obecně mocenským autoritám, podporujeme decentralizaci,
- hackeři mají být posuzováni podle jejich dovedností jinými hackery a ne nějakou formální organizací nebo jinými nerelevantními kritérii,
- na počítači je možné vytvořit i umění a krásu,
- hacker nikdy nepoškodí systém,
- hacker se nikdy neprolamuje do státních počítačů.

O hackerské etice je možno psát dlouho a stavět názory jednoho hackera proti druhému. V komunitě silných individualit se množství názorů na jedno téma nevyhneme. Nicméně posedlost technologiemi, síla myšlení a protest proti nechápajícímu světu, který dal vznik nové kultuře, může dokreslit citát z hořkého pohledu hackera s přezdívkou The Mentor, který ve svém hackerském manifestu uveřejněném krátce po uvěznění píše: ***„Ano, jsem zločinec. Mým zločinem je zvědavost, jeho podstatou je posuzování lidí podle toho co říkají a co si myslí, nikoli podle toho jak vypadají. Můj zločin spočívá v tom, že jsem chytřejší než vy, což mi nikdy neodpustíte…“***

[145] JIROVSKÝ, V. *Kybernetická kriminalita.* První vydání. PRAHA: Grada Publishing, a.s. 2007, 288 s. ISBN 978-80-247-1561-2. s. 52-53.

[146] PORTÁL PUBLIC-DOMAIN-PHOTOS, *Hacker Emblem.* [počítačový soubor], [ on-line], [cit. 2010-04-19]. Dostupný z <http://www.public-domain-photos.com/free-cliparts/other/games/hacker_emblem-3706.htm>.

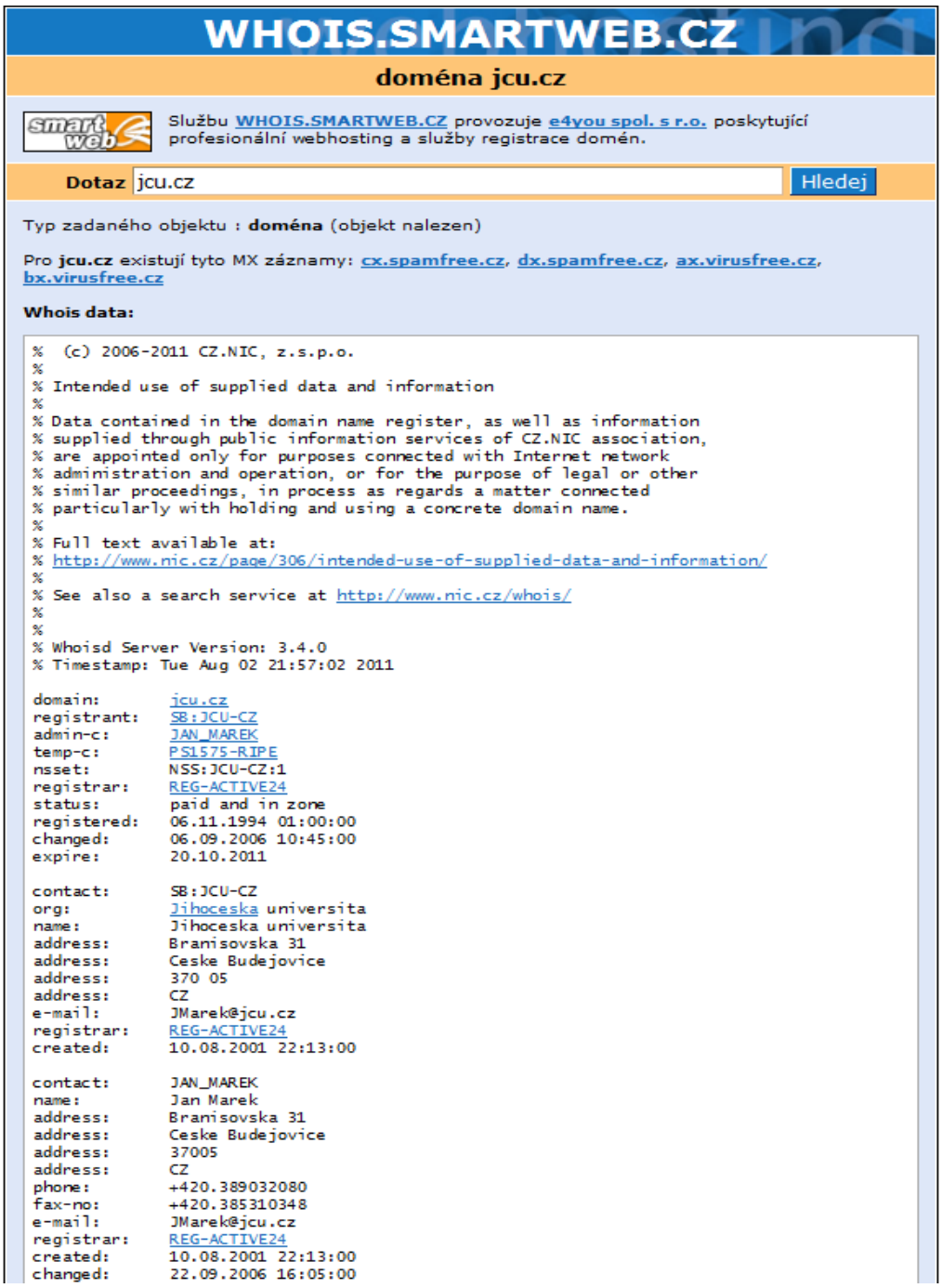
*Příloha č.: 5 - Pokročilé operátory používané ve vyhledávači Google*

| Pokročilý operátor vyhledávání | Výskyt hledané hodnoty |
|---|---|
| | |
| **intitle** | **V titulku stránky** |
| **allintitle** | **Vše v titulku stránky** |
| **inurl** | **V URL stránky** |
| **allinurl** | **Vše v URL stránky** |
| **filetype** | **V souboru konkrétního typu** |
| **allintext** | **Vše v textu stránky** |
| **site** | **Ve specifických stránkách** |
| **link** | **V odkazech na stránky** |
| **inanchor** | **V textu odkazů** |
| **numrange** | **V určitém číselném rozsahu** |
| **daterange** | **V určitém období** |
| **cache** | **V archivu stránek** |
| **info** | **V souhrnných informacích** |
| **related** | **V podobných stránkách** |
| **phonebook** | **V telefonním seznamu** |
| **author** | **V odkazech na autory** |
| **group** | **V titulku skupin** |
| **insubject** | **V předmětu skupin** |
| **stock** | **V akciích** |

**Zdroj: Google.com**

Je potřeba si uvědomit, že vyhledávač Google prohledává i data ukrytá ve svých dřívějších archivech.

*Příloha č.: 6 - Ukázka výpisu typu WHOIS - registrace domény*



WHOIS.SMARTWEB.CZ

doména jcu.cz

Službu WHOIS.SMARTWEB.CZ provozuje e4you spol. s r.o. poskytující profesionální webhosting a služby registrace domén.

Dotaz jcu.cz Hledej

Typ zadaného objektu : **doména** (objekt nalezen)

Pro **jcu.cz** existují tyto MX záznamy: cx.spamfree.cz, dx.spamfree.cz, ax.virusfree.cz, bx.virusfree.cz

**Whois data:**

```
%  (c) 2006-2011 CZ.NIC, z.s.p.o.
%
% Intended use of supplied data and information
%
% Data contained in the domain name register, as well as information
% supplied through public information services of CZ.NIC association,
% are appointed only for purposes connected with Internet network
% administration and operation, or for the purpose of legal or other
% similar proceedings, in process as regards a matter connected
% particularly with holding and using a concrete domain name.
%
% Full text available at:
% http://www.nic.cz/page/306/intended-use-of-supplied-data-and-information/
%
% See also a search service at http://www.nic.cz/whois/
%
%
% Whoisd Server Version: 3.4.0
% Timestamp: Tue Aug 02 21:57:02 2011

domain:       jcu.cz
registrant:   SB:JCU-CZ
admin-c:      JAN_MAREK
temp-c:       PS1575-RIPE
nsset:        NSS:JCU-CZ:1
registrar:    REG-ACTIVE24
status:       paid and in zone
registered:   06.11.1994 01:00:00
changed:      06.09.2006 10:45:00
expire:       20.10.2011

contact:      SB:JCU-CZ
org:          Jihoceska universita
name:         Jihoceska universita
address:      Branisovska 31
address:      Ceske Budejovice
address:      370 05
address:      CZ
e-mail:       JMarek@jcu.cz
registrar:    REG-ACTIVE24
created:      10.08.2001 22:13:00

contact:      JAN_MAREK
name:         Jan Marek
address:      Branisovska 31
address:      Ceske Budejovice
address:      37005
address:      CZ
phone:        +420.389032080
fax-no:       +420.385310348
e-mail:       JMarek@jcu.cz
registrar:    REG-ACTIVE24
created:      10.08.2001 22:13:00
changed:      22.09.2006 16:05:00
```

ZDROJ: whois.smartweb.cz

Z výpisu je patrné jméno, příjmení, funkce, tel. číslo, e-mail adresa, název firmy a lokační adresa, což jsou výchozí informace pro další vyhledávání.

*Příloha č.: 7- Tabulka - Dílčí odpovědnosti za splnění zákonných povinností*

| Zákon | Oblast | Odpovídá |
|---|---|---|
| zák. č. 365/2000 Sb. §5 odst. 2 písm. a | spolupracovat s Ministerstvem vnitra při plnění jeho úkolů | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. a | spolupracovat s Ministerstvem vnitra při provádění kontroly na místě dle zákona o státní kontrole | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. b | předložit Ministerstvu vnitra k vyjádření návrhy dokumentací programů obsahující pořízení, obnovu a provozování informačních a komunikačních technologií | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. b | předložit Ministerstvu vnitra k vyjádření investiční záměry akcí pořízení, obnovy a provozování informačních a komunikačních technologií - přesné podmínky viz zákon | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. c | uveřejňovat číselníky, pokud jsou jejich správci a není zákonem stanoveno jinak, a to i způsobem umožňujícím dálkový přístup | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. c | předávat Ministerstvu vnitra údaje do informačního systému o datových prvcích v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. d | zajistit, aby vazby jimi provozovaného informačního systému na informační systémy jiného provozovatele byly uskutečňovány prostřednictvím referenčního rozhraní s využitím datových prvků vyhlášených ministerstvem a vedených v informačním systému o datových prvcích | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. d | prokázat atestem způsobilost informačního systému k realizaci výše uvedených vazeb | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. e | zpřístupňovat ministerstvu v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem, bez zbytečného odkladu informace o jimi provozovaném informačním systému a jím poskytovaných službách a používaných datových prvcích, a to za účelem uveřejnění v IS o ISVS a IS o DP | starosta obce |
| zák. č. 365/2000 Sb. §5 odst. 2 písm. f | odstranit zjištěné nedostatky ve lhůtě stanovené Ministerstvem vnitra | starosta obce |
| zák. č. 365/2000 Sb. §5a odst. 1 | vytvářet a vydávat informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování | starosta obce |
| zák. č. 365/2000 Sb. §5a odst. 2 | vytvářet a vydávat provozní dokumentaci k jednotlivým ISVS, uplatňovat ji v praxi a vyhodnocovat její dodržování | starosta obce |
| zák. č. 365/2000 Sb. §5a odst. 3 | zajistit si atest dlouhodobého řízení ISVS | nepodléhá povinnosti atestace |
| zák. č. 365/2000 Sb. §5b odst. 1 až odst. 2 | zajišťovat bezpečnost ISVS v rozsahu odpovídajícím alespoň minimálním bezpečnostním požadavkům k zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací dle prováděcího předpisu | starosta obce |

Zdroj: http://www.mvcr.cz/soubor/informacni-koncepce-obce-s-vykonem-prenesene-pusobnosti-v-zakladnim-rozsahu.aspx