Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Ochrana osobních dat a údajů

Aneta PACÁKOVÁ

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra práva

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Aneta Pacáková

Veřejná správa a regionální rozvoj

Název práce

Ochrana osobních dat a údajů

Název anglicky

Personal data protection

Cíle práce

Představení zkoumané problematiky z pohledu platné právní úpravy ČR a USA.
Porovnání obou právních úprav a praxe formou srovnávací analýzy, případné návrhy na opatření.

Metodika

- analýza právní úpravy ČR a USA .
- porovnání teorie a praxe ČR a USA.
- srovnávací analýza ekonomických a právních aspektů.
- doporučení a případné návrhy na opatření.

Doporučený rozsah práce

60-80 stran

Klíčová slova

osobní údaje, ochrana dat, zpracování, zabezpečení, zneužití, mlčenlivost, archivace, likvidace

---

Doporučené zdroje informací

Další literatura a odborné články po konzultaci s vedoucí DP
Zákon č. 101/2000 Sb., o ochraně osobních údajů
Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných čísel
Zákon č. 159/2006 Sb., o střetu zájmů
Zákon č. 21/1992 Sb., o bankách
Zákon č. 2/1993 Sb., Listina základních práv a svobod
Zákon č. 227/2000 Sb., o elekronickém podpisu
Zákon č. 273/2008 Sb., o Policii České republiky
Zákon č. 301/2000 Sb., o matrikách, jménu a příjmení
Zákon č. 329/1999 Sb., o cestovních dokladech
Zákon č. 337/1992 Sb., o správě daní a poplatků
Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích
Zákon č. 499/2004 Sb., o archivnictví a spisové službě
Zákon č.1/1993 Sb., Ústava České republiky
Zákon č.127/2005 Sb., o elekronických komunikacích

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Mgr. Ivana Hájková

Elektronicky schváleno dne 21. 10. 2014

JUDr. Jana Borská

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 03. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Ochrana osobních dat a údajů" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 30.3.2015 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucímu práce paní Mgr. Hájkové Ivaně za cenné rady a připomínky, které mi velmi pomohly při zpracování mé diplomové práce. Také děkuji rodině, která mě vytrvale podporovala při psaní této práce a při celém studiu. Dále bych chtěla poděkovat všem respondentům za jejich ochotu a věnování svého času.

Ochrana osobních dat a údajů

Personal data protection

Souhrn

Tématem této diplomové práce je problematika týkající se ochrany osobních údajů v ČR a USA. Diplomová práce se zabývá porovnáním právních úprav a praxe formou srovnávací analýzy v České republice a USA. Cílem mé diplomové práce je analyzovat právní úpravu v ČR a USA. Hlavním cílem však je obě právní úpravy detailně srovnat a na základě jejich vzájemné komparace vyvodit nejlepší možná řešení v praxi pro Českou republiku. Následně upozorňuje na nedostatky v současné právní úpravě. Součástí práce jsou také návrhy na možná řešení diskutovaných problémů. První kapitola práce vymezí základní pojmy používané v oblasti ochrany osobních údajů nutné k celému jejímu pochopení dále k objasnění základních principů a pravidel ochrany osobních údajů a souvisejících právních oblastí. V následujících dvou kapitolách se diplomová práce zaměřuje individuálně na ČR a USA a jejich legislativu. ČR chrání své občany, ale díky svému byrokratickému aparátu a velice přísným pravidlům nedostatečně podporuje obchod. Spojené státy na druhou stranu příliš spoléhájí na autoregulaci průmyslu a zanedbávají význam státní legislativy.

Abstract

The topic of this diploma thesis is the issue of the protection of personal data in the Czech Republic and the USA. This diploma thesis compares in the form of comparative analysis both legislations and practices in the Czech Republic and the USA. The aim of my thesis is to analyze the legislation in the Czech Republic and the USA. The main objective is, first, to compare in detail both legislations and, second, based on the comparison, to draw the best possible solutions for the practice in the Czech Republic. The next objective is to draw the attention to shortcomings in the current legislation with some suggestions for a possible solution of the discussed issues. Chapter one sets basic terms used in the area of personal

data privacy that are indispensable for the understanding of the area and for clarifying basic principles and rules of personal data privacy in the related areas of law. Chapters two and three of this work focus on the Czech Republic and the USA and their legislation respectively. The Czech Republic on the one hand protects its citizens, but on the other hand it does not boost business. On the contrary, the USA relies too much on self-regulation of industry and neglects the importance of state legislation.

Klíčová slova: archivace, likvidace, mlčenlivost, ochrana dat, osobní údaje, zabezpečení, zneužití, zpracování

Keywords: archiving, liquidation, secrecy, data protection, personal information, security, misusage, processing

Obsah

Seznam zkratek:

COPPA - Zákon na ochranu dětí online (v USA)

FTC - Federální komise pro obchod (Federal Trade Commissionn)

GLB - Zákon Gramm-Leach-Bliley

HHS - Federální ministerstvo zdravotnictví a sociálních služeb

HIPAA -zákon o zdravotním pojištění ((The Health Insurance Portability and Accountability Act)

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

ObčZ – zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů

ObchZ – zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů

OchOsÚ – ochrana osobních údajů

TrZ – zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

ÚOOÚ – Úřad pro ochranu osobních údajů

ZoOU – zákon č. 101/2000 Sb, o ochraně osobních údajů, ve znění pozdějších předpisů

1 Úvod

Dvacáté první století bývá často nazýváno informačním věkem. Tato myšlenka je založena na představě, že lidská činnost závisí na výměně informací. Moderní technologie nám umožňují shromažďovat, vyhodnocovat, přenášet a zpracovávat dosud nevídané množství dat. Lidé dnes mají přístup k informacím, které dříve k dispozici nebyly. Úměrně tomu se zvyšuje i riziko průniku do soukromí jednotlivce a dalších nechtěných důsledků. Ochrana osobních údajů hraje významnou roli při posilování důvěry uživatelů v informační technologie.[1]

Osobní údaje nás prakticky provázejí v každém okamžiku našeho života- existence jedince je stvrzena zápisem do matriky, přidělením rodného čísla, rodným listem, přihlášením k trvalému pobytu. V průběhu života údajů o každém jedinci přibývá. Zaznamenávány jsou osobní údaje identifikační: jméno, příjmení, adresa bydliště, e-mailová adresa. Osobní údaje číselné: datum narození, rodné číslo, telefonní číslo, číslo platební karty, osobní číslo zaměstnance, číslo občanského průkazu nebo cestovního dokladu, číslo pojištěnce aj. Citlivé údaje: zdravotní stav, DNA, sexuální orientace, členství v politické straně, náboženství atd. Informace se staly vysoce cenným a ceněným artiklem. Jejich zneužití však může vyústit v závažný zásah do základních lidských práv. Stále více tedy získává na důležitosti právo na soukromí, resp. právo na ochranu osobních údajů.

O osobních údajích můžeme hovořit na úvod 21. Století v nejrůznějších souvislostech: například jako o objektu ochrany ze strany státu, ale též je zájmu komerčních společností, útoků pachatelů trestných činů a zřejmě by bylo možno shledat další kritéria. V každém případě se jedná o záležitost důležitou, o čemž svědčí množství monografií, komentářů, článků v odborném tisku a nikoli na místě posledním také judikatury, která se jí zabývá. [2]

Osobní údaje mají v dnešní době obrovskou ekonomickou hodnotu, která může v případě detailních databází jít až do milionů či desítek milionů eur. Shromažďování, analyzování nebo předávání dat, ať už vnitrostátně nebo do zahraničí, se stalo velkým byznysem, v jehož rámci jsou právě osobní údaje hlavním zbožím. A mohou to být i Vaše osobní údaje.

[1] Ochrana osobních údajů vybrané otázky. Příručka pro podnikatele. Úřad pro ochranu osobních údajů. [online]. ©2011 [cit. 2014-11-27]. Dostupné z :http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3025

[2] MATES, P., JANEČKOVÁ, E., BARTÍK,V. *Ochrana osobních údajů*, s. 7

Je proto důležité vědět, s kým data sdílíte a co se bude se všemi Vašimi osobními údaji dále dít. Je důležité si uvědomit, že jednou sdělený údaj už lze těžko vzít zpět. [3]

Problematika zpracování osobních údajů se dotýká široké odborné veřejnosti, zejména praxe soudců, advokátů, exekutorů, lékařů, zdravotnického personálu, soukromých bezpečnostních agentur, správců a zpracovatelů osobních údajů zejména z oblasti veřejné správy a obcí, a i podnikatelských subjektů, dále svoje místo může najít i například na pracovištích personalistů, bankovních úředníků, může jej ovšem využít i laická veřejnost. S osobními údaji se setkáváme v soukromém i pracovním životě.

Ochrana osobních údajů má nepochybně svoje ukotvení v předpisech práva správního, tedy veřejného. Ke zpracování osobních údajů však dochází nejen ve vztazích regulovaných právem veřejným, ale i soukromým. [4]

Stěžejním důvodem pro výběr tohoto tématu byla možnost porovnání právní úpravy ochrany osobních údajů v České republice a USA. První kapitola práce vymezí základní pojmy používané v oblasti ochrany osobních údajů nutné k celému jejímu pochopení dále k objasnění základních principů a pravidel ochrany osobních údajů a souvisejících právních oblastí. V následujících dvou kapitolách se zaměřuje individuálně na ČR a USA a jejich legislativu. Příklady, které jsou aktuálně řešeny a komentovány, tak zdaleka nepředstavují vyčerpávající soubor všech paragrafů zákona, ale soustřeďují se především na ustanovení, která jsou vnímána jako problematická a díky tomu je kladen větší důraz na jejich vysvětlení.

Cílem mé diplomové práce je analyzovat právní úpravu v ČR a USA. Hlavním cílem však je obě právní úpravy detailně srovnat a na základě jejich vzájemné komparace vyvodit nejlepší možná řešení v praxi pro Českou republiku. Následně upozorňuje na nedostatky v současné právní úpravě. Součástí práce jsou také návrhy na možná řešení diskutovaných problémů.

[3] Úřad pro ochranu osobních údajů, ochrana osobních údajů na pracovišti, příručka pro zaměstnance. Pro úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2014, ISBN 978-80-210-6819-3 [online]. ©2014 [cit. 2014-11-27]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

[4] MATES, P., JANEČKOVÁ, E., BARTÍK, V. *Ochrana osobních údajů*, s. 51

2 Cíl práce a metodika

Cílem této diplomové práce je představení zkoumané problematiky z pohledu platné právní úpravy ČR a USA. Dílčími cíli je podat přehled o platné právní úpravě v ČR a USA.

Hlavním cílem však je obě právní úpravy detailně srovnat a na základě jejich vzájemné komparace vyvodit nejlepší možná řešení v praxi pro Českou republiku. Následně upozorňuje na nedostatky v současné právní úpravě. Součástí práce jsou také návrhy na možná řešení diskutovaných problémů.

Teoretická část byla zaměřena na studium odborných publikací a jiných zdrojů vztahujících se k dané problematice, kde byly vysvětleny odborné pojmy a právní legislativa v praktické části byla provedena srovnávací analýza ekonomických a právních aspektů v ČR a USA za účelem komparace. V další části práce bylo provedeno dotazníkové šetření a doporučeny případné návrhy a opatření.

Metodika šetření

Práce byla zpracována na základě prostudování odborné literatury a ostatních zdrojů týkající se ochrany osobních dat a údajů. Při zpracování práce byly použity metody dedukce, komparace, popisu a zhodnocení. Dále bylo provedeno anketní šetření v ČR.

Cílovou populaci anketního šetření tvořili občané Prahy a Litoměřic. Sběr dat byl realizován (tzn. názory veřejnosti byly získány), prostřednictvím anketních lístků (strukturovaných dotazníků), které respondenti vyplňovali v tištěné i internetové podobě- dotazníky viz přílohy.

Termín realizace: sběr dat probíhal od 1. 1. 2015 do 25. 3. 2015.

Celkem bylo získáno a analyzováno 252 anketních lístků. U dílčích otázek se počet respondentů, kteří na danou otázku odpověděli, liší (zodpovězení otázek bylo dobrovolné – respondenti nemuseli odpovídat na všechny otázky). Absolutní i relativní četnosti u jednotlivých otázek jsou vypočítány pouze z relevantních odpovědí, nerelevantní (chybějící a nejednoznačné) odpovědi nebyly do výpočtů zahrnuty.

3 Teoretická východiska

3.1 Osobní údaje a jejich druhy

Osobním údajem je jakákoliv informace týkající se určené nebo identifikovatelné fyzické osoby, subjektu údajů.

Příklady osobních údajů:

Osobní údaje identifikační: jméno, příjmení, adresa

Osobní údaje číselné: datum narození, rodné číslo, telefonní číslo, SPZ motorového vozidla, číslo platební karty, základní či agendové identifikátory v systému základních registrů, osobní číslo zaměstnance, číslo občanského průkazu nebo cestovního dokladu, číslo pojištěnce.

Citlivé údaje: zdravotní stav, DNA, sexuální orientace, členství v politické straně nebo odborovém hnutí, náboženské, filozofické nebo politické myšlení, odsouzení za trestný čin, biometrické údaje.

Osobní údaje audiovizuální: fotografie, snímky nebo záznamy obrazové nebo zvukové.

Osobní údaje biometrické: otisky prstů či dlaně, scany dalších identifikovatelných částí těla, zachycení způsobu chůze. [5]

Související ustanovení zákona č. 101-2000 Sb. o ochraně osobních údajů

§ 4 Vymezení pojmů

Pro účely tohoto zákona se rozumí:

Osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,

[5] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s. 9

Citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů, citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,

anonymní údaj takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů,

subjektem údajů fyzická osoba, k níž se osobní údaje vztahují,

zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,

shromažďováním osobních údajů systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování,

uchováváním osobních údajů udržování údajů v takové podobě, která je umožňuje dále zpracovávat,

blokováním operace nebo soustava operací, kterými se na stanovenou dobu omezí způsob nebo prostředky zpracování osobních údajů, s výjimkou nezbytných zásahů,

likvidací osobních údajů se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.[6]

[6] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, , [online]. [cit. 2014-11-27]. Dostupné z: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-kvetna-2014/ds-3109/archiv=0&p1=1261

3.2 Vybrané základní zásady ochrany osobních údajů

Zásada legitimity zpracování

Osobní údaje musí být získány a zpracovány v souladu se zákony. Musejí být přitom dodržovány základní svobody a práva osob, jichž se osobní údaje týkají, zejména pak právo na soukromí uznané také v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod. Toto právo je zakotveno také v obecných zásadách práva Evropské unie. Je uvedeno, že Unie je založena na zásadách svobody, demokracie, dodržování lidských práv a základních svobod a právního státu, zásadách, které jsou společné členským státům, a dále, že Unie ctí základní práva zaručená Evropskou úmluvou o ochraně lidských práv a základních svobod podepsanou v Římě dne 4. Listopadu 1950 a ta, jež vyplývají z ústavních tradic společných členským státům, jako obecné zásady práva Společenství.

Zákon o ochraně osobních údajů tuto zásadu rozvedl především v § 5 odst. 1 písm. c) věta: „správce je povinen zpracovávat pouze přesné osobní údaje, které získal v souladu s tímto zákonem“ a § 5 odst. 3. Těmito ustanoveními je zajištěno, že osobní údaje budou (měly by být) zpracovávány legálně a že údaje byly také legálně získány ke zpracování. Další aspekt legality a poctivosti zpracování se týká způsobu, jakým mají a mohou být údaje zpracovávány. Tato zásada je uvedena v § 5 odst. 1 písm. g). Je tak zajištěno, že shromažďovat se osobní údaje mohou pouze otevřeně, je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti. Existují ovšem i výjimky z tohoto pravidla. Tak např. Bezpečnostní informační služba může informace a informační systémy sdružovat a získávat informace pod krytím jiným účelem nebo jinou činností. Obdobně to platí i pro Vojenské zpravodajství nebo Policii České republiky. K tomuto základnímu postulátu je pak třeba přiřadit zásadu z ní vyplývající, tedy pravidlo, že osobní údaje mohou být zpracovávány především na základě souhlasu subjektu údajů. Samozřejmě platí, že ne ve všech případech zpracování je takového souhlasu potřeba (§ 5 odst. 2 písm. a) g)), nicméně jedná se o zákonné výjimky, které základní princip jen akcentují.[7]

[7] MATES, P., JANEČKOVÁ, E., BARTÍK, V. *Ochrana osobních údajů*, s. 9-10

Zásada omezení účelem

Tato zásada má dva klíčové aspekty. Za prvé vlastně stanovuje, že údaje musejí být shromažďovány pro specifické, vyjádřené a legitimní účely. Není tedy dovoleno shromažďovat osobní údaje pro nedefinované, resp. obecně vymezené účely. Stanovení účelu musí vždy předcházet vlastnímu shromažďování údajů. Způsobů, jak stanovit legitimní účel, je mnoho, musejí však vždy být v souladu s domácím právním řádem. Nelze tedy stanovit účel zpracování, který byl v rozporu s právními předpisy. Za druhé pak vyžaduje, že údaje nesmějí být zpracovány pro účely neslučitelné s původním účelem. [8]

Zásada časového omezení

Při zpracování osobních údajů je nutno respektovat pravidlo, že údaje jsou zpracovávány jen po dobu nezbytnou pro naplnění stanoveného účelu. Každé zpracování by mělo být omezeno časovým úsekem. Všeobecně se má za to, že „ neomezená doba“ (indefinite period) není pro ochranu osobních údajů všeobecně dobou splňující požadavek časového rámce. Po naplnění stanoveného účelu smějí být údaje uchovány pouze pro účely historického, vědeckého nebo statistického výzkumu. V některých případech smějí být údaje použity pro opětovné právní posouzení (např. soudní spisy, účetní doklady apod.). Uchováním údajů však musí být doprovázeno dostatečnými ochrannými a bezpečnostními opatřeními, aby se zabránilo použití údajů pro jiné účely. Tato zásada je promítnuta v ZoOU v § 5 odst. 1 písm. e), tak, že je stanovena povinnost správců uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné. [9]

[8] MATES, P., JANEČKOVÁ, E., BARTÍK, V. *Ochrana osobních údajů*, s.11
[9] Tamtéž , s.13

Zásada průhlednosti

Zásada průhlednosti v podstatě vyžaduje plnou informovanost subjektu údajů o všech okolnostech zpracování osobních údajů, které se ho týkají. Poskytnutá informace musí být úplná a také pro subjekt údajů srozumitelná. Není tedy možno mu např. zaslat výpis paměti počítače, který by byl pro subjekt údajů nečitelný a nesrozumitelný. Informace musí obsahovat přehled kategorií osobních údajů, účel jejich shromáždění a zpracování a také ovšem identifikaci správce, zpracovatele, případně jiných subjektů, kterým jsou či budou osobní údaje předávány. Výjimka z této povinnosti je možná pouze v případech, kdy subjekt údajů již nepochybně informován je (např. jinou formou komunikace s ním) nebo pokud by to vyžadovalo neúměrné úsilí. Zásada je do ZoOU promítnuta v § 11 tak, že správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, [10]nejsou-li subjektu údajů tyto informace již známy. Součástí informace musí být také poučení o tom, zda je poskytnutí údajů povinné, také o důsledcích případného neposkytnutí. Subjekt údajů musí být také informován o jeho právu na přístup ke svým osobním údajům.

Informační povinnost je pak stanovena v tom případě, kdy dochází ke zpracování osobních údajů na základě souhlasu (výše uvedená informační povinnost se týká vesměs těch zpracování, která jsou realizována na základě zvláštních zákonů). Platí totiž (podle § 5 odst. 4 ZoOU), že subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Rozsah základních informací tedy prakticky totožný.

Zásada ovšem předpokládá i situace, kdy se výše uvedená povinnost aplikovat nebude, tedy, že základní informace poskytnuty nebudou. Je tomu tak zejména v případech, kdy správce nezískává zpracovávané osobní údaje přímo od dotčených fyzických osob, neboť tuto povinnost již měl splnit ten správce, který osobní údaje získal prvotně. Nemělo by se tak stát, že by subjekt údajů neměl o zpracování svých údajů minimálně základní

[10] MATES, P., JANEČKOVÁ, E., BARTÍK, V. *Ochrana osobních údajů*, s. 17

informace. A pokud je nemá, jedná se buď o pochybení správce, nebo o situaci, kdy se informace na základě jiných právních předpisů neposkytnou.[11]

Zásada bezpečnosti

Zásada bezpečnosti je do Zákona o ochraně osobních údajů promítnuta především v § 13. Povinnost přijmout bezpečnostní opatření má zvláštní význam. V řadě situací totiž bezpečnostní opatření buď znemožňují, nebo naopak umožňují porušování zákona. Přijetím dostatečných bezpečnostních opatření se tak minimalizuje hrozba zásahu do soukromí. Z toho vyplývá, že případné zásahy do soukromí tak, jak o nich mluví § 1 Zákona o ochraně osobních údajů, je třeba hodnotit i prostřednictvím provedených bezpečnostních opatření. Konstrukci zabezpečení osobních údajů při jejich zpracování stanoví § 13 odst. 1 Zákona o ochraně osobních údajů v zásadě v obecné rovině. To znamená, že normuje základní rámce a právní povinnosti při zpracování osobních údajů, tak aby se každý správce „vešel" do zákonných ustanovení, současně má vzhledem ke své dikci výrazně preventivní charakter. Lze tak usuzovat z použité terminologie, kde slovní spojení „ aby nemohlo dojít" znamená právě výraz prevence. Rámec pro řádné plnění povinnosti přijmout bezpečností opatření je určován především prostředky a způsobem zpracování osobních údajů. Ty zpravidla určuje z vlastního rozhodnutí sám správce, samozřejmě, pokud mu to nestanoví zákon. Jeho rozhodnutí, které vychází z jeho vlastních lidských, finanční, prostorových atd. Možností, tak vytváří základní prostor pro bezpečnostní opatření. Bezpečnostní opatření při zpracování osobních údajů musí zajistit, s ohledem na odbornou úroveň a náklady na jejich provedení, odpovídající úroveň bezpečnosti v souvislosti s riziky vyplývajícími ze zpracování údajů a z povahy údajů, které mají být chráněny. Bezpečnostní opatření mají být přiměřená charakteru zpracovávaných osobních údajů. Přijímaná bezpečnostní opatření musejí být účinná vůči úmyslnému nebo nedbalostnímu jednání, tak i vůči působení dalších činitelů. Protože zákon o ochraně osobních údajů předpokládá při ochraně osobních údajů jistou komplexnost a prevenci, musí každý, kdo pracuje s osobními údaji, vyhodnotit rizika i v širších rámcích. [12]

[11] MATES, P., JANEČKOVÁ, E., BARTÍK, V. *Ochrana osobních údajů*, s. 18
[12]Tamtéž , s. 19

3.3 Práva a povinnosti při zabezpečení osobních údajů

Každý přímo odpovědný subjekt (správce nebo zpracovatel) a každý další subjekt, který se na průběhu zpracování podílí (poskytovatel služeb, technický správce, provozovatel technické platformy), by měl pro zpracování osobních údajů zajistit podmínky v zásadě srovnatelné s podmínkami ochrany utajovaných informací.

Oblasti zabezpečení:

Personální bezpečnost, která je zajišťována určením skupiny zaměstnanců a jiných fyzických osob, jež mají přístup k osobním údajům včetně kontroly využívání tohoto přístupu, do této oblasti patří institut osobní odpovědnosti zaměstnance v případě porušení povinnosti mlčenlivosti a vzdělávání zaměstnanců.

Fyzická (dříve také objektová) bezpečnost je tvořena systémem aktivních opatření, jejichž cílem je zabránit neoprávněnému přístupu k uchovávaným osobním údajům včetně kontroly této reálně existující hrozby v porovnání s účinností přijatých opatření.

Administrativní bezpečnost, která se vztahuje zejména ke způsobu provádění spisové a archivní činnosti, tvoří ji většinou systém opatření pro výkon administrativní činnosti, která vychází z působnosti a předmětu činnosti odpovědného subjektu, v závislosti na existenci listinné nebo elektronické formy dokumentace se mohou jednotlivá opatření v této oblasti prolínat, patří sem provádění kontroly naplňování jednotlivých administrativních úkonů, výchova a ochrana.

Technická nebo také technologická bezpečnost informačních systémů a úrovně jejich komunikace je skupina převážně technických opatření, směřující k zajištění důvěrnosti a integrity průběhu zpracování[13] osobních údajů, do této skupiny patří i systém opatření prosazující použití kryptografických metod a materiálů.

Související ustanovení zákona o ochraně osobních údajů

§13 Povinnosti osob při zabezpečení osobních údajů[14], §14 Zaměstnanci správce nebo zpracovatele a jiné osoby, §15 Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby.[15]

[13] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s.99
[14] Tamtéž, s. 100-101

3.4 K určení osoby správce, zpracovatele a zpracovatelská smlouva

Subjekty, které provádějí zpracování osobních údajů, jsou v postavení buď správce, který určuje účel a stanoví prostředky zpracování, případně je mu určité zpracování uloženo zvláštním zákonem, anebo jsou správcem pro zpracování najmutí, tedy získají postavení zpracovatele. V této části se dále autoři věnují problematice podmínek smluvního vztahu mezi správcem a zpracovatelem.

Související ustanovení zákona o ochraně osobních údajů

§ 4 Vymezení pojmů pro účely tohoto zákona se rozumí

správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,

zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona,

o) příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněnu, za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g).

Dále je související ustanovení zákona obsaženo v §6 , §7 a § 8 .[16]

3.5 Právní titul ke zpracování osobních údajů

Aby zpracování osobních údajů bylo v režimu zákona o ochraně osobních údajů legální, musí probíhat na základě alespoň jednoho právního titulu, tedy v zákonem předvídané situaci, kdy lze osobní údaje zpracovávat. Pokud zpracování probíhá bez právního titulu, pak je celé od počátku protiprávní. Zákon o ochraně osobních údajů uvádí taxativní, tedy uzavřený výčet možných právních titulů pro zpracování osobních údajů v § 5 odst. 2 a pro zpracování citlivých údajů v § 9. Jestliže správce v rámci jednoho procesu zpracovává osobní i citlivé údaje, postačí, pokud disponuje právním titulem ke zpracování citlivých údajů.

[15] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s.101
[16] Tamtéž, s.33

Související ustanovení zákona o ochraně osobních údajů

§ 5 odst. 2 a § 9 . [17]

3.6 Zpracování osobních údajů pro účely Marketingu

Marketing je komplexní soubor činností, jejichž cílem je zjišťovat potřeby zákazníka a trhu. Právě nutnost předvídatelnosti a stimulace těchto potřeb se stala součástí obchodní politiky všech subjektů, které v této oblasti podnikají. Původně klasický marketing je dnes již masově nahrazen díky vzniku a vývoji internetu IT marketingem, který je schopen monitorovat a ovlivňovat chování zákazníků mnohem podrobněji. Bariérou proti neomezenému přístupu k informacím vypovídajících o našem soukromí je jak zákon o ochraně osobních údajů, tak zákon o některých službách informační společnosti.

Související ustanovení zákona o ochraně osobních údajů

§ 5 odst. 5 až 9. [18]

3.7 Informační povinnost podle § 11 a § 12

Informační povinnost je jednou ze zásadních povinností odpovědného subjektu, která musí být splněna vždy, ideálně před zahájením zpracování, případně při shromáždění osobních údajů přímo od subjektu údajů.

Jsou-li osobní údaje shromažďovány a dále zpracovávány z jiných zdrojů, lze pro tyto případy aplikovat výjimky z informační povinnosti správce nebo zpracovatele.

Příklady realizace informační povinnosti:

Informační leták předcházející akci- sběru dat, jako je například průzkum veřejného mínění, podpisové archy k podpoře iniciativy, marketingová aktivita.

Ústní informace, podávaná příslušným zaměstnancem budoucího správce, obchodním zástupcem, zaměstnancem obchodníka v souvislosti s uzavíráním smlouvy.

[17] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s.43
[18] Tamtéž s.78

Informace na webové stránce obchodníka, poskytovatele elektronických služeb, provozovatele elektronického obchodu, prodejce po internetu.

Informační tabulka v případě provozovatele kamerového systému se záznamem.

Písemná informace jakou součást smluvních podmínek.

Související ustanovení zákona o ochraně osobních údajů

§ 11 a §12 Přístup subjektu údajů k informacím.[19]

3.8 Oznamovací povinnost podle § 16 na násl.

Pro plnění oznamovací povinnosti je nezbytné splnit několik základních předpokladů. Povinným subjektem je zásadně subjekt v postavení správce. Správce musí splnit oznamovací povinnost ještě dříve, než zahájí první operaci zpracování osobních údajů. Správce musí zvážit, zda se pro splnění oznamovací povinnosti neuplatní výjimka obsažená v § 18 odst. 1) zákona o ochraně osobních údajů. Také končení zpracování a likvidaci osobních údajů by měl povinný subjekt oznámit.

Související ustanovení zákona o ochraně osobních údajů

§16 Oznamovací povinnost §17, §18, §19 a § 20 Likvidace osobních údajů.[20]

3.9 Předávání osobních údajů podle § 27

Pro účel regulace přeshraničního pohybu osobních údajů, jejichž předávání často velmi úzce souvisí s přeshraničním pohybem zboží, služeb, kapitálu případně pracovní síly, je v zákoně o ochraně osobních údajů začleněno ustanovení § 27, které ve vztahu k požadavkům článku 2 Úmluvy Rady Evropy č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat a článků 25 a 26 směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů vytváří ucelený právní rámec podmínek upravujících přenos osobních údajů mimo území České republiky.

[19] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s. 87
[20] Tamtéž, s. 115

Související ustanovení zákona o ochraně osobních údajů**:** Hlava III - předání osobních údajů do jiných států § 27.[21]

3.10 Poskytování osobních údajů postupem dle zákona o svobodném přístupu k informacím

Povinnost poskytovat informace na základě žádosti podané podle zákona o svobodném přístupu k informacím dopadá na široký okruh subjekt: orgány státní správy, samosprávy, soudy, veřejné instituce typu České televize, státní podniky i subjekty soukromého práva, pokud byly založeny a jsou kontrolovány státem. Mezi požadovanými informacemi jsou často osobní údaje, proto je při jejich poskytování nezbytné zohlednit i zásady a pravidla zákona o ochraně osobních údajů. Související ustanovení zákona o ochraně osobních údajů §5 odst. 2 písm. f**).** Správce může osobní údaje zpracovávat bez souhlasu subjektu údajů, pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení. § 5 odst 3. provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů.

Související ustanovení zákona o svobodném přístupu k informacím § 8 a, b. [22]

[21] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s. 127
[22] Tamtéž, s. 150

3.11 Legislativa v ČR

Základem práva na ochranu osobních údajů (jako součásti práva na soukromí) je vedle evropských a mezinárodních právních předpisů, které budou zmíněny, především ústavní pořádek České republiky, zejména pak Listina základních práv a svobod, která garantuje právo každého na ochranu před neoprávněným zasahováním do soukromí. Ve svém článku 10 každému přiznává právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno, právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Nejedná se však o jediný její článek, který se principy ochrany soukromí zabývá. Již v článku 7 odst. 1 LPS je zaručena nedotknutelnost osoby a jejího soukromí. Omezena může být jen v případech stanovených zákonem. Rovněž záruky týkající se listovního tajemství, vyjádřené v článku 13 LPS, podle kterého nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon, jsou součástí práva na ochranu před nezákonným zpracováním osobních údajů. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

V oblasti soukromého práva je ochrana soukromí vymezena v § 11 a násl. ObčZ, podle něhož má fyzická osoba právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy. Ochrana osobních údajů je dále provedena také řadou zvláštních zákonů a prováděcích právních předpisů, z nichž za nejvýznamnější lze považovat v oblasti veřejnoprávní zákony upravující provoz informačních registrů veřejné správy, jako je katastr nemovitostí, obchodní nebo živnostenský rejstřík, registr evidence obyvatel, insolvenční rejstřík apod. V oblasti soukromoprávní pak nepochybně půjde o zákon o bankách, zákon o pojišťovnictví, ale také zákon o zdravotních službách nebo zákoník práce.

V oblasti veřejného práva poskytuje soukromí zásadní ochranu trestní zákoník, a to zejména prostřednictvím § 180 odst. 1 TrZ, kdy se postihuje jako neoprávněné nakládání s osobními údaji chování každého, kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděny v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo

oprávněných zájmech osoby, jíž se osobní údaje týkají. Takové osobě hrozí trest odnětí svobody až na tři léta nebo zákaz činnosti.

Zákon o ochraně osobních údajů pak v sobě kombinuje úpravu soukromoprávní (zejména § 21 OchOsÚ) a veřejnoprávní (zejména část týkající se výkonu dozorových činností Úřadu). Základem české právní úpravy ochrany osobních údajů jsou přitom v současné době zejména předpisy práva EU. V roce 2004 v souvislosti se vstupem České republiky z Asociační smlouvy bylo nutné v souladu s Úmluvou 108 a zejména se Směrnicí 95/46/ES [23]stanovit použitelná ustanovení českého právního řádu pro všechny subjekty (právnické i fyzické osoby) se sídlem v České republice a pro pobočky zahraničních subjektů (evropských či mimoevropských) podnikajících v České republice, které hodlají zpracovávat osobní údaje na území České republiky nebo takové informace přes území České republiky přenášet. Základní principy pro zpracování osobních údajů jsou upraveny normami komunitárního práva, jež působí na území členských států Evropské unie.

Vedle již citované směrnice 95/46/ES jde dále o tyto dokumenty: Směrnice č. 2000/31/ES o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu, Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (tato směrnice byla změněna Směrnicí Evropského parlamentu a Rady 2006/24/ES o uchování údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně Směrnice 2002/58/ES, a také Směrnici Evropského parlamentu a Rady 2009/136/ES, 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. Dále je třeba zmínit i Rámcové rozhodnutí Rady 2008/977/SVV o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech a Doporučení Komise 2009/387/ES o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence.[24]

[23] KUČEROVÁ, A. , Zákon o ochraně osobních údajů: komentář, s. 2
[24] Tamtéž, s. 3

Hlavním zákonem upravujícím ochranu osobních údajů v České republice je zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“), který je nedílnou součástí právního řádu České republiky, a to ve dvou směrech:

– Vztahuje se k článkům 10 a 17 Listiny základních práv a svobod zakotvující právo na informace i právo na ochranu soukromí. Zákon o ochraně osobních údajů řeší potenciální protichůdnost výše uvedených práv. Není však jediným právním předpisem tohoto druhu; občanský zákoník (zákon č. 40/1964 Sb., ve znění pozdějších předpisů) totiž obsahuje ustanovení na ochranu osobnosti, což zásadním způsobem souvisí 2. Evropská a národní legislativa a základní definice 7s pojmy „zpracování osobních údajů“ a „subjekt údajů“, jak jsou definovány zákonem o ochraně osobních údajů.

– Zákon o ochraně osobních údajů je obecný zákon upravující zpracování osobních údajů na území České republiky, s výjimkou zpracování údajů prováděného fyzickými osobami čistě pro jejich vlastní potřeby. Zákon o ochraně osobních údajů však umožňuje zpracování osobních údajů pro zvláštní účely (v souladu se směrnicí 95/46/ES) také za účelem splnění úkolů stanovených zvláštním zákonem. Podnikatelé musejí prověřit, zda zamýšlený nebo již probíhající úkon zpracování osobních údajů nespadá pod zvláštní právní předpis. Pokud tomu tak je, má tento zákon přednost před obecným zákonem o ochraně osobních údajů.

Český zákon o ochraně osobních údajů (jakož i zákony o ochraně osobních údajů v dalších zemích) lze rozdělit do tří tematických částí: 1. Ustanovení, která upravují podmínky pro zpracování osobních údajů (obsažena v § 5–19 a § 27 zákona o ochraně osobních údajů) a pokládají právní základy pro zpracování osobních údajů (například souhlas subjektu údajů, povinnost plnit smlouvu nebo provedení úkolů stanovených zvláštním zákonem). 2. Ustanovení upravující důsledky při porušení povinností zpracování osobních údajů jsou následující: – nápravná opatření: ta mohou mít formu likvidace údajů, ukončení nezákonného zpracování atd. (viz § 40 zákona o ochraně osobních údajů); – pokuty (viz hlava VII zákona o ochraně osobních údajů); – trestní sankce – neoprávněné nakládání s osobními údaji je trestným činem dle § 180 trestního zákoníku; – satisfakční opatření – náhrady škody. V těchto případech platí ustanovení občanského zákoníku a obchodního zákoníku. 3. Procedurální ustanovení upravující metody vynutitelnosti práv v případě porušení pravidel ochrany osobních údajů. Satisfakčních opatření – náhrady škody – je

nutno se domáhat prostřednictvím soudu. Trestní případy řeší orgány činné v trestním řízení. Ostatní případy – nápravná opatření, pokuty – spadají do kompetencí Úřadu pro ochranu osobních údajů (dále jen ÚOOÚ), jakožto nezávislého kontrolního orgánu (viz hlava V zákona o ochraně osobních údajů). V České republice přísluší kompetence v oblasti ochrany osobních údajů Úřadu pro ochranu osobních údajů (http://www.uoou.cz/). Pouze úkony prováděné v oblasti ochrany osobních údajů zpravodajskými službami leží mimo kompetence ÚOOÚ. Úřad je mimo jiné odpovědný za vyřizování stížností týkajících se porušení pravidel ochrany osobních údajů (stížnost nebo podnět může být podán bezplatně kýmkoli, i osobami, které nejsou občany České republiky) a také poskytuje bezplatné konzultace.[25]

3.12 Vývoj zákona o ochraně osobních údajů v ČR

Úvodem lze zmínit, že ochrana osobních údajů je relativně novou právní disciplínou. Této problematice je obecně věnována větší pozornost přibližně od osmdesátých let minulého století, v České republice však spíše až od druhé poloviny let devadesátých. Právní úprava týkající se ochrany osobních údajů v České republice nemá nijak dlouhou historii- první norma v této oblasti byla přijata v roce 1992. Větší důležitosti tato oblast práva však nabyla až v souvislosti s přípravou České republiky na vstup do Evropské unie. Součástí tohoto procesu bylo i převzetí pravidel stanovených Směrnicí 95/46/ES do českého právního řádu, přičemž výsledkem tohoto procesu bylo přijetí komentovaného zákona o ochraně osobních údajů. Od počátku své účinnosti prošel tento zákon již mnoha změnami (do začátku roku 2012 byl novelizován již více než dvacetkrát), z nichž ty zásadnější byly reakcí na změnu společenské situace, konkrétně vstup České republiky do EU a do schengenského prostoru, stručnější novely se více či méně pokoušely reagovat na nejrůznější problémy, které vznikly při aplikaci tohoto právního předpisu. [26]

[25]Úřad pro ochranu osobních údajů, ochrana osobních údajů vybrané otázky Příručka pro podnikatele. Pro úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011, ISBN 978-80-210-5572-8 [online]. ©2011 [cit. 2014-11-27]. Dostupné z: http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3025

[26] KUČEROVÁ, A., *Zákon o ochraně osobních údajů: komentář*, s. V

Principy právní úpravy ochrany osobních údajů jsou poměrně starého data. Lze bez nadsázky říci, že tyto principy vyvěrají z mezinárodněprávních pramenů. Prvním významným dokumentem, který je vlastně pojmenoval a systematicky zpracoval, je Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ETS č. 108, Štrasburk, 28.1.1981- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981 byla publikována pod č. 115/2001 Sb. m. s. Dále její dodatkový protokol – sdělení č. 29/2005 Sb. m. s. Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice, uveřejněno v č. 15/2005 Sbírky mezinárodních smluv na straně 363.[27]

3.13 Změny zákona o ochraně osobních údajů

Historie: Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech - zrušen zákonem č. 101/2000 Sb.

Původní zákon o ochraně osobních údajů platnost 25. dubna 2000, účinnost 1.června 2000, s výjimkou ustanovení § 16, §17 a § 35, které nabyly účinnosti 1. prosince 2000

Zákon č 227/2000 Sb. platnost 26. července 2000, účinnost 1. října 2000

Zákon č. 177/2001 Sb. platnost a účinnost 31. května 2001

Zákon č. 450/2001 Sb. platnost a účinnost 31. prosince 2001

Zákon č. 107/2002 Sb. platnost a účinnost 20. března 2002

Zákon č. 309/2002 Sb. platnost 12. července 2002, účinnost 1. ledna

Zákon č. 310/2002 Sb. platnost a účinnost 12. července 2002

Zákon č. 517/2002 Sb. platnost 13. prosince 2002, účinnost 1. ledna 2003

Zákon č. 439/2004 Sb. platnost a účinnost 26. července 2004, s výjimkou ustanovení čl. I bodů 49 a 50, které nabyly účinnosti 1. ledna 2005

Zákon č 480/2004 Sb. platnost a účinnost 7. září 2004

Úplné znění zákona z r. 2004 (včetně novely č. 480/2004 Sb.)

Zákon č. 626/2004 Sb. platnost 10. prosince 2004, účinnost 1. ledna 2005

[27] MATES, P., JANEČKOVÁ, E., BARTÍK, V., *Ochrana osobních údajů*, s. 9

Zákon č. 413/2005 Sb. platnost 18. října 2005, účinnost 1. ledna 2006

Zákon č. 444/2005 Sb. platnost 11. listopadu 2005, účinnost 1. ledna 2006

Zákon č. 109/2006 Sb. platnost 31. března 2006, účinnost 1. ledna 2007

Zákon č. 112/2006 Sb. platnost 31. března 2006, účinnost 1. ledna 2007

Zákon č. 267/2006 Sb. platnost 7. června 2006, účinnost 1. ledna 2010

Zákon č. 342/2006 Sb. platnost a účinnost 3. července 2006

Zákon č. 170/2007 Sb. platnost 12. července 2007, účinnost 1. září 2007

Zákon č. 41/2009 Sb. platnost 9. února 2009, účinnost 1. ledna 2010

Zákon č. 52/2009 Sb. platnost 26. února 2009, účinnost 1. dubna 2009

Zákon č. 227/2009 Sb. platnost 24. července 2009, účinnost 1. července 2010

Zákon č. 281/2009 Sb. platnost 3. září 2009, účinnost 1. ledna 2011

Zákon č. 468/2011Sb. platnost 30. prosince 2011, účinnost 1. ledna 2012

Zákon č. 375/2011 Sb. platnost 8. prosince 2011, účinnost 1. dubna 2012

Zákon č. 64/2014 Sb. platnost 7. dubna 2014, účinnost 1. května 2014[28]

[28] Úřad pro ochranu osobních údajů, změny zákona o ochraně osobních údajů. [online]. [cit. 2015-11-27]. Dostupné z: http://www.uoou.cz/zmeny-zakona-o-ochrane-osobnich-udaju/ds-3112/archiv=0&p1=1257&rd=1000

3.14 Oblasti zpracování osobních údajů

Ústavní zakotvení ochrany osobních údajů, právo na ochranu soukromí	Pojišťovnictví
Archivnictví	Policejní postupy, veřejný pořádek, vnitřní a vnější bezpečnost
Bankovnictví, finance	Poskytování informací veřejnou správou, veřejné rejstříky a evidence
Daňové řízení	Pracovněprávní vztahy, zaměstnanost
Doprava	Předávání osobních údajů do zahraničí
Elektronická veřejná správa (e-government)	Rodná čísla
Elektronické komunikace	Rozhlasové a televizní poplatky
Evidence obyvatel, matriky a notáři	Sociální zabezpečení
Kamerové systémy	Statistická zjišťování
Kasina	Školství
Katastr nemovitostí	Územní samospráva
Nevyžádaná obchodní sdělení	Volby
Osobní doklady	Zdravotnictví

29

[29] Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

Oblasti zpracování osobních údajů

- **ústavní zakotvení ochrany osobních údajů, právo na ochranu soukromí**

usnesení č. 2/1993 Sb. předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

zákon č. 40/1964 Sb., občanský zákoník, ochrana osobnosti (§ 11 až § 16).

- **archivnictví**

zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činností bývalé Státní bezpečnosti svazek s osobními údaji.[30]
Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
Vyhláška 645/2004 Sb. ze dne 13. Prosince 2004, kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů, ve znění vyhlášky č. 213/2012 Sb. [31]

- **bankovnictví, finance**

Finanční instituce, banky nevyjímaje, jsou již dlouhou dobu běžnou součástí našeho života. Tak dlouhou dobu, že ani možná nevnímáme, jak se postupně mění jejich postavení a význam. Právě proto, že se banky staly běžnou součástí našeho života a člověk je v zásadě potřebuje stále víc i proto, že mu usnadňují život, jsou vztahy mezi uživatelem služeb bank, tedy občanem, fyzickou osobou, nebo chceme-li, subjektem údajů a bankou velmi specifické. Zmíněný právní rámec tvoří celý komplex zákonů a podzákonných norem, z nichž je třeba zmínit minimálně zákon č.21/1992 Sb. o bankách, ve znění pozdějších předpisů (dále jen „zákon o bankách“), zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (dále jen „ zákon o opatřeních proti legalizaci výnosů z trestné činnosti“)a zákon č. 284/2009 Sb., zákon o platebním styku. Složitost a komplikovanost vztahů klientů a bank a snaha o řešení některých sporů

[30] Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

[31] Ministerstvo vnitra České republiky, [online] ©2015 [cit. 2015-02-22].Dostupné z:http://www.mvcr.cz/clanek/vyhlasky.aspx

pokud možno mimosoudní cestou vyústily v přijetí zákona č. 229/2002 Sb., o finančním arbitrovi. Existují však také zákonné normy, které nejsou běžnou veřejností příliš vnímány. Jedná se např. o zákon č. 254/2004 Sb., o omezení plateb v hotovosti a o změně zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů. Součástí právního rámce je také samozřejmě zákon č.40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „ ObčZ“) a zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů (dále jen „ ObchZ“), a velké množství podzákonných předpisů, které podrobněji upravují některé činnosti v bankovnictví, tedy zejména vyhlášky České národní banky. [32]

zákon č. 21/1992 Sb., o bankách

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

zákon č. 26/2000 Sb., o veřejných dražbách

- **daňové řízení**

zákon č. 337/1992 Sb., o správě daní a poplatků

- **doprava**

zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu)

zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích a o změně zákona č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla), ve znění zákona č. 307/1999 Sb.

[32] BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: vybrané problémy*, s.11-12

Zákon č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla) [33]

elektronická veřejná správa (e-government)

zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

zákon č. 111/2009 Sb., o základních registrech

- **elektronické komunikace**

zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

evidence obyvatel, matriky a notáři

zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)

zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů

zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení

zákon č. 344/1992 Sb., o katastru nemovitostí České republiky (katastrální zákon)

zákon č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky

zákon č. 283/1993 Sb., o státním zastupitelství

zákon č. 153/1994 Sb., o zpravodajských službách České republiky

[33] Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

zákon č. 269/1994 Sb., o Rejstříku trestů

zákon č. 89/1995 Sb., o státní statistické službě

zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činností bývalé Státní bezpečnosti

zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů

zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu)

zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

zákon č. 108/2006 Sb., o sociálních službách

zákon č. 111/2006 Sb., o pomoci v hmotné nouzi

- **kamerové systémy**

zákon č. 273/2008 Sb., o Policii České republiky

zákon č. 553/1991 Sb., o obecní policii

zákon č. 262/2006 Sb., zákoník práce

zákon č. 129/2008 Sb., o výkonu zabezpečovací detence a o změně některých souvisejících zákonů

zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních a o změně dalších zákonů

zákon č. 202/1990 Sb., o loteriích a jiných podobných hrách

- **kasina**

zákon č. 202/1990 Sb., o loteriích a jiných podobných hrách [34]

vyhláška Ministerstva financí 285/1998 Sb. - Vyhláška o podmínkách monitorování a uchovávání záznamů v kasinu[35]

- **katastr nemovitostí**

zákon č. 344/1992 Sb., o katastru nemovitostí České republiky (katastrální zákon)

nevyžádaná obchodní sdělení

zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

- **osobní doklady**

zákon č. 328/1999 Sb., o občanských průkazech zákaz používat občanský průkaz jako zástavu nebo jej odebírat při vstupu do objektů či na pozemek (§ 2 odst. 5) zákaz pořizovat kopie občanského průkazu bez souhlasu jeho držitele (§ 2 odst. 6)

zákon č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Polici České republiky, ve znění pozdějších předpisů (zákon o cestovních dokladech) zákaz používat cestovní doklad jako zástavu nebo jej odebírat při vstupu do objektů či na pozemek (§ 2 odst. 2), zákaz pořizovat kopie cestovního dokladu bez souhlasu jeho držitele (§ 2 odst. 3)

zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu), zákaz používat řidičský průkaz jako zástavu nebo jej

[34] Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

[35] Zákonyprolidi.cz, [online]. [cit. 2014-11-22]. Dostupné z: http://www.zakonyprolidi.cz/hledani?text=kasina+

odebírat při vstupu do objektu či na pozemek (§ 103), údaje zapisované do řidičského průkazu a mezinárodního řidičského průkazu, změna údajů (§ 105 až § 108)

zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů

zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů

zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)

zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

zákon č. 18/2004 Sb., o uznávání odborné kvalifikace a jiné způsobilosti státních příslušníků členských států Evropské unie a některých příslušníků jiných států a o změně některých zákonů (zákon o uznávání odborné kvalifikace)

- **pojišťovnictví**

zákon č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla)

zákon č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky

zákon č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách

zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění

zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů

zákon č. 187/2006 Sb., o nemocenském pojištění

- **policejní postupy, veřejný pořádek, vnitřní a vnější bezpečnost**

zákon č. 273/2008 Sb., o Policii České republiky

zákon č. 553/1991 Sb., o obecní policii

zákon č. 185/2004 Sb., o Celní správě České republiky

zákon č. 283/1993 Sb., o státním zastupitelství

zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

zákon č. 269/1994 Sb., o Rejstříku trestů

zákon č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky

zákon č. 129/2008 Sb., o výkonu zabezpečovací detence a o změně některých souvisejících zákonů

zákon č. 325/1999 Sb., o azylu a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o azylu)

zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů

zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

zákon č. 153/1994 Sb., o zpravodajských službách České republiky

zákon č. 154/1994 Sb., o Bezpečnostní informační službě

zákon č. 289/2005 Sb., o Vojenském zpravodajství

zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon)

zákon č. 119/2002 Sb., o střelných zbraních a střelivu a o změně zákona č. 156/2000 Sb., o ověřování střelných zbraní, střeliva a pyrotechnických předmětů a o změně zákona č. 288/1995 Sb., o střelných zbraních a střelivu (zákon o střelných zbraních), ve znění zákona č. 13/1998 Sb., a zákona č. 368/1992 Sb., o správních poplatcích, ve znění pozdějších předpisů, a zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, (zákon o zbraních)

- **poskytování informací veřejnou správou, veřejné rejstříky a evidence**

zákon č. 106/1999 Sb., o svobodném přístupu k informacím

zákon č. 123/1998 Sb., o právu na informace o životním prostředí

zákon č. 159/2006 Sb., o střetu zájmů

zákon č. 273/2008 Sb., o Policii České republiky

zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

zákon č. 128/2000 Sb., o obcích (obecní zřízení)

zákon č. 129/2000 Sb., o krajích (krajské zřízení)

zákon č. 131/2000 Sb., o hlavním městě Praze

zákon č. 513/1991 Sb., obchodní zákoník

zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon)

zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon)

zákon č. 36/1967 Sb., o znalcích a tlumočnících

zákon č. 85/1996 Sb., o advokacii

zákon č. 262/2006 Sb., zákoník práce

zákon č. 435/2004 Sb., o zaměstnanosti

zákon č. 251/2005 Sb., o inspekci práce [36]

[36]Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

- **Pracovně právní vztahy, zaměstnanost**

Ochrana soukromí zaměstnanců

Ochrana soukromí a osobních údajů zaměstnanců podléhá kromě zákona o ochraně osobních údajů i právní úpravě v zákoníku práce. Zaměstnavatel má právo kontrolovat, jak zaměstnanec plní pracovní úkoly a zda používá pracovní pomůcky, včetně prostředků výpočetní techniky, v souladu s pokyny a interními předpisy zaměstnavatele, na druhé straně zaměstnanec má právo na respektování svého soukromí v přiměřené míře i na pracovišti. Právě střet těchto dvou zájmů může vyústit v konfliktní situace, pro jejichž řešení je nezbytný správný výklad dotčených ustanovení obou právních předpisů. [37]

Související ustanovení zákoníku práce

§ 316 Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance

Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.

Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.

Zaměstnavatel nesmí vyžadovat od zaměstnance informace, které bezprostředně nesouvisející s výkonem práce a se základním pracovně-právním vztahem uvedeným v § 3. Nesmí vyžadovat informace zejména o těhotenství, rodinných a majetkových poměrech, sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách

[37] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s. 140

nebo hnutích, příslušnosti k církvi nebo náboženské společnosti, trestněprávní bezúhonnosti.[38]

zákon č. 262/2006 Sb., zákoník práce

zákon č. 435/2004 Sb., o zaměstnanosti

zákon č. 251/2005 Sb., o inspekci práce

- **předávání osobních údajů do zahraničí**

výjimku z povinnosti podle § 27 odst. 4 zákona č. 101/2000 Sb. žádat Úřad pro ochranu osobních údajů o vydání povolení upravují tato ustanovení:

§ 2 odst. 1 písm. i) zákona č. 381/1991 Sb., o Komoře veterinárních lékařů České republiky

§ 22a odst. 3 zákona č. 360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě

§ 23a odst. 2 písm. c) zákona č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky

§ 12i odst. 2 písm. b) zákona č. 283/1993 Sb., o státním zastupitelství

§ 71a zákona č. 325/1999 Sb., o azylu a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o azylu)

§ 35 odst. 3 zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí

§ 54 zákona č. 221/2003 Sb., o dočasné ochraně cizinců

§ 5b odst. 3 zákona č. 185/2004 Sb., o Celní správě České republiky

§ 17 odst. 3 zákona č. 435/2004 Sb., o zaměstnanosti

§ 119 odst. 4 zákona č. 187/2006 Sb., o nemocenském pojištění

[38] Zákon č. 262/2006 Sb., zákoník práce. [online]. [cit. 2014-11-22] .Dostupné z: http://business.center.cz/business/pravo/zakony/zakonik-prace/cast13h8.aspx

§ 39 odst. 2 písm. c) zákona č. 129/2008 Sb., o výkonu zabezpečovací detence a o změně některých souvisejících zákonů

§ 80 zákona č. 273/2008 Sb., o Policii České republiky

- **rodná čísla**

zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), rodné číslo, jeho definice a struktura, přidělení, doklad o přidělení, registr rodných čísel, rámec oprávnění k jeho užívání nebo rozhodování o jeho využívání (§ 13 až 17c), přestupky a jiné správní delikty spočívající v neoprávněném nakládání s rodným číslem nebo v neoprávněném využívání rodných čísel (§ 17d a § 17e)

- **rozhlasové a televizní poplatky**

zákon č. 348/2005 Sb., o rozhlasových a televizních poplatcích a o změně některých zákonů

- **sociální zabezpečení**

zákon č. 100/1988 Sb., o sociálním zabezpečení, náležitosti průkazu mimořádných výhod (§ 86), ohlašovací povinnost občanů (§ 106)

zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, povinnost mlčenlivosti, poskytování informací (§ 11 až § 16a), poskytování údajů z informačního systému evidence obyvatel v souvislosti s prováděním sociálního zabezpečení (§ 11a) , registr pojištěnců (§ 16c)

zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, uschovávání účetních záznamů (§ 22c)

zákon č. 108/2006 Sb., o sociálních službách, informační systém o příspěvku na péči (§ 30), poskytování údajů z informačního systému evidence obyvatel a registru rodných čísel pro účely příspěvku na péči (§ 30 odst. 3 a 4)

zákon č. 111/2006 Sb., o pomoci v hmotné nouzi, informační systém pomoci v hmotné nouzi (§ 52), poskytování údajů z informačního systému evidence obyvatel orgánům pomoci v hmotné nouzi (§ 53)

zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), poskytování údajů Českou správou sociálního zabezpečení Ministerstvu vnitra (§ 22c)

- **statistická zjišťování**

zákon č. 89/1995 Sb., o státní statistické službě, vymezení pojmů týkajících se osobních údajů a identifikace (§2), rozsah osobních údajů shromažďovaný při statistickém zjišťování (§8), využití administrativních zdrojů údajů (§9), oprávnění Českého statistického úřadu k přístupu k údajům informačního systému evidence obyvatel (§ 9a), povinnost mlčenlivosti a poskytování osobních údajů jiným subjektům (§ 16 a § 17), statistické registry (§ 19a až § 20b).

- **školství**

zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), dokumentace škol a rozsah osobních údajů vedený ve školní matrice (§ 28 odst. 1 až 4), sdružování údajů z dokumentace škol a školních matrik Ministerstvem školství (§ 28 odst. 5).

zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), náležitosti přihlášky ke studiu na vysoké škole (§ 50 odst. 1), matrika studentů a rozsah zde vedených údajů, sdělování údajů z matriky (§ 88).

zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních a o změně dalších zákonů, audiovizuální systémy, možnosti jejich využití (§ 15).

- **územní samospráva**

zákon č. 128/2000 Sb., o obcích (obecní zřízení), právo nahlížet do usnesení a zápisů z jednání zastupitelstva, do usnesení rady, výborů zastupitelstva a komisí rady a pořizovat si z nich výpisy [§ 16 odst. 2 písm. e)], zveřejnění informace o záměru obce nakládat se svým majetkem (§ 39 odst. 1), informování o programu zasedání zastupitelstva, veřejnost zasedání, zápis o průběhu zasedání (§ 93 a § 95), nahlížení do zápisu ze schůze rady obce (§ 101 odst. 3)

zákon č. 129/2000 Sb., o krajích (krajské zřízení), právo nahlížet do usnesení a zápisů z jednání zastupitelstva, do usnesení rady, výborů zastupitelstva a komisí rady a pořizovat si z nich výpisy [§ 12 odst. 2 písm. c)], zveřejnění informace o záměru kraje nakládat se svým majetkem (§ 18 odst. 1), informování o programu zasedání zastupitelstva, veřejnost zasedání, zápis o průběhu zasedání (§ 42 odst. 1 a § 43), nahlížení do zápisu ze schůze rady kraje (§ 58 odst. 3).

zákon č. 131/2000 Sb., o hlavním městě Praze, právo nahlížet do usnesení a zápisů z jednání zastupitelstva hlavního města Prahy, do usnesení rady hlavního města Prahy, výborů zastupitelstva hlavního města Prahy a komisí rady hlavního města Prahy a pořizovat si z nich výpisy [§ 7 písm. e)], zveřejnění informace o záměru hlavního města Prahy nebo městské části nakládat se svým majetkem (§ 36 odst.1), informování o programu zasedání zastupitelstva hlavního města Prahy, veřejnost zasedání, zápis o průběhu zasedání (§ 60 a § 65), nahlížení do zápisu ze schůze rady hlavního města Prahy (§ 70 odst. 3).

zákon č. 553/1991 Sb., o obecní policii, oprávnění vyžadovat poskytnutí údajů z informačních systémů (§ 11a), oprávnění strážníka požadovat prokázání totožnosti (§ 12), pravidla pro zpracování osobních údajů obecní policií (§ 24a), oprávnění obecní policie k pořizování zvukových, obrazových nebo jiných záznamů (§ 24b).

zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, obsah petice voličů podporujících kandidaturu volební strany a obsah kandidátní listiny (§ 21 a § 22), stálý seznam voličů (§ 28).

- **volby**

zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů, zvláštní seznam voličů (§ 6), náležitosti kandidátní listiny (§ 32)

zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, obsah petice voličů podporujících kandidaturu volební strany a obsah kandidátní listiny (§ 21 a § 22), stálý seznam voličů (§ 28).[39]

[39] Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

- **zdravotnictví**

Ke zpracování osobních údajů nevyhnutelně dochází i v souvislosti s pokytováním zdravotní péče, jehož nedílnou součástí by měla být i ochrana soukromí. Zejména v situacích, kdy se jedná o lidské zdraví, jsou lidé velmi citliví nejen na kvalitu péče, ale také a to stále více na informace a údaje, které jsou o nich vedeny ve zdravotnické dokumentaci, a rovněž na to, kdo má k těmto informacím přístup, tedy jinak řečeno, kdo se může seznámit s údaji o jejich zdravotním stavu. Lékaří vždy vedli zdravotnickou dokumentaci a poskytovali informace o zdravotním stavu nejen svým pacientům, ale i příbuzným, případně pozůstalým. Právní úprava všech těchto záležitostí se vyvíjela postupně, a to od stavu, kdy úprava absentovala prakticky absolutně, až po stav, kdy jsou stanovena poměrně přesná a podrobná pravidla, jak se zdravotní dokumentací zacházet a jak a komu poskytovat informace.[40]

Zákon č. 20/1966 Sb., o péči o zdraví lidu, povinnost mlčenlivosti zdravotnických pracovníků [§ 55 odst. 2 písm. d)], vedení zdravotnické dokumentace, její rozsah a obsah, právo nahlížet do zdravotnické dokumentace (§ 67a a § 67b), národní zdravotnický informační systém a jeho registry (§ 67c až § 67e), poskytování údajů z informačního systému evidence obyvatel v souvislosti se zdravotnickou péčí (§ 67g až § 67i).

zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, poskytování údajů z informačního systému evidence obyvatel orgánům veřejného zdraví (§ 47b), předávání údajů orgánům ochrany veřejného zdraví v souvislosti s očkováním (§ 51 a § 52) , povinnost zdravotnického zařízení hlásit orgánu ochrany veřejného zdraví osobní údaje fyzických osob trpících infekčními onemocněními, která vylučují choroboplodné zárodky (§ 54) , hlášení infekčních nemocí (§ 62 odst. 1) , sběr a zpracování osobních údajů orgány ochrany veřejného zdraví (§ 79).

zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), ochrana subjektů hodnocení (§ 52 odst. 1), centrální úložiště elektronických receptů (§ 81)

zákon č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, informační systém Všeobecné zdravotní pojišťovny, povinnost mlčenlivosti (§ 24 až § 24c)

[40] BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: vybrané problémy*, s.99

zákon č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách, informační systém zaměstnanecké pojišťovny, povinnost mlčenlivosti (§ 21 a § 22)

zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, povinnost mlčenlivosti, poskytování údajů zdravotní pojišťovnou (§ 23).

zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, náležitosti průkazu pojištěnce (§ 40 odst. 3 a 4), seznam nositelů výkonů (§ 40 odst. 5), informační centrum zdravotního pojištění (§ 41)

zákon č. 187/2006 Sb., o nemocenském pojištění, sdělování údajů a informační systémy pojištění (§ 113 až § 123), povinnost zachovávat mlčenlivost (§ 113), sdělování údajů (§ 114 až § 119), informační systémy pojištění (120 až § 123)

zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), národní zdravotní registry související s transplantacemi (§ 18) [41]

[41] Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

3.15 Legislativa v USA

3.16 Obecné zákony

Jaké právní předpisy upravují shromažďování a využívání osobních údajů?

V USA neexistuje jediný, komplexní federální (národní) právní předpis upravující shromažďování a využívání osobních údajů. Místo toho, USA má tzv. “patchwork” systém federálních a státních zákonů a předpisů, které se navzájem překrývají a mohou si vzájemně protiřečit. Kromě toho, existuje mnoho směrnice, které jsou vypracované vládními agenturami a průmyslovými skupinami, které nejsou právně vymahatelné, ale jsou součástí samoregulačních snah a jsou považovány za "nejlepší praxi". V posledních letech se rozšířilo narušení bezpečnosti a to vedlo k rozšíření „patchwork" systému“ týkajícího se zákonů na ochranu soukromí, předpisů a směrnic, které se stávají jedním z nejrychleji rostoucích oblastí právní úpravy.

Kombinace zvýšení mezistátního a přeshraničního toku dat, spolu s větším přijetím souvisejících zákonů na ochranu osobních údajů zvyšuje riziko porušování soukromí a vytváří významnou výzvu pro správce údajů vyjednávat svazující a často rozporné požadavky pro každý stát při provozu na národní úrovni.

Významný zákonodárný vývoj v letech 2013 a 2014:

Dva nové zákony v Kalifornii. První poskytuje mladistvým "právo být zapomenut" on-line. Další vyžaduje, aby internetové stránky uživatelům sdělovaly, zda se ctí právo uživatele nebýt sledován.

Nové rozhodnutí IAB (Interactive Advertising Bureau) o shodě a dodržování samoregulačního programu pro v oblasti bezpečnosti behaviorální reklamy a internetového vyhledávání.

Rozhodnutí z Nejvyššího soudu státu Massachusetts, podle kterého poštovní směrovací čísla mohou představovat osobní údaje.

Prováděcí příkaz prezidenta Baracka Obamy o kyberbezpečnosti, kterým se stanoví rámec pro ochranu vlády a klíčové infrastruktury proti kybernetickým útokům.[42]

3.17 Federální zákony na ochranu soukromí

Federální komise pro obchod (FTC, Federal Trade Commissionn) i nadále aktivně prosazuje dodržování zákonů a nařízení v oblasti ochrany soukromí a na ochranu dat. V roce 2013-14, Federální komise pro obchod učinila následující opatření:

Vznesla obvinění proti mobilní aplikaci Flashlight (Svítilna), která sdílela s inzerenty lokace uživatelů i jedinečnou identifikaci zařízení, aniž by o tom uživatele uvědomila či si vyžádala jejich souhlas.

Vyřešila spor se zdravotnickou fakturační firmou, obviněnou z toho, že svým zákazníkům nedokázala zajistit dostatečnou a účinnou ochranu osobních a soukromých údajů včetně citlivých medicinských záznamů.

Ohlásila vypořádání donucovacích opatření nařízených proti firmám, které nepravdivě tvrdily, že mají vlastní certifikace splňující požadavky programu „bezpečný přístav“ (EU-US Safe Harbor cross-border data protection program).

Obvinila firmu, která provozovala internetové kamery, aniž by přijala dostatečná bezpečností opatření, čímž umožnila komukoli, kdo znal internetovou adresou kamery, sledovat její přímé přenosy.

V roce 2012 dodatkovala Zákon na ochranu dětí online (COPPA), s tím, že změny vešly v platnost hned následujícího roku. Klíčová změna se týká rozšíření definice osobní informace tak, že zahrnuje i využití geolokační data a souborů cookies.

Federální ministerstvo zdravotnictví a sociálních služeb (HHS) oznámilo vyrovnání v žalobě týkající se nedodržení federálních předpisů o nahlížení do lékařských záznamů (na základě zákona o zdravotním pojištění HIPAA) a zaplacení pokuty 1,5 milionu US dolarů zdravotní pojišťovnou za údajné narušení HIPAA. HHS také vydal novou směrnici „Omnibus“ (Omnibus Rule), které reviduje směrnice HIPAA o utajení, bezpečnosti, oznámení o narušení bezpečnosti a prosazení práva (Privacy, Security, Breach Notification

[42]Data protection in United States ©2014 [cit. 2015-02-27]. Dostupné z: http://uk.practicallaw.com/6-502-0467

and Enforcement Rules). Směrnice Omnibus je účinná od 26. března 2013 a shoda s ní je závazná pro většinu smluvních klauzulí nejpozději od 23. září 2013.

V roce 2014 byly přijaty následující federální zákony na ochranu osobních údajů:

S. 1995 (o ochraně osobních údajů a odpovědnosti při narušení bezpečnosti zákon roku 2014, Personal Data Protection and Breach Accountability Act of 2014), který výžaduje aby podnikatelské subjekty, učinily všechny následujících kroky:

- zavedení komplexního programu, který zajišťuje soukromí, bezpečnost a důvěrnost citlivých osobních údajů;
- stanovení rizik budoucích narušení bezpečnosti a navržení programu bezpečnosti a kontroly ochrany osobních údajů;
- ustanovení postupu na federální úrovni pro oznamování narušení bezpečnosti;

S. 2025 (Data Broker Accountability Act a Transparency)- návrh zákona vyžadujícího, aby datoví makléři stanovili přiměřené postupy pro zajištění co největší přesnosti osobních údajů, které shromažďují, sestavují nebo spravují. To poskytne spotřebitelům právo na přezkoumání údajů shromážděných datovými makléři a umožní jim zabránit tomu, aby jejich osobní údaje byly sdílené pro marketingové účely.

Reklamní průmysl pokračuje v budování svých samoregulačního programu pro internetové behaviorální reklamy. Tento program vyžaduje, aby členové různých obchodních, reklamních a průmyslových skupin postupovali v souladu se zásadami dané skupiny pro on-line behaviorální reklamu, které do značné míry odrážejí hlavní direktivy FTC. Program obsahuje ikonu, kterou by členové skupiny měli umístit na svých internetových stránkách, shromažďují-li či sledují data. Ikona odkazuje na informace o způsobu sběru dat a informuje o tom, jak se uživatel webové stránky může určitému sledování vyhnout. Několik rozhodnutí ohledně dodržování tohoto programu bylo zveřejněno v roce 2013. Týkala se firem, které informaci o sledování na své stránky neumístilo, ačkoli tam ke sledování docházelo nebo obsahovaly cílenou reklamu.

3.18 Odvětvové zákony

Existuje mnoho federálních zákonů spojených s ochranou soukromí, které upravují shromažďování a používání osobních údajů. Některé se týkají určitých kategorií informací, jako například finančních nebo zdravotních, či informací o elektronické komunikaci. Jiné upravují činnosti, při kterých se osobní informace používají, jako například telemarketing a komerční e-mailová sděleni. Navíc existuje širší zákony spotřebitelské ochrany, které jako takové nejsou zákony na ochranu soukromí, ale jsou aplikovány proti nekalým a podvodným praktikám a cílem odhalit osobní informace.

Mezi nejvýznamnější federální zákony na ochranu soukromí patří následující:

The Federal Trade Commission Act (15 U.S.C. §§41-58; FTC Act) je federální zákon na ochranu spotřebitele, který postihuje nekalé a podvodné praktiky. Je aplikován na bezpečnostní postupy ohledně offline i online údajů. Na základě tohoto zákona je prosazováno právo proti společnostem, které při nakládání s osobními údaji nedodržují bezpečnostní postupy a u kterých dochází k neoprávněnému prozrazení těchto údajů. Uvedený zákon je také primárním prostředkem k prosazování zákona na ochranu soukromí dětí Children's Online Privacy Protection Act (COPPA; 15 U.S.C. §§6501-6506), který se týká online shromažďování informací od dětí, a prostředkem k prosazování zásad samoregulace v oblasti behaviorální reklamy (Self-Regulatory Principles for Behavioural Advertising).

Zákon o modernizaci finančních služeb (The Financial Services Modernization Act, Gramm-Leach-Bliley Act (GLB Act), 15 U.S.C. §§6801-6827) upravuje sbírání, užívání a zveřejňování finančních informací. Lze jej široce aplikovat na takové finanční instituce, jako jsou banky, bezpečnostní služby, pojišťovny a další firmy, které poskytují finanční služby a produkty. Tento zákon omezuje prozrazení neveřejných osobních informací a v některých případech nutí finanční instituce, aby informovaly o své bezpečnostní politice, a poskytuje osobám možnost vyslovit nesouhlas se zveřejněním či sdílením jejich osobních informací. Kromě toho existuje řada bezpečnostních norem (Privacy Rules) schválených národními bankovními orgány a Pravidlo bezpečnostních pojistek (Safeguards Rule), Pravidlo odstranění (Disposal Rule) a Pravidlo signálů (Red Flags Rule) vyhlášené Federální agenturou na ochranu spotřebitele (FTC), které se vztahují na ochranu a odstranění finančních údajů.

Zákon o přenositelnosti a kontinuitě zdravotního pojištění (The Health Insurance Portability and Accountability Act, HIPAA; 42 U.S.C. §1301 et seq.) reguluje nakládání se zdravotními informacemi. Lze jej široce uplatňovat na poskytovatele zdravotní péče, zpracovatele dat, farmaceutické a jiné subjekty, které přicházejí do styku se zdravotními informacemi. Soubor norem týkajících se soukromí zdravotních údajů (Standards for Privacy of Individually Identifiable Health Information, HIPAA Privacy Rule;45 C.F.R. Parts 160 and 164) se zabývá shromažďováním a manipulací s chráněnými zdravotními údaji. Další normy jsou stanoveny pro elektronické zpracování lékařských informací (Security Standards for the Protection of Electronic Protected Health Information, HIPAA Security Rule; 45 C.F.R. 160 and 164). Také elektronické přenášení lékařských informací je chráněno předpisy (Standards for Electronic Transactions, HIPAA Transactions Rule; 45 C.F.R. 160 and 162). Na počátku roku 2013 byly všechny tyto směrnice zkorigovány podle „směrnice Omnibus“. Jejich dodržování je povinné od 23. září 2013.

Směrnice Omnibus také zkorigovala nařízení o oznámení o narušení bezpečnosti (Security Breach Notification Rule, 45 C.F.R. Part 164), které vyžaduje, aby instituce, které přímo zpracovávají osobní zdravotní údaje, informovaly o narušení utajení těchto údajů. Podle upraveného znění musí tyto instituce oznámit získání zdravotních údajů, přístup k nim, použití nebo odtajnění přestupující bezpečnostními normou Privacy Rule. Výjimkou z této povinnosti je situace, kdy uvedené instituce prokáží, že existuje jen malá pravděpodobnost zneužití chráněných zdravotních informací.

Dodatky k zákonu o čestném hlášení zůstatku (Fair Credit Reporting Act; 15 U.S.C. §1681; a Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159) doplňují zákon o čestném hlášení zůstatku (Fair Credit Reporting Act). Týkají se firem, které podávají a používají reporty o spotřebitelích (jako například poskytovatelé půjček a společnosti vydávající kreditní karty/úvěrových společností). Za report spotřebiteli se označuje jakákoli komunikace ze strany takové společnosti, která se používá pro stanovení způsobilosti spotřebitele k získání úvěru či pojištění a týká se jeho bonity, úvěrové historie, úvěruschopnosti, povahy a celkové pověsti.

Shromažďování a používání e-mailových adres a telefonních čísel upravují následující zákony: zákon na ochranu před nevyžádanou pornografií a marketingem (Controlling the Assault of Non-Solicited Pornography and Marketing Act, CAN-SPAM Act; 15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) a zákon na ochranu spotřebitele při telefonním kontaktu (Telephone Consumer Protection Act, 47 U.S.C. §227 et seq.)

Odposlechy a zachycování elektronické komunikace se zabývá zákon o elektronickém soukromí (Electronic Communications Privacy Act (18 U.S.C. §2510) a zákon o neoprávněné a podvodné manipulaci s počítači (Computer Fraud and Abuse Act,18 U.S.C. §1030). Hromadná stížnost podaná roku 2008 upozornila na to, že poskytovatelé internetových služeb a společnost pro cílenou reklamu porušili uvedená ustanovení tím, že pomocí technologie DPI (Deep Packet Inspection) odposlouchávali údaje posílané mezi soukromými počítači a servery poskytovatelů internetových služeb.

3.19 Další zákony a nařízení

Existuje mnoho federálních zákonů o bezpečnosti a zákonů na prosazování práva, které upravují používání osobních údajů, ty však leží mimo téma této kapitoly. Mimo výše uvedené zákony, je mnoho nařízení vydaných průmyslovými skupinami. Tato nařízení nejsou právně vymahatelná, ale jsou všeobecně uznávanými „nejlepšími postupy“ v daných odvětvích (například v oblasti platebních karet, mobilního marketingu či online reklamy).

3.20 Státní zákony na ochranu soukromí

Mnoho zákonů na úrovni státu reguluje shromažďování a používání osobních údajů a jejich počet každoročně roste. Některé z nich jsou předjímány federálními zákony na dané téma. Například federální zákon o komerčních e-mailech a sdílení e-mailových adres předjímá většinu státních zákonů upravujících tyto oblasti. Naproti tomu je mnoho federálních zákonů ochraňujících soukromí, které státní zákony nepředcházejí. To znamená, že firma může zjistit, že usiluje o dodržování federálních a státních zákonů, které však regulují stejný typ údajů (například lékařské a zdravotní) nebo stejnou činnost.

Většina států schválila nějakou formu legislativní ochrany soukromí. V čele však stojí stát Kalifornie, který uzákonil množství těchto zákonů, z nichž některé mají dalekosáhlý dopad na i národní úrovni. Na rozdíl od mnoha federálních zákonů na ochranu soukromí lze v kalifornských zákonech najít podobnost s evropským přístupem k této problematice.

Například zákon Shine the Light (Osvětlit), (Cal. Civil Code. §§1798.83-1798.84), požaduje, aby společnosti oznamovaly podrobnosti ohledně třetích stran, s nimiž sdílejí osobní informace. Zákon o bezpečnosti dat (Data security law, Cal. Civil Code §1798.81.5) ukládá firmám zajišťovat a udržovat přiměřené bezpečnostní postupy na ochranu osobních informací před neoprávněným přístupem, poškozením, zneužitím, úpravou či zveřejněním. Kalifornie také patří k oněm nemnoha státům, které na ochranu soukromí vytvořily úřad (Office of Privacy Protection, www.privacy.ca.gov).

Kalifornie byla také první stát, který schválil zákon o oznámení narušení bezpečnosti (California Civil Code §1798.82). Tento zákon ukládá každé osobě i každé firmě, která vlastní nebo licencuje počítačová data obsahující osobní informace, aby oznámila jakékoli narušení bezpečnosti systému všem obyvatelům Kalifornie, jejichž nešifrovaná data byla narušitelem získána.

Většina předchozích zákonů o oznámení narušení zrcadlila Kalifornský zákon a přikláněla se k reaktivním opatřením, tj. požadovala uplatňování odvetných opatření. Teprve v poslední době byla přijata hrstka státních zákonů, které jsou normativní a preventivní. To znamená, že tyto zákony jsou tvrdší a svou kodifikací de facto snižují nebezpečí narušení bezpečnosti. Nejlepším příkladem preventivního zákona je Massachusetts Regulation (201 CMR 17.00), který značně detailně předepisuje rozsáhlý seznam technických, fyzických a administrativních bezpečnostních pravidel zaměřených na ochranu osobních informací. Všechny společnosti, kterých se to týká, je musí zabudovat do své bezpečnostní architektury a detailně je písemnou formou specifikovat v plánu informační bezpečnosti.

Všechny státy včetně District of Columbia, Portorika a americké části Panenských ostrovů uzákonily v březnu 2014 požadavek oznámení narušení bezpečnosti osobních informací. Přinejmenším 29 států zavedlo zákon vyžadující zničení, odstranění či jiné znečitelnění osobních dat.

V roce 2013 zavedla Kalifornie dva nové zákony týkající se soukromí. Kalifornský zákon o ochraně soukromí a internetu (Online Privacy Protection Act) požaduje, aby komerční webové stránky a online služby uvedly ve známost následující skutečnosti:

- jak nakládají s požadavkem osob pohybujících se na internetu nebýt sledován.

- zda a jak třetí strany shromažďují od návštěvníků webových stránek identifikační informace.

Nový zákon, který začal platit od 1. ledna 2014, se vztahuje na jakéhokoli provozovatele komerční webové stránky nebo online služby shromažďujícího osobní identifikační informace o residentovi státu Kalifornie, bez ohledu na to, zda má provozovatel fyzické sídlo v Kalifornii nebo ne. Kalifornie také přijala zákon, který poskytuje návštěvníkům webových stránek mladším 18 let právo vymazat obsah, který na stránky poslali. Podle tohoto zákona, který platí od 1. ledna 2015, je provozovatel webové stránky, online služby, online aplikace nebo mobilní aplikace povinen umožnit mládeži pod 18 let odstranit obsah, který tam vložili, nebo požadovat jeho odstranění.

Tato kapitola se zabývá: Federálním zákonem na ochranu spotřebitele (FTC Act) a několika nařízeními a principy prosazovanými Federální agenturou na ochranu spotřebitele (Federal Trade Commission , FTC) Zákonem Gramm-Leach-Bliley (GLB Act) upravujícím finanční informace.HIPAA upravujícím lékařské informace. Následující dva zákony jsou nejvýznamnějšími státními zákony odrážející se v mnoha pozdějších státních zákonech.

3.20.1 Rozsah legislativy

Zákon FTC platí pro většinu firem a podnikajících fyzických osob v USA, kromě určité dopravy, telekomunikačních společností a finančních společností (neboť tato odvětví jsou primárně upraveny jinými národními agenturami). FTC principy jsou dobrovolné povahy, i když mnoho firem je považují za "nejlepší praxi". Platí pro provozovatele webových stránek, které se angažují v kontextové a cílené reklamě.

Zákon GLB platí pro finanční instituce, které provádí finanční činnosti. Například pro instituce jako jsou banky, obchodníci s cennými papíry a pojišťovny. Vztahuje i na třetí osoby, které nejsou finančními institucemi, ale které dostávají neveřejné osobní informace přidružených finančních institucí.

HIPAA. Týká se institucí přímo zpracovávajících osobní zdravotní údaje i jejich obchodních společníků. Tyto instituce zahrnují poskytovatele zdravotních programů, instituce shromažďující, třídící a distribuující zdravotní informace a poskytovatele zdravotní péče, kteří provádějí určité finanční a administrativní úkony elektronicky. Obchodní společník je osoba nebo subjekt, který za nebo pro instituci zpracovávající zdravotní údaje vykonává určité funkce nebo činnosti vyžadující použití nebo zveřejnění osobních zdravotních údajů**.**Zpracování pohledávek a administrace**,** analýza a zpracování dat**,** záruka kvality**,** fakturace**,** řízení benefitů.

Zákon státu Kalifornie o oznámení narušení bezpečnosti. Vztahuje se na jakoukoliv osobu nebo firmu, která podniká v Kalifornii a vlastní či licencuje digitalizovaná data obsahující osobní informace.

3.20.2 Jaké údaje jsou regulovány?

Federální zákon na ochranu spotřebitele (FTC Act) se nezabývá kategoriemi údajů, ale zakazuje nečestné nebo podvodné jednání, které by ovlivnilo osobní údaje spotřebitele. Zásady behaviorální reklamy vyhlášené Federální agenturou na ochranu spotřebitele (FTC) se vztahují na dlouhodobé sledování online chování spotřebitele včetně jeho vyhledávání, navštívených webových stránek a obsahu, který prohlíží za účelem zasílání reklamy cílené na jeho osobní zájmy.

Zákon Gramm-Leach-Bliley (GLB Act) se vztahuje na neveřejné osobní informace shromažďované finančními institucemi. Jde o informace poskytnuté nebo jinak získané od spotřebitelů či zákazníků, kteří od finanční instituce obdrželi finanční produkt nebo služby primárně pro osobní nebo rodinné účely.

Spotřebitel (uživatel) je ten, kdo od finanční instituce získal finanční produkt nebo službu, ale neudržuje s ní žádný další vztah. Může to být například někdo, kdo si nechal proplatit šek u šekové společnosti nebo provedl elektronický převod či požádal o půjčku. Zákazník je podskupinou spotřebitele. Je to někdo, kdo má s institucí pokračující vztah. Neveřejné osobní informace, na které se vztahuje GLB Act se týkají informací, které nejsou veřejně dostupné a které mohou spotřebitele nebo zákazníka osobně identifikovat.

HIPAA upravuje chráněné identifikační zdravotní a lékařské informace uchovávané nebo sdílené institucí přímo zpracovávající tyto informace nebo jejími obchodními partnery.

Zákon státu Kalifornie o oznámení narušení bezpečnosti reguluje osobní informace, tj. jméno nebo jeho iniciálu a příjmení v kombinaci s jedním nebo více dole uvedenými údaji, pokud jméno nebo prvky dat nejsou zašifrovány:

- číslo sociálního pojištění
- číslo řidičského průkazu nebo číslo identifikačního průkazu státu Kalifornie
- číslo účtu, kreditní nebo debetní karty v kombinaci s jakýmkoli požadovaným bezpečnostním kódem, přístupovým kódem nebo heslem, které umožňují přístup k peněžnímu účtu osoby.
- osobní informace nezahrnuje veřejně dostupné informace, které jsou legálně přístupné široké veřejnosti ve federální, státní nebo místní evidenci.

Zákon státu Kalifornie o ochraně soukromí na internetu definuje osobní identifikační informace jako informace, které identifikují spotřebitele a jsou provozovatelem o dané osobě shromažďované online a spravované v přístupné formě. Patří mezi ně následující:

jméno a příjmení, adresa bydliště nebo jiná fyzická adresa, včetně názvy ulice a města, e-mailová adresa, telefonní číslo, číslo sociálního pojištění. Jakýkoli další identifikátor, který umožňuje fyzický nebo internetový kontakt s danou osobou.

Informace týkající se uživatele webové stránky nebo online služby, které její poskytovatel od uživatele shromažďuje na internetu a uchovává v podobě, která v kombinaci s výše uvedenými identifikátory může osobu identifikovat.

3.20.3 Které aktivity jsou regulovány?

Federální zákon na ochranu spotřebitele (FTC Act) zakazuje nečestné nebo podvodné jednání. Federální agentura na ochranu spotřebitele (FTC) využívá své pravomoci obvinit společnosti z následujících zanedbání:Zanedbání ochrany osobních údajů spotřebitele, změna strategie ochrany soukromí bez dostatečného upozornění, neschopnost vyhovět oznámeným podmínkám ochrany soukromí.

Zákon Gramm-Leach-Bliley (GLB Act) upravuje shromažďování, použití, sdílení a odtajnění neveřejných finančních informací. Požadavky na písemné upozornění na bezpečnostní postupy a obdržení souhlasu (a možnosti neudělit souhlas k určitému zveřejnění) se liší podle toho, zda se jedná o zákazníka nebo spotřebitele, se kterým finanční instituce tyto údaje sdílí. Nejnáročnější povinností finančních institucí je povinnost zavést program na ochranu neveřejných osobních informací před neoprávněným vyzrazením.

Zákon o přenositelnosti a kontinuitě zdravotního pojištění (HIPAA) upravuje používání a zveřejňování chráněných identifikačních zdravotních a lékařských informací a shromažďování, používání, uchovávání či přenos těchto informací v elektronické podobě. Požaduje také zveřejnění postupů na ochranu soukromí.

Zákon státu Kalifornie o oznámení narušení bezpečnosti požaduje, aby každá osoba nebo firma podnikající v Kalifornii a licencující digitalizovaná data s osobními informacemi oznámila narušení bezpečnnosti jakmile je odhalí nebo je na ně upozorněna. Oznámení o narušené sdělí každému obyvateli Kalifornie, jehož nešifrované údaje byly získány neoprávněnou osobou nebo je důvodné podezření, že se tak mohlo stát. Toto oznámení musí sdělit, jakmile takové narušení zjistí nebo je na ně upozorněna. Mimo to, každá osoba nebo firma spravující digitalizovaná data, která obsahují osobní informace nevlastněné danou osobou či firmou, musí oznámit majiteli nebo držiteli licence jakékoli narušení bezpečnosti dat, jakmile je zjistí, pokud byla osobní informace získána neoprávněnou osobou nebo existuje důvodné podezření, že se tak stalo.

Zákon státu Kalifornie o ochraně soukromí na internetu požaduje, aby komerční webové stránky viditelně umístily informace o své bezpečnostní politice a svých postupech. Zákon byl novelizován v roce 2013. Provozovatelům webových stránek, internetových služeb a mobilních aplikací směrovaných na mladistvé nebo majících znalost o tom, že je mladiství používají, novela ukládá:

- umožnit mladistvým odstranit určité online informace nebo požadovat jejich odstranění
- uveřejnit informace o tom, jakým způsobem může mladistvý svůj obsah odstranit nebo požadovat jeho odstranění. Zákon také zakazuje těmto provozovatelům

inzerci a marketing produktů, které jsou podle zákona mladistvými nedostupné (včetně alkoholu, palných zbraní, tabáku, tetování a loterijních sázenek).

3.20.4 Jaká je jurisdikční působnost těchto nařízení?

Federální zákon na ochranu spotřebitele (FTC Act) spolu s nařízeními a směrnicemi vyhlašovanými z moci Federální agentury na ochranu spotřebitele (FTC) se vztahují na společnosti i jednotlivce podnikající ve Spojených státech.

Zákon Gramm-Leach-Bliley (GLB Act) platí pro finanční instituce (ty jsou definovány velmi široce, viz Otázka 2) a na přidružené i nepřidružené třetí strany, které získají neveřejné osobní informace od finančních institucí. Vztahuje se i na osoby, které obdrží neveřejné osobní informace od finančních institucí na základě nepravdy nebo podvodnými metodami.

Zákon o přenositelnosti a kontinuitě zdravotního pojištění (HIPAA) zahrnuje subjekty (definované v Otázce 2) spadající pod pravomoc státu. Avšak některé partnerské firmy institucí přímo zpracovávajících osobní zdravotní údaje, včetně těch, které se nalézají mimo jurisdikci Spojených států, mohou mít smluvní závazky o poskytnutí ochrany osobních zdravotní informací.

Zákon státu Kalifornie o oznámení narušení bezpečnosti se vztahuje na každou osobu nebo firmu, která podniká v Kalifornii, a na firmu která vlastní nebo licencuje digitální data obsahující osobní informace.

Zákon státu Kalifornie o ochraně soukromí na internetu se vztahuje na provozovatele komerčních webů nebo online služeb, kteří o jednotlivých spotřebitelích, návštěvnících a uživatelích s bydlištěm v Kalifornii shromažďují osobní identifikační informace pomocí internetu.

3.20.5 Jaké jsou hlavní výjimky (pokud existují)?

Nařízení a směrnice vydávané FTC obsahují výjimky z požadavků na ochranu soukromí pro potřeby prosazení práva.

Podle zákona Gramm-Leach-Bliley (GLB Act), může finanční instituce pro přidružený subjekt odtajnit neveřejné osobní informace o spotřebiteli, pokud tento krok oznámí. Finanční instituce nemusí k takovému odtajnění obdržet souhlas. Přidruženým subjektem je každá společnost, která řídí nebo je řízena, či je pod kontrolou skupiny osob spolu s další společností, včetně finančních a nefinančních institucí.

Pokud budou platit všechny následující podmínky, může finanční instituce odtajnit neveřejné osobní informace o spotřebiteli nepřidruženému subjektu, aniž by spotřebiteli poskytla právo to odmítnout:

Jde o sdělení informací třetí straně, která je používá k tomu, aby finanční instituci poskytla služby. Finanční instituce tento krok oznámí. Finanční instituce a třetí strana uzavřou smlouvu, která vyžaduje, aby třetí strana dodržovala požadavek důvěrnosti informací a používala je jen určeným způsobem.

Finanční instituce může odtajnit neveřejné osobní informace o spotřebiteli nepřidruženému subjektu, aniž by spotřebiteli poskytla právo to odmítnout, pokud je informace nutná k provedení, řízení nebo vynucení transakce. V takovém případě finanční instituce nemusí tento krok oznamovat spotřebiteli. Finanční instituce může odtajnit neveřejné osobní informace pro účely shody (například s organizací, která stanovuje finanční bonitu pro pojištění). To platí i pro účely prosazení práva. Finanční instituce může odtajnit veřejně dostupné finanční informace (jako například veřejně dostupné daňové záznamy).

Zákon o přenositelnosti a kontinuitě zdravotního pojištění (HIPAA) se nevztahuje na zdravotní informace, které nejsou identifikační (například agregátní data). Nevztahuje se také na zdravotní informace používané jednotlivci nebo subjekty, které nespadají do definice „instituce přímo zpracovávající osobní zdravotní údaje“ nebo „partnerská firma instituce přímo zpracovávající osobní zdravotní údaje“. Pod tento zákon nespadají například některé vzdělávací a zaměstnanecké záznamy (jako třeba doklad o zdravotním stavu pro žádost o zaměstnání). Ze zákazů odtajnění osobních zdravotních informací

existuje mnoho výjimek, například v zájmu prosazení práva nebo při hrozbě ohrožení veřejného zdraví.

Oznámení o narušení bezpečnosti vyžadované Zákonem státu Kalifornie o oznámení narušení bezpečnosti může být odloženo, pokud orgán prosazující právo rozhodne, že oznámení by ztěžovalo vyšetřování trestního činu. Mimo to, společnost, která v rámci své politiky bezpečnosti informací zachovává své vlastní oznamovací postupy pro nakládání s osobními údaji, je považována za toho, kdo vyhověl oznamovacím požadavkům, pokud v případě narušení systému bezpečnosti osoba nebo firma vyrozumí dotčenou osobu v souladu se svou bezpečnostní politikou.

3.20.6 Hlavní nařízení a zásady ochrany dat

Hlavní povinnosti a požadavky na zpracování

Jaké jsou hlavní povinnosti zajišťující správné nakládání s daty ukládané controlingu?

Federální agentury na ochranu spotřebitele (FTC) aplikuje část 5 Federálního zákona na ochranu spotřebitele (FTC Act) na společnosti, které nedodržely svou vlastní politiku bezpečnosti nebo neuhlídaly údaje, které shromáždily. FTC Act výslovně neukládá, aby společnosti měly nebo zveřejnily politiku ochrany soukromí, FTC však zastává názor, že pokud společnost svou bezpečnostní politiku zveřejní, musí ji také dodržovat. Vedle toho je podle FTC také porušení zákona (FTC Act), pokud společnost zpětně změní svou bezpečností politiku, aniž by o tom uvědomila subjekty, jichž se data týkají, a dala jim možnost od nových podmínek odstoupit.

GLB Act má za cíl chránit finanční soukromí spotřebitele tím, že určuje, kdy může finanční instituce sdělit neveřejné osobní údaje o spotřebiteli nepřidruženým třetím stranám. Finanční instituce musí své zákazníky obeznámit s praxí sdílení informací a poučit je o jejich právu odstoupit od smlouvy, pokud nesouhlasí s tím, aby jejich data byla sdílena s určitou nepřidruženou třetí stranou. (Pro definice termínů zákazník a klient viz Otázka 3.) Další částí zákona GLB je Pravidlo bezpečnostních pojistek (Safeguards Rule), které požaduje, aby společnosti vypracovaly písemný plán bezpečnosti informací, který popisuje jejich program na ochranu zákaznických záznamů a informací. Federální a státní úřady s jurisdikcí GLB nad finančními institucemi musí zavést normy požadující, aby tyto

instituce zavedly do svého bezpečnostního programu bezpečnostní pojistky, včetně těch které:

- chrání proti neoprávněnému přístupu k záznamům či informacím a jejich použití, které by zákazníkovi způsobily značnou újmu nebo nesnáz. Pro vyloučení neoprávněného přístupu byly navrženy následující společné standardy:
- šifrování dat
- ověřovací mechanizmy
- prověrky pozadí
- časté monitorování a prověřování bezpečnostních protokolů a systémů
- zajištují bezpečnost a důvěrnost zákaznických záznamů a informací
- chrání proti každé předvídané hrozbě, nebezpečí narušení ochrany nebo celistvosti těchto záznamů

U „ krytých účtů“ implementují a ztotožní Program prevence krádeží

Implementují regule programu (tzv. program odezvy), který vyžaduje, aby finanční instituce vyrozuměly správce (a v určitých případech i zákazníka), pokud došlo k neoprávněnému přístupu k citlivým informacím zákazníka

Kromě toho každý subjekt, který přijde do styku s finančními informacemi od finanční instituce, může být omezen v možnosti dané informace znovu použít a znovu zjistit.

HIPAA vyžaduje (s určitými výjimkami), aby instituce, které přímo zpracovávají osobní zdravotní údaje, činily následující kroky:

Používaly, vyžadovaly a zveřejňovaly minimální množství osobních zdravotních informací potřebné k provedení transakce (Pravidlo soukromí, HIPAA Privacy Rule)

Implementovaly postupy zajišťující bezpečnost dat, protokolů a postupů na administrativní, fyzické i organizační úrovni ochrany dat (Pravidlo bezpečnosti, HIPAA Security Rule)

Vyhověly konkrétním jednotným standardům stanoveným pro konkrétní elektronické transakce (Transakční pravidlo, HIPAA Transactions Rule)

Spouštěcím mechanismem pro působení Zákona státu Kalifornie o oznámení narušení bezpečnosti je neoprávněné prozrazení nešifrovaných informací, proto jsou společnosti nabádány k tomu, aby osobní informace Kaliforňanů šifrovaly. Jiný kalifornský zákon, Občanský zákoník §1798.81.5 (Civil Code), vyžaduje, aby určité firmy používaly k zajištění bezpečnosti osobních informací obyvatel Kalifornie bezpečnostní pojistku (jméno plus číslo sociálního zabezpečení, řidičský průkaz nebo státní identifikační průkaz a číslo finančního účtu) a aby smluvně zavázaly třetí strany ke stejnému postupu. Občanský zákoník v paragrafech §§1798.85-1798.86, 1785.11.1, and 1785.11.6 zakazuje firmám a státním i místním úřadům veřejně vystavovat nebo posílat čísla sociálního zabezpečení a zakazují nahrazovat zákonem požadované odstranění čísla sociálního zabezpečení jeho vložením na kartu nebo do dokumentů pomocí čárového kódu, chipu, magnetického proužku nebo jiné technologie. Občanský zákoník v paragrafech §§1798.80 to 1798.81 and 1798.84 vyžaduje, aby firmy skartovaly, vymazaly nebo jinak upravily osobní informace, které mají pod svou správou.

3.20.7 **Platí zvláštní předpisy pro určité typy osobních údajů, jako jsou například citlivé údaje**?

Zásady behaviorální reklamy vydané Federální agenturou na ochranu spotřebitele (FTC) doporučují provozovatelům webových stránek, aby od spotřebitele získali jasný souhlas dříve, než jeho citlivá data použijí.

Zákon Gramm-Leach-Bliley (GLB) se specificky nezabývá jednotlivými kategoriemi dat, ale i podle něj správci musí zavést regule programu odezvy, podle nichž finanční instituce musí vyrozumět správce (a v některých případech zákazníka), pokud dojde k neoprávněnému přístupu k citlivým údajům o zákazníkovi.

Zákon o čestném hlášení zůstatku (Fair Credit Reporting Act, 15 U.S.C. §1681), souvisící s GLB, upravuje, jak lze používat a uvádět výpisy a čísla účtů kreditních karet. Finanční instituce nesmějí sdělovat číslo účtu nepřidruženému subjektu (jinému než je výkaznická agentura zákazníka) za účelem telemarketingu, e-mailového marketingu nebo přímého marketingu.

V souladu s HIPAA existují speciální pravidla upravující sdělování psychoterapeutických záznamů. Instituce přímo zpracovávající osobní zdravotní údaje musí před sdělením

psychoterapeutických záznamů obyčejně získat písemný souhlas, a to i pro účely léčení, lékařských úkonů nebo plateb.

Několik kalifornských zákonů uvádí zvláštní nařízení ohledně zpracování, shromažďování, přenosu a sdělování určitý typů dat bez omezení:

- finanční a lékařské údaje
- čísla sociálního zabezpečení
- telekomunikační záznamy
- radiofrekvenční identifikace
- knihovnické záznamy

3.20.8 Mají subjekty právo požadovat vymazání svých dat?

Zásady behaviorální reklamy vydané Federální agenturou na ochranu spotřebitele (FTC) neposkytují subjektům právo požadovat vymazání dat. Avšak Zpráva o právu na soukromí vydaná roku 2012 Bílým domem a Návrh zákona o právu spotřebitele na soukromí (Privacy Report 2012; Consumer Privacy Bill of Rights), které mohou být základem nové dobrovolné etiky, prohlašují, že „společnosti by také měly spotřebitelům poskytnout v rozumné míře přístup k jejich osobním údajům, která shromažďují nebo uchovávají, včetně odpovídající ch prostředků a možností oprav nepřesných údajů a možnosti požádat o vymazání nebo omezení jejich použití“.

HIPAA umožňuje, aby osoby žádaly doplnění svých osobních informací, pokud jsou nepřesné nebo neúplné, avšak instituce přímo zpracovávající osobní zdravotní údaje není povinna této žádosti vyhovět.

Zákon státu Kalifornie o ochraně soukromí na internetu vyžaduje, aby provozovatelé webových stránek, internetových služeb a mobilních aplikací, které jsou směřovány na mladistvé, nebo o nichž je známo, že je mladiství používají, dovolit mladistvému, který je registrovaným uživatelem, aby odstranil určité online informace, které zaslal, nebo požádal o jejich odstranění. Zákon nepožaduje, aby společnosti odstraňovaly údaje ze svých serverů, pokud je vymažou z webových stránek. Zákon se nevztahuje na obsah, za který mladistvý ‘získal nějakou kompenzaci nebo protihodnotu‘.

3.20.9 Bezpečnostní požadavky

Jaké bezpečnostní požadavky jsou vzneseny ve vztahu k osobním údajům? Zásady behaviorální reklamy vydané Federální agenturou na ochranu spotřebitele (FTC) doporučují provozovatelům webových stránek, kteří shromažďují a uchovávají data spotřebitelů pro behaviorální reklamu, aby těmto datům poskytli rozumné zabezpečení a aby tato data zůstala daty jen po dobu nutnou pro naplnění legitimního podnikání nebo potřeby prosazení zákona. Ochrana spotřebitelských dat by měla být založena na následujících principech:

- Citlivost údajů
- Povaha obchodních operací společnosti
- Druhy rizika, kterému je společnost vystavena
- Rozumná ochrana společnosti dostupná

Pravidlo bezpečnostních pojistek (Safeguards Rule) pod GLB vyžaduje, aby společnosti vypracovaly písemný plán bezpečnosti informací, který vysvětlí jejich zákazníkům jejich bezpečnostní program. Tento plán musí odpovídat velikosti společnosti, složitosti, povaze a rozsahu jejích aktivit a citlivosti zákaznických informací, se kterými nakládá. Plán každé společnosti musí:

Určit jednoho nebo více zaměstnanců pro koordinaci programu informační bezpečnosti

Identifikovat a stanovit rizika pro zákaznické informace v každé relevantní oblasti činnosti společnosti vyhodnotit efektivitu dosavadních bezpečnostních pojistek pro kontrolu těchto rizik.

Navrhnout a zavést program bezpečnostních pojistek a pravidelně ho monitorovat a testovat.

Vybrat poskytovatele služeb, kteří jsou schopni dodržovat odpovídající bezpečnostní pojistky, smluvně zajistit, aby tyto pojistky udržovali a kondolovat, jakým způsobem se zákaznickými informacemi zacházejí.

Vyhodnotit a nastavit tento program podle konkrétních okolností, včetně změn v podnikatelské činnosti firmy či provozovatelů, nebo změn v monitoringu či ve výsledcích bezpečnostních testů.

Tyto požadavky jsou navrženy tak, aby byly flexibilní. Podle FTC by společnosti měly zavést bezpečnostní pojistky odpovídající jejich situaci. Pravidlo FTC o odstranění (Disposal Rule) upravuje likvidaci reportů o zákaznících. Nedávno vydané Pravidlo signálů (Red Flags Rule) požaduje, aby finanční a věřitelské instituce vypracovaly písemný program, který by identifikoval a detekoval odpovídající varovné signály upozorňující na krádež identity. Může to být například neobvyklá aktivita na účtu, znepokojující signály na účtu spotřebitele upozorňující na podvod, nebo pokus použít podezřelé přihlašovací doklady. Tento program musí také popisovat reakce, které trestnému činu zabrání nebo sníží jeho nebezpečí; musí také detailně popsat plán aktualizace programu.

HIPAA požaduje, aby instituce přímo zpracovávající osobní zdravotní údaje učinily následující:

- používaly a sdělovaly jen minimální množství osobních zdravotních informací potřebné k provedení transakce
- zavedly postupy ochrany dat a politiku bezpečnosti dat
- vytvořily shodu se standardy stanovenými pro elektronické transakce

K dispozici je také Návod pro vzdálený přístup a užívání elektronicky chráněných zdravotních informací (Guidance for Remote Use of and Access to Electronic Protected Health Information), který se konkrétně zabývá riziky spojenými s uchováváním, dosažitelností a přenosem lékařských dat na noteboocích, bezdrátových zařízeních, domácích počítačích, flash drivech, pomocí e-mailů a na veřejných počítačích.

Spouštěcím mechanismem pro působení Zákona státu Kalifornie o oznámení narušení bezpečnosti je neoprávněné sdílení nešifrovaných informací, proto jsou společnosti nabádány k tomu, aby osobní informace občanu Kalifornie šifrovaly.

3.20.10Přenos dat v mezinárodním měřítku

Jaká pravidla upravují přenos dat mimo vaši jurisdikci?

Přenos osobních údajů mimo Spojené státy má několik omezení. Některé státy přijaly zákony, které omezují státní agentury a státní dodavatele v získávání dat z externích zdrojů mimo hranice Spojených států nebo jim je nedoporučují. Tyto zákony se typicky omezují na vládní agentury a soukromé společnosti, které mají smlouvy na poskytování služeb nebo zboží státním úřadům.

Nicméně, názor FTC a jiných regulačních subjektů je ten, že odpovídající zákony a nařízení Spojených států platí i poté, co data Spojené státy opustí. Subjekty pod jurisdikcí Spojených států i nadále odpovídají za následující:

Data exportovaná mimo USA

Zpracování dat subdodavateli v zahraničí

Používání stejných ochranných opatření subdodavateli (například pomocí bezpečnostních pojistek, protokolů, auditů a smluvních ustanovení).

3.20.11Vymáhání a sankce

Jaké donucovací možnosti má národní dohledový orgán?

Primárním prosazovatelem národních zákonů na ochranu soukromí ve Spojených státech je FTC. Také další národní úřady (například bankovní) jsou oprávněny prosazovat různé zákony na ochranu soukromí, avšak FTC v této oblasti vykonává výrazně více aktivit než jiné orgány. FTC může iniciovat vyšetřování, vydat příkaz k zastavení aktivity, upustit od příkazu a podat soudní žalobu. FTC také podává zprávu o bezpečnosti soukromí Kongresu a doporučuje uzákonění potřební legislativy v této oblasti.

Zákon GLB je vymahatelný FTC, federálními bankovními orgány a státními pojišťovnami. FTC je však jako vymahatel aktivnější než ostatní orgány.

HIPAA je vymahatelný Úřadem pro občanská práva (Office of Civil Rights) v rámci Ministerstva zdraví a služby lidem (Department of Health and Human Services). Tento úřad může iniciovat vyšetřování způsobu jakým, postupují instituce přímo

zpracovávajících osobní zdravotní údaje, rozhodnout, zda pracují v souladu s „Pravidlem soukromí „ a umožnit osobám podávat stížnosti na porušení soukromí.

Zákona státu Kalifornie o oznámení narušení bezpečnosti a Zákon státu Kalifornie o ochraně soukromí na internetu jsou vymahatelné generálním prokurátorem a státními žalobci.

Jaké jsou sankce a opravné prostředky v případě nedodržení zákonů na ochranu soukromí?

Federální zákon na ochranu spotřebitele (FTC Act) stanoví peněžitý trest až do výše 16,000 US$ za každé porušení. FTC může také dosáhnout soudního příkazu, odškodnění zákazníkovi, splacení nákladů na vyšetřování a trestní stíhání. Trestním postihem může být i uvěznění až na 10 let. V roce 2006 zaplatil datový makléř 15 milionů US$ jako vypořádání v obvinění podaném FTC na nedostatečnou ochranu dat milionů zákazníků. Vypořádání se státnímu úřady se může týkat také nerovných reportingových povinností, auditů a monitoringu od třetích stran. Jeden z nejvýznamnějších maloobchodníků/prodejců, který čelil vyrovnání za neposkytnutí dostatečné ochrany čísel kreditních karet zákazníků, přistoupil na úplné prověrky svého datového zabezpečení, které budou vedeny po dobu 20 let.

Tresty za porušení zákona GLB jsou určeny úředním statutem organizace, která prosazení zákona navrhuje. Například prosazení navržené FTC by se mohlo týkat pokuty až do výše 16,000 US$ za jedno porušení zákona. Osoby mohou být potrestány pokutou ale i vězením až na 5 let, pokud od finanční instituce získají nebo se pokusí podvodně získat zákaznické informace vztahující se k jiné sobě, způsobí jejich zveřejnění/sdílení nebo se o to pokusí. Kromě toho existují trestní postihy za spáchání trestného činu narušení soukromí. Pro osoby je to 500,000 US$, pro instituce 1 milion US$, pokud je takový čin spáchán nebo byl učiněn pokus jej spáchat spolu s porušením jiného zákona Spojených států nebo jako součást protizákonné činnosti, která způsobila škodu vyšší než 100,000 US$ za jeden rok.

HIPAA ukládá občanskoprávní postihy jako pokuty od 100 do 1,5 milionu US$ v závislosti na množství činitelů vytvářejících trestný čin, včetně toho, zda provozovatel věděl, že určitá činnost byla narušením bezpečnosti, zda bylo toto narušení rychle

napraveno či zda šlo o vědomou nedbalost provozovatele. Trestní postih může dosáhnout až 250,000 US$ a až 10 let vězení, pokud je čin spáchán na základě falešných údajů nebo s cílem prodat data pro finanční zisk.

Některé státní a federální zákony dovolují, aby se jednotlivé osoby nebo skupiny osob soudně bránily narušení soukromí. Soudní rozhodnutí v takových případech může také uložit značnou pokutu nebo odškodné. K nejrozsáhlejšímu narušení datového soukromí ve Spojených státech došlo ke konci roku 2013 u obchodního řetězce Target. Tímto narušením bylo možno porušit utajení informací o platebních kartách u více než 40 milionů zákazníků a u dalších 70 milionů mohlo jít o narušení soukromí osobních informací. Target byl obžalován zákazníky a akcionáři a vyšetřován Kongresem a státními žalobci. Druhý největší případ stál významného obchodníka přinejmenším 256 milionů US$, ale odhaduje se, že to bylo až 500 milionů. Tato společnost čelila několika skupinovým žalobám podaným zákazníky a také žalobám ze strany kreditních společností a bank, které musely znovu vydat miliony karet.

Podle výpočtů Ponemon Institute byly v roce 2013průměrné náklady amerických firem na každý smír 188 US$. Vedle trestních a občanskoprávních sankcí může mít narušení soukromí pro firmy dalekosáhlé důsledky v souvislosti se ztrátou důvěry, snížením obliby, snížením tržeb, ztrátou podílu na trhu a ztrátou ceny značky a akcií.[43]

Strategické cíle FTC

chránit spotřebitele: zabránit podvodům a nekalým obchodním praktikám na trhu

udržet soutěž: zabránit protisoutěžním obchodním praktikám na trhu

zvýšit výkon prostřednictvím organizace, individuálním a vynikajícím řízením[44]

[43]Data protection in United States, ©2014 [cit. 2015-02-27]. Dostupné z: http://uk.practicallaw.com/6-502-0467

[44] Federal Trade Commission,©2014 [cit. 2015-02-27]. Dostupné z: http://www.ftc.gov/about-ftc

3.20.12Safe Harbor

Předání osobních údajů do USA na základě využití institutu tzv. Safe Harbor (bezpečný přístav) jako předání podle § 27 odst. 2 zákona o ochraně osobních údajů a požadavek souhlasu Úřadu pro ochranu osobních údajů pro takové předání.

Pojmem Safe Harbor se označuje komplex technických a administrativních opatření, které mají zaručit adekvátní ochranu osobních údajů předávaných členských zemí Evropské unie do Spojených států. USA nemají v současné době společnou všeobecně platnou legislativu, jež by zajišťovala ochranu údajů v soukromém sektoru a současně se, jako je tomu u legislativy Evropské unie, opírala o specifické institucionální řešení. Americké společnosti se proto mohou „pouze" dobrovolně přihlásit k dodržování zásad „bezpečného přístavu". V takovém případě je americké federální Ministerstvo obchodu zařadí do on-line seznamu, který průběžně aktualizuje a zveřejňuje na svém webu. Dohoda smluvních stran (odpovědných subjektů) obsahují podmínky Safe Harbor tak již nevyžaduje splnění dalších podmínek vyžadovaných § 27 odst. 3 zákona o ochraně osobních údajů, tedy podání žádosti o povolení předání osobních údajů do třetích zemí Úřadu pro ochranu osobních údajů. [45]

3.20.13Zákon o svobodě informací

Zákon o svobodě informací (FOIA), 5 USC (United States Code) § 552, byl přijat v roce 1966 a obecně stanoví, že:

Každý jednotlivec, má právo podat žádost o federální záznamy agentury nebo informace.

Všechny agentury vlády Spojených států jsou povinny zveřejňovat záznamy na základě písemné žádosti o ně.

Existuje devět výjimky, omezení na FOIA, které chrání některé záznamy z vyzrazení.

Federální FOIA neposkytuje přístup k záznamům v držení státu nebo místní vládní agentury, nebo soukromými podniky či jednotlivci. Většina států, a některé místní jurisdikce, mají své vlastní zákony o přístupu ke státním a místním záznamy.[46]

[45] KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v praktických příkladech*, s. 129
[46] Federal Trade Commission, , ©2014 [cit. 2015-02-27]. Dostupné z: http://www.ftc.gov/about-ftc/foia

4 Analytická část

4.1 Problémy při zpracovávání osobních dat a údajů v praxi v ČR

4.1.1 Spotřebitelské soutěže

Kdo by nechtěl vyhrát zájezd, fotoaparát či jinou hodnotou cenu stačí vyplnit jméno, přímení, přesnou adresu a číslo telefonu, informace, které jsou potřeba pro doručení výhry. Útočí na nás z reklamních letáků i časopisů a osobně se s nimi setkal snad každý, kdo někdy nakupuje v hypermarketu nebo třeba navštívil nějakou komerční výstavní akci. Je s podivem, kolik se všude najde lidí ochotných sdělit své osobní údaje, a ani je přitom nezajímá, kdo všechno a jak s nimi bude nakládat**.** Nezneklidní je ani to, když mají uvést například datum narození, počet členů domácnosti, měsíční příjem nebo banku, v níž mají veden účet.

Na anketním lístku si povšimněte drobným písmem psaného textu, který vyjadřuje váš souhlas s použitím vašich osobních údajů k marketingovým účelům, a to většinou i třetími osobami, dokud jej písemně neodvoláte. Než budete vyplňovat nějaký dotazník, zamyslete se, zda malá možnost výhry stojí za to, že údaje o vaší osobě a majetku budou k dispozici někomu neznámému, o jehož serióznosti nic nevíte. Uvědomte si, že bude mít k dispozici v podstatě tytéž údaje jako vaše banka, a to i s vaším podpisovým vzorem**!**

Když už se ankety mermomocí chcete zúčastnit**,** vaši šanci na výhru asi nesníží, když své narozeniny v dotazníku o den či měsíc posunete, místo pevné linky uvedete číslo mobilního telefonu a místo podpisu uděláte muří nohu.

Zákon č. 101/2000 Sb., o ochraně osobních údajů, stanoví pro získávání, zpracování a uchovávání osobních údajů poměrně přísná pravidla, za jejichž nedodržení hrozí miliónové pokuty. To však neznamená, že je bude každý respektovat.

4.1.2 Osobní doklady

Občanský průkaz, cestovní pas a řidičský průkaz, tyto doklady obsahují spoustu údajů, které lze zneužít. V zásadě byste je tedy neměli dávat z ruky a nenechat nikoho, aby si pořizoval jejich fotokopie. Úplně by mělo stačit, když se jimi prokážete, a je-li to nezbytné, necháte oprávněnou osobu, aby si z nich opsala potřebné údaje. Většinou by mělo stačit jméno, příjmení a bydliště, popř. číslo osobního odkladu. Naopak rodné číslo už je vyloženě citlivý údaj a rozhodně ho po vás nemůže požadovat nikdo třeba na recepci firmy, kterou jdete navštívit.

Zcela běžnou praxí, která je většinou dána provozními důvody, je ponechání občanského průkazu či pasu v hotelové recepci. Hodně opatrný člověk své doklady neopustí a raději si chvíli počká, než recepční potřebné údaje opíše. Přestože to zákon přímo zakazuje, stále se ještě lze setkat s požadavkem nechat občanku v zástavě jako záruku toho, že nezapomenete vrátit vypůjčenou věc nebo se třeba odhlásit při odchodu z budovy.

Když už musíte někde nechat nějaký průkaz v zástavě, asi bude lepší, když to místo občanky bude třeba průkazka do knihovny nebo tramvajenka. Není na nich uvedeno tolik osobních údajů a možnost jejich přímého zneužití je daleko menší.

Pořízení fotokopie občanského průkazu je běžnou praxí v řadě půjčoven všeho druhu. Majitelé půjčoven se tím snaží bránit rozmáhajícímu se nevracení vypůjčených věcí.

Ten kdo takto postupuje, sice zákon přímo neporušuje, ale při nakládání s pořízenými fotokopiemi osobních dokladů, stejně jako s jinými databázemi osobních údajů, se musí zákonem řídit. Tomu, kdo by je zneužil nebo jejich zneužití umožnil, hrozí pokuta až deset milionů a při opakovaném porušení zákona až dvacet milionů korun.

Pokud někdo fotokopii vašich dokladů zneužije, můžete po něm vymáhat náhradu škody občanskoprávní cestou. Musíte ovšem prokázat zavinění, což nebývá jednoduché. Urgence plateb od splátkové společnosti nebo důrazný požadavek na vrácení vypůjčeného auta vás mohou překvapit až po určité době, a až opadne vaše zděšení, budete marně vzpomínat, kdo všechno s vašimi doklady disponoval. Nejlepším řešením je tedy vzniku těchto problémů předcházet.

Zákon porušuje ten, kdo občanský průkaz do zástavy požaduje, i ten, kdo mu jej svěří. Pokud dáte své doklady na delší dobu z ruky, nikdy nemůžete vědět, kdo s nimi co dělal.

4.1.3 Dokumenty

Každému, kdo má bankovní účet, obvykle chodí výpisy v papírové podobě. Hodně lidí má také stavební spoření, penzijní připojištění nebo například investuje do akcií. Se všemi institucemi, které spravují finanční či jiný majetek, každý koresponduje, podepisuje smlouvy, podpisové vzory, převodní příkazy atd. Na těchto dokumentech jsou většinou všechny údaje, které podvodníci a pobertové potřebují, aby se dostali k vašemu majetku.

Při nakládání s dokumenty obsahujícími citlivé informace i jejich kopiemi se vyplatí nutná dávka obezřetnosti. Ekologie velí recyklovat, ale zvažte, zda je nutné, aby si každý bezdomovec sbírající u popelnic starý papír mohl prostudovat váš výpis z účtu. Stačí, když je roztrháte a přibalíte ke kuchyňskému odpadu. Bude to podstatně bezpečnější, než je se starými novinami vkládat do ekologického kontejneru.

4.1.4 Internet

Internet je jedním z největších fenoménů dnešní doby. Ten, kdo je připojen, má především možnost snadného přístupu téměř k jakýmkoliv informacím. Informace lze díky internetu nejen získat, ale také o ně přijít.

Chcete-li zaručeně přijít o důležitá data nebo majetek, rezignujte na jakoukoliv antivirovou ochranu a otevírejte všechnu poštu, která vám do schránky dorazí, a to samozřejmě včetně všech připojených souborů. Obratem posílejte všechny požadované údaje každému, kdo se podepíše jako administrátor.

Pořiďte si internetové bankovnictví s přístupem chráněným pouze jednoduchým heslem, které zásadně neměňte, a z banky pro jistotu vždy rovnou skočte na stránky s lechtivým obsahem. Často se také přihlašujte na svůj účet z cizích počítačů, nejlépe z internetových kaváren. Pokud by to nestačilo, zkuste používat k placení v pokud možno neznámých internetových obchodech svou běžnou platební kartu. To by v tom byl čert, aby to nevyšlo![47]

[47] Mesec.cz,Petr Bukač [online]. ©2004 [cit. 2015-02-22]. Dostupné z: http://www.mesec.cz/clanky/hlidejte-si-osobni-udaje/

4.2 Úniky osobních dat a údajů v ČR a USA

USA: Tři externí zaměstnanci ministerstva zahraničí si prohlíželi spisy prezidentských kandidátů

Do osobních údajů uchazečů o křeslo amerického prezidenta, které jsou součástí spisu k cestovnímu pasu, nahlíželi bez povolení tři zaměstnanci externích firem pracujících pro ministerstvo zahraničí. Oznámil to mluvčí ministerstva Sean McCormack s tím, že dva z těchto zaměstnanců již přišli o místo a že se zatím zdá, že z jejich strany šlo pouze o neopatrnou zvědavost. Ministryně zahraničí Condoleezza Riceová se omluvila Obamovi, Clintonové i McCainovi. Spisy se žádostí o vystavení pasu obsahují nejen osobní údaje žadatelů, ale i číslo sociálního pojištění, které banky používají při udělování úvěrů nebo seznam zemí, které žadatel navštívil a hodlá navštívit. Mluvčí Obamovy kampaně Bill Burton nazval incident „šokujícím narušením bezpečnosti a soukromí“.[48]

USA: Hackeři se dostali k 70 miliónům PINů platebních karet zákazníků obchodního řetězce

Rozsáhlá krádež zakódovaných osobních identifikačních čísel (PIN) ke kreditním a debetním kartám, k níž došlo v předvánočních týdnech u amerického maloobchodního řetězce Target, zasáhla až 70 miliónů jeho zákazníků. Podrobnější informace zveřejnila firma v lednu.[49]

USA: Tajné služby sbíraly osobní údaje o hráčích Angry Birds

Americká Národní agentura pro bezpečnost (NSA) a britská tajná služba GCHQ sbíraly osobní údaje i uživatelů mobilních aplikací, například populární hry Angry Birds. Napsal to americký deník The New York Times a britský The Guardian s odvoláním na dokumenty, které jim poskytl bývalý pracovník NSA Edward Snowden. Podle listů se obě

[48] Úřad pro ochranu osobních údajů, Výběr ze zahraničních médií. [online]. [cit. 2015-02-22]. Dostupné z: https://www.uoou.cz/verejna-sprava-zakonodarstvi-a-soudnictvi/ds-2083/p1=2083

[49] Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: : http://www.novinky.cz/internet-a-pc/324208-hackeri-se-dostali-k-70-milionum-pinu-platebnich-karet-zakazniku-obchodniho-retezce.html

tajné služby pomocí aplikací pro mobilní telefony iPhone a pro telefony se systémem Android dostávaly k informacím o místu pobytu hráče, o jeho stáří a pohlaví.[50]

USA: Hackeři ukradli data k e-mailům společnosti Yahoo

Některé účty elektronické pošty provozované americkou internetovou společností Yahoo se staly terčem útoku. Hackeři při něm ukradli některá uživatelská jména a hesla, která pak byla použita k získání osobních údajů o lidech, s nimiž si uživatelé zasažených účtů v nedávné době psali. Ve čtvrtek to sdělila sama firma. Neuvedla přitom, kolika účtů se útok týká.[51]

ČR: V Česku padla rekordní pokuta za spam. Firma musí zaplatit 480 tisíc

Historicky nejvyšší pokutu za šíření spamu uložil tento týden Úřad pro ochranu osobních údajů (ÚOOÚ). Za nevyžádaná obchodní sdělení tak společnost eMarketing CZ zaplatí 480 000 Kč. Novinkám to v pátek potvrdila ředitelka tiskového odboru úřadu Hana Štěpánková. Úřad uložil pokutu 480 000 Kč společnosti eMarketing CZ za šíření nevyžádaných obchodních sdělení. Uvedená společnost rozesílala po dobu přibližně jednoho roku obchodní sdělení v rozporu se zákonem o některých službách informační společnosti," uvedla Štěpánková s tím, že zákon umožňuje udělit pokutu až do výše deseti miliónů korun.[52]

[50] Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.novinky.cz/zahranicni/amerika/325794-tajne-sluzby-sbiraly-osobni-udaje-o-hracich-angry-birds.html

[51] Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.novinky.cz/internet-a-pc/326184-hackeri-ukradli-data-k-e-mailum-spolecnosti-yahoo.html

[52] Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.novinky.cz/internet-a-pc/331114-v-cesku-padla-rekordni-pokuta-za-spam-firma-musi-zaplatit-480-tisic.html

ČR: Dlužili jste? Z registru dlužníků se jen tak nedostanete.

Praha – Možná už se vám to někdy stalo. Chtěli jste si koupit pračku na splátky nebo sjednat tarif u mobilního operátora a tam vám řekli: smlouvu s vámi neuzavřeme, jste veden v registru SOLUS jako dlužník. Ano, před lety jste se opozdili se splácením půjčky, ale dluh už je dávno uhrazen. Jak žádat o výmaz z registru dlužníků? A může vůbec registr zveřejňovat informace o vašich dluzích? Registr dlužníků SOLUS shromažďuje údaje pouze o těch občanech, kteří dlouhodobě neplní své smluvní závazky u členů sdružení SOLUS. Mezi členy figurují velké banky, nebankovní společnosti, stavební spořitelny, mobilní operátoři i energetické firmy. Když dlužník své závazky uhradí, z registru ale nezmizí okamžitě. "Pokud občan již závazek po splatnosti uhradil, v takovém případě běží lhůta pro výmaz, která trvá tři roky, v případě dluhu ze služeb elektronických komunikací jeden rok," upřesnil mluvčí sdružení SOLUS Miroslav Beneš. Podmínkou výmazu je tedy kromě úhrady dlužné částky také uplynutí stanovené lhůty. Jenže podle nezávislých expertů by tomu tak být nemělo. Postup, kdy k výmazu údajů nedochází ihned po zaplacení celé dlužné částky, ale až s časovou prodlevou, je v rozporu se zákonem. "Likvidaci osobních údajů je jejich správce povinen provést, jakmile pomine účel, pro který byly osobní údaje zpracovány, a tuto likvidaci musí správce provést neprodleně," míní právník Petr Šustek. Jinými slovy, pokud jste svůj dluh uhradili, není důvod, abyste byli v registru dlužníků nadále vedeni. A navíc registry mohou zveřejňovat údaje o dlužnících pouze s jejich souhlasem. Rozhodl o tom loni v říjnu Úřad pro ochranu osobních údajů. Jestliže registr bez zbytečného odkladu tyto údaje neodstraní, je možné se obrátit na Úřad pro ochranu osobních údajů s žádostí o zajištění opatření k nápravě," doporučuje právník Šustek. Úřad může správci nebo zpracovateli těchto údajů vedle opatření k nápravě uložit i pokutu, a to až do výše pěti milionů korun.[53]

[53] Česká televize, ČT 24, Pavla Freiwaldová [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/274905-dluzili-jste-z-registru-dluzniku-se-jen-tak-nedostanete/

ČR: Úřad na ochranu osobních údajů udělil Komerční bance pokutu 1,8 milionu korun za červencový únik dat a červencový exces, během nějž se běžný uživatel webové aplikace KB Penzijní společnosti omylem dostal k osobním údajům mnoha tisíc evidovaných potenciálních zájemců o penzijní spoření, padla pokuta. Penzijní společnost musí zaplatit celkem 1,8 milionu korun. „Uložili jsme pokutu za to, že společnost zpřístupnila osobní údaje nejméně 45 645 zájemců o penzijní spoření," zdůvodnila udělení pokuty za Úřad pro ochranu osobních údajů jeho mluvčí Hana Štěpánková. Dodala zároveň, že rozhodnutí je již pravomocné, když ve lhůtě do 13. prosince nedošel na úřad rozklad proti rozhodnutí. Prozatím nejvyšší pokutou, která za porušení §13 zákona o ochraně osobních údajů padla, činila dle Štěpánkové 3,5 milionu korun. "KB Penzijní společnost se rozhodla nepodat odvolání proti rozhodnutí Úřadu pro ochranu osobních údajů a uhradí zároveň stanovenou pokutu ve výši 1,8 milionu korun," vyjádřila se k přijetí pokuty mluvčí Komerční banky (i KB Penzijní společnosti) Monika Klucová. [54]

USA a ČR:Únik dat z aukčního portálu ebay

Největší globální internetový aukční portál eBay, který má 128 milionů aktivních uživatelů z celého světa, včetně České republiky, oznámil ve středu 21. Května 2014, že v důsledku kybernetického útoku došlo k úniku osobních údajů jeho uživatelů. Událost se stala na přelomu února a března a společnost eBay jej zaznamenala začátkem května. Varovat uživatele dřív podle zástupců firmy eBay nešlo, aby nebylo zmařeno vyšetřování úniku.[55]

USA a ČR: Facebook zaznamenal další únik údajů

Je to už po několikáté, co díky chybě Facebooku unikl velký počet uživatelských údajů, které mohou být snadno zneužity. Společnost sice říká, že není důkaz o jakémkoli zneužití

[54] Byznys.ihned.cz, Aleš Černý, [online]. ©2013 [cit. 2015-02-20]. Dostupné z: http://byznys.ihned.cz/c1-61453470-uoou-udelil-komercni-bance-pokutu-1-8-milionu-korun-za-cervencovy-unik-dat

[55] Ictsecurity.cz,Nezávislý odborný online magazín ICT security [online]. ©2014 [cit. 2015-02-22].Dostupné z: http://ictsecurity.cz/aktualne/jak-reagovat-na-unik-dat-z-aukcniho-portalu-ebay.html

těchto údajů, počet těchto údajů je však enormní**.** Udává se, že unikly e-mailové adresy a telefonní čísla 6 milionů uživatelů a dostaly se k dalším uživatelům, kteří s nimi mohli nakládat dle svého uvážení.. K chybě došlo díky neúmyslně špatnému uložení údajů, jež Facebook shromažďuje a na jejichž základě posílá doporučení na přidání některých přátel. Facebook ve svých prohlášeních dále oznamuje, že k uniklým údajům neměli přístup vývojáři ani firmy**,** neunikly žádné další citlivější informace a společnost nezaznamenala žádné stížnosti uživatelů**.** [56]

Krádeže identity v USA

Trestné činy krádeže identity jsou stále na vzestupu**.** Počet: 13 100 000 dospělých se stalo obětmi podvodu krádeže identity ve Spojených státech v průběhu roku 2013. Krádeže identity byly hlavním tématem Federal Trade Commission v roce 2013**.** Pomocí různých metod, zločinci ukradli čísla sociálního zabezpečení, čísla řidičských průkazů, čísla debetních karet a další údaje týkající se identity jednotlivců jako například datum narození. [57]

Úniky dat budou největším reputačním rizikem v roce 2015

Ani mohutné investice do zabezpečení informačních technologií nestačí. Přestože firmy vynaložily za rok (2014) přes 70 miliard USD a v příštím roce vynaloží až 77 miliard USD na bezpečnosti IT (údaje spol. Gartner), téměř 90 % specialistů v oblasti IT má velkou obavu, že budou v roce 2015 čelit úniku dat.[58]

[56] Prisma.cz, [online]. ©2013 [cit. 2015-02-22]. Dostupné z: http://prisma.cz/facebook-zaznamenal-dalsi-unik-osobnich-udaju/

[57] Privacy Rights Clearinghouse, ,©2014 [cit. 2015-02-27]. Dostupné z: https://www.privacyrights.org/coping-identity-theft-reducing-risk-fraud

[58] Hkstrategies.cz, [online]. ©2015 [cit. 2015-02-22]. Dostupné z: :http://hkstrategies.cz/cs/Aktuality/%C3%9Aniky-dat-budou-nejv%C4%9Bt%C5%A1%C3%ADm-reputa%C4%8Dn%C3%ADm-rizikem-v-roce-2015#.VQREXY6G--0

4.3 Postavení veřejnosti k ochraně osobních údajů v ČR

Pro komplexní pochopení dané problematiky týkající se ochrany osobních údajů a eventuální přizpůsobení legislativy je třeba znát i názory těch, na které právní úprava dopadá, tedy občany daného státu, konkrétně pro tuto diplomovou práci jsou dotazováni respondenti z ČR.

4.3.1 Charakteristika vlastního dotazníkového šetření

Cíl a předmět ankety

Anketa měla za cíl zjistit postavení veřejnosti k ochraně osobních údajů v ČR.

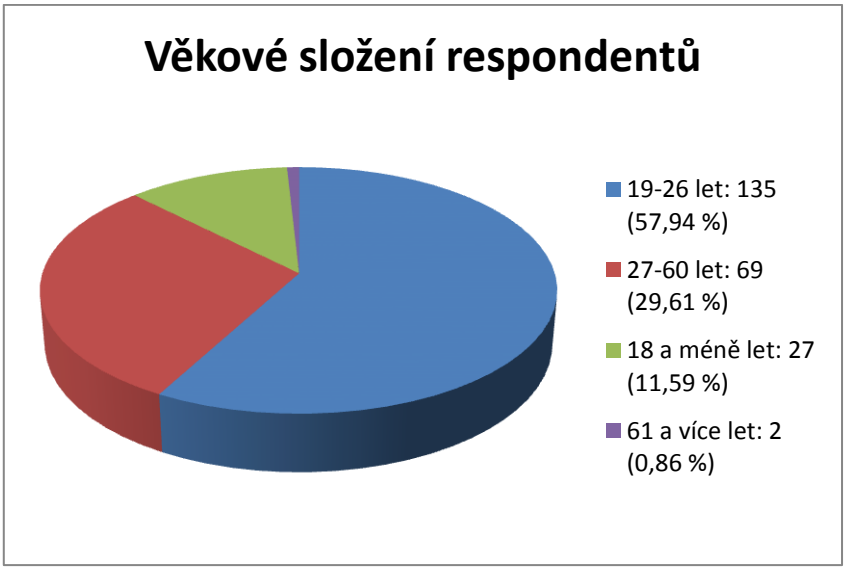
Předmětem šetření byly názory respondentů na tyto otázky:

1. „Myslíte si, že je ochrana osobních údajů v ČR bezpečně právně ošetřena?“
2. „ Dáváte si pozor na své osobní údaje?“
3. „Setkal/a jste se někdy s tím, že bylo s vašimi osobními údaji nezákonně zacházeno?“
4. „Ponechali jste někdy své osobní doklady například občanský průkaz či pas v hotelové recepci či ve firmě?“
5. „Myslíte si, že ochrana osobních údajů na sociálních sítích jako je např. facebook.cz je dostatečná?“
6. „Čtete si poučení týkají se ochrany osobních dat a údajů?“
7. „Již jste se někdy setkali se zneužitím Vašich osobních údajů? „

4.3.2 Charakteristika respondentů

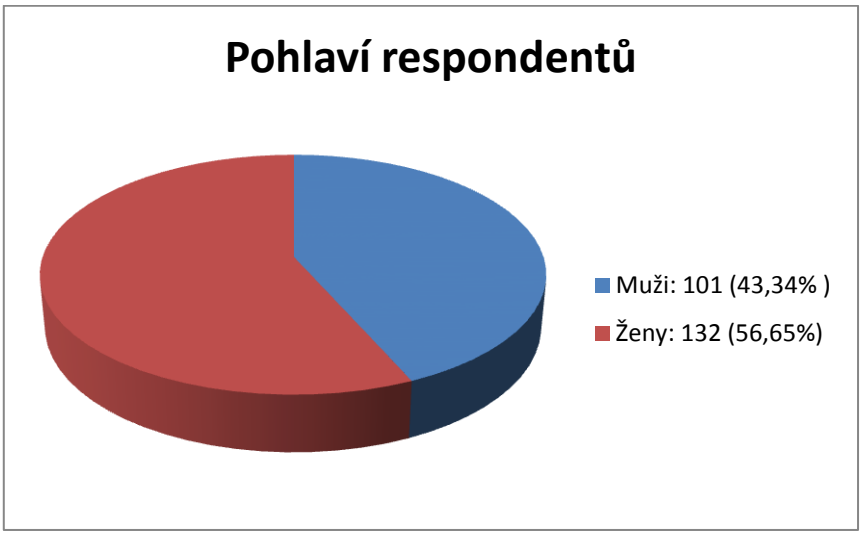
Cílovou populaci anketního šetření tvořili občané měst Prahy, Litoměřic, z toho odpovědělo 164 žen, 69 mužů a zbytek dotázaných pohlaví neuvedlo. Nejmladší respondent má 17 let a nejstaršímu je 72 let. Nejvíce respondentů bylo ve věku 19-26 let (57,94 %).[59]

[59] Vlastní zpracování



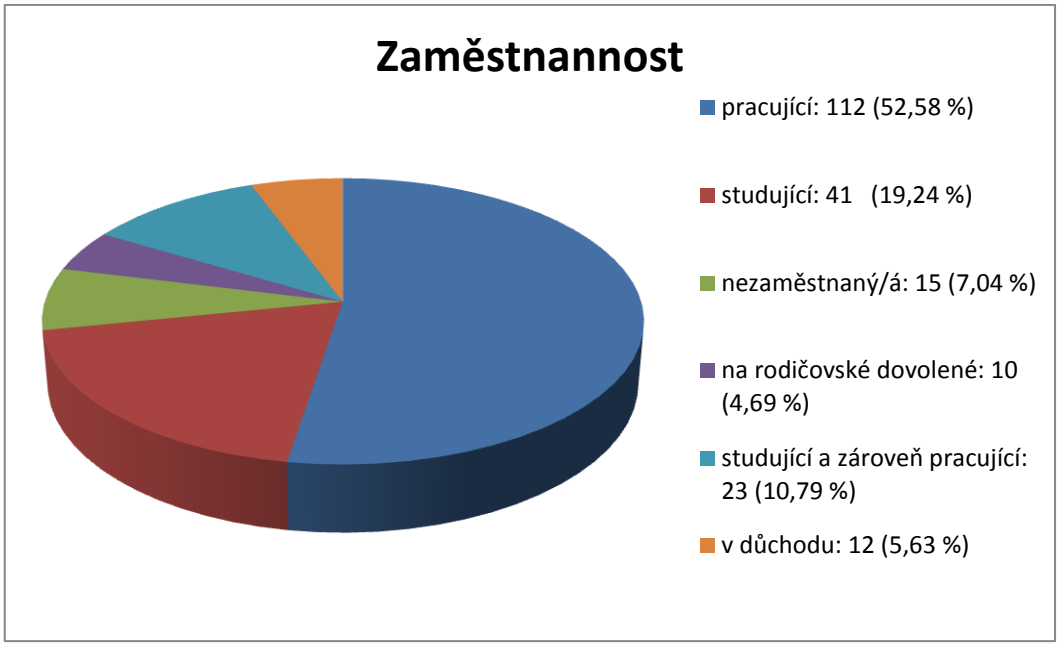
Graf č.1: Věkové složení respondentů

Zdroj dotazníkového šetření: vlastní zpracování



Graf č. 2: Pohlaví respondentů

Zdroj dotazníkového šetření: vlastní zpracování



Graf č. 3: Zaměstnanost (nezaměstnanost) respondentů

Zdroj dotazníkového šetření: vlastní zpracování

4.3.3 Analýza dat

Cekem bylo získáno a analyzováno 252 anketních lístků. U dílčích otázek se počet respondentů, kteří na danou otázku odpověděli, se liší. Zodpovězení otázek bylo dobrovolné. Absolutní i relativní četnosti u jednotlivých otázek jsou vypočítány pouze z relevantních odpovědí, nerelevantní chybějící a nejednoznačné odpovědi nebyly do výpočtu zahrnuty.

Termín realizace: sběr dat probíhal od 1. 1. 2015 do 25. 3. 2015.

4.3.4 Otázky a odpovědi dotazníkového šetření a grafické zpracování

Otázka č. 1: Myslíte si, že je ochrana osobních údajů v ČR bezpečně právně ošetřena?

Graf č. 4: Myslíte si, že je ochrana osobních údajů v ČR bezpečně právně ošetřena?

Zdroj dotazníkového šetření: vlastní zpracování

Otázka č. 2: Dáváte si pozor na své osobní údaje?

Graf č. 5:Dáváte si pozor na své osobní údaje?

Zdroj dotazníkového šetření: vlastní zpracování

Otázka č. 3: Setkal/a jste se někdy s tím, že bylo s vašimi osobními údaji nezákonně zacházeno?

Graf č. 6: Setkal/a jste se někdy s tím, že bylo s vašimi osobními údaji nezákonně zacházeno?

Zdroj dotazníkového šetření: vlastní zpracování

Otázka č. 4: Ponechali jste někdy své osobní doklady například občanský průkaz či pas v hotelové recepci či ve firmě?

Graf č. 7: Ponechali jste někdy své osobní doklady například občanský průkaz či pas v hotelové recepci či ve firmě?

Zdroj dotazníkového šetření: vlastní zpracování

Otázka č. 5: Myslíte si, že ochrana osobních údajů na sociálních sítích jako je např. facebook.cz je dostatečná?

Graf č. 8: Myslíte si, že ochrana osobních údajů na sociálních sítích jako je např. facebook.cz je dostatečná?

Zdroj dotazníkového šetření: vlastní zpracování

Otázka č. 6: Čtete si poučení týkající se ochrany osobních dat a údajů?

Graf č. 9: Čtete si poučení týkající se ochrany osobních dat a údajů?

Zdroj dotazníkového šetření: vlastní zpracování

Otázka č. 7: Již jste se někdy setkali se zneužitím Vašich osobních údajů?

Graf č. 10: Již jste se někdy setkali se zneužitím Vašich osobních údajů?

Zdroj dotazníkového šetření: vlastní zpracování

4.3.5 Shrnutí dotazníkového šetření

Z dat získaných anketním šetřením lze vyvodit tyto závěry:

Otázka č. 1.: „Myslíte si, že je ochrana osobních údajů v ČR bezpečně právně ošetřena?“Celkem odpovědělo: 230 respondentů, z toho 143 zvolilo možnost NE, 87 respondentů odvědělo ANO.

Otázka č. 2. : „Dáváte si pozor na své osobní údaje?“ Odpovědělo celkem 195 respondentů. Nejvíce respondentů 123 odpovědělo:„Snažím se, ale občas polevím v obezřetnosti“ .

Otázka č. 3.: „Setkal/a jste se někdy s tím, že bylo s vašimi osobními údaji nezákonně zacházeno?“ Odpovědělo celkem: 230 respondentů, z toho 151 zvolilo možnost NE, ANO odpovědělo 79.

Otázka č. 4.: „Ponechali jste někdy své osobní doklady například občanský průkaz či pas v hotelové recepci či ve firmě?“ Celkem odpovědělo:230 respondentů, z toho 99 zvolilo možnost NE, ANO 131.

Otázka č. 5.: „Myslíte si, že ochrana osobních údajů na sociálních sítích jako je např. facebook.cz je dostatečná?“ Celkem odpovědělo: 228 respondentů, z toho 173 zvolilo možnost NE, pouze 55 ANO.

Otázka č. 6: „Čtete si poučení týkající se ochrany osobních dat a údajů?“Celkem odpovědělo 233 respondentů. ANO 35, NE 198

Otázka č. 7: Již jste se někdy setkali se zneužitím Vašich osobních údajů? Odpovědělo celkem: 232 respondentů, z toho 168 zvolilo možnost NE, ANO odpovědělo 64.[60]

5 Zhodnocení výsledků

5.1 Komparace ČR a USA

V USA je ochrana osobních údajů řešena způsobem, který se svou koncepcí podstatně odlišuje od přístupu evropského. K dnešnímu dni USA nemá jediný zákon o ochraně osobních dat a údajů, který by se dal přirovnat směrnici EU o ochraně údajů. Legislativa týkající se ochrany dat ve Spojených státech má tendenci být přijata na základě ad hoc, s právními předpisy vyplývající pokud to okolnosti vyžadují. Tyto zákony se obvykle vztahují pouze na situace, v nichž jednotlivci by nebyli schopni kontrolovat používání svých osobních údajů prostřednictvím samoregulace. Jako příklady lze uvést zákony o: „Zákon týkající se video ochrany soukromí z roku 1988, „ zákon o ochraně hospodářské soutěže a kabelové televize z roku 1992, zákon Fair Credit Reporting z roku 2010“. Spojené státy preferují přístup odvětvových právních předpisů na ochranu údajů, tento přístup se opírá o kombinaci právních předpisů, nařízení a samoregulace. Spojené státy spoléhají na autoregulaci průmyslu a „ bezstarostnou nedbalostí ekonomiku „ a zanedbávají význam státní legislativy.

Evropská unie na druhé straně, má jednotný zákon o ochraně osobních údajů a to směrnici EU o ochraně osobních údajů. Směrnice EU o ochraně osobních údajů upravuje zpracování osobních údajů v rámci Evropské unie a je důležitou součástí práva EU o ochraně soukromí a lidských práv. Rozsálhlé evropské nařízení o ochraně osobních je odůvodněno s ohledem na zkušenosti v rámci druhé světové války – éra fašistické vlády a poválečných

[60] Vlastní zpracování, Survio.com , [online]. ©2015 [cit. 2015-03-27].Sběr dat byl realizován online formou dostupné z: http://www.survio.com/survey/d/K5S4A2D9E0H2Y8F7O dále ve vytištěné podobě- dotazníky viz přílohy.

komunistických režimů, kde bylo rozšířeno nekontrolovatelné použití osobních údajů. Druhá světová válka poválečné období byla doba v Evropě, že zveřejnění rasy nebo etnického původu vedlo k tajným výpovědím v pracovních táborech a koncentračních táborech.

Jednoduše řečeno, ochrana údajů ve Spojených státech je téměř zcela zabývá bezpečností citlivých a utajovaných informací. V Evropě (a dalších zemí), ochrana dat má málo co do činění s bezpečností, ale co do činění s právy jednotlivců napadat vlády a podniky ve způsobu, jakým nakládá s osobními soukromých informací uchovávaných v počítačových systémech.

ČR chrání své občany, ale díky svému byrokratickému aparátu a velice přísným pravidlům nedostatečně podporuje obchod. Spojené státy na druhou stranu příliš spoléhají na autoregulaci průmyslu a zanedbávají význam státní legislativy.

Komparace Sankce a postihy za porušení zákonů týkajích se ochrany osobních dat a údajů v ČR a USA

USA: Federální zákon na ochranu spotřebitele (FTC Act) stanoví peněžitý trest až do výše 16,000 US$ za každé porušení. FTC může také dosáhnout soudního příkazu, odškodnění zákazníkovi, splacení nákladů na vyšetřování a trestní stíhání. Trestním postihem může být i uvěznění až na 10 let.Tresty za porušení zákona GLB jsou určeny úředním statusem organizace, která prosazení zákona navrhuje. Například prosazení navržené FTC by se mohlo týkat pokuty až do výše 16,000 US$ za jedno porušení zákona. Osoby mohou být potrestány pokutou ale i vězením až na 5 let, pokud od finanční instituce získají nebo se pokusí podvodně získat zákaznické informace vztahující se k jiné sobě, způsobí jejich zveřejnění/sdílení nebo se o to pokusí. Kromě toho existují trestní postihy za spáchání trestného činu narušení soukromí. Pro osoby je to 500,000 US$, pro instituce 1 milion US$, pokud je takový čin spáchán nebo byl učiněn pokus jej spáchat spolu s porušením jiného zákona Spojených států nebo jako součást protizákonné činnosti, která způsobila škodu vyšší než 100,000 US$ za jeden rok.

HIPAA ukládá občanskoprávní postihy jako pokuty od 100 do 1,5 milionu US$ v závislosti na množství činitelů vytvářejících trestný čin, včetně toho, zda provozovatel věděl, že určitá činnost byla narušením bezpečnosti, zda bylo toto narušení rychle

napraveno či zda šlo o vědomou nedbalost provozovatele. Trestní postih může dosáhnout až 250,000 US$ a až 10 let vězení, pokud je čin spáchán na základě falešných údajů nebo s cílem prodat data pro finanční zisk.[61]

ČR: Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů § 44-46 . Přestupku se dopustí a pokutou do výše 50 000 Kč bude potrestána osoba, která je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru nebo pro něj vykonává činnosti na základě dohody, nebo osoba, která v rámci plnění zákonem uložených oprávnění a povinností přichází do styku s osobními údaji správce nebo zpracovatele, pokud poruší povinnost mlčenlivosti uloženou podle tohoto zákona. Přestupku se dopustí a pokutou do výše 25 000 Kč bude potrestána osoba uvedená v odstavci 1, pokud poruší jinou povinnost stanovenou tímto zákonem. Na přestupky a jejich projednávání se vztahuje zvláštní právní předpis. K projednávání přestupků je příslušný Úřad. § 45 Pořádková pokuta Osobě, která neposkytne Úřadu při výkonu kontroly potřebnou součinnost, může být uložena pořádková pokuta do výše 25 000 Kč, a to i opakovaně.

Pokutou do výše 10 000 000 Kč bude potrestán správce nebo zpracovatel, který poruší povinnost stanovenou tímto zákonem při zpracování osobních údajů. Pokud správce nebo zpracovatel do 1 roku ode dne, kdy nabylo rozhodnutí o uložení pokuty právní moci, porušil povinnosti stanovené tímto zákonem při zpracování osobních údaj opakovaně, může mu být uložena pokuta do výše 20 000 000 Kč. Správce nebo zpracovatel, který maří kontrolu prováděnou Úřadem, může být potrestán pořádkovou pokutou do výše 1 000 000 Kč, a to i opakovaně. Porušení povinností projednává Úřad. Při ukládání pokuty podle tohoto zákona vychází Úřad zejména z povahy, závažnosti, způsobu jednání, míře zavinění, doby trvání a následků protiprávního jednání. Pokutu lze uložit do 1 roku ode dne, kdy příslušný orgán porušení povinnosti zjistil, nejdéle však do 3 let ode dne, kdy k porušení povinnosti došlo. Pokutu vybírá Úřad. Pokutu vymáhá územní finanční orgán podle zvláštního právního předpisu. Více viz Zákon č. 337/1992 Sb., o správě daní a poplatků , ve znění pozdějších předpisů. Výnos pokut je příjmem rozpočtu republiky.[62]

[61] Data protection in United States, ©2014 [cit. 2015-02-27]. Dostupné z: http://uk.practicallaw.com/6-502-0467

[62] Museums.cz, [online]. [cit. 2015-02-22]. Dostupné z: http://www.cz-museums.cz/UserFiles/File/Legislativa/zakon-101-2000.pdf

6 Závěr

Ochrana osobních údajů představuje jednu z klíčových oblastí ochrany soukromí. Právo na soukromí je ústředním pilířem každé demokratické společnosti a v dnešním silně informačním věku, klade proti sobě dvě frakce jak jednotlivce, tak organizace, které vedou debatu o omezení přístupu k osobním údajům. Na jedné straně máme občany a jejich práva na soukromí týkající se osobních údajů a na druhé straně máme společnosti, které tvrdí, že ochrana údajů brání toku dat a tím brání obchodu. Jako dozor a dohled fungují vlády, které by měly chránit soukromí a zároveň posilovat obchod.

Když se podíváme kolem sebe, všude vidíme a slyšíme o moderních technologiích, globalizaci a bydlení v moderní progresně řízené společnosti. Za posledních 30 let nastal obrovský skok ve světě počítačů, automatizace a jejich tvůrci mají významné postavení v globální ekonomice. Problematika soukromí je propojena s rozvíjejícími se novými technologiemi, které mají vliv na soukromý sektor působící na trhu, na koncové uživatele a také vládu, která nese odpovědnost dohledu.

Předmětem této srovnávací studie je Česká republika a Spojené státy Americké, které na jedné straně představují výrazně odlišný přístup ke koncepci ochrany údajů v demokratické zemi, a na druhé straně představují významné pravomoci a vzory na mezinárodní scéně. Vzhledem k odlišné historii každé země a mnoha různých kulturních hodnot, neexistuje jednotný zastřešující právní předpis, protože každá země přistupuje k ochraně osobních údajů svým vlastním způsobem.

ČR je parlamentní, demokratický právní stát s liberálním státním režimem a politickým systémem založeným na svobodné soutěži politických stran a hnutí. Ochrana osobních údajů je tématem rozvíjejícím se až od 70. let 20. století. V České republice do roku 1989 ochrana soukromí a ochrana osobních údajů takřka neexistovala, prvním zákonem byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, poté následoval zákon č. 101/2000 Sb., o ochraně osobních údajů, poté vše završil zákon č.439/2004 Sb., tzv. Euronovela.

USA je federativní prezidentská republika v Severní Americe. Spojené státy se skládají z 50 států, 1 federálního území s hlavním městem a sídlem prezidenta, Kongresu a Nejvyššího soudu (District of Columbia) a celkově 14 zámořských území, z nichž 5 je obydlených. Ochrana dat je velmi komplexní a široké téma. V USA je ochrana osobních údajů řešena způsobem, který se svou koncepcí podstatně odlišuje od přístupu evropského.

V USA neexistuje jediný, komplexní federální (národní) právní předpis upravující shromažďování a využívání osobních údajů. Místo toho, USA má tzv. "patchwork" systém federálních a státních zákonů a předpisů, které se navzájem překrývají, zapadají a mohou si vzájemně protiřečit. Kromě toho, existuje mnoho směrnice, které jsou vypracované vládními agenturami a průmyslovými skupinami, které nejsou právně vymahatelné, ale jsou součástí samoregulačních snah a jsou považovány za "nejlepší praxi" Samoregulace je chápána jako klíčový prvek vyrovnat s rychlým pokrokem a stále se měnícím prostředí moderních technologií v provozu.

Zatímco se někteří domnívají, že v ČR je nadměrná byrokracie hlavně týkající se překážek pro volný trh, někteří zvažují samoregulaci jen jako mýtus, protože neprodukuje žádná vymahatelná pravidla a tedy nedostatečnou ochranu jednotlivců.

ČR chrání své občany, ale díky svému byrokratickému aparátu a velice přísným pravidlům nedostatečně podporuje obchod. Spojené státy na druhou stranu příliš spoléhají na autoregulaci průmyslu a zanedbávají význam státní legislativy.

Právní úprava v České republice je poměrně ucelená, avšak je nutné podotknout, že z pohledu běžného občana je náročné se v ní orientovat.

Postavení veřejnosti k ochraně osobních dat a údajů je následující, z provedeného průzkumu vyplývá, že Internet hraje pro občany dominantní roli, osobní údaje je prakticky provázejí v každém okamžiku jejich života, například při zřízení bankovního účtu, použití kreditní karty, zřízení zákaznických karet apod. Při všech těchto činnostech lidé poskytují své osobní údaje a často si neuvědomují následky, které mohou vzniknout poskytnutím osobních údajů.

Je třeba si uvědomit, že pro nalezení informací týkajících se osobních dat dnes stačí například to, že podnikáme nebo jsme vlastníky nemovitého majetku. Dnes je již možné najít naše komplexní osobní informace (místo trvalého pobytu, jméno a příjmení, rodné číslo, datum narození aj.) a to prostřednictvím veřejně dostupných databází jako je například Administrativní registr ekonomických subjektů, či náhled do katastru nemovitostí, tyto informace však byly dostupné již dříve a to prostřednictvím veřejné správy. Ovšem dříve se podávala žádost a případně platil příslušný poplatek. Z toho vyplývá, že osobní údaje nebylo tak jednoduché získat jako je tomu dnes. Je proto nezbytně nutné, aby těmto skutečnostem odpovídala platná legislativa a byla také dodržována. Ochrana osobnosti a ochrana osobních údajů je v každé demokratické společnosti bezesporu jedním z nejdůležitějších práv.

7 Použitá literatura

Knižní literatura

1. BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané problémy*. 3. vydání. 277 pages. ISBN 978-808-6131-962.
2. KUČEROVÁ, Alena a František NONNEMANN. *Ochrana osobních údajů v praktických příkladech*. Vyd. 1. Praha: BOVA POLYGON, 2013, 167 s. ISBN 978-80-7273-173-2.
3. KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Vyd. 1. Praha: C.H. Beck, 2012, xvii, 516 s. Beckova edice komentované zákony. ISBN 978-80-7179-226-0
4. MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. *Ochrana osobních údajů*. Praha: Leges, 2012, 206 s. Praktik. ISBN 978-808-7576-120.

Internetové zdroje

1. Byznys.ihned.cz, Aleš Černý, [online]. ©2013 [cit. 2015-02-20]. Dostupné z: http://byznys.ihned.cz/c1-61453470-uoou-udelil-komercni-bance-pokutu-1-8-milionu-korun-za-cervencovy-unik-dat
2. Česká televize, ČT 24, Pavla Freiwaldová [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/274905-dluzili-jste-z-registru-dluzniku-se-jen-tak-nedostanete/
3. Hkstrategies.cz, [online]. ©2015 [cit. 2015-02-22]. Dostupné z: :http://hkstrategies.cz/cs/Aktuality/%C3%9Aniky-dat-budou-nejv%C4%9Bt%C5%A1%C3%ADm-reputa%C4%8Dn%C3%ADm-rizikem-v-roce-2015#.VQREXY6G--0
4. Ictsecurity.cz,Nezávislý odborný online magazín ICT security [online]. ©2014 [cit. 2015-02-22].Dostupné z: http://ictsecurity.cz/aktualne/jak-reagovat-na-unik-dat-z-aukcniho-portalu-ebay.html
5. Mesec.cz,Petr Bukač [online]. ©2004 [cit. 2015-02-22]. Dostupné z: http://www.mesec.cz/clanky/hlidejte-si-osobni-udaje/
6. Ministerstvo vnitra České republiky, [online] ©2015 [cit. 2015-02-22].Dostupné z:http://www.mvcr.cz/clanek/vyhlasky.aspx
7. Museums.cz, [online]. [cit. 2015-02-22]. Dostupné z: http://www.cz-museums.cz/UserFiles/File/Legislativa/zakon-101-2000.pdf
8. Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: : http://www.novinky.cz/internet-a-pc/324208-hackeri-se-dostali-k-70-milionum-pinu-platebnich-karet-zakazniku-obchodniho-retezce.html

9. Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.novinky.cz/internet-a-pc/326184-hackeri-ukradli-data-k-e-mailum-spolecnosti-yahoo.html
10. Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.novinky.cz/internet-a-pc/331114-v-cesku-padla-rekordni-pokuta-za-spam-firma-musi-zaplatit-480-tisic.html
11. Novinky.cz, [online]. ©2014 [cit. 2015-02-22]. Dostupné z: http://www.novinky.cz/zahranicni/amerika/325794-tajne-sluzby-sbiraly-osobni-udaje-o-hracich-angry-birds.html
12. Prisma.cz, [online]. ©2013 [cit. 2015-02-22]. Dostupné z: http://prisma.cz/facebook-zaznamenal-dalsi-unik-osobnich-udaju/
13. Survio.com , [online]. ©2015 [cit. 2015-03-27]. Dostupné z: http://www.survio.com/survey/d/K5S4A2D9E0H2Y8F7O
14. Úřad pro ochranu osobních údajů, oblasti zpracování osobních údajů. [online]. ©2014 [cit. 2014-11-27]. Dostupné z: Dostupné z:https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267
15. Úřad pro ochranu osobních údajů, ochrana osobních údajů na pracovišti, příručka pro zaměstnance. Pro úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2014, ISBN 978-80-210-6819-3 [online]. ©2014 [cit. 2014-11-27]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691
16. Úřad pro ochranu osobních údajů, ochrana osobních údajů vybrané otázky Příručka pro podnikatele. Pro úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011, ISBN 978-80-210-5572-8 [online]. ©2011 [cit. 2014-11-27]. Dostupné z: http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3025
17. Úřad pro ochranu osobních údajů, Výběr ze zahraničních médií. [online]. [cit. 2015-02-22]. Dostupné z: https://www.uoou.cz/verejna-sprava-zakonodarstvi-a-soudnictvi/ds-2083/p1=2083
18. Úřad pro ochranu osobních údajů, změny zákona o ochraně osobních údajů. [online]. [cit. 2015-11-27]. Dostupné z: http://www.uoou.cz/zmeny-zakona-o-ochrane-osobnich-udaju/ds-3112/archiv=0&p1=1257&rd=1000
19. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, [online]. [cit. 2014-11-27]. dostupný z: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-kvetna-2014/ds-3109/archiv=0&p1=1261
20. Zákon č. 262/2006 Sb., zákoník práce. [online]. [cit. 2014-11-22] Dostupný z: http://business.center.cz/business/pravo/zakony/zakonik-prace/cast13h8.aspx

21. Zákony pro lidi. [online]. [cit. 2014-11-22] Dostupné z: http://www.zakonyprolidi.cz/hledani?text=kasina+

Internetové zdroje zahraniční:

1. Data protection in United States ©2014 [cit. 2015-02-27]. Dostupné z: http://uk.practicallaw.com/6-502-0467
2. Federal Trade Commission,©2014 [cit. 2015-02-27]. Dostupné z: http://www.ftc.gov/about-ftc
3. Federal Trade Commission,©2014 [cit. 2015-02-27]. Dostupné z: http://www.ftc.gov/about-ftc/foia
4. Privacy Rights Clearinghouse, ©2014 [cit. 2015-02-27]. Dostupné z: https://www.privacyrights.org/coping-identity-theft-reducing-risk-fraud

České Právní předpisy

1. usnesení č. 2/1993 Sb. předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.
2. Vyhláška 645/2004 Sb. ze dne 13. Prosince 2004, kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů, ve znění vyhlášky č. 213/2012 Sb.
3. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
4. vyhláška Ministerstva financí 285/1998 Sb. - Vyhláška o podmínkách monitorování a uchovávání záznamů v kasinu
5. zákon č. 100/1988 Sb., o sociálním zabezpečení, náležitosti průkazu mimořádných výhod
6. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů dostupný
7. zákon č. 106/1999 Sb., o svobodném přístupu k informacím
8. zákon č. 108/2006 Sb., o sociálních službách, informační systém o příspěvku na péči
9. zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních a o změně dalších zákonů
10. zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách

11. zákon č. 111/2006 Sb., o pomoci v hmotné nouzi
12. zákon č. 111/2009 Sb., o základních registrech
13. zákon č. 119/2002 Sb., o střelných zbraních a střelivu
14. zákon č. 123/1998 Sb., o právu na informace o životním prostředí
15. zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
16. zákon č. 128/2000 Sb., o obcích (obecní zřízení)
17. zákon č. 129/2000 Sb., o krajích (krajské zřízení)
18. zákon č. 129/2008 Sb., o výkonu zabezpečovací detence a o změně některých souvisejících zákonů
19. zákon č. 131/2000 Sb., o hlavním městě Praze
20. zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)
21. zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činností bývalé Státní bezpečnosti svazek s osobními údaji.
22. zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
23. zákon č. 153/1994 Sb., o zpravodajských službách České republiky
24. zákon č. 154/1994 Sb., o Bezpečnostní informační službě
25. zákon č. 159/2006 Sb., o střetu zájmů
26. zákon č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla)
27. zákon č. 18/2004 Sb., o uznávání odborné kvalifikace a jiné způsobilosti státních příslušníků členských států Evropské unie a některých příslušníků jiných států a o změně některých zákonů (zákon o uznávání odborné kvalifikace)
28. zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon)
29. zákon č. 185/2004 Sb., o Celní správě České republiky
30. zákon č. 187/2006 Sb., o nemocenském pojištění
31. Zákon č. 20/1966 Sb., o péči o zdraví lidu,
32. zákon č. 202/1990 Sb., o loteriích a jiných podobných hrách
33. zákon č. 21/1992 Sb., o bankách
34. zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

35. zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů
36. zákon č. 251/2005 Sb., o inspekci práce
37. zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
38. zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů
39. zákon č. 26/2000 Sb., o veřejných dražbách
40. zákon č. 262/2006 Sb., zákoník práce
41. zákon č. 269/1994 Sb., o Rejstříku trestů
42. zákon č. 273/2008 Sb., o Policii České republiky
43. zákon č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách
44. zákon č. 283/1993 Sb., o státním zastupitelství
45. zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon)
46. zákon č. 289/2005 Sb., o Vojenském zpravodajství
47. zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
48. zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů
49. zákon č. 325/1999 Sb., o azylu a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o azylu)
50. zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů
51. zákon č. 328/1999 Sb., o občanských průkazech
52. zákon č. 329/1999 Sb., o cestovních dokladech
53. zákon č. 337/1992 Sb., o správě daní a poplatků
54. zákon č. 344/1992 Sb., o katastru nemovitostí České republiky (katastrální zákon)
55. zákon č. 348/2005 Sb., o rozhlasových a televizních poplatcích a o změně některých zákonů
56. zákon č. 36/1967 Sb., o znalcích a tlumočnících

57. zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu)
58. zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
59. zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech),
60. zákon č. 40/1964 Sb., občanský zákoník
61. zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
62. zákon č. 435/2004 Sb., o zaměstnanosti
63. zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon)
64. zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů
65. zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)
66. zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů
67. zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
68. zákon č. 513/1991 Sb., obchodní zákoník
69. zákon č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky
70. zákon č. 553/1991 Sb., o obecní policii
71. zákon č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky
72. zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích
73. zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)
74. zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení
75. zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení
76. zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon)
77. zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti
78. zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění
79. zákon č. 85/1996 Sb., o advokacii
80. zákon č. 89/1995 Sb., o státní statistické službě

7.1 Seznam grafů

7.2 Seznam příloh

8 Přílohy

Příloha č. 1

Anketa v ČR

Vaše odpovědi prosím **ZAKROUŽKUJTE** u jednotlivých otázek vždy 1 číslo odpovědi, která nejlépe odpovídá Vašemu názoru či postoji.

Na úvod Vás prosím o několik statistických údajů (nejsou povinné).

Kolik Vám je let? …….

Pohlaví žena/muž

Jste:

studující

pracující

nezaměstnaný /á

na rodičovské dovolené

studující a zároveň pracující

v důchodu

1. **Myslíte si, že je ochrana osobních údajů v ČR bezpečně právně ošetřena?**

Ano

Ne

2. Dáváte si pozor na své osobní údaje?

Ano, dodržuji všechna pravidla

Snažím se, ale občas polevím v obezřetnosti

Jak kdy

Ne, když je někdo bude chtít, tak je stejně získá

Ne

3. **Setkal/a jste se někdy s tím, že bylo s vašimi osobními údaji nezákonně zacházeno?**

Ano

Ne

4. **Ponechali jste někdy své osobní doklady například občanský průkaz či pas v hotelové recepci či ve firmě?**

Ano

Ne

5. Myslíte si, že ochrana osobních údajů na sociálních sítích jako je např. facebook.cz je dostatečná?

1. Ano

2. Ne

6. Čtete si poučení týkající se ochrany osobních dat a údajů?“

Ano

Ne

7. Již jste se někdy setkali přímo se zneužitím Vašich osobních údajů?

Ano

Ne

DĚKUJEME VÁM ZA VAŠE ODPOVĚDI A ČAS ZTRÁVENÝ VYPLŇOVÁNÍM TÉTO ANKETY

Příloha č. 2

Ochrana osobních dat a údajů v ČR

Dobrý den,

věnujte prosím několik minut svého času vyplnění následujícího dotazníku.

1

Kolik vám je let?

- 18 a méně
- 19-26 let
- 27-60 let
- 61 a více let

2

Jste:

- žena
- muž

3

Jste:

- studující
- pracující
- nezaměstnaný/á
- na rodičovské dovolené
- studující a zároveň pracující
- v důchodu

4

Myslíte si, že je ochrana osobních údajů v ČR bezpečně právně ošetřena?

- ANO
- NE

5

Dáváte si pozor na své osobní údaje?

- Ano, dodržuji všechna pravidla
- Snažím se, ale občas polevím v obezřetnosti
- Jak kdy
- Ne, když je někdo bude chtít, tak je stejně získá
- Ne

6

Setkal/a jste se někdy s tím, že bylo s vašimi osobními údaji nezákonně zacházeno?

- ANO
- NE

7

Ponechali jste někdy své osobní doklady například občanský průkaz či pas v hotelové recepci či ve firmě?

- ANO

NE

8

Myslíte si, že ochrana osobních údajů na sociálních sítích jako je např. facebook.com je dostatečná?

ANO

NE

9

Čtete si poučení týkají se ochrany osobních dat a údajů?

ANO

NE

10

Již jste se někdy setkali přímo se zneužitím Vašich osobních údajů?

ANO

NE

ODESLAT DOTAZNÍK