Univerzita Karlova v Praze
Právnická fakulta

Ondřej Pavelka

Ochrana informací a osobních údajů v pracovněprávních vztazích

Diplomová práce

Vedoucí diplomové práce: JUDr. Martin Štefko Ph.D.

Katedra: Pracovního práva a práva sociálního zabezpečení

Datum vypracování práce (uzavření rukopisu): 4. 2011

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

V Praze dne 5. 4. 2011 Ondřej Pavelka

Obsah

Úvod

Máme-li se zabývat problematikou osobních údajů, musíme si uvědomit, že nás tento fenomén provází po celý život od okamžiku narození až do naší smrti. Takovýmto údajem je ostatně i rodné číslo, které každý považuje za samozřejmost. Jejich samotná existence, následné zpracování a manipulace s nimi nám mohou život značně zjednodušit, ale mohou také znamenat nemalé komplikace.

Běžný život si žádá neustálé zpřístupňování celé řady informací o naší osobě. Pokud se budeme kupříkladu ucházet o novou pracovní pozici, jistě sdělíme našemu budoucímu zaměstnavateli některé osobní údaje, které si od nás vyžádá. Tyto informace ale mohou být použity proti nám samotným, pokud se dostanou do neoprávněných rukou a budou zneužity. Je proto namístě věnovat tématu ochrany osobních údajů značnou pozornost.

Jistě nás nenapadne, pozastavit se nad tím, co jiným o sobě prozradíme a jak s touto informací tyto osoby naloží. Přitom je možné řadu skutečností o nás zjistit zcela běžně v rámci sociálního kontaktu (například mezi členy rodiny nebo na pracovišti) a nemusí být ani naším prvotním záměrem tyto informace komukoliv zpřístupnit. Osobním údajem je pak taková informace, která o nás jako o fyzické osobě něco vypovídá a je součástí našeho soukromí. Proto je nezbytné takovéto informace chránit a v moderní demokratické společnosti je právo na jejich ochranu považováno za samostatné základní lidské právo.

Ochrana osobních údajů nepochybně představuje v katalogu základní práv a svobod občanů jejich „*moderní dimenzi*“[1] a jako taková začíná být v poslední době brána vážně. Jako právní a společenský fenomén se začala výrazněji utvářet až na konci dvacátého století a to konkrétně v 70. letech. S tím se postupně začala hromadit i právní úprava, která se jejich zakotvením zabývá. Je to na jednu stranu spojeno s expanzí výpočetní techniky a elektronických komunikací a jejich začleňováním do každodenního života, které dramaticky zvýšilo riziko zpracování osobních údajů proti zájmům jednotlivce, na stranu druhou se jedná o projev celkové globalizace společnosti, s níž je spojena stále větší nutnost sdílet náš soukromý i pracovní život s ostatními.

[1] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. VI.

Jak již bylo naznačeno výše, jsou osobní údaje a jejich ochrana zařazovány na roveň základním právům každého, a proto také podléhají normativní úpravě v podobě právních předpisů různé právní síly. Nejde o úpravu ucelenou v jediný kodex, ale o celou soustavu zvláštních zákonů, které vznikají jako reakce na možnosti jednotlivce se svými osobními údaji manipulovat, a které mu mají poskytnout určité záruky a jistotu ochrany. Tyto zvláštní zákony mají i umožnit nalezení konkrétního a speciálního řešení pro každý případ, a to v souladu s právem vymezenými podmínkami. Podle mého názoru není toto řešení příliš vhodné pro občany, jelikož nepřehledná a neucelená právní úprava, která je takto vytvářena, neprospívá obecnému povědomí dané problematiky ochrany osobních údajů, dává prostor pro výskyt sporů a může způsobit interpretační i aplikační potíže. Na druhou stranu je tato problematika velmi mladá a prochází neustálými změnami nedovolujícími trvalé a přehledné uspořádání norem v jeden kodex. Projevem tohoto vývoje je i samotný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který je vždy třeba citovat právě s oním přídomkem „…ve znění pozdějších předpisů“. Tento zákon si za svou existenci prošel již sedmnácti dílčími novelizacemi a další budou v krátkém časovém horizontu nepochybně následovat. Dalším problémem, se kterým se zákonodárce při utváření norem upravujících ochranu osobních údajů potýká, je samozřejmě soulad těchto předpisů s mezinárodními dokumenty. Obšírněji se jimi budu zabývat na dalších stránkách této práce.

Vidíme, že není jednoduché ani pro tvůrce norem na ochranu před zneužíváním osobních údajů a norem týkajících se jejich zpracováváním upravit vše a postihnout každý možný případ. Mým záměrem je pokusit se v této práci popsat jednak obecné otázky, jako je samotné přiblížení pojmu „osobní údaj“, dále se blíže pozastavit nad jednotlivými fázemi zpracování osobních údajů a nad subjekty, kterých se toto zpracování týká. Nemohu opomenout ani konkrétní práva a povinnosti účastníků pracovněprávních vztahů, tedy zaměstnavatele a zaměstnance vyplívající z platné legislativy. Na závěr se pak budu snažit odkrýt některé praktické problémy vyskytující se v souvislosti se zpracováním osobních údajů, jako jsou kamerové systémy v prostorách zaměstnavatele nebo tzv. Preemployment Background Screening, tedy možnost zaměstnavatele si ověřit informace mu poskytnuté uchazeči o zaměstnání.

1. Právní úprava ochrany osobních údajů v České republice

1.1 Ústavněprávní rovina

Jako jinde i v případě principů ochrany soukromí jednotlivce a tím i osobních údajů jsou východiskem právní úpravy ustavně právní principy. Jejich cílem je nastolit rovnováhu mezi ochranou práv a právem chráněných zájmů jednotlivce, na straně druhé garantovat právo každého jedince na informace.

Základem pro současnou právní úpravu je evropská Úmluva o ochraně lidských práv a základních svobod (dále jen „Úmluva“). Na ni se vztahuje čl. 10 ústavního zákona č. 1/1993 Sb., Ústava České Republiky, ve znění pozdějších ústavních předpisů (dále jen „Ústava“), podle něhož „ *vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, jsou součástí právního řádu; stanoví-li mezinárodní smlouva něco jiného než zákon, použije se mezinárodní smlouva*.“ Ve svém čl. 8 Úmluva deklaruje, že *„ každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence*“. Dále pak v čl. 10 Úmluva stanoví svobodu projevu, což je protikladem výše zmíněného práva na respektování soukromí.

V České republice se nesetkáme s vyjádřením těchto práv přímo v Ústavě, ale další pramen práva nejvyšší právní síly a to Listina základních práv a svobod, vyhlášena ústavním zákonem č. 23/1991 Sb. a republikována usnesením předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku ČR, ve znění zákona č. 162/1998 Sb. (dále jen „Listina“) je již vymezuje. Konkrétně v čl. 10 a 17 Listiny nalezneme ustanovení deklarující zároveň právo na šíření a shromažďování informací, ale i právo na ochranu před jejich šířením a shromažďováním. Článek 10 Listiny v odstavci 2 stanoví, že „ *každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života*.“ V odstavci 3 pak, že „ *každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě*.“ Následně v ustanovení čl. 17 Listina zaručuje každému právo „ *svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice států*.“

Nelze prohlásit, že by byla ochrana našeho soukromí neomezená a absolutní není ani právo na informace. Kromě zásahů neoprávněných budou jistě existovat i případy, kdy k zásahu do našeho soukromí dojde v souladu se zákonem, Listina nám v tomto smyslu však žádné bližší informace neposkytuje. Zde se jako příklad nabízí již výše zmiňované právo „ *svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice států*."

Chceme-li informace vyhledávat, setkáme se s dalším úskalím. Nikde v Listině totiž nenajdeme ustanovení, které by subjektu ukládalo povinnost předmětné údaje poskytovat. Je evidentní, že pokud by je zákonodárce takto stanovil, zcela by tím popřel ono Listinou garantované právo na ochranu soukromí. Jistá povinnost určité informace poskytovat však v Listině upravena je a to v ustanovení čl. 17 odst. 5, kde je stanoveno, že „ *státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti*." Dalo by se tedy říci, že záleží na konkrétní osobě, do jaké míry bude ochotna informace o sobě sdělit a následně umožní i jejich šíření. V Listině existuje ale i jiné omezení práva informace vyhledávat a šířit. Nalezneme jej v ustanovení čl. 17 odst. 4, podle kterého je možné toto právo „*omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti*." Navíc je toto ustanovení „*určitým logickým doplňkem ustanovení čl. 10 Listiny*"[2], protože samo o sobě vyzývá k ochraně práv druhých.

Z jednotlivých článků Listiny je zřejmé, že právo na ochranu soukromí je vázáno na konkrétní vymezení oprávněných a neoprávněných zásahů. Naproti tomu pro právo šířit a vyhledávat informace není takového vymezení třeba. V tomto případě je pouze stanovena možnost ho v určitých zákonem stanovených případech omezit.

1.2 Zákonná úprava

Jak již bylo zmíněno v úvodu této práce, zvláštní zákonná úprava má za cíl nalezení konkrétního řešení pro každý případ. Je na běžném zákonu, aby blíže specifikoval Listinou stanovené mantinely ochrany osobních údajů a práva na informace. Zákon může vymezit míru ochrany soukromí jakožto i míru ochrany před

[2] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 7.

neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů a současně tím může právo informace svobodně vyhledávat, jak stanoví Listina v čl. 17, omezit. Nebo zákon přímo určí, které informace jsou subjekty povinny poskytovat nebo strpět případy, kdy s nimi bude nakládáno. Zde se upřednostní právo na přístup k informacím a zároveň se zdůrazní skutečnost, že se v tomto případě nejedná o zásahy do soukromí neoprávněné.

Uděláme-li malý exkurz do naší právní historie, od roku 1948 až do pádu komunistického režimu se o ochraně osobních údajů a obecně ochraně soukromí v naší legislativě nedalo hovořit. Teprve zformováním katalogu základních práv a svobod, který představovala Listina, se otevřel prostor pro formulaci a zakotvení dané problematiky.

Po přijetí Listiny byl přijat **zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech**, který našel inspiraci v Úmluvě Rady Evropy č. 108/1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat (dále jen „Úmluva č. 108“). Ta zakotvila principy ochrany osobních údajů, které jsou dále rozvedeny právními předpisy jednotlivých členských zemí Evropské unie, a lze ji v tomto směru považovat za „*základní evropský dokument*“[3]. Zákon definoval klíčové pojmy dané oblasti a stanovil podmínky nakládání s osobními údaji včetně povinností, které byly s nakládáním spojeny (jednalo se o povinnosti provozovatelů takových informačních systémů a také fyzických a právnických osob provádějících činnost v souvislosti s provozem informačních systémů). Již se však nevztahoval na manuální zpracování osobních údajů a v tomto směru bylo nutné jeho ustanovení přiměřeně aplikovat. Dále text zákona neobsahoval ani úpravu sankcí pro případ jeho porušení, nebyl zřízen ani zvláštní dozorový orgán. To byl také hlavní důvod, proč Česká republika k Úmluvě č. 108 zpočátku nepřistoupila.

Zlepšení situace nastalo až s přípravami na vstup České republiky do Evropské unie. Kritika nedostatečné právní ochrany a nutnost dosažení kompatibility českého práva s komunitárním vedla k přijetí **zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“)**

[3] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 11.

Zavedení tohoto předpisu do našeho právního řádu znamenalo jednak garanci před neoprávněným zásahem do soukromí každého člověka a současně posílilo postavení jednotlivce jako subjektu údajů, jelikož mu zákon o ochraně osobních údajů propůjčil postavení oprávněné osoby. Do praxe byly uvedeny instituty jako je souhlas subjektu údajů se zpracováním údajů o své osobě, možnost být informován o krocích, kterými osobní údaje procházejí v rámci jejich zpracování a návrh zákona byl zároveň koncipován tak, že rozlišil automatizované a neautomatizované zpracování osobních údajů, což se dá považovat za velký přínos.

Zákon o ochraně osobních údajů v současné podobě pokrývá ochranu osobních údajů týkajících se fyzických osob, práva a povinnosti při jejich zpracování, podmínky přenosu osobních údajů do zahraničí, zřizuje Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) jako orgán dozoru a jeho ustanovení by měla být vyvážena tak, *„aby se nestala komplikací v běžném životě občana, ale reflektovala jeho běžné potřeby*“[4]. Je z mého pohledu asi nejdůležitější součástí legislativní úpravy ochrany osobních údajů v České republice. Definuje základní pojmy, bez kterých by bylo možno ochranu zajistit jen velmi komplikovaně, a i přes některá jeho ustanovení umožňující někdy, dle mého názoru, až příliš široký výklad je plně životaschopný. I v rámci pracovněprávních vztahů bude aplikace tohoto právního předpisu klíčová a rozbor jeho jednotlivých částí tak bude hlavní náplní této práce.

Oblast práva chránícího soukromí, kam patří i ochrana osobních údajů, je velice široká a pokrývá ji hned několik zákonů, proto na tomto místě uvedu ty podstatné.

Obecným právním předpisem z pohledu ochrany soukromí je **zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)**. Základem této právní úpravy je v § 11 uvedený výčet jednotlivých dílčích osobnostních práv, kterými jsou právo na ochranu života a zdraví, občanské cti, lidské důstojnosti, soukromí, jména a projevů osobní povahy. Každé fyzické osobě je garantována možnost nakládat se svými osobnostními právy dle jejího uvážení a v mezích právního řádu. Vyplývá to z dikce § 12 občanského zákoníku, který říká, že „*písemnosti osobní povahy, podobizny, obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy, smějí být pořízeny nebo použity jen s jejím svolením*.“ Svolení pak není zapotřebí k úředním účelům na základě zákona a stejná

[4] Důvodová zpráva k vládnímu návrhu zákona o ochraně osobních údajů.

výjimka platí i pro účely vědecké, umělecké či pro potřeby hromadných sdělovacích prostředků.

Relativně nová úprava obsažená v zákoně č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „zákoník práce“) umožňuje, aby byl dle zásady „co není zakázáno, je dovoleno“ na vztahy vyplývající z pracovní smlouvy, dohody o provedení práce nebo dohody o pracovní činnosti aplikován i občanský zákoník. Výše vyjmenovaná osobnostní práva tak budou chráněna před neoprávněnými zásahy ze strany zaměstnavatele např. ve formě rozšiřování nepravdivých údajů z osobního života zaměstnance, uveřejňování nepravdivých údajů ve sdělovacích prostředcích apod. Zaměstnanci mohou v případě porušení svých práv požadovat od zaměstnavatele jednak formu morálního zadostiučinění, a pokud by toto nestačilo, je možno se domáhat se náhrady nemajetkové újmy v penězích.

Ochrana poskytovaná občanským zákoníkem je široká a to i v porovnání s úpravou zákona na ochranu osobních údajů, která je konkrétnější a snaží se více apelovat na prevenci. V § 1 občanského zákoníku se uvádí, že vztahy „ *vyplývající z práva na ochranu osob*“ jsou předmětem jeho úpravy, pokud tyto vztahy neupravují zákony jiné, což znamená, že v případě zpracování osobních údajů by se měl přednostně aplikovat zákon o ochraně osobních údajů.

Dalším právním předpisem, který má chránit soukromí na pracovišti bude z našeho pohledu již výše zmiňovaný **zákoník práce**. I přes to, že je tento zákon pro úpravu pracovněprávních vztahů podstatný, působí jeho obsah z hlediska ochrany osobních práv zaměstnanců a jejich soukromí velmi povrchně. Velká část řešení této problematiky je tak ponechána na jiných právních předpisech nebo na rozhodovací činnosti soudů.

Zásadním ustanovením je § 316 zákoníku práce, kde je konstatováno, že „*zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovišti 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*.“ Pokud existuje na straně zaměstnavatele závažný důvod spočívající ve zvláštní povaze jeho činnosti, mohou být výše zmíněné kontrolní mechanizmy zavedeny pouze po předchozím informování

zaměstnance. Tomu musí být zároveň znám rozsah prováděné kontroly stejně jako její způsob. Zaměstnanec tak může očekávat, že bude přiměřeně zachováno jeho právo na soukromí i v pracovněprávních vztazích, ovšem nejsou opomenuty ani zájmy zaměstnavatele, který má logicky oprávnění vyžadovat od zaměstnance efektivní plnění pracovních úkolů po celou pracovní dobu včetně jejich kontroly. Sledována mohou být za těchto podmínek rovněž i rizika spojená s ochranou majetku zaměstnavatele, který může být poškozen zaměstnanci při výkonu práce.

Dále zaměstnavatel nesmí vyžadovat od svých zaměstnanců informace, které bezprostředně nesouvisejí s výkonem práce a příslušným pracovněprávním vztahem (jsou to informace o těhotenství, rodinných a majetkových poměrech, původu, sexuální orientaci, členství v odborové organizaci, členství v politických stranách nebo hnutích, příslušnost k církvi nebo náboženské společnosti a trestněprávní bezúhonnosti) a takové informace nesmí zaměstnavatel získávat ani prostřednictvím třetích osob[5]. Výjimky z uvedeného zákazu zákon připouští u informací o těhotenství, rodinných a majetkových poměrech a trestněprávní bezúhonnosti a to za předpokladu, že je pro to dán důvod v povaze vykonávané práce. Touto úpravou je respektován zákaz přímé i nepřímé diskriminace a dodržování rovnosti v pracovněprávních vztazích. Ve spojení s § 30 zákoníku práce jsou touto cestou rovněž zaručeny totožné „startovací“ podmínky pro uchazeče o zaměstnání.

Zákonem, který má zajišťovat právo veřejnosti na přístup k informacím a souvisí s osobními údaji, **je zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdější předpisů (dále jen „zákon o svobodném přístupu k informacím“).** Jako subjekty povinné uvádí v § 2 státní orgány, orgány územní samosprávy a veřejné instituce hospodařící s veřejnými prostředky, ty potom poskytují informace týkající jejich činnosti. Dalšími subjekty zákonem označené za povinné, jsou ty, které rozhodují na základě zákona o právech a povinnostech občanů a právnických osob. Z výše uvedeného vyplývá, že zákon o svobodném přístupu k informacím tak v žádném případě nestanoví povinnost pro soukromé subjekty. Oprávněným je dle této právní úpravy žadatel, tedy každá právnická nebo fyzická osoba, která žádá o informaci.

Nemohu opomenout ani zákon **č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon**

[5] Viz § 316 odst. 4 zákoníku práce.

o evidenci obyvatel“). Ten neupravuje pouze problematiku základního identifikátoru každého z nás, tedy rodného čísla a jeho využití. Kromě toho tento právní předpis svěřuje ÚOOÚ dohled nad neoprávněným nakládáním s rodnými čísly.

Pokud bychom uvažovali o zpracování veřejně přístupných osobních údajů, mohli bychom zmínit i příklady speciální právní úpravy k zákonu o ochraně osobních údajů. Je to jednak **zákon č. 513/1991 Sb., obchodní rejstřík, ve znění pozdějších předpisů**, do kterého se zapisují údaje o podnikatelích včetně některých osobních údajů. Dalším příkladem je i **zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů**, který řeší vedení živnostenského rejstříku obsahujícího také osobní údaje.

2. Evropská úprava

Z hlediska ochrany jsou základními prameny již výše zmíněná Úmluva č. 108 a dále Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů (dále jen „směrnice 95/46/ES“). Principy v nich obsažené našly svůj předobraz v Pravidlech pro ochranu soukromí a přeshraniční toky osobních údajů (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), jakožto dokumentu Organizace pro hospodářskou spolupráci a rozvoj (OECD). Tato pravidla byla vydána v roce 1980 a stala se jakousi kolébkou úpravy ochrany osobních údajů na celosvětové úrovni.

Úmluva č. 108 byla přijata ve Štrasburku dne 28. 1. 1981 a jako ucelený dokument se stala pro všechny k ní přistoupivší státy závaznou. Česká republika ji podepsala až dne 8. 9. 2000 a tímto datem byl zahájen i proces její ratifikace, který byl završen v červenci 2001. Zpoždění s jejím přijetím zapříčinily problémy s naší legislativou, která neodpovídala standardům stanovených v Úmluvě č. 108, a bylo nutné tento nesoulad odstranit. Následně na základě iniciace ze strany ÚOOÚ Česká republika ratifikovala v září 2003 dodatkový protokol k úmluvě a stala se v pořadí čtvrtým státem, který k němu přistoupil.

Jak je uvedeno v preambuli k Úmluvě č. 108, signatářské státy podpisem úmluvy potvrdily své závazky ve prospěch svobody informací bez ohledu na hranice za současného zachování základní hodnoty úcty k soukromí a zachování volného toku informací mezi lidmi. V článku 1 pak nalezneme vymezení předmětu a účelu této právní úpravy, kterým je „ *zaručit na území každé smluvní strany každé fyzické osobě, ať je jakékoliv národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují („ochrana údajů“)*.“

Směrnice 95/46/ES stanoví základní povinnosti při zpracování osobních údajů a dále upravuje práva jednotlivců vyplývající ze zneužití jejich osobních údajů. V článku 1 je deklarováno odstraňování překážek bránících společnému hospodářskému a sociálnímu pokroku a zachování standardů základních lidských práv přiznávaných v ústavách a zákonech členských států a ustanoveními Evropské úmluvy o ochraně

lidských práv a základních svobod. V souladu s tím zavedení společných standardů ochrany soukromí umožňuje volný pohyb osobních údajů v rámci celé Evropské unie. Článek 2 pak tuto volnost pohybu informací omezuje konstatováním, že „*systémy zpracování údajů slouží lidem*“ a tudíž „*musí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat základní svobody a práva těchto osob, zejména právo na soukromí*“.

Směrnice ovšem nemá obecnou závaznost, „*je adresována členským státům a závaznost se omezuje na cíle*“[6]. Členské státy mají určitou lhůtu na dosažení předepsaného stavu, přičemž je jim ponechám výběr metody a formy, jak takto učiní.

Mimo tyto dva klíčové právní předpisy tedy Úmluvu č. 108 a směrnici 95/46/ES mohu zmínit ještě Rozhodnutí Komise 2001/497/ES o standardních smluvních podmínkách pro přenos osobních údajů zpracovatelům umístěným ve třetích zemích, které bere postup subjektu přenášejícího údaje do zemí mimo EU v souladu se směrnicí 95/46/ES jako poskytnutí odpovídajícího stupně právní ochrany.

Aktivity Rady Evropy v oblasti ochrany osobních údajů se ovšem netýkají pouze legislativní činnosti. Vydává řadu doporučení zaměřených na ochranu dat v citlivých nebo problémových oblastech jako jsou např. sociální zabezpečení, policejní činnost, personalistika, veřejná správa a nové informační technologie. Rada Evropy rovněž průběžně monitoruje proces přistupování jednotlivých států k Úmluvě č. 108 a úroveň jejich ochrany osobních údajů podle rozličných kritérií, jako např.: zda byla Úmluva č. 108 podepsána (ratifikována), existence specifické národní legislativy v oblasti ochrany osobních údajů, rozsah aplikační oblasti (manuální či automatizované zpracování), působnosti legislativy (právnické či fyzické osoby, veřejný a soukromý sektor), dále kritérium provádění oznamovací povinnosti či registrace a její rozsah, uplatňování institutu žádostí o přenos dat do zahraničí a existence orgánu pro ochranu osobních údajů.

Za zmínku rovněž stojí existence a s ní spojená činnost pracovní skupiny zřízené podle čl. 29 směrnice 95/46/ES (Working party 29 - dále jen „Pracovní skupina WP 29“) působící v rámci Evropské komise. Mezi její úkoly patří zejména posuzovat jednotné provádění právních předpisů přijatých na základě směrnice 95/46/ES,

[6] König, P., Lacina, L., Přenosil, J. Učebnice evropské integrace. 2. vydání. Brno: Barrister & Principal, 2007, s. 159.

přijímání stanovisek k úrovni ochrany jak ve Společenství, tak i ve třetích zemích a dále poradenství týkající se nových opatření, která by měla být přijata pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů. V případě vzniku rozporů mezi právními předpisy a praxí členských státu, které by mohly narušit ochranu osob v souvislosti se zpracováním osobních údajů, uvědomí skupina Komisi.

3. Klíčové pojmy

3.1 Osobní údaj

Pro potřeby této práce je z mého pohledu nezbytně nutné vysvětlit a definovat pojmy, které jsou pro většinu z nás notoricky známé, ale ne vždy víme, co doopravdy představují. Prvním z nich je samotný pojem „osobní údaj“, který je v zákoně o ochraně osobních údajů definován velmi stručně jako „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů*“[7].

Tato definice vychází z ustanovení článku 2 Úmluvy č. 108, kde je konstatováno, že „*osobní údaje znamenají každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby*“. V souladu s tímto pojem vykládá i směrnice 95/46/ES.

Prvním, co by nás mělo zajímat, je druhá část v nadpisu zmíněného slovního spojení, tedy slovo „údaj“ a jeho význam. Platná legislativa se obsahem pojmu „údaj“ dále nezabývá, dá se z ní nicméně dovodit, že údaj představuje jistou formu informace, která se pojí ke konkrétnímu subjektu. Právě ono spojení je důležité, protože obecně panuje mylná představa, že osobním údajem je pouze údaj doložený nějakým úředním rozhodnutím nebo výkazem. Častá je dále představa, že určité naše osobní údaje mění svou roli jako „chameleon“ a někdy osobním údajem jsou a někdy ne a to i tam, kde je povinnost jejich užití v tomto smyslu upravena zákonem.

Sám zákon o ochraně osobních údajů ve své definici obsažené v § 4 vymezuje vztah údaje(ů) k tomu, o kterém tyto údaje něco vypovídají (hovoříme o subjektu údaje, respektive údajů). V aplikační praxi je tak „*osobní údaj vždy vztahem mezi reálnou fyzickou osobou a hodnotou údaje*.“[8] Jinak tedy, že osobní údaj konkrétní fyzickou osobu identifikuje, charakterizuje z různých hledisek v závislosti na typu údaje a představuje i hodnotu této charakteristiky. Ne nadarmo se s vyjádřením osobních údajů hojně setkáváme v tabulkách a formulářích, kde tyto slouží jistému srovnání. Pro naplnění pojmu osobní údaj pak zákon o ochraně osobních údajů nestanoví žádné

[7] Viz § 4 písm. a) zákona o ochraně osobních údajů.

[8] Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer, 2008, s. 18.

formální požadavky. Osobní údaj tak může mít podobu slovní, numerickou, obrazovou nebo je vytvořen na základě jejich kombinace.

Vyřešíme-li otázku, co je míněno pojmem „údaj“, je vhodné se zaměřit na termín „určený“ a „určitelný“. Zákon o ochraně osobních údajů k tomu říká, že „*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*.“[9] Není tu přitom rozdíl mezi určeností a určitelností subjektu, je pouze podstatné, aby byl subjekt zjištěn objektivně a absolutně na základě jednoho či několika osobních údajů. Formulace směrnice 95/46/ES je v tomto směru odlišná, jelikož je z její strany klíčová určitelnost.

Chápejme to tak, že k naplnění pojmu osobní údaj musíme konkrétní osobu na základě konkrétního údaje nebo souboru údajů identifikovat. Postačí však, je-li tato osoba alespoň identifikovatelná. Jinak řečeno, určitelností označujeme možnost identifikace osoby na základě dostupných údajů, tedy její rozpoznání od ostatních. Určenost subjektu pak znamená, že s přihlédnutím k okolnostem a údajům, které máme k dispozici, můžeme subjekt údaje(ů) jednoznačně určit, případně ho kontaktovat (například máme-li k dispozici jméno, příjmení, rodné číslo nebo datum narození).

Literatura ještě dále rozlišuje objektivní určenost a neurčenost. Zmiňuji se o tom proto, že nám to pomůže tyto termíny ještě více přiblížit. Objektivní určeností míníme jasné označení pro subjekt údajů, tedy lidského jedince, člena určité společnosti. Toto označení je stálé a nezaniká ani naší smrtí, proto je z hlediska ochrany osobních údajů důležité. Patří sem naše jméno a příjmení, které máme již od narození a díky pokroku v oblasti genetiky a výpočetní techniky se v budoucnu možná setkáme i s naší identifikací na základě osobního kódu DNA. Ten je ještě více charakterizující, protože podobně jako jméno splňuje požadavek stálosti a na rozdíl od jména je skutečně jedinečný, příznačný právě jen pro konkrétní osobu. Naopak objektivní neurčeností míníme případ, kdy hodnota údaje, jako je výše uvedené jméno, nemůže být spojována s reálným subjektem. Typickým příkladem jsou jména fiktivních filmových či literárních postav. V praxi se setkáme s určeností a určitelností také v kontextu úředním

[9] Viz § 4 písm. a) věta druhá zákona o ochraně osobních údajů.

a to konkrétně tam, kde je nutno údaje vypovídající o totožnosti vyhledávat. Subjekt bude považován za určený, pokud k jeho vyhledání není zapotřebí velkého úsilí. Malá pracnost s vyhledáním znamená, že hovoříme o subjektu určitelném a v situaci, kdy bude osobu možno identifikovat jen s vynaložením nadměrného úsilí a zdrojů, bude se jednat o subjekt neurčitelný a současně údaje o něm nebudou údaji osobními.

Na tomto místě si neodpustím poznamenat, že za subjekt údajů je v rámci zákona o ochraně osobních údajů považována skutečně pouze fyzická osoba (včetně jedince dosud nenarozeného - tzv. nascitura). I přes zákonnou definici a také návaznost úpravy na článek 10 Listiny se stále objevují snahy domoci se ochrany dle zákona o ochraně osobních údajů pro právnické osoby. Jak ale plyne z judikatury zabývající se touto otázkou, je spojení zákona o ochraně osobních údajů s právnickými osobami ve vztahu k ochraně jejich práv nemístné.

Důležitost objektivního přístupu k pojmu „osobní údaj“ je spatřována v tom, že pokud by každý pohlížel na údaje pouze skrze konkrétní situaci a vlastní přesvědčení o tom, že zpracovávané a poskytované informace mají, či nemají být v tom či onom okamžiku chráněny, prakticky by se tak relativizovalo nebo zcela vyloučilo použití zákona o ochraně osobních údajů. Stejně tak by se mohla zdát nadbytečnými ustanovení ukládající povinnosti při zpracování osobních údajů zejména proto, že by tyto povinnosti byly jen obtížně vymahatelné. Správce by totiž v konkrétním případě mohl tvrdit, že údaje jím zpracovávané za „osobní“ nepovažuje a tudíž pro něj dané povinnosti neplatí.

V tom také vidím přínos současné právní úpravy. Snahu postihnout a definovat údaje, které jsou a mají být chráněny a to navzdory stále se měnícímu prostředí a podmínkám, na které musí být zákon o ochraně osobních údajů aplikován.

3.2 Anonymní údaje

Pokud opět využijeme definici zákona o ochraně osobních údajů, bude anonymním údajem takový, který „*buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů*“[10]. V tomtéž

[10] Viz § 4 písm. c) zákona o ochraně osobních údajů.

zákoně se setkáme i s termínem „anonymizovat“[11], což můžeme interpretovat jako úpravu osobního údaje do takové podoby, ve které bude po zpracování anonymní. Míra s jakou bude tento úkon proveden, pak určuje míru anonymity subjektu údajů. Za plně anonymizovaný bude označen takový údaj, ze kterého již nebude možno subjekt údajů určit. Částečně anonymizovaný bude údaj, kde je subjekt údajů možno určit za splnění určitých podmínek. To ovšem neznamená, že by se subjekt údajů nemohl „odtajnit“ a údaje o své osobě anonymizované na sebe znovu vztáhnout.

Nejčastěji se s institutem anonymizace setkáme ve zdravotnictví, kde je chráněno soukromí pacienta. Dále se pro účely vědecké a statistické smí zpracovávat osobní údaje bez souhlasu subjektu údajů právě pouze pod podmínkou jejich urychlené anonymizace, jak uvádí zákon o ochraně osobních údajů v § 5 odst. 1 písm. e).

Realizace anonymizace se po technické stránce provádí například začerněním předmětného textu v dokumentu, použitím speciálních formulářů nebo šablon, případně u informací v elektronické podobě jejich vymazáním z pevného disku počítače.

3.3 Identifikační údaje

Tato skupina osobních údajů je hojně využívána a bylo by možno ji dále rozdělit na údaje, které jsou nám vlastní od narození, dále na ty, které nám byly přiděleny v rámci úředního postupu a jako takové jsou i zaznamenány. Poslední skupinou jsou pak údaje přidělené ad hoc, vykazující prvky nahodilosti a vážící se k určité události či stavu (například identifikační čísla zaměstnanců určitého podniku).

Do první skupiny, tedy k údajům získaným od narození patří naše jméno a příjmení. Právní zakotvení jména a příjmení najdeme v zákoně č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých zákonů, ve znění pozdějších předpisů. Jejich používání je jistě právem každého z nás, můžeme k němu být ale i povinni a to například v úředním styku, kdy je často uvádění jména a příjmení založeno zákonem. Pokud tyto dva základní identifikační údaje využíváme, je nám poskytována ochrana za předpokladu, že k nim uvádíme i jiné osobní údaje mající soukromí charakter, i když zde zákon může z tohoto pravidla stanovit výjimky. Situace se ovšem změní v okamžiku, kdy se staneme osobou veřejně známou nebo tehdy, kdy se naše jméno

[11] Např. § 5 odst. 1 písm. e) zákona o ochraně osobních údajů.

využívá pro interní komunikaci v určitém kolektivu nebo pro styk s úřady. V takovém případě právo na ochranu ztrácíme.

Mezi údaje, které byly jednou zjištěny, jako takové úředně zaznamenány nebo přiděleny, řadíme rodné číslo a dále například datum a místo narození. Jsou to údaje stálé a ke změně v čase může dojít jen v případě místa narození, které může změnit svůj název.

O datu a místu narození se nebudu dále rozepisovat. Každý si pod těmito pojmy jistě dokáže jejich význam představit, a proto jen upřesním, že jsou oba upraveny také zákonem č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. Zapisují se do rodného listu a matriční knihy a samy o sobě k pozitivní identifikaci jedince nevedou. Mají smysl pouze v kombinaci s dalšími osobními údaji, jako jsou jméno a příjmení, případně k upřesnění identifikace lze užít i adresu.

O to významnějším údajem je rodné číslo, které v pojetí naší právní úpravy představuje něco jako „*jedinečný soubor číselných údajů individuálně přidělených fyzické osobě*.“[12]

Jeho využívání je velmi diskutováno v odborných kruzích a to zejména z toho důvodu, že si široká veřejnost dle některých odborníků na danou problematiku neuvědomuje dopady neuváženého zpřístupnění rodného čísla jakožto osobního údaje. RNDr. Karel Neuwirt, bývalý předseda ÚOOÚ je toho názoru, že: „*rodná čísla, od doby jejich vzniku, automaticky uvádíme, aniž bychom si uvědomili, že tento číselný kód je klíč k trezoru našich osobních údajů*.“[13] Z mého osobního pohledu se to zdá být poněkud přehnané. Jistě, že musíme být každý nadán přiměřenou mírou opatrnosti, z praktického hlediska je však užívání rodného čísla nutností a záleží na konkrétních subjektech, jak s ním naloží. Musí být stanovena míra odpovědnosti konkrétních osob, které se podílejí na jeho zpracování pro případ, že dojde k jeho zneužití. Zároveň bude institut odpovědnosti spolu s přiměřenými bezpečnostními standardy jednotlivých pracovišť působit preventivně.

Základním posláním rodného čísla by mělo být odlišit jednu osobu od druhé a stát se univerzálním vodítkem ke zjištění totožnosti jedince. Naskýtá se však otázka, zda

[12] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 18.

[13] Géblová, A. Češi, nenechte si šacovat soukromí!. Podnikání v praxi, 2003, č. 28, s. 4.

je rodné číslo osobním údajem vždy nebo jen v určitých případech. Pokud totiž vlastníme číselnou řadu odpovídající rodnému číslu a současně nemáme reálnou možnost na jejím základě vlastníka rodného čísla dohledat, o osobní údaj by se hypoteticky jednat vůbec nemuselo. Vracím se tak k výše zmíněné určenosti a určitelnosti subjektu údajů. K plnému využití rodného čísla coby identifikátoru tak dojde až spolu s dalšími údaji používanými k identifikaci subjektů (jménem a nejlépe i adresou).

Právní úpravu rodných čísel najdeme v zákoně o evidenci obyvatel. Je subjektu údajů po jeho narození propůjčeno jako „*konstantní osobní údaj, a je proto osobním údajem primárním.*“[14] Přidělují se obyvatelům narozeným na území České republiky a těm, kteří požádají o pobyt podle zvláštních právních předpisů a občanům narozeným v zahraničí. Samotné přidělení je pak prvotním zpracováním tohoto osobního údaje. Čísla, které zůstanou nepřidělena, pak osobními údaji nejsou.

Chceme-li zjistit podmínky, které jsou stanoveny pro používání rodných čísel, podívejme se na § 13c zákona o evidenci obyvatel, kde je uvedeno, že „*Rodná čísla lze využívat jen a) jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, vyplývající z jejich zákonem stanovené působnosti, nebo notářů pro potřebu vedení Centrální evidence závětí, b) stanoví-li tak zvláštní zákon nebo c) se souhlasem nositele rodného čísla nebo jeho zákonného zástupce.*“

V posledních letech se legislativa snaží používání rodných čísel omezit a to zejména v souvislosti s jejich uváděním na různých průkazech a v dokumentaci sloužící k nejrůznějším účelům. Rodné číslo je tak postupně nahrazováno datem narození, ale jeho užití je stále aktuální v občanských a řidičských průkazech nebo cestovních pasech. Pokud je rodné číslo na některé veřejné listině uvedeno, znamená to, že bude jako takové i zpracováváno a je na místě posoudit, jsou-li v rámci tohoto zpracování splněny všechny zákonem o ochraně osobních údajů stanovené podmínky. Zda jsou shromažďovány jednak osobní údaje odpovídající stanovenému účelu a dále v rozsahu, který k naplnění tohoto účelu postačuje [viz § 5 odst. 1) písm. d) zákona o ochraně osobních údajů].

[14] Matoušová, M.,Hejlík, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer, 2008, s. 60.

Ač jsme oprávněni na základě naší svobodné vůle rozhodovat o udání rodného čísla, najdou se v běžném životě situace, kdy jsme nuceni tento údaj sdělit, jinak bychom riskovali, že nám nebude poskytnuta určitá služba nebo budeme v jistém smyslu znevýhodněni oproti ostatním. Typickým příkladem budiž kopírování občanských průkazů a jiných obdobných dokladů. Setkáme se s ním ostatně i u některých zaměstnavatelů, kdy je kopie občanského průkazu přiložena ke spisu zaměstnance. Pokud tedy dobrovolně náš osobní doklad vydáme s tím, že bude pořízena jeho kopie, měl by ten, kdo kopii pořizuje vědět, že je takovou činnost z hlediska souboru dat na dokladu obsažených možno pokládat za zpracování osobních údajů ve smyslu zákona o ochraně osobních údajů a toto zpracování by tak mělo splňovat podmínky § 5 odst. 1) písm. d) zákona.

Nakonec zmíním poslední, tedy třetí, skupinu identifikačních údajů a to těch, které jsou vytvářeny ad hoc a fyzické osobě náhodně přiděleny. Patří sem například čísla služebních průkazů vydávaných zaměstnavatelem, využitelná při kontrole osob před vstupem do budov, dále identifikační čísla umístěná na stejnokroji strážníků obecní policie nebo osobní čísla zaměstnanců sloužící pro interní potřeby zaměstnavatele při vedení mzdové nebo personální agendy.

3.4 Adresní (kontaktní) údaje

Máme-li k dispozici jméno nebo rodné číslo, samo o sobě to nutně nemusí znamenat, že jistou osobu nalezneme nebo jsme schopni nalézt. Pokud ovšem údaje identifikační doplníme a zpřesníme pomocí údajů adresných, máme jistě větší šanci kontaktovat osobu, které se tyto údaje týkají.

Mezi adresní údaje můžeme zařadit jednak adresu trvalého pobytu (dle dikce zákona „*adresu pobytu občana v České republice, kterou si občan zvolí zpravidla v místě, kde má rodinu, rodiče, byt nebo zaměstnání*“[15], dále adresu zaměstnavatele a také tzv. účastnické adresy, tedy takové, jejichž podstata je založena zejména na poskytování určité služby (v současnosti zejména internet a mobilní telefonní síť).

Pojďme se nyní právě na výše zmíněné účastnické adresy blíže podívat. Jejich snad neznámějším zástupcem je telefonní číslo, které je blíže upraveno zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících

[15] Viz § 10 odst. 1 zákona o evidenci obyvatel.

zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále je „zákon o elektronických komunikacích“). Telefonní čísla je možno dělit z hlediska ochrany osobních údajů na čísla sloužící k soukromým účelům (domácí pevná linka, soukromý mobilní telefon) a na čísla určená pro komunikaci veřejnou nebo služební. Toto rozdělení je na místě, jelikož ochrany z hlediska soukromí logicky požívají soukromá čísla a u čísel služebních pak závisí na obsahu hovoru a konkrétní situaci. Základem přitom je, za jakých podmínek se tato čísla budou považovat za oprávněně zveřejněné údaje.

Ochrana týkající se telefonních čísel je zajištěna na základě §§ 87 až 92 zákona o elektronických komunikacích. Jejím předmětem je obsah přepravovaných nebo jinak zprostředkovaných zpráv a dalších údajů a skutečností.

Účastnickou adresou je také adresa elektronické pošty (e-mail). Pomocí ní je možné identifikovat elektronickou poštovní schránku umístěnou na internetovém serveru. Zda je však email osobním údajem či nikoli, o tom panují v odborných kruzích stále diskuze. Můžeme říci, že podstatným v daném případě bude objektivní existence vazby mezi subjektem údajů a elektronickou adresou. Pakliže budu ze svého osobního e-mailu posílat někomu zprávu, případně naopak určitou zprávu obdržím, je tato adresa mým osobním údajem. Na základě toho se dají adresy elektronické pošty dělit na tzv. individuální, tj. obsahující identifikační osobní údaje jako jsou příjmení nebo zkratka jména účastníka elektronické komunikace, a kolektivní (institucionální), tj. individuální jmenné údaje neobsahující. V praxi pak bude někdy problém, vazbu mezi subjektem údajů a elektronickou adresou prokázat. Děje se tak díky velké proměnlivosti tohoto údaje. Vždyť jak velký počet e-mailů v současnosti každý z nás využívá a jak dlouho zůstanou aktuální. Vhodné je za osobní údaj považovat zejména adresu elektronické pošty, kterou nám adresát sám poskytl nebo jsme s ním skrze ni opakovaně navázali oboustranně kontakt.

Nakonec se jen okrajově zmíním o IP adrese, tedy údaji sloužícímu k identifikaci konkrétního počítače v prostředí internetu. Je jím 32 (128) bitové číslo zapsané v desítkové soustavě ve tvaru xxx.xxx.xxx.xxx. Zejména stanoviska Pracovní skupiny WP 29, podle kterých by IP adresa měla být považována za osobní údaj, rozvířila čilé diskuze. Existuje již i judikát v SRN na toto téma, který se názorem Pracovní skupiny WP 29 ztotožňuje. Obecně je sice možné konkrétní počítač

identifikovat, problém ovšem nastane ve chvíli, kdy se u téhož počítače například na pracovišti střídá větší počet osob a účastnický vztah popsaný výše tedy nemusí vůbec existovat. Nelze tedy subjekt určit a nedá se považovat ani za určitelný. Základní požadavky definice osobního údaje, by tak nebyly naplněny.

3.4 Popisné údaje

Považujeme za ně všechny údaje, které dohromady utvářejí komplexní obraz fyzické osoby, jako jsou fyzická podoba, původ, chování, názory, fyzické a psychické dispozice, dosažené vzdělání, majetkové poměry atd. Tato kategorie tak v sobě odráží nejširší sféru osobního života. Právě zde je nesmírně obtížné určit, co ještě osobním údajem je a co není. Nespočet formulářů u zaměstnavatele tyto popisné údaje na jednu stranu vyžaduje, nicméně na straně druhé je následně nevyužívá. Smysl v kontextu zákona o ochraně osobních údajů mají popisné údaje tam, kde existuje úmysl je jako údaje vypovídající o subjektu využívat a to k předem stanovenému účelu, který by měl být také realizovatelný.

3.6 Citlivé údaje

Citlivé (nebo také sensitivní) osobní údaje jsou poslední kategorií, kterou zmíním. Současně jsou ale i kategorií nejdůležitější, jelikož jejich nezákonné zpracování či dokonce zneužití může subjektu údajů zvláště uškodit. Zejména v oblasti základních lidských práv hrozí diskriminace jedince odlišujícího se od většiny a je proto nezbytné pojem citlivý údaj přesně definovat a stanovit pro něj přísnější režim.

Zvláštní zacházení s těmito údaji je právně zakotveno jak v našem zákoně o ochraně osobních údajů v § 9, dále je upravuje směrnice 95/46/ES v článku 8 a povinnost stanovit vnitrostátním předpisem zvláštní záruky jejich ochrany uvádí také Úmluva č. 108. Srovnáme-li dikci směrnice 95/46/ES s naším zákonem o ochraně osobních údajů, nalezneme i přes jejich harmonizaci rozdíl. Směrnice oproti zákonu pojem citlivý údaj nezná a nahrazuje ho termínem „zvláštní kategorie údajů“. Členské státy pak mají ve své legislativě zakázat zpracování osobních údajů, které „ *odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i zpracování údajů týkajících se zdraví a sexuálního*

života.“[16] Zákaz zpracování těchto údajů však není absolutní a je možné tak učinit po výslovném písemném souhlasu subjektu údajů, výslovném povolení zákonem, dále za výskytu kritické události nebo v rámci poskytnutí vhodné záruky.

Nutno říci, že legislativní vymezení pojmu citlivý údaj nelze brát jako zcela definitivní a rigidní. Existují snahy o rozšíření definice o další údaje, jako jsou např. majetkové poměry jednotlivých subjektů údajů (zejména informace o jejich bankovních účtech případně finančních operacích). Je ovšem nesporné, že pojem citlivý údaj jakožto zákonem vymezenou kategorii musíme respektovat a nelze jej vykládat subjektivně.

Problémy nastávají zejména tam, kde je ze strany správce vidět snaha obcházet přísnější režim pro manipulaci s citlivými údaji. Jako příklad poslouží údaje v rubrice zdravotní stav v dotazníku vyplňovaném uchazečem o zaměstnání. Zaměstnavatelova argumentace tím, že většina budoucích zaměstnanců uvede do příslušné kolonky slovo „dobrý“ a že toto o jejich skutečném zdravotním stavu pramálo vypovídá, tudíž se nejedná o citlivý údaj, z hlediska ochrany osobních údajů neobstojí.
Teď pár slov o jednotlivých druzích citlivých údajů tak, jak je uvádí zákon o ochraně osobních údajů v § 4 písm. b).

3.6.1 Citlivé údaje o členství v odborové organizaci

S nimi se u zaměstnavatele jako správce osobních údajů setkáme v souvislosti s placením příspěvků odborové organizaci v souladu se zákoníkem práce. Jsou-li tyto příspěvky placeny právě prostřednictvím zaměstnavatele a platba je jako členský odborářský příspěvek označena, mělo by se na tato data pohlížet jako na citlivý údaj.

3.6.2 Údaje vypovídající o národnostním, etnickém a rasovém původu

Definovat tyto pojmy není vždy zcela jednoduché a to díky odlišnému vyjádření v různých jazycích. Zejména termín „národnost“ je třeba v českém jazyce odlišit od pojmu „státní příslušnost“. Například angličtina pojem „nationality“ (ekvivalent českého slova národnost) používá primárně pro označení státní příslušnosti. V českém právním systému je však „národnost“ chápána jednoznačně a to jako příslušnost k etniku, charakterizovaném společným jazykem a dalšími znaky.

[16] Viz Čl. 8 odst. 1 směrnice 95/46/ES.

3.6.3 Údaje vypovídající o odsouzení za trestný čin

Jsou jimi údaje o osobách pravomocně odsouzených soudy České republiky, které byly následně zaznamenány v Rejstříku trestů. Ten dle zákona č. 269/1994 Sb., o Rejstříku trestů obsahuje informace o: a) osobě odsouzeného, b) soudu a spisové značce trestní věci, c) rozhodnutí o vině, trestu a ochranném opatření stejně tak jako i jejich následném výkonu, d) rozhodnutí o podmíněném odsouzení, propuštění nebo upuštění od výkonu zbytku trestu, e) udělení milosti, f) účasti odsouzeného na amnestii a konečně za g) zahlazení odsouzení. Stejně tak obsahuje Rejstřík trestu informace o odsouzení cizozemským soudem, pakliže bylo toto rozhodnutí uznáno Nejvyšším soudem ČR.

Nepatří sem tedy ani údaje o jednání, které vykazuje znaky přestupku, stejně tak za údaj vypovídající o odsouzení za trestný čin nelze považovat ani sdělení, že daná osoba odsouzena nebyla. V poslední řadě sem nemůžeme řadit jednání, které sice naplňuje znaky trestného činu, z určitých důvodů nedošlo k odsouzení (jednalo se např. o nezletilou osobu).

3.6.4 Údaje o politických postojích

Citlivými údaji jsou politické názory vyjádřené v písemné i v ústní podobě. Patří sem např. údaje o členství v politických stranách, vyjádření politické orientace v dotazníku, zpracování fotografií z různých politických akcí jako jsou demonstrace nebo stávky, záznamy setkání subjektu údajů s osobnostmi politického života, uvedení identifikačních údajů u petice apod.

3.6.5 Údaje o náboženském a filosofickém přesvědčení

Řadí se mezi ně údaje o příslušnosti k určité církvi nebo jiné náboženské společnosti a dále náboženské projevy subjektu údajů. Zjistit náboženské a filozofické smýšlení subjektu údajů můžeme nejen z dokumentů o institucích spojovaných s určitým přesvědčením, přístup k nim umožňují ale i veřejné zdroje v čele s internetem, kde se v rámci různých weblogů s těmito údaji setkáme.

3.6.6 Údaje vypovídající o sexuálním životě

Údaje o sexuálním životě zahrnují především sexuální orientaci subjektu údajů, sexuální praktiky jím provozované nebo informace o jeho sexuálních partnerech

(postačí identifikační). V souvislosti s právní úpravou v zákoně č. 115/2006 Sb., o registrovaném partnerství a o změně některých souvisejících zákonů, se za údaj o sexuálním životě považuje také zpracování údajů týkajících se registrovaného partnerství.

3.6.7 Údaje o zdravotním stavu

Za tyto údaje lze považovat jednak konkrétní informace kvalifikující zdravotní stav subjektu údajů (zda trpí určitou chorobou) a současně také údaje, ze kterých je možno zdravotní stav bezprostředně odvodit (např. výsledky krevních testů).

3.6.8 Biometrické a genetické údaje

Tato kategorie je relativně nová a není upravena ani směrnicí 95/46/ES. Aby biometrické prvky naplňovaly definiční znaky pojmu „osobní údaj“, musí představovat měřitelné nebo objektivně klasifikovatelné hodnoty lidského těla, na základě kterých lze objektivně subjekt údajů určit (např. otisk prstu, obraz duhovky, sítnice, rysy obličeje, tělesné rozměry apod.). Jak uvádí zákon o ochraně osobních údajů, biometrický údaj je sensitivním (citlivým), pakliže „*umožňuje přímou identifikaci nebo autentizaci subjektu údajů*“[17]. Zjednodušeně řečeno, biometrický údaj musí být natolik jedinečný, aby dovoloval jednotlivé osoby navzájem od sebe odlišit.

Kromě výše uvedeného by biometrické a genetické údaje měly být jednak universální tj. vyskytující se u všech osob, zároveň by měly být stálé, proto by se u každého z nás neměly během času měnit.

[17]Viz § 4 písm. b) zákona o ochraně osobních údajů.

4. Zpracování osobních údajů

4.1 Pojem zpracování

Definování pojmu zpracování osobních údajů je z pohledu jejich ochrany velmi důležité, jelikož ochraně dle zákona o ochraně osobních údajů nepodléhá každý osobní údaj, ale pouze ty, které jsou zpracovávány.

Zpracováním se myslí jakákoliv operace nebo soustava operací, které správce systematicky provádí s osobními údaji. Legální definice je obsažena v § 4 písm. e) zákona o ochraně osobních údajů, kde je zároveň uveden demonstrativní výčet jednotlivých operací nejčastěji prováděných. Mezi tyto operace patří „*zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace"*. Naše právní úprava je plně slučitelná s dikcí směrnice 95/46/ES, v jejímž článku 2 je uvedeno, že „*Pro účely směrnice se rozumí zpracováním osobních údajů jakýkoli úkon nebo soubor úkonů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů a které jsou používány na osobní údaje, jako je sběr, záznam, uspořádání, uchovávání, přizpůsobování nebo pozměňování, výběr, konzultace, použití, sdělení pomocí přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či propojení, jakož i zajištění, vymazání nebo zničení."* Výčty jsou v obou případech demonstrativní proto, aby byl dán prostor pro technický pokrok, s nímž jsou neodmyslitelně spojeny nové termíny a postupy, které by v případě taxativního výčtu v budoucnu mohly zapříčinit výkladové a aplikační potíže. Současně výčet jednotlivých operací usnadňuje ze zákona povinným i oprávněným subjektům přehled.

Za klíčové je přitom možno považovat shromažďování, uchovávání, zpřístupňování, blokování a likvidaci osobních údajů. Všechny tyto operace, tak jak jsou seřazeny, utváří logickou strukturu celého procesu zpracování od jeho počátku až do konce. V § 4 písm. f) a následujících jsou uvedeny krátké definice jednotlivých fází.

Za **shromažďování** je možno označit jako systematický postup, jehož cílem je získat údaje do svého držení. Následně jsou tyto údaje uloženy na nosič informací se záměrem je bud okamžitě nebo později zpracovávat.

Uchovávání je definováno zákonem jako „*udržování údajů v takové podobě, která je umožňuje dále zpracovávat*“[18]. Tím je myšleno hlavně vytvoření souboru těchto údajů, který je představován např. databází nebo kartotékou.

Zpřístupňováním osobních údajů se rozumí jejich postoupení k využití. Je nezbytné, aby příjemce údajů byl k jejich převzetí a užití řádně oprávněn. Krajním případem zpřístupnění osobních údajů je jejich zveřejnění, tedy situace, kdy je příjemcem údaje kdokoliv a to bez splnění dalších předpokladů.

Blokování je zákonem definováno jako vytvoření takového stavu, kdy je osobní údaj na určitou dobu vyloučen z dalších operací s tím, že podléhá určitému posuzování (např. se posuzuje jeho přesnost). Po uplynutí lhůty pro jeho blokaci, a pakliže je vše v pořádku, může být osobní údaj dále zpracováván.

Za závěr celého procesu zpracování můžeme označit **likvidaci** osobního údaje. Ta představuje trvalé vyloučení osobních údajů z procesu zpracování a to zejména fyzickým zničením nosiče, na kterém jsou údaje zaznamenány, případně jejich vymazáním. Za likvidaci se dá považovat i anonymizace údajů, kdy je odstraněna jakákoli spojitost mezi konkrétními údaji a subjektem, kterému náleží.

V souladu s evropskými předpisy je možno zpracování členit na automatizované a neautomatizované podle toho, zda se využívá výpočetní techniky či nikoli. Volba některého z těchto způsobů je na správci případně zpracovateli, je však jasné, že automatizované zpracování je více efektivní a vedení počítačové databáze je současně i spolehlivější.

Podstatné ovšem je, že prováděné zpracování musí být systematické. Jinak řečeno, že zpracování osobních údajů musí sledovat předem stanovený účel, jsou k němu dány stanovené prostředky a způsob provedení. Údaje jsou shromážděny od neuzavřeného počtu fyzických osob a operace s těmito údaji se „*provádí opakovaně a jejich realizace je z technologického hlediska totožná nebo kompatibilní*“[19]. Vždy přitom platí, že osobní údaje musí být získány se záměrem jejich opakovaného využití, minimálně s cílem je hromadně uchovávat. Účelovost celého procesu zpracování (pořádání osobních údajů, jejich vyhledávání atd.) vyplývá i z toho, že se dá stejným opakovaným postupem za využití stejných prostředků dosáhnout stejného, nebo alespoň

[18] Viz § 4 písm. g) zákona o ochraně osobních údajů.

[19] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 29.

obdobného výsledku. Logicky tak můžeme konstatovat, že jednorázové nakládání s osobními údaji jako např. spontánní přijetí vizitky nebo získání údaje pro řešení konkrétního případu není možné považovat za zpracování a jako takové nebude spadat pod režim zákona o ochraně osobních údajů. Potvrzuje to i ustanovení § 3 odst. 4 zákona o ochraně osobních údajů, které říká, že se *„tento zákon nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány*". Jestliže však s nahodile získanými údaji dále operujeme (advokátní spisy vytvořené ke konkrétnímu případu uspořádáme do kartotéky) hovoříme v tomto případě o tzv. následném zpracování, které již zákonu o ochraně osobních údajů podléhá.

K usnadnění procesu zpracování bude často vhodné vytvoření specifického pracovního postupu, technického a organizačního zázemí, ze kterého bude vyplývat jednoduché a přehledné vyhledání a zpřístupnění údajů na základě určitých kritérií. Zpracováním tak bude zejména vedení registrů, evidencí, nebo informačních systémů. Nezáleží na formě, tedy zda bude zpracování automatizované či nikoli.

O započetí a konci procesu zpracování rozhoduje ve většině případů subjekt sám jako správce. Možnost volby je v některých případech omezena zákonem, který zpracování osobních údajů k určitému účelu přímo ukládá. Jednotlivá zpracování se dají v tomto směru rozdělit na institucionalizovaná a neinstitucionalizovaná. Prvně jmenovaná souvisí s činností státních orgánů a jsou bez výjimky založena zákonem. Neinstitucionalizovaná zpracování (početně převládající) jsou taková, o jejichž účelu, rozsahu, způsobu, použitých prostředcích zpracování a zabezpečení osobních údajů rozhoduje výlučně správce. Nelze ovšem prohlásit, že by neinstitucionalizovaná zpracování byla zákonem neupravena a rozhodování bylo ponecháno jen na správci. Tabulka na následující stránce[20] uvádí příklady zpracování osobních údajů uložená zákonem všem zaměstnavatelům.

[20] Údaje v tabulce jsou převzaty z publikace Matoušová, M.,Hejlík, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer, 2008, s. 179-181.

Název evidence	Právní předpis	Konkrétní ustanovení
dokumentace požární ochrany	zák. č. 133/1985 Sb. vyhl. č. 246/2001 Sb.	§ 15 § 27
evidence o náhradách za ztrátu na výdělku (po skončení pracovní neschopnosti po úrazu)	zák. ČNR č. 584/1991 Sb.	§ 37
evidence o skutečnostech oznamovaných zdravotní pojišťovně	zák. č. 48/1997 Sb.	§ 9, 10
evidence o uskutečněných platbách pojistného (zdravotní pojištění)	zák. ČNR č. 592/1992 Sb.	§ 25
evidence o zaměstnancích pro účely pojištění	zák. č. 187/2006 Sb.	§ 95-96
evidence o zaměstnancích v souvislosti se zajišťováním bezpečnosti a ochrany zdraví při práci	zák. č. 262/2006 Sb. (zákoník práce)	§ 103
evidence pracovní doby zaměstnance, účet pracovní doby	zák. č. 262/2006 Sb. (zákoník práce)	§ 96
evidence rizikových prací	zák. č. 258/2000 Sb.	§ 40
evidence zaměstnanců, u nichž byla uznána nemoc z povolání	zák. č. 262/2006 Sb. (zákoník práce)	§105
evidenční listy důchodového pojištění/evidence o občanech pro účely důchodového pojištění	zák. ČNR č. 582/1991 Sb.	§ 38-39, 41
kniha úrazů (evidence o všech úrazech)	zák. č. 262/2006 Sb. (zákoník práce) nař. vl. č. 494/2001 Sb.	§ 105, 108
mzdové listy pro účely daně z příjmu fyzických osob ze závislé činnosti	zák. ČNR č. 586/1992 Sb., zák. č. 582/1991 Sb.	§ 38j § 35a
účet mzdy zaměstnance	zák. č. 262/2006 Sb. (zákoník práce)	§ 96
záznamy a podklady potřebné pro provádění úrazového pojištění	zák. č. 266/2006 Sb. **(od 1. 1. 2013)**	§ 84

4.2 Zpracování citlivých údajů

Jak již bylo uvedeno výše, kategorie citlivých údajů si žádá zvláštní režim zacházení a speciální právní titul k jejich zpracování. Účelem těchto omezení je totiž snaha omezit manipulaci s citlivými údaji na nezbytné minimum.

Pro operace s citlivými údaji je v prvé řadě zapotřebí získat souhlas subjektu údajů. O souhlasu v rámci „běžného zpracování“ bude pojednáno podrobněji v kapitole o povinnostech správce. Základní odlišnost lze spatřovat v tom, že u citlivých údajů

musí být tento souhlas výslovný[21]. Vyžaduje se pro něj forma jednoznačného prohlášení subjektu údajů.

Bez tohoto souhlasu je možné údaje zpracovávat, pokud je subjekt údajů zveřejnil a to nejčastěji prostřednictvím hromadných sdělovacích prostředků, jiným veřejným sdělením nebo vydáním veřejně přístupného seznamu. Zveřejněním se myslí projev vůle subjektu údajů, který by měl být také výslovný a to z titulu většího zájmu na ochraně citlivých údajů.

Dalším právním titulem pro zpracování citlivých osobních údajů je zajištění a uplatnění právních nároků. V tomto případě ovšem existuje výslovná podmínka, že takovéto zpracování nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Je tomu tak z toho důvodu, že tento druh zpracování bude v řadě případů uskutečňován proti vůli subjektu údajů.

Konečně zákon o ochraně osobních údajů povoluje zpracovávat citlivé údaje bez souhlasu subjektu údajů v případech: 1) zajišťování zdravotní péče, ochrany veřejného zdraví, zdravotního pojištění, výkonu státní správy v oblasti zdravotnictví, případně jiného posuzování zdravotního stavu, 2) dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, 3) provádění nemocenského pojištění, důchodového pojištění, úrazového pojištění, státní sociální podpory a dalších státních sociálních dávek, sociálních služeb, sociální péče, pomoci v hmotné nouzi a sociálně-právní ochrany dětí, 4) archívnictví, 5) předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách. Ve všech těchto případech je ale nezbytně nutné, aby byly tyto výjimky podloženy příslušným ustanovením zvláštního zákona.

4.3 Zpracování vyňatá z působnosti zákona o ochraně osobních údajů

4.3.1 Zpracování pro osobní potřebu

Evropské předpisy (směrnice 95/46/ES, Úmluva č. 108) stejně jako zákon o ochraně osobních údajů obsahují ve svých ustanoveních výjimky, které vylučují z působnosti těchto předpisů operace s osobními údaji jinak naplňující definiční znaky zpracování.

[21] Viz § 9 písm. a) zákona o ochraně osobních údajů.

V § 3 odst. 3 zákona o ochraně osobních údajů je tak stanoveno, že se „*tento zákon nevztahuje na zpracování osobních údajů, která provádí fyzická osoba výlučně pro svoji potřebu*“. Bude se nejčastěji jednat o záznamy obsahující jména, telefonní čísla nebo adresy.

Pokud by došlo ke zveřejnění údajů zpracovaných tímto způsobem, nelze subjektu údajů, kterému bylo zveřejněním zasaženo do jeho soukromí, poskytnout ochranu prostřednictvím zákona o ochraně osobních údajů. Pokud bude chtít postižený docílit patřičného zadostiučinění, bude muset využít ustanovení občanského zákoníku, která směřují k ochraně osobnosti.

4.3.2 Nahodilé shromažďování

Jak jsem již zmínil v rámci definování pojmu zpracování, zákon o ochraně osobních údajů v § 3. odst. 4 vylučuje ze své působnosti „*nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány*“.

Je tomu tak proto, že nahodilé shromažďování není systematické, tudíž nenaplňuje všechny pojmové znaky zpracování dle zákona o ochraně osobních údajů. Sám zákon však nikde nahodilé zpracování nedefinuje a to způsobuje interpretační potíže. Je totiž velmi složité odhadnout, co zákonodárce myslel formulací „dále zpracovávány“.

Ani novelizace zákona o ochraně osobních údajů tento problém blíže neosvětlily novým výkladem a tak nezbývá, než se obrátit na směrnici 95/46/ES. Ta pojímá nahodilé shromažďování osobních údajů jako „neautomatizované“ zpracování a v úvodním ustanovení č. 27 stanoví, že „*Pokud jde o manuální zpracování, týká se tato směrnice pouze kartoték a nikoli neuspořádaných spisů;…obsah kartotéky musí být zejména uspořádán podle stanovených hledisek týkajících se osob, které umožňují snadný přístup k osobním údajům;…spisy nebo soubory spisů, stejně jako jejich obaly, které nejsou uspořádány podle určených hledisek, nespadají v žádném případě do oblasti působnosti této směrnice.*“ Z výše citovaného lze dovodit, že o nahodilé shromažďování osobních údajů půjde u spisů (manuálně zpracovaných osobních údajů), které nejsou uspořádány na základě cíleně zvoleného kritéria. Jinak řečeno, údaje jsou shromažďovány „případ od případu“ a není zde úmysl je dále zpracovávat. Jako příklad nám poslouží životopisy uchazečů o zaměstnání. Pokud zaměstnavatel životopisy od

uchazeče obdrží, získá pro něj podstatné informace a následně životopis zničí nebo uloží na blíže nespecifikované místo, jedná se o nahodilé shromažďování. Pokud ale zaměstnavatel strukturované životopisy uspořádá za použití jakéhokoli osobního údaje (např. je abecedně seřadí na základě příjmení), jedná systematicky, s určitým cílem a jeho počínání je zpracováním ve smyslu zákona o ochraně osobních údajů se všemi důsledky.

5 Subjekty zpracovávající osobní údaje

5.1 Správce-zaměstnavatel

Správce je v zákoně o ochraně osobních údajů definován jako „*subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj*“[22]. V rámci celého procesu zpracování pak největší porce povinností připadá právě na správce.

Může se jednat jak o právnickou, tak i o fyzickou osobu, subjekt veřejného i soukromého práva. V každém případě však takový subjekt musí být nadán právní subjektivitou. Za správce tak musíme považovat vždy celý subjekt osobní údaje zpracovávající, nikoli jen jeho organizační část (např. celé ministerstvo a ne jen jeho odbor), správcem pak v žádném případě není jednotlivý zaměstnanec (např. v rámci personálního oddělení).

Zaměstnavateli dává zákon stejně jako i směrnice 95/46/ES možnost, aby celý proces zpracování nebo jeho jednotlivé fáze svěřil jinému subjektu - zpracovateli (viz dále). I v takovém případě se ale odpovědnosti a povinností vyplývajících ze zákona o ochraně osobních údajů nezbaví.

Správcem se určitý subjekt stane buď na základě vlastního rozhodnutí, nebo mu toto postavení určí zákon. Při výkonu veřejné správy můžeme uvažovat druhou možnost, u jiných činností státních orgánů (např. právě role zaměstnavatele) mohou být i tyto orgány zpracovateli z vlastní vůle. Stejně tak i soukromé subjekty nebudou vždy zpracovávat osobní údaje jen na základě svého svobodného rozhodnutí, ale řada z nich tak bude činit na základě zvláštního zákona[23]. Podstatné ovšem je, že pokud zákon zaměstnavateli, jakožto správci, ukládá povinnost určité osobní údaje zpracovávat, stanoví mu účel tohoto zpracování a dá mu zpravidla k dispozici i prostředky a způsob, jak účelu dosáhnout. V tomto světle je třeba interpretovat zákonnou definici správce tak, že „*správce určuje účel a prostředky zpracování osobních údajů, pokud mu je*

[22] § 4 písm. j) zákona o ochraně osobních údajů.

[23] Viz tabulka v kapitole 4.1.

nestanoví zvláštní zákon a předpis vydaný k provedení takového zákona, a v míře, v níž tak tyto právní předpisy nečiní“[24].

5.2 Zpracovatel

Zaměstnavatel může zpracování osobních údajů svěřit jiné právnické nebo fyzické osobě, která je označována jako zpracovatel, pokud toto zmocnění není vyloučeno zákonem. Zpracovatel následně provádí všechny nebo jen dílčí operace s osobními údaji. Je přitom ale vázán právním titulem, kterým disponuje správce, a tento právní titul nesmí v žádném případě překročit. Zaměstnavatel si tak může najmout podnikatelský subjekt např. na zpracování mezd, účetnictví nebo na vyhodnocování konkurzních řízení v rámci procesu přijímaní nových zaměstnanců.

Při zpracování postupuje zpracovatel zásadně dle pokynů správce (v našem případě zaměstnavatele) a obecně platí, že kdo je správcem ve vztahu k nějakému zpracování, nemůže být současně zpracovatelem. Situace v opačném případě je možná a zpracovatel může v jistém okamžiku působit i jako správce. Aby se tak stalo, musí zpracovatel stanovit pro prováděné zpracování osobních údajů svůj vlastní účel a k tomuto účelu skutečně údaje zpracovávat. V takovém případě je však nutné si opatřit souhlas původního správce a v některých případech také informovaný souhlas subjektu údajů dle ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů.

Vztahy mezi správcem a zpracovatelem jsou odvozeny od smlouvy o zpracování osobních údajů. Smlouva musí být uzavřena vždy v případě, kdy zákon zpracovatele ke zpracování osobních údajů sám nezmocní a je pro ni vyžadována písemná forma. Z hlediska jejího obsahu je podstatné zejména vymezení účelu zpracování, stejně jako stanovení rozsahu, v jakém tak bude učiněno. Dále musí smluvní strany určit dobu zpracování a je jejich povinností stanovit i přiměřené bezpečnostní a organizační záruky, které by měly odstranit riziko zásahu nepovolaných osob. Článek 17 odst. 3 směrnice 95/46/ES ještě připojuje požadavek, aby zpracovatel jednal pouze dle instrukcí správce.

Odpovědnost za legalitu zpracování a dodržení všech zákonem uložených povinností nese zaměstnavatel jako správce, zpracovatel však veškeré odpovědnosti

[24] Matoušová, M.,Hejlík, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer, 2008, s. 197.

zbaven není. Na základě § 8 zákona o ochraně osobních údajů má například povinnost neprodleně upozornit zaměstnavatele v případě, kdy ten porušuje zákon. V takovém případě musí zpracovatel jím prováděné zpracování ukončit, a pokud tak neučiní, bude solidárně odpovídat za škodu, která vznikla subjektu údajů (v našem případě zaměstnanci), spolu se zaměstnavatelem.

6 Povinnosti zaměstnavatele při zpracování osobních údajů

6.1 Povinnosti před zahájením zpracování

6.1.1 Povinnost stanovit účel zpracování

Hodlá-li zaměstnavatel jakkoli zpracovávat osobní údaje svých zaměstnanců, musí v prvé řadě vytyčit účel tohoto zpracování[25]. Jinak řečeno, z jakého důvodu bude předmětné informace a údaje zpracovávat. Podstatné je to zejména proto, že je-li účel zpracování překročen, je nutno takové jednání považovat za zneužití osobních údajů. Nelze připustit situaci, kdy by byly osobní údaje shromažďovány bez konkrétní potřeby.

Přesnou formulaci účelu zákon o ochraně osobních údajů nestanoví a reflektuje tak mnohotvárnost situací, v rámci kterých jsou údaje zpracovávány. Podobně směrnice 95/46/ES v článku 6 klade pouze podmínku, že osobní údaje „*musejí být sbírány pro stanovené účely, výslovně vyjádřené a legitimní*“. U zpracování uložených zaměstnavateli zákonem (např. vedení osobních údajů personálním oddělením pro účely plnění zákonem stanovených úkolů v oblasti sociálního zabezpečení), je účel zpracování v právním předpise vyjádřen. V některých případech však na první pohled nemusí být zřejmý pro subjekt údajů. Přinejmenším bude tedy třeba, aby zaměstnavatel vhodným způsobem jím prováděné zpracování vhodně pojmenoval a zamezil tak pochybnostem (např. „mzdová účtárna“) V praxi je běžné zvláště u zaměstnavatelů s větším počtem zaměstnanců a složitou organizační strukturou označení konkrétního procesu zpracování ve vnitřním aktu řízení (používány jsou zejména směrnice nebo písemné pokyny).

Na závěr poznamenám, že by byla mylná představa zaměstnavatele, který by nepokládal za zpracování takové operace s osobními údaji, u nichž není stanoven účel, a na základě toho by považoval zákon o ochraně osobních údajů za neaplikovatelný. Jak ale vyplývá z definice zpracování v§ 4 písm. e) zákona o ochraně osobních údajů, každou systematickou operaci s osobními údaji lze považovat za zpracování, bez ohledu na to, zda je stanoven účel. Hromadění osobních údajů o zaměstnancích týkajících se jejich nejbližších příbuzných nebo výlučně jejich zálib tak nepochybně zpracováním je.

[25] Viz § 5 odst. 1 písm. a) zákona o ochraně osobních údajů.

6.1.2 Povinnost stanovit prostředky a způsob zpracování

Je uvedena v § 5 odst. 1 písm. b) zákona o ochraně osobních údajů a zaměstnavatel ji má jako správce pouze v případě, kdy mu prostředky a způsob zpracování osobních údajů jeho zaměstnanců nestanoví zvláštní zákon (pokud taková právní úprava existuje). Mimo oblast pracovněprávních vztahů je pak podrobná úprava prostředků a způsobu zpracování osobních údajů obsažena např. v zákoně č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů (požadavky týkající se vedení zdravotnické dokumentace).

Logiku má tato povinnost ve spojení s povinností dostatečně zabezpečit zpracování osobních údajů, aby nedocházelo k jejich nahodilému zpřístupnění, ztrátě nebo přenosu. Díky tomu, že má zaměstnavatel již ve fázi příprav na proces zpracování vytyčit, jak bude předmětné údaje zpracovávat a jakých prostředků k tomu využije, lze pak snáz nedostatečné zabezpečení odhalit a podniknout patřičné kroky k nápravě.

Stejně jako tomu je u formulace účelu zpracování, ani v případě stanovení prostředků a způsobu zpracování osobních údajů, zákon zvláštní formu, jakou tak má zaměstnavatel učinit, nepředepisuje. Děje se tak opět nejčastěji prostřednictvím vnitřních předpisů zaměstnavatele a to především dokumentů určujících odpovědnost a ukládajících úkoly v rámci jednotlivých pracovišť.

6.1.3 Povinnost získat souhlas zaměstnance

Každý subjekt zpracovávající osobní údaje zaměstnavatele nevyjímaje je povinen dbát na to, aby ten, jehož údaje jsou zpracovávány, neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti. K tomu je zaměstnavatel též povinen se vyvarovat neoprávněných zásahů do soukromého a osobního života subjektu údajů[26].

Ve smyslu těchto povinností je zaměstnavatel, ještě dříve než se samotným zpracováním započne, povinen ověřit, zda ke zpracování není zapotřebí získat souhlas jeho zaměstnanců. Ti tak mají právo rozhodnout, jak bude s jejich osobními údaji naloženo, a současně bude velmi obtížné jimi jednou odsouhlasené zpracování následně z jejich strany zpochybnit.

[26] Viz § 10 zákona o ochraně osobních údajů.

Podmínky souhlasu jsou v zákoně o ochraně osobních údajů uvedeny v § 5 odst. 2 a 4 a v § 9 písm. a). Souhlas není nutno udělit písemnou formou, v praxi bude ale upřednostňována. Mělo by z něj být patrno jednak: 1) kdo souhlas poskytuje, 2) v jakém rozsahu (tedy na zpracování jakých osobních údajů) je poskytován, 3) komu a k jakému účelu je poskytován a 4) na jaké období. Platí také, že všechny výše zmíněné informace je zaměstnavatel povinen zaměstnanci zajistit. Kromě toho musí souhlas splňovat obecné náležitosti právního úkonu, jak stanoví příslušná ustanovení občanského zákoníku. Klíčovým ustanovením se jeví zejména § 37 odst. 1 občanského zákoníku, dle kterého „*právní úkon musí být učiněn svobodně a vážně, určitě a srozumitelně; jinak je neplatný*“, což koresponduje s podmínkou § 4 písm. n) zákona o ochraně osobních údajů. Není nutné souhlas projevit výslovně, měl by však být někomu adresován a adresát by ho měl vzápětí přijmout. Bez akceptace zaměstnavatelem by daný souhlas postrádal jakýkoliv smysl a nemohlo by dojít ani ke zpracování osobních údajů.

Zákonná podmínka souhlasu ovšem není absolutní. Případy, kdy zpracování nevyžaduje souhlas subjektu údajů, najdeme v § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů. Jde o situace, kdy: 1) zaměstnavatel provádění zpracování nezbytné pro dodržení své právní povinnosti jako správce, 2) zpracování je nezbytné pro plnění smlouvy, jejíž stranou je zaměstnanec, případně pro uzavření či změnu takové smlouvy na návrh zaměstnance, 3) jedná se o osobní údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci veřejné zprávy (a to jen údaje související s výkonem úřední činnosti, případně týkající funkčního nebo pracovního zařazení), 4) je třeba chránit životně důležité zájmy zaměstnance, zaměstnavatel však musí souhlas získat bez zbytečného odkladu, jinak je nucen zpracování ukončit a údaje zlikvidovat, 5) dále je umožněno zpracovávat bez souhlasu osobní údaje oprávněně zveřejněné pod podmínkou, že nesmí dojít k porušení práva na ochranu soukromého a osobního života zaměstnance, 6) zpracování je nezbytné pro ochranu práv a právem chráněných zájmů zaměstnavatele, opět však nesmí být zasaženo do práva na ochranu soukromého a osobního života subjektu údajů, tedy zaměstnance, 7) jde o zpracování výhradně pro účely archivnictví dle zvláštního zákona.

6.1.4 Oznamovací povinnost

Kromě možné potřeby získat souhlas zaměstnance musí zaměstnavatel zjistit, zda se na jím zamýšlené zpracování osobních údajů nevztahuje oznamovací povinnost stanovená zákonem o ochraně osobních údajů v § 16.

Toto opatření má zajistit transparentnost procesu zpracování a předejít protiprávním zásahům do soukromí osob. Jednotlivé prvky oznámení vypočítává zákon v § 16 odst. 2 a jsou jimi: „*a) identifikační údaje správce, b) účel nebo účely zpracování, c) kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají, d) zdroje osobních údajů, e) popis způsobu zpracování, f) místo nebo místa zpracování, g) příjemce nebo kategorie příjemců osobních údajů, h) předpokládaná předání osobních údajů do jiných států, i) popis opatření k zajištění ochrany osobních údajů dle § 13*“.

Výjimky z této povinnosti jsou v zákoně uvedeny v § 18. Dle prvního odstavce se oznamovací povinnost nevztahuje na zpracování osobních údajů, která: „*a) jsou součástí datových souborů veřejně přístupných na základě zvláštního zákona, b) správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona, c) jde-li o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti sdružení, a které se týká pouze členů sdružení, nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů*“.

V praxi někteří zaměstnavatelé podávají oznámení ÚOOÚ týkající se zpracování osobních údajů svých zaměstnanců v rámci mzdové a personální agendy. Takovýto postup je ale nadbytečný. Údaje zaměstnanců slouží potřebám zaměstnavatele uložených mu v tomto případě zvláštními zákony (např. zákoníkem práce nebo zákonem č. 586/1992 Sb., o daních z příjmu, ve znění pozdějších předpisů) a tudíž lze takové zpracování jednoznačně podřadit pod výjimku z oznamovací povinnosti uvedenou v § 18 odst. 1 písm. b) zákona o ochraně osobních údajů. Ostatní povinnosti dle zákona o ochraně osobních údajů zůstávají nadále zachovány. Stejná výjimka platí i v případě zpracování osobních údajů při sjednávání pracovněprávního vztahu.

Oznamovací povinnost není rovněž nutná tehdy, když zaměstnavatel vyžaduje od svých zaměstnanců předložení výpisu z rejstříku trestů, jestliže je účelem ověření

způsobilosti pro výkon určitého zaměstnání (např. § 4 odst. 7 zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů).

Lze shrnout, že oznamovací povinnost má zaměstnavatel v případech, kdy osobní údaje svých zaměstnanců zpracovává i pro jiné účely, než které mu ukládá zvláštní zákon.

6.2 Povinnosti při zpracování

6.2.1 Povinnost zpracovávat přesné údaje

Tato povinnost vychází ze skutečnosti, že zaměstnavatel zpracovávající nepřesné osobní údaje nemůže v zásadě naplnit jím stanovaný účel zpracování. Některé zvláštní zákony však mohou stanovit, že v určitých případech má správce nepřesné údaje zpracovávat a sám zákon o ochraně osobních údajů toto stanoví v § 5 odst. 1 písm. c) s odkazem na podmínky § 3 odst. 6. Oprávnění zpracovávat nepřesné údaje se tak omezuje jen na taxativně vyjmenované účely, jejichž naplnění přísluší na základě zvláštních zákonů vymezeným institucím (např. Policii České republiky při předcházení, vyhledávání a odhalování trestné činnosti a stíhání trestných činů dle zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů).

Nyní ale zpět ke zpracování pouze přesných údajů. Samotný pojem „přesnost" může mít dvě dimenze. Jednou je úplnost, tedy předpoklad, že osobní údaj odráží určitý stav v celé jeho šíři, druhou dimenzi představuje objektivnost, tedy fakt, že osobní údaj je odrazem skutečného stavu[27]. Je zajímavé, že stávající zákon o ochraně osobních údajů již neobsahuje požadavek pravdivosti osobních údajů, na rozdíl od jeho dřívějšího znění, ostatně jako i znění zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Stalo se tak zejména s přihlédnutím k subjektivní povaze pravdivosti, kdy každý jedinec určité skutečnosti hodnotí rozdílně a využívá přitom různých kritérií. Literatura v této souvislosti odkazuje na Listinu garantující svobodu myšlení i svědomí, z čehož lze vyvodit, že „*pravdivost nelze zavádět jako předmět právních ustanovení, která musí být vyhodnotitelná z objektivního pohledu*"[28].

[27] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 82.

[28] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 82.

Jak má zaměstnavatel reálně plnit tuto povinnost? V první řadě je nutno konstatovat, že bude samozřejmě vhodné brát ohled na účel zpracování. Pokud zaměstnavatel potřebuje v zásadě aktuální osobní údaje, jistě nebude zkoumat přesnost údajů získaných jím v minulosti. Stejně tak záleží na výběru dostupných prostředků, pomocí kterých si informace o zaměstnancích ověřovat. Tato povinnost totiž sama o sobě nezakládá právo zaměstnavatele na zpřístupnění dalších osobních údajů. Preferuje se kontakt se zaměstnancem a především je na místě ho zavázat k nahlášení případných změn např. na bázi smluvního vztahu. Ve zpracování osobních údajů pro úřední potřebu je povinnost na subjekt údajů uvalena obvykle přímo zákonem. Za všech okolností je nepřesné údaje po jejich odhalení třeba opravit, a pakliže to není možné, musí být zlikvidovány. V případě pochybností je vhodné osobní údaje označit a blokovat po celou dobu, kdy probíhá ověřování jejich správnosti.

Obecně lze na závěr prohlásit, že zaměstnavatel pochybí pouze tehdy, pokud mu je na základě známých okolností jasné, že zpracovává osobní údaje nepřesné a i přes tuto skutečnost ve zpracování dále pokračuje.

6.2.2 Povinnost shromažďovat údaje odpovídající účelu a v nezbytném rozsahu

Z důvodové zprávy k zákonu o ochraně osobních údajů lze vyčíst, že „ *rozsah, v němž mohou být osobní údaje shromažďovány, je stanoven buď pouze zákonem (zejména pokud se týče státních a jiných orgánů), nebo plyne z účelu, pro který jsou shromažďovány (jsou-li údaje shromažďovány soukromými subjekty), které ovšem nemohou shromažďovat údaje v rozporu se zákony*.“ Z výše uvedeného můžeme vyvodit, že rozsah zpracování osobních údajů by neměl jakkoli přesahovat rámec stanoveného účelu. Pozor by si zaměstnavatel měl dávat zejména tehdy, kdy v průběhu zpracování omezí jeho účel a jím na počátku zpracování nashromážděné osobní údaje se pak stanou nadbytečnými.

Příkladem, kdy zákon vymezí rozsah zpracování osobních údajů, je § 38j zákona č. 586/1992 Sb., o daních z příjmů, ve znění pozdější předpisů. V odstavcích 1 až 3 rozsah definován takto: „*Plátci daně jsou povinni vést pro poplatníky, z jejichž mezd sráží zálohy, mzdové listy, rekapitulaci o sražených zálohách a dani srážené podle zvláštní sazby daně za každý kalendářní měsíc i za celé zdaňovací období. Mzdový list*

musí pro účely daně obsahovat: a) poplatníkovo jméno a příjmení, též dřívější, b) rodné číslo a u poplatníka uvedeného v § 2 odst. 3 datum narození, číslo pasu nebo jiného dokladu prokazujícího jeho totožnost, kód státu, jehož je rezidentem a bylo-li mu tímto státem přiděleno, i daňové identifikační číslo a rodné číslo, c) bydliště a u poplatníka uvedeného v § 2 odst. 3 bydliště ve státě, jehož je rezidentem, d) jméno, příjmení a rodné číslo osoby, na kterou poplatník uplatňuje slevu na dani…" Zaměstnavatel má tedy v tomto případě zákonem stanoveny pevné mantinely, které při zpracování nesmí překročit.

Mají-li osobní údaje odpovídat účelu zpracování, vyjadřuje se tím požadavek na jejich jistou kvalitu. Článek 6 směrnice 95/46/ES uvádí, že „*osobní údaje musí být přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou sbírány a pro které jsou dodatečně zpracovávány*". Zaměstnavateli bych proto doporučil, aby zvážil, které osobní údaje bude po zpracování nadále využívat a zda bude některých údajů vůbec potřeba. Mám-li např. v úmyslu svého zaměstnance kontaktovat, za tímto účelem od něj získám adresu trvalého bydliště, email, telefonní číslo pracovní i soukromé a budu tyto údaje skutečně pravidelně používat, jistě účel zpracování nepřekročím. Naopak, budu-li reálně ke kontaktu se zaměstnanci využívat pouze jejich osobní email a přesto si od nich výše zmíněné kontaktní údaje vyžádám, rozsah a současně i účel zákonitě překročím.

6.2.3 Povinnost uchovávat osobní údaje pouze po nezbytnou dobu

Zákon o ochraně osobních údajů tuto povinnost uvádí v § 5 odst. 1 písm. e). Je jí myšlena zejména potřebnost stanovit takovou lhůtu pro zpracování a uchování osobních údajů, která zaměstnavateli umožní, nebo alespoň může umožnit, naplnění zamýšleného účelu zpracování.

Provádí-li zaměstnavatel zpracování uložené mu zákonem, je lhůta stanovena v jeho ustanovení a to nejběžněji výslovně. Z hlediska praktického využití osobních údajů, je toto pro zaměstnavatele poněkud složité a v mnoha situacích by jistě uvítal větší flexibilitu. Vhodným řešením se zdá být lhůta „přezkumná", která by umožňovala po uplynutí vymezeného času na zpracování osobních údajů ověřit, zda stále existuje důvod zpracování a akcentovala by tak aktuální potřeby zaměstnavatele. Na druhou

stranu by se však jednalo nepochybně o náročnější proceduru pro dozorový orgán, a čím delší je lhůta pro zpracování, tím je zároveň obtížnější udržovat přesné osobní údaje.

Delší lhůtu pro zpracování osobních údajů stanoví zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů, kde v § 35a odst. 4 nalezneme, že „*Zaměstnavatelé jsou povinni uchovávat mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění po dobu 30 kalendářních roků následujících po roce, kterého se týkají a jde-li o mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění vedené pro poživatele starobního důchodu, po dobu 10 kalendářních roků následujících po roce, kterého se týkají*.“ Asi nejdelší lhůtu zpracování osobních údajů pak ukládá zaměstnavatelům zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. V § 40 tohoto zákona je stanoveno, že „*Zaměstnavatel, na jehož pracovištích jsou vykonávány rizikové práce, je dále povinen a) u každého zaměstnance ode dne přidělení rizikové práce vést evidenci 1. o jménu, příjmení a rodném čísle, 2. o počtu směn odpracovaných při rizikové práci, s výjimkou rizika infekčního onemocnění, 3. o datech a druzích provedených lékařských preventivních prohlídek a zvláštních očkováních souvisejících s činností na pracovišti zaměstnavatele nebo o imunitě (odolnosti) k nákaze, 4. údajů o výsledcích sledování zátěže organismu zaměstnanců…b) ukládat evidenci podle písmene a) po dobu 10 let od ukončení expozice, a jde-li o práce 1. s chemickými karcinogeny stanovenými zvláštním právním předpisem, 2. s azbestem, 3. v riziku fibrogenního prachu, a 4. s biologickými činiteli…po dobu 40 let od ukončení expozice*“.

Při stanovování lhůt u zpracování prováděných z vlastní vůle zaměstnavatele, bude na místě, aby lhůta pokrývala pokud možno celou dobu trvání pracovněprávního vztahu. Pokud je se zpracováním osobních údajů zaměstnanců spojen jejich souhlas, bude ohraničení lhůty pro zpracování shodné právě s dobou trvání tohoto souhlasu. Z mého pohledu tak bude nejjednodušší a asi nejvýhodnější formou pro obě strany pracovní smlouva, která obsáhne jak souhlas zaměstnance s konkrétním zpracováním, tak současně dobou, na kterou je mezi stranami uzavírána, vymezí časový rámec pro operace s osobními údaji.

Jakmile příslušným způsobem stanovená doba k naplnění účelu zpracování uplyne, je na základě zákona o ochraně osobních údajů zaměstnavatel, případně na jeho

pokyn zpracovatel, povinen dosud zpracovávané osobní údaje zlikvidovat. Zachovány mohou být pouze pro účely vědecké, statistické, nebo pro účely archivnictví dle zvláštních zákonů.

6.2.4 Povinnost přijmout bezpečnostní opatření

Důležitou součástí systému ochrany osobních údajů je povinnost přijmout taková bezpečnostní opatření, aby nedocházelo k „*neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.*“[29]. Tato povinnost platí jak pro zaměstnavatele, tak případně pro jím pověřeného zpracovatele a trvá výslovně i po ukončení procesu zpracování osobních údajů (např. do doby, než zaměstnavatel jako správce předá osobní údaje jinému správci). Pokud tedy potřebná opatření nemůže, ať zcela či částečně, přijmout zaměstnavatel, protože provádí jen některé kroky zpracování nebo nenakládá s osobními údaji vůbec, je v tomto rozsahu povinen přijmout bezpečností opatření zpracovatel. Považuji přitom za nutné podotknout, že zákonem uváděný termín „přijmout“ je vykládán tak, že nestačí opatření k zabezpečení pouze implementovat do procesu zpracování, ale je nutné tyto i **zajistit**[30]. Jinak řečeno, zaměstnavatel je povinen garantovat, že osobní údaje budou chráněny jak před úmyslným, nedbalostním i nezaviněným jednáním osob včetně jeho zaměstnanců, tak i vůči dopadům přírodních událostí (např. požár nebo výpadek elektrického proudu).

Zákon o ochraně osobních údajů však konkrétní bezpečnostní prvky neuvádí, pouze v § 13 odst. 3 a 4 stanoví oblasti, na které by se měly povinné subjekty zaměřit. Určujícím pro zvolené zabezpečení tak bude zejména účel a prostředky využité při zpracování, stejně jako jeho ekonomická náročnost.

V souladu se směrnicí 95/46/ES, která v úvodním ustanovení č. 46 vyslovuje požadavek na „*přijetí příslušných technických a organizačních opatření, jak při přípravě zpracování, tak při jeho provádění, s cílem zajistit především bezpečnost a zabránit jakémukoliv nepovolenému zpracování*…“, je možno dělit postup vedoucí k zabezpečení osobních údajů v rámci jejich zpracování na prvky organizační a technické. Pouhé zajištění technických prostředků totiž nemůže plně zaručit, že nedojde

[29] Viz § 13 odst. 1 zákona o ochraně osobních údajů.

[30] Viz rozhodnutí ÚOOÚ č. j. VER-6243/08-17.

k selhání lidského faktoru a organizační opatření zachycená nejlépe v určitém dokumentu jsou tak jejich vhodným doplňkem.

Opatření technického rázu nebude dle mého názoru třeba podrobně specifikovat s ohledem na vývoj v oblasti výpočetní i zabezpečovací techniky. Patří sem zejména nejrůznější softwarové vybavení počítačů (bezpečnostní zálohy, antivirová ochrana, kryptování), které obsahují uložené soubory s osobními údaji, zabezpečení interní a externí počítačové sítě, stejně jako ochrana nosičů informací. K tomu lze připočíst patřičné zabezpečení prostor, kde zpracování osobních údajů probíhá včetně důkladného zajištění likvidace souborů s osobními údaji. Např. by neměly být údaje zpracovávány v síti, která je přístupná zvnějšku, kartotéky nesmějí být umístěny v prostorách veřejně přístupných, budovy a místnosti, ve který ke zpracování osobních údajů dochází, je nutno dostatečně zabezpečit nejen proti protiprávnímu vniknutí, ale také např. proti požáru apod.

Každopádně ale povinnost nelze chápat absolutně, což reflektuje i směrnice, která říká, že zabezpečovací opatření „*musejí zajistit odpovídající úroveň bezpečnosti s ohledem na odbornou úroveň a náklady na jejich provedení v souvislosti s riziky vyplývajícími ze zpracování údajů a z povahy údajů, které mají být chráněny*“. Volně přeloženo, opatření musejí přiměřeně odpovídat „*současnému stavu technického rozvoje a nákladům na jejich zavedení a použití vzhledem k rizikům při takovém zpracování*“[31].

Opatření organizačního charakteru mají v prvé řadě zajistit, aby bylo zabráněno přístupu neoprávněných osob k osobním údajům a případně také prostředkům sloužícím pro jejich zpracování. Typickým příkladem jak toho lze docílit je např. zajištění identifikace jednotlivých uživatelů přicházejících do styku s osobními údaji, vymezení přístupu k zařízením a datovým souborům nebo stanovení režimu nakládání s nosiči údajů. Další oblastí, kterou je třeba podchytit, je monitoring zaměstnanců mající za cíl určit a následně ověřit, komu byly osobní údaje předány a jak s nimi bylo naloženo. Nelze totiž připustit situaci, kdy nebude známo, kdo konkrétní údaje zpracovával, předal nebo kam tyto údaje po jejich zpravování přišly. Porušením povinnosti uvedené v § 13 odst. 1 zákona o ochraně osobních údajů tak může být neodborně provedená likvidace nebo dokonce ztráta listin obsahujících osobní údaje.

[31] Matoušová, M.,Hejlík, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer, 2008, s. 262.

Docílit bezpečnostního standardu tak není jednoduché a pro zaměstnavatele to znamená přijmout náležité vnitřní normy a organizační strukturu umožňující stanovit odpovědnost jednotlivých pracovníků. Zákon o ochraně osobních údajů proto ukládá zaměstnavatelům a zpracovatelům, aby určili jak rozsah, tak podmínky, za nichž mohou jejich zaměstnanci a jiné osoby osobní údaje zpracovávat[32]. Odpovědnost zaměstnanců za dodržování jejich povinností se bude řídit ustanoveními zákoníku práce. Pokud zaměstnavatel využívá interní organizační normy (pracovní řád, organizační řád), musí být do jejich textu odpovědnost za zpracování osobních údajů včleněna a také na jejich podkladě prokazatelně vymáhána. To znamená, že formálně vyhlášená odpovědnost v jednom z interních předpisů zaměstnavatele je v praxi naplňována (např. že určitou fázi zpracování bude provádět jen k tomu příslušný útvar, jemuž je to organizačním řádem uloženo, a ne útvar jiný). Důležitá je v tomto smyslu kontrolní činnost vedoucích pracovníků, obecně vymezená v § 302 písm. a) zákoníku práce.

Zaměstnavatel a zpracovatel osobních údajů nesou podle zákona o ochraně osobních údajů odpovědnost za provedení náležitých opatření vylučujících rizika spojená s předmětným zpracováním osobních údajů, přičemž tato jejich odpovědnost je odpovědností objektivní, tedy za následek jednání či opominutí (za protiprávní stav). K tomu, aby kterýkoli z těchto subjektů povinnosti dle § 13 odst. 1 zákona o ochraně osobních údajů porušil, přitom postačí pouze vznik stavu, kdy jsou osobní údaje určitým způsobem ohroženy, přestože doposud nedošlo nebo ani nedojde k jejich neoprávněnému zpracování či zneužití. Za pochybení zaměstnavatele tak můžeme v tomto smyslu označit i neúplné nebo chybné určení odpovědnosti za zpracování osobních údajů, v důsledku čehož vnikne riziko, že osobní údaje budou neoprávněně či nahodile zpřístupněny.

Zaměstnavatel se může odpovědnosti za správní delikt zbavit, jestliže dostatečně prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti dle § 13 odst. 1 zákona o ochraně osobních údajů zabránil. Posuzování naplnění liberačního ustanovení je přitom závislé vždy na konkrétních okolnostech daného případu a důkazní břemeno nese zaměstnavatel.

Jako podpůrný institut k povinnosti přijmout bezpečnostní opatření slouží **povinnost mlčenlivosti**. Ta se týká nejen všech zaměstnanců správce a zpracovatele,

[32] Viz § 14 zákona o ochraně osobních údajů.

vztahuje se ale i na ostatní osoby, které ať již na základě smlouvy nebo v zájmu plnění svých zákonných oprávnění a povinností přicházejí do styku s osobními údaji. Je přitom absolutní povahy, trvá i po skončení pracovního nebo obdobného poměru ke správci či zpracovateli, a pokrývá jak osobní údaje samotné, tak i bezpečnostní opatření, pokud by jejich zveřejnění znamenalo ohrožení zabezpečení osobních údajů. Důležité také je, že povinnost mlčenlivosti platí přímo na základě § 15 zákona o ochraně osobních údajů a není k ní vyžadován žádný další formální úkon (např. prohlášení zaměstnance).

Vedle toho mohou být zaměstnanci povinni zachovávat mlčenlivost též dle ustanovení zvláštního zákona (např. auditoři, zaměstnanci v bankovnictví a pojišťovnictví).

Povinnost mlčenlivosti podle zákona o ochraně osobních údajů se však nelze dovolávat tam, kde zákon ukládá některé informace sdělit (např. v ustanovení § 368 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů).

6.3 Povinnosti při ukončení zpracování

6.3.1 Uchování osobních údajů zaměstnance i po skončení pracovního poměru

Tato eventualita není v zákoníku práce nikterak řešena, i když k ní v praxi dochází, a jak bylo zmíněno výše u povinnosti zpracovávat osobní údaje jen po nezbytnou dobu, odkazují na ni i zvláštní právní předpisy.

Uchovávání osobních údajů zaměstnanců, jako jedna z forem zpracování, musí splňovat všechny podmínky, které zákon o ochraně osobních údajů uvádí. Zejména musí být, v souladu s § 5 odst. 1 písm. e), doba, po kterou jsou osobní údaje zpracovávány, přiměřená účelu zpracování. Po uplynutí této doby je dovoleno předmětné osobní údaje dále využívat jen pro účely statistické, vědecké, nebo pro účely archivnictví podle zvláštního právního předpisu. V takovém případě je však nutno údaje anonymizovat, jakmile je to možné.

Dobou nezbytnou pro zpracování osobních údajů zaměstnanců bude obecně doba trvání pracovního nebo obdobného poměru k osobě zaměstnavatele a následně po jejich skončení doba potřebná k vypořádání vzájemných práv a povinností. Rozsah zpracovávaných údajů v osobním spisu zaměstnance nebo v jiných evidencích vedených zaměstnavatelem je přitom limitován na informace, které jsou nezbytné pro

výkon práce v pracovněprávním vztahu[33]. O jaké osobní údaje se konkrétně v této souvislosti jedná, nalezneme v § 150 zákoníku práce. V něm je stanoveno, že „*zaměstnavatel eviduje údaje, jimiž jsou jméno, popřípadě jména a příjmení, adresa, jde-li o fyzickou osobu, název a sídlo, jde-li o právnickou osobu, a písemnosti týkající se prováděných srážek mzdy a to po stejnou dobu jako ostatní údaje a doklady týkající se mzdy nebo platu*“, přičemž je odkázáno na zákon č. 499/2004 Sb., o archivnictví a o spisové službě a o změně některých zákonů, ve znění pozdějších předpisů. Ten pak v § 3 vyjmenovává subjekty (mezi něž spadá valná většina zaměstnavatelů) povinné uchovávat dokumenty, jejichž specifikaci však nenalezneme ani v samotném zákoně č. 499/2004 Sb., ani v prováděcích předpisech. Příkladem, kdy právní předpis stanoví jak lhůtu pro uchování osobních údajů tak i konkrétní dokumenty, tak budiž již jednou v tomto kontextu zmiňovaný zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení a také zákon č. 258/2000 Sb., o ochraně veřejného zdraví (viz str. 37 a 38).

V souladu se zákonem je rovněž uchovávání osobních údajů bývalých zaměstnanců z důvodu probíhajících nebo v budoucnu reálně hrozících soudních a jiných sporů. Tato forma zpracování je plně slučitelná se zněním § 5 odst. 2 písm. e) zákona o ochraně osobních údajů a za dodržení podmínky, že nebude dotčeno právo subjektu údajů na ochranu jeho soukromého a osobního života, nemusí zaměstnavatel disponovat ani souhlasem zaměstnance.

Shrňme závěrem, že takto určené lhůty jsou zároveň dobou, po kterou je pro zaměstnavatele potřebné uchovávat osobní údaje zaměstnanců i po skončení pracovního poměru. Je třeba poznamenat, že mezi uschovávané dokumenty by rozhodně neměly patřit např. životopisy zaměstnanců, které by měl zaměstnavatel po skončení pracovního poměru zaměstnanci vrátit nebo je prokazatelně zlikvidovat. Jen tak bude naplněn smysl ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů.

6.3.2 Povinnost osobní údaje zlikvidovat

S výjimkou výše uvedeného případu, kdy uchování osobních údajů stanoví zvláštní právní předpis, je nezbytné, aby byly po uplynutí doby potřebné k naplnění účelu zpracování osobní údaje zlikvidovány. Tato povinnost se dotýká jednak

[33] Viz § 312 odst. 1 zákoníku práce.

samotného zaměstnavatele jako správce, postihuje ovšem i zpracovatele, který tak činí na správcův pokyn.

Likvidací osobních údajů se v § 4 písm. i) zákona o ochraně osobních údajů rozumí „*fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování*“. Vyloučením ze zpracování se myslí zejména situace, kdy není z nějakého důvodu možné osobní údaje zničit spolu s jejich nosičem, případně nelze provést takový jejich výmaz, který znemožní zpětnou obnovu dat. Tento postup je možné po formální stránce ztotožnit s blokací, kdy osobní údaje sice reálně existují, jsou ovšem pro každého nepřístupné.

Způsob provedení likvidace bude záležet na tom, jakou povahu má nosič údajů. U papírových nosičů bude vhodná jejich skartace, v některých případech pokud bude potřeba odstranit jen některé údaje, postačí jejich anonymizace začerněním. V případě elektronických nosičů budou osobní údaje vymazány nebo překryty novým textem.

Likvidací není pouhé vyřazení složek z kartotéky, stejně jako odstranění pouze některých souborů z počítače, pokud osobní údaje obsahují soubory jiné a tyto jsou i nadále aktivně používány ke stejnému účelu. Poněkud extrémní jsou situace, kdy se správce vypořádá s povinností zlikvidovat osobní údaje tak, že dokumenty s osobními údaji předá do sběrných surovin nebo je přímo vyhodí do odpadkového kontejneru. Tento postup nelze v žádném případě doporučit. Jednak jím povinnosti zlikvidovat osobní údaje nelze dostát, jelikož správce tímto postupem sám nosiče osobních údajů fyzicky nezničí, současně také nedokáže zaručit, že budou osobní údaje vůbec zlikvidovány. Pokud by osobní údaje byly navíc ve formě, která naplňuje znaky zpracování (např. seznamy, evidence nebo spisy uspořádané podle jména) mohlo by dojít i k porušení povinnosti dle § 13 zákona o ochraně osobních údajů, tedy povinnosti přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

S odkazem na výše uvedené budou tedy za vyhovující brány jen postupy, které dostatečně zaručí vyloučení osobních údajů z jejich dalšího možného zpracování. V případě technické a finanční náročnosti nelze než navrhnout zaměstnavateli, aby likvidaci osobních údajů svěřil na základě smlouvy odborné firmě. Ta se stane zpracovatelem, který je na základě smlouvy ve spojení s ustanovením § 6 zákona o

ochraně osobních údajů povinen zaručit náležité technické a organizační zabezpečení ochrany osobních údajů.

7 Práva zaměstnance jako subjektu údajů

Zákon o ochraně osobních údajů definuje subjekt údajů v § 4 písm. d) jako „*fyzickou osobu, k níž se osobní údaje vztahují*“. Pro naše potřeby budou tyto znaky vykazovat zaměstnanci nebo i osoby ucházející se o zaměstnání. Zákon stejně jako mezinárodní předpisy pak těmto vybraným subjektům přiznává určitá práva, nikoli povinnosti, čímž se chce především zdůraznit jejich specifické postavení.

Přesto, že právní normy ve svých ustanoveních povinnosti subjektu údajů výslovně neuvádí, nelze říci, že by neexistovaly. Jsou pouze skryté a to dokonce v samotném zákoně o ochraně osobních údajů. Například § 5 odst. 1 písm. c) stanoví povinnost správce zpracovávat pouze přesné osobní údaje, se kterou je neodmyslitelně spojena oznamovací povinnost subjektu údajů, zejména pokud jde o údaje identifikační a kontaktní.

Za základní právo subjektu údajů je považováno právo být informován o tom, kdo a k jakému účelu bude jeho osobní údaje zpracovávat nebo o tom, jaké údaje jsou již zpracovávány. S tím se pojí i právo na přístup k osobním údajům a právo souhlasit nebo nesouhlasit se zpracováním osobních údajů tam, kde to zákon předpokládá. O souhlasu se zpracováním osobních údajů a to i údajů citlivých bylo pojednáno výše a z mého pohledu není třeba se k němu vracet. Pouze podotknu, že parametry souhlasu lze shrnout tak, že by se mělo jednat o svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů přijímá zpracování jeho osobních údajů. Dalším a neméně důležitým oprávněním je možnost obrátit se na dozorový orgán, v našich podmínkách představovaný ÚOOÚ.

7.1 Právo na informace o zpracování

V zájmu transparentnosti celého procesu zpracování osobních údajů je potřeba zajistit, aby měl subjekt údajů - zaměstnanec představu o tom, jaká zpracování osobních údajů probíhají nebo budou probíhat, a následně do nich mohl v případě jakýchkoli nejasností zasáhnout případně docílit žádoucích korektur.

Právo na informace o zpracování je typickým příkladem situace, kdy v právním vztahu mezi dvěma subjekty odpovídá právu jednoho z nich povinnost toho druhého. Konkrétně zde lpí zákonná povinnost poskytovat patřičné informace na straně zaměstnavatele. Lze ji členit na dva základní typy podle toho, v jaké fázi zpracování

osobních údajů figuruje. Jednak hovoříme o povinnosti plněné správcem - zaměstnavatelem při shromažďování osobních údajů nebo může být tato povinnost plněna v průběhu samotného zpracování[34].

Poskytování informací při shromažďování osobních údajů je zákonem o ochraně osobních údajů blíže upraveno v § 11. Ten ukládá zaměstnavateli informovat zaměstnance 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, nejsou-li subjektu údajů tyto informace již známy*“. Současně musí zaměstnavatel upozornit zaměstnance na jeho právo přístupu k osobním údajům, právo na opravu osobních údajů stejně jako i na ostatní práva garantovaná v § 21. Každému zaměstnanci tak musí být známa jeho práva, rozsah zpracování a jeho účel. Všechny tyto informace by měl zaměstnavatel poskytovat automaticky se zahájením každého procesu zpracování (tedy se sběrem prvních osobních údajů za účelem jejich dalšího zpracování). O tom, v jaké formě tak má učinit, zákon mlčí. Měl by to však v jeho vlastním zájmu provést v podobě, která splnění informační povinnosti v případě potřeby doloží (např. předtištěný formulář).

Dochází-li ke zpracování osobních údajů získaných přímo od zaměstnance, má zaměstnavatel povinnost ho poučit, zda je zaměstnanec předmětné údaje povinen poskytnout či nikoli. Je tomu tak proto, že se tím jednak zaměstnanci připomíná jeho pozice vůči zaměstnavateli jako správci a současně v případě, kdy poskytnutí osobních údajů ukládá zákon, je zaměstnanec touto cestou informován o důsledcích případného nepředání příslušných osobních údajů.

V případě, kdy jsou osobní údaje získány z jiného zdroje než přímo od osoby zaměstnance, je zaměstnavatel informační povinnosti zbaven, pokud: „*a) zpracovává osobní údaje výlučně pro účely výkonu státní statistické služby, vědecké nebo archivní účely a poskytnutí takových informací by vyžadovalo neúměrné úsilí nebo nepřiměřeně vysoké náklady; nebo pokud ukládání na nosiče informací nebo zpřístupnění je výslovně stanoveno zvláštním zákonem, b) zpracování osobních údajů mu ukládá zvláštní zákon nebo je takových údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštních zákonů, c) zpracovává výlučně oprávněně zveřejněné osobní údaje, nebo*

[34] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 85.

d) zpracovává osobní údaje získané se souhlasem subjektu údajů“[35]. Zde se zohledňuje fakt, že by informování zaměstnance bylo v těchto situacích spojeno s neúměrnou zátěží pro zaměstnavatele a současně by zaměstnanec tyto informace již měl mít k dispozici z jiných zdrojů.

Konečně tam, kde se jedná o zpracování osobních údajů nezbytné pro ochranu práv a právem chráněných zájmů zaměstnavatele nebo jde o zpracování citlivých údajů potřebných pro zajištění a uplatnění právních nároků, je zaměstnavatel povinen informovat zaměstnance o takovémto zpracování bez zbytečného odkladu.

Informace poskytované v průběhu zpracování jsou druhou kategorií informační povinnosti dané zaměstnavateli, která je vyjádřena v § 12 zákona o ochraně osobních údajů. Smyslem tohoto ustanovení je jednak zajistit, aby byl subjekt údajů-zaměstnanec informován i v průběhu zpracování a zároveň mu je v rámci tohoto paragrafu zajištěn přístup ke zpracovávaným osobním údajům.

Zatímco by měly být informace při shromažďování osobních údajů poskytovány automaticky, je povinnost zaměstnavatele dle § 12 zákona o ochraně osobních údajů vázána na žádost zaměstnance a je zde tedy vyžadován jeho aktivní přístup. Forma žádosti o poskytnutí informací není zákonem striktně stanovena, ale stejně jako i v jiných případech je preferován projev písemný. Co se týče lhůty, ve které by měly být výše zmíněné informace poskytnuty je zákon o ochraně osobních údajů opět velmi strohý a nezbývá než se spokojit s formulací, že by se tak mělo stát bez zbytečného odkladu.

Obsahem informací je vždy sdělení o: „*a) účelu zpracování osobních údajů, b) údajích případně kategoriích osobních údajů, které jsou předmětem zpracování, včetně veškerých dostupných informací o jejich zdroji, c) povaze automatizovaného zpracování v souvislosti s jeho využitím pro rozhodování, jestliže jsou na základě tohoto zpracování činěny úkony nebo rozhodnutí, jejichž obsahem je zásah do práva a oprávněných zájmů subjektu údajů, d) příjemci, případně kategoriích příjemců*“[36]. K tomu zbývá dodat, že přístup k informacím pod bodem b) je pro zaměstnance podstatný z hlediska ověření správnosti a přesnosti zpracovávaných osobních údajů a zároveň je touto cestou možno odhalit jejich případné falzifikování. Pokud se tak stane, je položen základ pro využití

[35] § 11 odst. 3 zákona o ochraně osobních údajů.

[36] § 12 odst. 2 zákona o ochraně osobních údajů.

dalšího práva a to možnosti domáhat se opravy, blokování případně likvidace nepřesných údajů.

Mohlo by se z výše uvedeného zdát, že práva i povinnosti jsou v tomto případě zřejmé a nebude tak ve velké míře docházet ke komplikacím. Pravda je ovšem poněkud odlišná. Tím, že zákon sám formu informační povinnosti nestanoví, otevírá prostor pro často diskutabilní jednání zaměstnavatelů. Naproti tomu se stává, že i subjekty oprávněné celou problematiku dezinterpretují. Dochází k případům, kdy se dobrovolné poskytování osobních údajů v nejrůznějších podobách zastírá, takže zaměstnanec vlastně nemá možnost si sám zvolit, zda údaje poskytne či nikoli, k čemuž by nedošlo, pokud by zaměstnavatel své zaměstnance řádně informoval. Naopak tam, kde je zaměstnanci právním předpisem přímo uloženo jeho osobní údaje sdělit, nemá ten o své zákonné povinnosti mnohdy vůbec tušení. V praxi oblíbenou metodou, jak seznámit subjekt údajů s jeho právy, je učinit tak na konci textu určitého ujednání, pokud možno co nejmenším písmem a v některých případech dokonce pod podpisem.

Osobně se neztotožňuji s představou, že by bylo nejvhodnějším řešením vyjmenovat v každé pracovní nebo obdobné smlouvě subjektu údajů všechna jeho práva i povinnosti za situace, kdy u nás obecně panuje nízké právní povědomí běžné populace a podobné informace se běžně zkrátka nečtou nebo jim je věnována jen minimální pozornost. Nemůžeme se tedy divit zaměstnavatelům, kteří nechtějí plýtvat zdroje a administrativní kapacity na dostatečně přesné a plně vyhovující poskytnutí předmětných informací. To ovšem v žádném případě neznamená, že tento postup schvaluji. Větší důraz by měl být kladen zejména na tu část ustanovení § 11 odst. 1 zákona o ochraně osobních údajů, která správce liberuje z informační povinnosti tehdy, jsou-li tyto informace subjektu údajů již známy. Předchozí znalost procesu zpracování nelze dokládat pouze tím, že takový postup upravuje zákon. Zřejmé ale zároveň je, že by zaměstnanci měli ochraně svých práv věnovat větší míru pozornosti a informace si přednostně zajistit sami (např. v kontextu výše zmíněného § 12 zákona o ochraně osobních údajů). To samozřejmě předpokládá i vstřícnost a otevřenost ze strany zaměstnavatelů.

Cesta k patřičnému zajištění informovanosti zaměstnanců může vést i skrze pravidelné podávání informací v podobě interních oběžníků připravených vedoucími pracovníky. Ty mohou být rozesílány přímo jednotlivým zaměstnancům v rámci

exponovaných pracovišť, kde dochází ke zpracování osobních údajů, přičemž tito zaměstnanci by následně svým podpisem ztvrdili jejich náležité prostudování. Tento postup je sice náročnější z hlediska administrativní agendy, má ale tu výhodu, že působí dostatečně preventivně a současně umožňuje zaměstnanci vyjádřit případný nesouhlas se zpracováním jeho osobních údajů.

Závěrem lze konstatovat, že by zaměstnanec k zajištění jeho práv informován být měl, ovšem formou jemu srozumitelnou a tato nepsaná zásada by měla být zároveň preferována před snahou dostát informační povinnosti doslovným a z mého pohledu zbytečným opisem zákona za každé situace.

7.2 Právo domáhat se ochrany svých práv

Zákon o ochraně osobních údajů vymezuje prostředky ochrany před protiprávním jednáním správce nebo zpracovatele v § 21. Pokud zaměstnanec zjistí nebo se domnívá, že je prováděným zpracováním osobních údajů zasahováno do jeho soukromého nebo osobního života, případně že je zpracování v rozporu zákonem, lze se nápravy domáhat přímo u svého zaměstnavatele nebo jím pověřeného zpracovatele.

Po nich je oprávněn požadovat aby: 1) podali vysvětlení, zdrželi se závadného jednání nebo poskytli na svoje náklady omluvu či jiné zadostiučinění (může např. požádat o ukončení zpracování, trvat na náležitém zabezpečení osobních údajů, nebo aby byly údaje využívány jen k vymezenému účelu, ke kterému byly poskytnuty), 2) provedli opravu či doplnění údajů tak, aby byly pravdivé a přesné, 3) osobní údaje zablokovali nebo zlikvidovali, tento postup bude vyžadován zejména tam, kde došlo k získání osobních údajů protiprávně nebo již uplynula doba vymezená k naplnění účelu zpracování, případně je objem shromážděných informací nadbytečný.

Vznikla-li v důsledku zpracování osobních údajů zaměstnanci škoda, postupuje se při uplatňování nároku dle příslušných ustanovení občanského zákoníku. Je-li charakter vzniklé újmy jiný než majetkový, budou se vztahy z toho vyplývající řešit na základě § 13 občanského zákoníku, tedy části týkající se ochrany osobnosti. Stejně se bude postupovat tam, kde nakládání s osobními údaji nebude možno považovat za zpracování ve smyslu zákona o ochraně osobních údajů.

Práva subjektu údajů uvedená v § 21 zákona o ochraně osobních údajů nekonkurují žádnému jinému právu a jsou uplatnitelná nezávisle. Je tedy pouze na

zaměstnanci zda bude požadovat jeden nebo třeba i všechny nároky a to i ty, které vyplývají z úpravy občanskoprávní.

Za situace, kdy zaměstnanec neuspěje se svými požadavky vůči zaměstnavateli nebo zpracovateli, může se obrátit na ÚOOÚ, aby zjednal nápravu. Alternativou je postup upravený v § 21 odst. 4 zákona o ochraně osobních údajů, který dává možnost obrátit se na ÚOOÚ přímo, aniž by bylo nutno se primárně domáhat svých práv u zaměstnavatele nebo zpracovatele. Úřad situaci prozkoumá a zjistí, zda existují důvody k provedení kontroly. V jeho působnosti není řešit spory mezi jednotlivými subjekty, obdobně jako mu nepřísluší rozhodovat o náhradě škody vzniklé v souvislosti se zpracováním osobních údajů. Pokud je na základě podnětu zaměstnance a po vyhodnocení kontroly zřejmé, že byl překročen zákon, jsou proti zaměstnavateli nebo zpracovateli použity prostředky pro správní úřad obvyklé. Těmi jsou sankce uložené v rámci správního trestání a jako specifický nástroj opatření k nápravě zjištěných nedostatků.

8 Předávání osobních údajů do zahraničí

8.1 Podmínky předávání

Osobní údaje jsou jakožto informace v nehmotné podobě velmi snadno přenositelné a jediným omezením, vyjma právních předpisů, je technická stránka věci a zejména pak forma nosiče, na kterém je osobní údaj zaznamenán. Není zjevně příliš obtížné osobní údaj přenést na cizí teritorium a zde potom provádět další zpracování, přičemž se ovšem tyto operace již vymykají právu státu, z něhož byly přijaty.

Nelze proto s dostatečnou jistotou zaručit, že ve státu příjemce bude respektován přiměřený standard ochrany osobních údajů a je dokonce představitelné, že cílem transferu osobních údajů do jiné země může být snaha obejít přísnější režim jejich ochrany.

Smyslem právní úpravy tedy pochopitelně je, aby na území přijímajícího státu panoval právní režim ochrany osobních údajů, který bude plně slučitelný s režimem zavedeným v České republice, přičemž prvořadými úkoly jsou zaručení transparentnosti přenosu a snížení rizik s přenosem spojených. Pravidla pro předávání osobních údajů do zahraničí jsou obsažena jednak v zákoně o ochraně osobních údajů, konkrétně v ustanovení § 27, a také v článcích 25 a 26 směrnice 95/46/ES. Záměrem je vytvoření takových podmínek přenosu osobních údajů, které jednak zajistí ochranu předávaných informací a nebudou současně kolidovat s principy fungování jednotného trhu v rámci Evropské unie, zejména pak v našem případě neohrozí volný pohyb zaměstnanců.

Důvody, proč zaměstnavatel hodlá předávat osobní údaje svých zaměstnanců, mohou být v zásadě dva. Prvním z nich je fakt, že zaměstnavatel v některých případech nechce osobní údaje zpracovávat sám a za tímto účelem je předává zpracovateli. Druhým důvodem jsou potřeby jiného subjektu v zahraničí, který osobní údaje dále využívá. V každém případě ovšem zaměstnavatel musí předem ověřit, zda lze osobní údaje předat do zahraničí volně, bez administrativních překážek, nebo je pro předání nutno získat povolení ÚOOÚ. Z § 27 odst. 1 zákona o ochraně osobních údajů lze dovodit, že o povolení není třeba ÚOOÚ žádat, jedná-li se o přenos mezi členskými státy Evropské unie, kde volný pohyb osobních údajů nemůže být omezován. Stejně tak dle § 27 odst. 2 mohou být osobní údaje do třetích zemí předány, „*pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž*

ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána“, přičemž se zejména jedná o státy, které ratifikovaly Úmluvu č. 108 a jejichž právní předpisy tedy zaručují dostatečnou ochranu osobních údajů odpovídající všem požadavkům směrnice 95/46/ES. Další skupinou států, do nichž je možno předávat osobní údaje bez povolení ze strany ÚOOÚ, jsou ty země, které za bezpečné z pohledu ochrany zpracování osobních údajů považuje ve svém rozhodnutí příslušný orgán (Komise) Evropské unie. V současné době se jedná o Argentinu, Faerské ostrovy, Guernsey, Ostrov Man, Jersey a Švýcarsko[37]. Specifický přístup je nutno uplatňovat při předávání osobních údajů do USA a Kanady. U těchto států je nutno zkoumat, zda jsou v konkrétních situacích splněny podmínky příslušného rozhodnutí Komise a je vhodné případné předání nejprve konzultovat s ÚOOÚ.

Nejedná-li se o výše uvedené případy, je nutné před předáním osobních údajů do třetích zemí požádat ÚOOÚ o povolení k předání (nestanoví-li zákon jinak). To bude vydáno zejména v případech, kdy cílový stát disponuje legislativní úpravou zakotvující základní principy ochrany osobních údajů a je zřízen i nezávislý orgán schopný přijímat stížnosti. V povolení o předání, které má povahu rozhodnutí ve smyslu správního řádu, ÚOOÚ stanoví primárně dobu, po kterou mohou být příslušné údaje předávány. Dojde-li ke změně okolností, za kterých bylo povolení uděleno (zejména na základě rozhodnutí orgánu Evropské unie), ÚOOÚ toto povolení změní nebo zruší. U jednotlivých předání musí zaměstnavatel v žádosti prokazatelně doložit, že jím deklarovaný důvod předání pokrývá jednu z následujících možností a to, že: 1) předání údajů se děje se souhlasem nebo na základě pokynu subjektu údajů, 2) jsou ve třetí zemi, kde mají být osobní údaje zpracovávány vytvořeny záruky ochrany osobních údajů a to např. vhodným zabezpečením, přijetím právních nebo profesních předpisů atd., 3) jde o osobní údaje, které jsou podle zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem, zpřístupnění je ovšem omezeno jen na rozsah zvláštním zákonem stanovený, 4) předání je nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zákona nebo mezinárodní smlouvy, kterou je Česká republika vázána, 5) předání je nezbytné pro jednání o uzavření nebo změně smlouvy

[37] Podrobný přehled jednotlivých rozhodnutí Komise viz http://www.uoou.cz, Předávání osobních údajů do zahraničí, Přehled případů předávání osobních údajů do zahraničí, u nichž není nutno žádat úřad o povolení.

uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, 6) předání je nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů, 7) předání je nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů.

Limity předávání zaměstnaneckých údajů do zahraničí ovšem nevyplývají pouze ze zákona o ochraně osobních údajů a § 27. Je nutno respektovat požadavky, které na zpracování osobních údajů klade celý právní řád a jeho jednotlivé součásti. Pro osobní údaje zaměstnanců budou jistě určující i ustanovení zákoníku práce, která umožňují zpracování pro konkrétní účely, jakými jsou např. mzdová a personální agenda.

Je nutné konstatovat, že pro režim předávání osobních údajů musí platit stejná pravidla, jako pro ostatní fáze zpracování. Jestliže zaměstnavatel údaje předává do třetí země s jasně definovaným účelem, neměl by tento účel překročit. Je totiž nesporné, že osobní údaje zaměstnanců nemusí nutně sloužit jen k zajištění trvání pracovněprávního vztahu, ale mohou pro zaměstnavatele plnit i řadu jiných funkcí (např. jako podklady pro vyhodnocení hospodaření a efektivity činností zaměstnavatele). Pokud má tedy zahraniční podnikatelský subjekt zájem na ekonomických výsledcích tuzemské společnosti, mohou být ekonomické souhrny předávány pouze s anonymizovanými osobními údaji zaměstnanců, protože zpracováním neanonymizovaných údajů by byl zřejmě překračován účel, v rámci kterého byly osobní údaje od zaměstnanců shromážděny.

Jako u kteréhokoli zpracování obecně, i zde platí, že by zaměstnavatel měl zaměstnanci, jakožto subjektu údajů, poskytnout informace o předávání jeho osobních údajů do zahraničí a tam, kde je zaměstnavatel povinen získat souhlas zaměstnance se zpracováním, si pak tento souhlas opatřit. V okamžiku, kdy jsou údaje zpracovávány v cizím státě specializovanými či odbornými pracovišti (zpracovateli), je nutné s těmito uzavřít smlouvu o zpracování v souladu s § 6 zákona o ochraně osobních údajů. Uvedený zpracovatel však není oprávněn předmětné osobní údaje zpracovávat pro jiné účely nebo pro jiné správce (takovéto operace je možno provádět pouze za současné anonymizace údajů).

Často také dochází k předávání osobních údajů do zahraničí v rámci zlepšování kvalifikace vymezených skupin zaměstnanců a v případech jejich vysílání na služební cesty do zahraničí. Předání v těchto případech naplňuje obvykle některou z podmínek

ustanovení § 27 zákona o ochraně osobních údajů, když je např. nezbytné respektovat předpisy o pobytu cizinců v dané zemi. Mohou ovšem nastat situace, jako např. dlouhodobý pobyt zaměstnance v cizině včetně členů jeho rodiny, kdy je nezbytné zpracovávat osobní údaje i jiných osob (rodinných příslušníků), přičemž je pro předání takových osobních údajů nezbytné získat jejich předchozí souhlas[38].

8.2 Standardní smluvní doložky a závazná podniková pravidla

Standardní smluvní doložky (standard contractual clauses) vznikly jako výsledek spolupráce Komise (ES), Pracovní skupiny WP 29 a podnikatelských kruhů. Jsou praktickým nástrojem, který je pokládám „*za dostatečné ochranné opatření s ohledem na ochranu soukromí a základních práv a svobod jednotlivců*“[39]. Komise svými rozhodnutími 2001/497/ES, 2002/16/ES a 2004/915/ES vytvořila tři typy smluvních řešení, při jejichž používání má zaměstnavatel v pozici správce jistotu, že ochrana předávaných osobních údajů bude odpovídat evropskému standardu. První, základní model řešení, pokrývá předávání osobních údajů mezi správcem nacházejícím se v zemi, odkud jsou údaje vyváženy (tzv. vývozce údajů), a právním subjektem, rovněž v postavení správce, zpracovávajícím osobní údaje ve státě přijímajícím (tzv. dovozce údajů). Druhé řešení postihuje situaci, kdy vývozcem údajů je opět správce, ovšem do pozice dovozce údajů se dostává zpracovatel. Třetí typ představuje alternativu k tipu prvnímu (vztah „správce-správce“), avšak zde je jeho použití pro správce výhodnější a je jimi výlučně používán. Rozdíl mezi prvním a třetím smluvním řešením je pro subjekt údajů a tedy zaměstnance v tom, že v posledně jmenovaném případě si nemůže vybrat, u koho se bude v případě porušení jeho práv domáhat nápravy. Primárně musí svůj nárok vznést u dovozce údajů v zahraničí a až při neúspěchu připadá v úvahu žádat o nápravu tuzemského vývozce.

Princip použití standardních smluvních doložek je přitom takový, že na znění jejich textu schváleného Komisí nelze již nic měnit a jednotlivá ustanovení nelze ani

[38] Viz http://www.uoou.cz, Předávání osobních údajů do zahraničí, K problémům z praxe, Předávání osobních údajů zaměstnanců do zahraničí.

[39] Bártík, V., Janečková, E. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 2. vydání. Praha: Linde, 2009, s. 162.

kombinovat mezi sebou. Na vůli zaměstnavatele tak zůstává, pro jaký z výše uvedených typů se v závislosti na okolnostech rozhodne, a který mu bude více vyhovovat.

Další možností, jak zajistit zpracování a přenos osobních údajů do třetích zemí jsou **závazná podniková pravidla (Binding Corporate Rules - dále jen „BCR“)**. Uplatnění najdou především v nadnárodních společnostech, kde zabezpečují volnou výměnu osobních údajů mezi jednotlivými pobočkami společnosti, aniž by přitom bylo porušeno právo na ochranu soukromí a základní práva a svobody subjektů údajů. Jde totiž o to, že v souladu se zněním směrnice 95/46/ES nelze osobní údaje předávat do třetích zemí, pokud v nich není dostatečně zajištěna náležitá úroveň ochrany[40]. To ovšem přestává platit v případě, kdy náležitá opatření k ochraně zabezpečí sám správce, přičemž je toho možno docílit právě s využitím BCR. Ty představují asi nejschůdnější a zároveň nejlevnější cestu, jak legálně zpracovávat a přenášet data uvnitř celé společnosti. Podrobné informace o tomto řešení poskytují materiály Pracovní skupiny WP 29, které obsahují zejména návody, jakým způsobem dosáhnout toho, aby BCR mohly být skutečně považovány za nástroj poskytující dostatečná ochranná opatření. BCR musejí být v souladu jednak se základními principy ochrany osobních údajů stanovené směrnicí 95/46/ES, stejně jako i legislativní úpravou členských zemí EU, ve kterých má nadnárodní společnost pobočky poskytující osobní údaje.

Zavádění BCR do praxe je relativně snadné, je ovšem nutné podotknout, že musí být přijaty všemi organizačními složkami nadnárodní společnosti a smí být používány výhradně jen uvnitř tohoto subjektu a nikoli navenek. Pro tyto případy, jež jsou označovány jako tzv. „onward transfer“, je pak možné využít např. standardní smluvní doložky. Pokud mají BCR představovat záruky ochrany osobních údajů, je potřeba, aby jejich obsah byl náležitě aplikován v každodenní praxi a zároveň byly garantovány vhodné postupy umožňující kontrolu jejich dodržování. Jinými slovy musí být dostatečně zajištěna vymahatelnost přijatých pravidel stejně jako i jejich obecná známost v rámci celé nadnárodní společnosti.

[40] Viz Čl. 25 odst. 1 směrnice 95/46/ES.

9 Praktické problémy

Oblast personalistiky, zejména pak výběr potenciálních zaměstnanců, je spolu s monitorováním činností na pracovišti jednoznačně nejvíce diskutovanou oblastí, která se týká ochrany osobních údajů v pracovněprávních vtazích. Je tomu tak zejména z toho důvodu, že se při těchto činnostech osobní údaje shromažďují ve značném rozsahu a současně dochází ke střetu zájmů zaměstnavatele na straně jedné a zaměstnanců, jakožto subjektů údajů na straně druhé. Možný konflikt práv a povinností je motivován především snahou zaměstnavatele chránit jeho majetek, stejně jako snahou vybrat do řad svých zaměstnanců schopné a důvěryhodné pracovníky, kteří budou plnit řádně pracovní úkoly. Naproti tomu stojí odůvodněný požadavek zaměstnanců, aby jejich právními předpisy garantovaná práva, především pak právo na ochranu osobního a soukromého života, nebyla neoprávněnými zásahy potlačena nebo jiným způsobem zkrácena. Následující kapitola uvádí příklady zacházení s osobními údaji, která jsou v zájmu zachování rovnováhy mezi oprávněnými zájmy na obou stranách nutná, avšak u nichž také nejednou hrozí překročení zákonných mezí zpracování osobních údajů.

9.1 Zpracování osobních údajů před uzavřením pracovního poměru

Legislativní zakotvení vztahů před vznikem pracovního poměru bylo v minulosti, a to až do přijetí zákona o zaměstnanosti, dosti vágní a aplikace zákonných ustanovení týkajících se ochrany osobních údajů způsobovala velké potíže. Problémy byly zejména při zpracování osobních údajů uchazečů o zaměstnání, které od nich požadovaly personální agentury samostatně působící na trhu práce a vystupující tak jako správci osobních údajů. Aniž by byla jejich činnost limitována konkrétními požadavky zaměstnavatelů, v mnohých případech shromažďovaly údaje svých klientů v rozsahu, který neměl vztah k potenciálnímu zaměstnání. Očividně tak tímto způsobem docházelo k porušování zákona o ochraně osobních údajů, konkrétně ustanovení § 5 odst. 1 písm. d) stanovícího povinnost „*shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v nezbytném rozsahu pro naplnění stanoveného účelu*“. Požadované údaje se týkaly např. formy bydlení (vlastní, nájemní, podnájemní), rodinných poměrů klientů, plánovaného počtu dětí apod. Zpracování takto velkého objemu osobních dat probíhalo na základě souhlasu subjektu údajů, který si personální agentury sice opatřily, ovšem nelze jednoznačně říci, že by udělený souhlas byl vždy „dobrovolný“. Dřívější znění

zákona o ochraně osobních údajů (do 25. 7. 2004) to víceméně umožňovalo, přičemž náprava přišla až s jeho novelizací, která souhlas subjektu údajů definuje v § 4 písm. n) jako „*svobodný a výslovný projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním*“. Nově musí být subjekt údajů rovněž informován o tom, k jakému účelu zpracování a jakých osobních údajů se jeho souhlas týká, stejně jako i jakému správci a na jakou dobu souhlas uděluje. Souhlas se zpracováním se tak i s přispěním judikatury a výsledků rozhodovací činnosti ÚOOÚ vyprofiloval jako jednostranný právní úkon, který je zcela v souladu s ustanoveními §§ 37 a 39 občanského zákoníku a jako takový musí být respektován.

Zákon o zaměstnanosti umožňuje od počátku jeho účinnosti vyčlenit kategorie osobních údajů, které není možné ve fázi výběru zaměstnanců zjišťovat. V § 12 odst. 2 zákona o zaměstnanosti je výslovně uvedeno, že „*zaměstnavatel nesmí při výběru zaměstnanců vyžadovat informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace, není-li jejich vyžadování v souladu s § 4 odst. 3 a 4, dále informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených zvláštním právním předpisem. Na žádost uchazeče o zaměstnání je zaměstnavatel povinen prokázat potřebnost požadovaného osobního údaje*“. Tato úprava má evidentně zabránit možnému diskriminačnímu jednání ze strany zaměstnavatele a současně kopíruje kategorie citlivých údajů tak, jak jsou vymezeny zákonem o ochraně osobních údajů v § 4 písm. b). Výraz „nesmí“ uvedený v § 12 odst. 2 větě první zákona o zaměstnanosti je možno považovat za zákaz relativní, a to s přihlédnutím k zákonné výjimce[41] týkající se případů, kdy je nutno předmětné osobní údaje uvést, aby bylo možno např. ověřit splnění předpokladů pro výkon určitých povolání. Přitom musí být prokázán oprávněný cíl a přiměřenost požadavku na sdělení údajů dle § 12 odst. 2 zákona o zaměstnanosti, aby takové jednání nepůsobilo diskriminačně.

Obdobně jako zákon o zaměstnanosti i současné znění zákoníku práce obsahuje ve svém textu ustanovení limitující zaměstnavatele co do informací, které je možno v rámci sjednávání budoucího pracovněprávního vztahu od zájemce o práci požadovat. V části druhé, hlavě I. nazvané Postup před vznikem pracovního poměru je v § 30 odst.

[41] Viz § 4 odst. 3 a 4 zákona o zaměstnanosti.

2 zákoníku práce uvedeno, že „*zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy*“. Je patrné, že ani aktuální úprava není příliš konkrétní a je nutno na ni nahlížet v kontextu § 316 odst. 4 zákoníku práce, který se jinak vztahuje pouze na zaměstnance a zabývá se ochranou jejich práv. Ten stanoví výčet osobních údajů, které se dají označit jako údaje citlivé a které zaměstnavatel vyžadovat výslovně nesmí. Údaje uvedené v § 316 odst. 4 se zároveň částečně překrývají s údaji vyjmenovanými v § 12 odst. 2 zákona o zaměstnanosti. Překryv je nutno interpretovat tak, že zákaz požadovat údaje uvedené v § 316 odst. 4 týkající se sexuální orientace, původu, členství v odborové organizaci, členství v politických stranách a hnutích stejně jako údaje o příslušnosti k církvi nebo náboženské společnosti je pro zaměstnavatele, na rozdíl od zákona o zaměstnanosti, absolutní a týká se nejen již existujícího pracovněprávního vztahu, ale dá se vztáhnout i na období před vznikem pracovního poměru. Tento zákaz je relativizován v případě údajů týkajících se těhotenství, rodinných a majetkových poměrů a trestněprávní bezúhonnosti uvedených v § 316 odst. 4 pod písmeny a), b) a h) zákoníku práce v případě, že je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána a je-li tento požadavek přiměřený.

Přesto, že je tedy obecně zaměstnavateli zakázáno požadovat informace o těhotenství, jak u uchazečů o zaměstnání tak i zaměstnanců, lze tento požadavek považovat za odůvodněný v souvislosti se sjednáváním pracovního poměru pro případ, že je zaměstnankyně přijímána na práci, která je těhotným ženám zakázána. To samé platí i pro informace týkající se trestněprávní bezúhonnosti budoucích zaměstnanců, zvláště pak tehdy, stanoví-li požadavek bezúhonnost zvláštní právní předpis. Pokud zaměstnavatel vybírá budoucího zaměstnance na pozici, kde může přijít do styku s větší peněžní hotovostí nebo se jedná o práci, při níž může dojít k ohrožení bezpečnosti a zdraví lidí, nelze než souhlasit s tím, aby byla minulost uchazečů o zaměstnání tímto způsobem prověřována. I zde ovšem platí, že nevyplývá-li požadavek na sdělení zmíněných údajů přímo z právního předpisu, je tyto osobní údaje nutno shromažďovat v souladu s § 5 odst. 1 písm. d) zákona o ochraně osobních údajů.

Nabízí se otázka, co lze považovat za přijatelný rozsah informací (osobních údajů), které lze s přihlédnutím k účelu, jakým má být výběr budoucích zaměstnanců,

oprávněně požadovat. V kontextu toho, co bylo výše popsáno, je nesporné, že půjde primárně pouze o údaje bezprostředně související s obsazovaným pracovním místem. Jsou jimi jednak základní identifikační údaje jako jméno, příjmení, adresa bydliště, datum narození (nikoliv však rodné číslo), informace o dosaženém vzdělání a praxi, případně i informace o zvláštních schopnostech, které mají vztah k obsazované pracovní pozici a také běžné kontaktní údaje, jako číslo telefonu nebo emailová adresa[42]. Ke zpracování těchto osobních údajů pak není zapotřebí získávat souhlas subjektu údajů, protože v souladu s ustanovením § 5 odst. 2 zákona o ochraně osobních údajů platí, že bez souhlasu je možno zpracovávat osobní údaje „*jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů*“. V případě náboru nových zaměstnanců se jedná právě o tento případ, tedy jednání o uzavření smlouvy byť v pouhém zahajovacím stádiu. Je přitom zřejmé, že uchazeči o zaměstnání jsou na základě požadavků, které zaměstnavatel zveřejní, obeznámeni jak s rozsahem požadovaných údajů, tak i s jejich účelem, kterým má být výběr vhodného uchazeče a uzavření pracovní smlouvy.

Zaměstnavatel se však tímto nezbavuje všech povinností, které mu zákon o ochraně osobních údajů ukládá. Zpracování většího počtu osobních údajů předem neurčeného počtu osob (uchazečů) s sebou přináší povinnost chránit je před zneužitím vyjádřenou v § 13 zákona o ochraně osobních údajů podobně tak jako povinnost využívat jej jen k účelu, k němuž byly shromážděny a to po dobu nezbytně nutnou k naplnění účelu takto stanoveného. To pro zaměstnavatele znamená dostatečně osobní údaje zabezpečit a stanovit přiměřenou dobu jejich zpracování s ohledem na konkrétní účel, kterým je v tomto případě uzavření pracovní smlouvy s vybraným uchazečem. Jakmile je smlouva uzavřena nebo jsou neúspěšní uchazeči vyrozuměni o tom, že nebyli vybráni, pominul důvod, pro který byly údaje shromážděny a je nutné je v souladu se zákonem buďto vrátit neúspěšným uchazečům nebo je patřičným způsobem zlikvidovat. Další zpracování pak musí probíhat za současného souhlasu subjektu údajů, který musí splňovat požadavky § 4 písm. n) a § 5 odst. 4 zákona o ochraně osobních údajů.

[42] Bártík, V., Janečková, E. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 2. vydání. Praha: Linde, 2009, s. 146.

Je tedy nutné se situací, kdy potencionálnímu zaměstnavateli sdělujeme naše osobní údaje, obávat? Moje odpověď zní nikoli. Je ovšem více než jasné, že to platí jen za předpokladu, že na jedné straně bude respektován zákon a na straně druhé bude dodržována jistá míra opatrnosti. Zaměstnavatel by měl v první řadě dodržovat ustanovení jak zákona o ochraně osobních údajů, tak zajisté i právních předpisů v oblasti pracovního práva. K tomu by měl dobře volit ty osobní údaje, které bude skutečně k výběru nových zaměstnanců potřebovat a to s přihlédnutím k přesně definované pracovní pozici. Naopak eventuální zaměstnanci, kterým je v mnoha případech ponechána svobodná vůle ohledně toho, jaké kvalifikační předpoklady v životopise skutečně uvedou, by měli zachovávat rozvahu a zbytečně nesdělovat něco, co po nich vlastně ani nikdo nechce. Jestliže totiž poskytnou informace, které jinak zaměstnavatel nesmí vyžadovat, dobrovolně, nelze tento postup považovat za porušení povinnosti ze strany zaměstnavatele, protože § 30 odst. 2 zákoníku práce mu zakazuje některé informace vyžadovat, nikoliv však přijímat. Podstatné je pak to, že poskytnutí údajů musí být skutečně svobodné a nesmí být vyvoláno ani nepřímým nátlakem ze strany zaměstnavatele.

9.2 Preemployment Background Screening

V návaznosti ne předchozí téma, tedy zpracování osobních údajů před vznikem pracovního poměru, je vhodné zmínit tzv. „Preemployment Background Screening“ (dále jen „PEBS“). Tato metoda může být charakterizována jako „*soustava činností, prováděných většinou před vznikem pracovního poměru, v rámci kterých zaměstnavatel shromažďuje zvolené osobní údaje, poskytované mu dobrovolně uchazeči o zaměstnání a ověřuje s jejich souhlasem úplnost, správnost a pravdivost těchto informací, vše s cílem vybrat nejvhodnějšího budoucího zaměstnance*“[43]. Metoda PEBS je ve světě a obzvláště pak v USA, kde ostatně i vznikla, obecně užívaným prostředkem prevence, který má zabránit výběru zaměstnanců s ne příliš dobrou minulostí. Ve Spojených státech má PEBS poměrně širokou legislativní základnu napříč jednotlivými státy (nejvýznamnějším federálním předpisem je v této oblasti asi „Fair Credit Reporting Act“), která umožňuje stanovit pevná pravidla pro její provádění a zaměstnavatelé

[43] Moroz, M. Jejich minulost vaše budoucnost - Preemployment Background Screening. Praha: Právnická fakulta Univerzity Karlovy. Přednáška ze dne 26. 11. 2009.

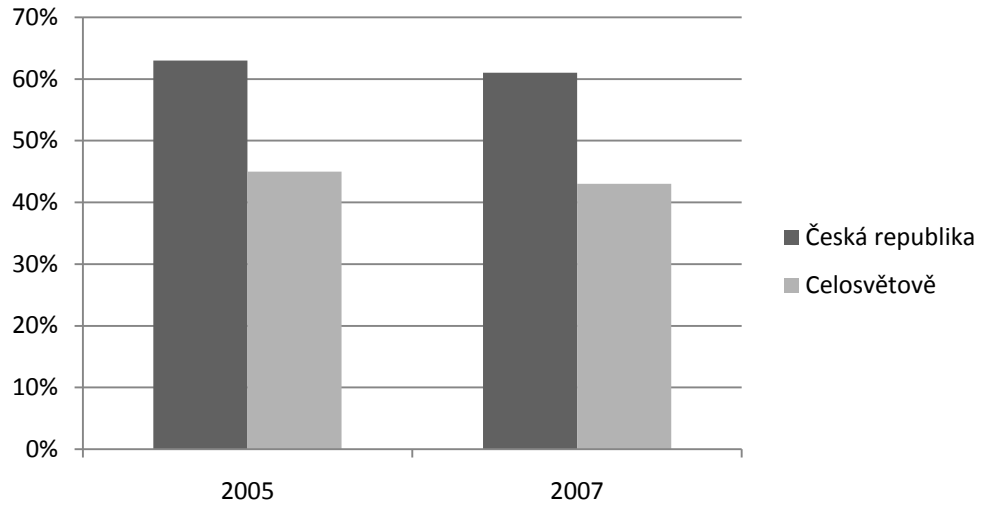
mohou jejím prostřednictvím vstupovat do vybraných registrů a z nich pak získávat potřebné informace. Vedle těchto právních norem existují i mezinárodně uznávané metodiky upravující Preemployment Background Screening, jako je např. metodika ASIS Internacional. ASIS Internacional představuje sdružení specialistů se zaměřením na bezpečnostní sektor, přičemž se pobočka této společnosti nachází i v České republice. ASIS působí v mnoha oblastech a mimo jiné vydává i vlastní publikace a periodika, z nichž se za nejdůležitější z hlediska metody PEBS dá považovat standard s názvem „Preemployment Background Screening Guidline" z roku 2009. Je zaměřena primárně na použití v USA, ale některé obecné principy lze využít i v prostředí České republiky.

Z výše uvedené definice PEBS víme, co je jejím základním cílem. Jak ale postup v rámci PEBS v reálu vypadá a co lze od něj očekávat? Podstatné je, že by ověřování identity a minulosti uchazeče o zaměstnání mělo být v souladu s platnou legislativou státu zaměstnavatele a měla by být respektována i jistá firemní kultura. Tato metoda je převážně využívána nadnárodními společnostmi a to zejména v oblasti bankovnictví nebo tam, kde zaměstnanci přicházejí do styku s citlivými informacemi nebo obchodním tajemstvím. Primárně pak budou prověřováni zájemci hlásící se na vrcholné manažerské posty nebo ti, pro které platí zvláštní kvalifikační požadavky. Základem PEBS je série „šetření" prováděná buď přímo osobou zaměstnavatele, nebo prostřednictvím jím pověřeného subjektu, která se snaží porovnat údaje poskytnuté uchazečem o zaměstnání s jeho reálnou pracovní i soukromou minulostí. Klíčovými jsou pro zaměstnavatele v závislosti na obsazované pracovní pozici především údaje o důvodu dřívějšího ukončení pracovního poměru, dosaženém vzdělání, podrobnosti o neskončených civilních nebo trestních řízeních a také informace týkající se kredibility budoucích zaměstnanců. Jak již bylo zmíněno, použití metody PEBS by mělo být odvislé od souhlasu uchazeče o zaměstnání s jejím provedením a tento uchazeč by měl být současně vyrozuměn o tom, jaké údaje a proč budou ověřovány, případně kdo k těmto údajům bude mít přístup. Následně jsou jednotlivé informace prověřovány jednak na základě uchazečem předložených dokumentů (v úvahu připadají např. osobní doklady nebo nejrůznější certifikáty) a dále z referencí získaných od bývalých zaměstnavatelů, které je možno pokládat za nestranné zhodnocení uchazečova chování

v rámci jeho předešlého zaměstnání stejně jako obraz jeho schopností spolupracovat s ostatními zaměstnanci[44].

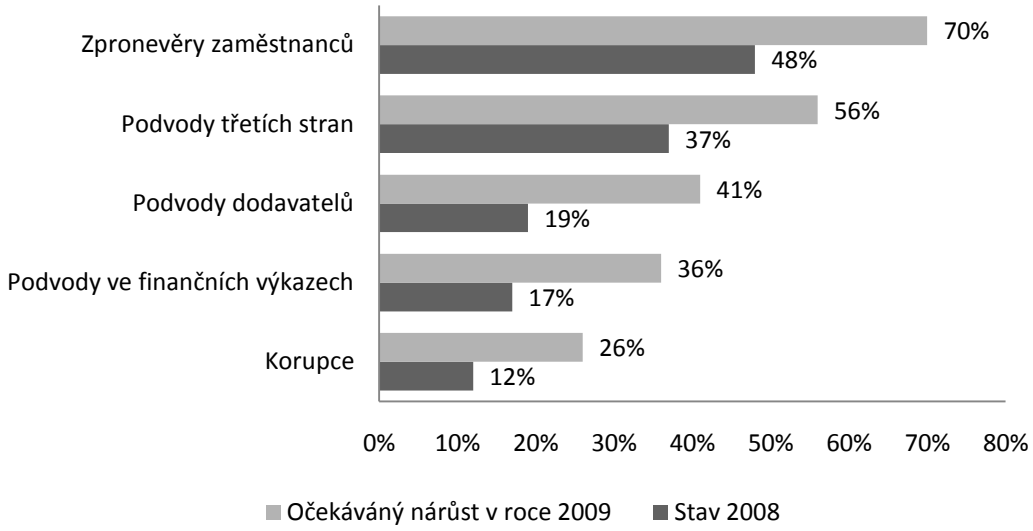
9.2.1 Realizace PEBS v podmínkách České republiky

S požadavkem ověřování minulosti uchazečů o zaměstnání přišly v České republice jako první především finanční instituce, které mají zájem na tom, aby jejich zaměstnanci operující často s velkými objemy peněz, byli spolehliví a bezúhonní. Z grafů znázorňujících globální data nelze říci, že by ověřování životopisů uchazečů o zaměstnání bylo zcela bezpředmětné a dokonce jsou zde prezentovaná čísla dosti alarmující. Jak u nově přijímaných, tak i mezi stálými zaměstnanci dochází stále častěji k podvodům nebo korupci a jejich odhalení není vždy zcela snadné. Tyto případy mohou ve výsledku pro zaměstnavatele znamenat velké finanční ztráty nebo ztrátu důvěry zavedených či potenciálních klientů.



Graf 1 znázorňuje počet společností, které se staly obětí podvodu.

[44] Řezníček, P. redaktor. Personalistika 2009 - 2010. Praha: ASPI, Wolters Kluwer, 2009, s. 117.



Graf 2 popisuje procentuální zastoupení jednotlivých typů podvodného jednání u dotázaných společností.[45]

Naše legislativa metodu podobnou PEBS v současnosti neupravuje. Některé prvky, které se v jejím rámci využívají, mají ale svůj zákonem upravený ekvivalent a je možné se na ně odvolat. Najdeme je jednak v zákoně o ochraně osobních údajů, dále v předpisech pracovního práva jakým jsou zákon o zaměstnanosti a zákoník práce, využít lze i ustanovení občanského zákoníku. Specifickým příkladem prověrek minulosti uchazečů o určité pracovní pozice jsou tzv. lustrace. Jejich výsledkem je vydání lustračního osvědčení pro výkon zákonem stanovených funkcí obsazovaných volbou, jmenováním nebo ustanovováním. Osvědčení deklaruje, zda lustrovaná osoba byla či nebyla v období od 25. 2. 1948 do 17. 11. 1989 příslušníkem Sboru národní bezpečnosti nebo zda byla evidována v materiálech Státní bezpečnosti jako spolupracovník ve smyslu ustanovení § 2 odst. 1 písm. b) zákona č. 451/1991 Sb. kterým se stanoví některé další předpoklady pro výkon některých funkcí ve státních orgánech a organizacích České a Slovenské Federativní Republiky, České republiky a Slovenské republiky, ve znění pozdějších předpisů. Žádost o vystavení takovéhoto osvědčení pro sebe může podat občan České republiky starší 18 let nebo státní organizace nebo organizace s většinovou účastí státu, pro kterou občan vykonává nebo bude vykonávat danou funkci.

[45] Zdroj: Moroz, M. Jejich minulost vaše budoucnost - Preemployment Background Screening. Praha: Právnická fakulta Univerzity Karlovy. Přednáška ze dne 26. 11. 2009.

Přesto že české právo nepředvídá postupy podobné PEBS, není důvod tuto metodu při dodržení existující zákonné úpravy právně zpochybňovat[46]. Zájemci o využití PEBS ze strany zaměstnavatelů se však musí pohybovat v rámci zákonných mantinelů a je dobré jim doporučit, aby vyhledali některou z poradenských společností, které se v Českém republice PEBS zabývají.

9.2.2 Podmínky užití PEBS v legislativě České republiky

Z pohledu zaměstnavatele, který bude v rámci metody PEBS zpracovávat osobní údaje uchazečů o zaměstnání, bude klíčovým předpisem vedle zákona o zaměstnanosti a zákoníku práce **zákon o ochraně osobních údajů.**

Podrobná analýza jeho jednotlivých ustanovení byla popsána již v předchozích kapitolách této práce a tak zopakuji jen ty nejpodstatnější povinnosti, které zaměstnavateli nebo jím pověřenému subjektu, který bude údaje uchazečů o zaměstnání prověřovat, z využití metody PEBS plynou. Je nutné v první řadě připomenout, že pokud povinnost shromažďovat a zpracovávat určité osobní údaje nevychází přímo ze zvláštního zákona nebo nenaplňuje některou z jiných výjimek uvedených v § 18 odst. 1 zákona o ochraně osobních údajů, je nutné, aby zaměstnavatel jako správce osobních údajů splnil oznamovací povinnost vůči ÚOOÚ. Jak bylo zmíněno v kapitole týkající se zpracování osobních údajů před vznikem pracovního poměru, není vždy nutné získat souhlas subjektu údajů se zpracováním a to zejména tehdy, směřuje-li zpracování k uzavření smlouvy na návrh subjektu údajů. Mimo tyto případy je obecně povinností správce si opatřit souhlas s předmětným zpracováním a současně subjekt údajů dostatečně informovat o všech operacích s jeho osobními údaji, jak stanoví § 5 odst. 4 zákona o ochraně osobních údajů. V rámci PEBS nelze vyloučit možnost nedovolené manipulace s osobními údaji uchazečů, přičemž mohou být takto ohrožena jejich práva. Proto by mělo být v zájmu zaměstnavatele stejně jako dalších osob podílejících se na zpracování dostatečně zajistit, v souladu s § 13 zákona o ochraně osobních údajů, aby nemohlo dojít neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení, neoprávněným přenosům apod. Dostatečné zabezpečení procesu zpracování osobních údajů je další povinností, která ze zákona o ochraně osobních údajů plyne. Konečně, jakmile je vybrán vhodný uchazeč na obsazovanou pracovní

[46] Bělina, M. a kol. Zákoník práce. Komentář. 2. vydání. Praha: C. H. Beck, 2010, s. 136.

pozici, nebo je ukončeno prověřování minulosti zaměstnance za trvání pracovněprávního vztahu, odpadl důvod, pro který byly osobní údaje zpracovávány, a je povinností zaměstnavatele nebo jím pověřených osob údaje zlikvidovat nebo je předat zpět osobám, jichž se týkají.

ÚOOÚ se dosud případy použití metody Preemployment Background Screeningu nezabýval, z čehož vyplývá, že k nim ani do této chvíle nebyla vydána žádná stanoviska nebo rozhodnutí. Z pohledu zaměstnavatele bych tak považoval za vhodné se před samotným zahájením postupu dle metodiky PEBS obrátit na ÚOOÚ a konzultovat s ním celý zamýšlený proces i jeho jednotlivé kroky.

Zákoník práce se dá na metodu PEBS vztáhnout hlavně díky ustanovení § 30 upravujícího postup před vznikem pracovního poměru a § 316, který se kromě ochrany majetkových práv zaměstnavatele týká i ochrany osobních práv zaměstnanců. Oba tyto paragrafy řeší oprávnění zaměstnavatele vyžadovat od svých zaměstnanců a uchazečů o zaměstnání určité informace, přičemž je z těchto ustanovení patrné, že se zaměstnavatel musí při získávání osobních údajů držet především účelu, který se bezprostředně dotýká povahy vykonávané práce. Současně je také ze znění § 30 odst. 1 zřejmé, že výběr budoucích zaměstnanců je plně v působnosti zaměstnavatele, kterému je tak dána možnost si nejvhodnějšího uchazeče při dodržení zákazu diskriminace a zachování práva uchazečů na rovné zacházení vybrat a to i za použití metody PEBS. Předpokladem pro nediskriminační jednání ze strany zaměstnavatele je, aby zaměstnavatel při svém rozhodování zohledňoval pouze ta kvalifikační kritéria, jež se vztahují k výkonu práce, o kterou se fyzická osoba uchází. Pokud je zvláštním právním předpisem stanoven okruh dalších náležitostí vyžadovaných pro výkon určité funkce nebo povolání, je jimi zaměstnavatel při svém výběru rovněž vázán.

Užitečnou pro aplikaci metody PEBS může být také část třináctá zákoníku práce s názvem Společná ustanovení. Ta obsahuje pravidla pro vydávání potvrzení o zaměstnání a pracovního posudku, přičemž tyto dokumenty mohou sloužit jako podkladový materiál pro hodnocení práceschopnosti a kvality budoucího zaměstnance.

Potvrzení o zaměstnání jsou povinni poskytnout všichni zaměstnavatelé bez ohledu na to, zda o něj zaměstnanec požádá a to nejpozději ke dni ukončení pracovního poměru nebo dohody o pracovní činnosti. Potvrzení obsahuje informace uvedené § 313 odst. 1 písm. a) až g) zákoníku práce, kterými jsou např. údaje o zaměstnání, zda se

jednalo o pracovní poměr nebo dohodu o pracovní činnosti a o době jejich trvání, druh konaných prací a dosaženou kvalifikaci nebo zda byl pracovněprávní vztah zaměstnavatelem ukončen z důvodu porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci zvlášť hrubým způsobem. Výčet informací v § 313 odst. 1 je doplněn Nařízením vlády č. 108/1994 Sb., kterým se provádí zákoník práce a některé další zákony, ovšem mimo tyto údaje, je možno po dohodě se zaměstnavatelem uvést i informace další[47]. Budoucí zaměstnavatel má na získání těchto informací jistě zájem, a protože nemá obecně právní povinnost sjednat s uchazečem o zaměstnání pracovní poměr, může předložením potvrzení o zaměstnání podmínit i jeho vznik, přičemž je tento postup v souladu se zákonem[48].

Posudek o pracovní činnosti (pracovní posudek) se vydává oproti potvrzení o zaměstnání pouze na žádost zaměstnance, která může být podána telefonicky, ústně, písemně nebo např. ve formě e-mailu a lze tak učinit kdykoli za trvání pracovního poměru nebo i po jeho skončení. Obsahuje zejména hodnocení zaměstnance, jeho kvalifikaci a schopnosti, stejně jako i další skutečnosti mající vztah k výkonu práce jako např. hodnocení přístupu k práci a spolupracovníkům, osobní vlastnosti mající bezprostřední vztah k dané práci jako je svědomitost, iniciativnost, schopnost řízení apod. Vždy je ovšem nutné pracovní posudek brát jako subjektivní náhled hodnotitele (zaměstnavatele) a je proto důležité, aby byl pokud možno založen na objektivních skutečnostech. Pokud totiž nebude zaměstnanec přijat do jiného zaměstnání na základě nepravdivého posudku, má možnost se obrátit dle ustanovení § 315 zákoníku práce na soud a požadovat po bývalém zaměstnavateli přiměřenou úpravu posudku. To samé platí i v případě potvrzení o zaměstnání.

Zaměstnavatel je co do informací, které se dají o uchazečích na jím obsazované pracovní místo shromažďovat, omezen také **zákonem o zaměstnanosti** a to konkrétně úpravou uvedenou v § 12. Jak bylo v předešlé kapitole uvedeno, § 12 odst. 2 zákona o zaměstnanosti spolu s § 316 odst. 4 zákoníku práce stanoví relativní a absolutní zákaz shromažďování určitých osobních údajů zaměstnavatelem, což znamená, že pokud zaměstnavatel jisté údaje nezíská, nemůže je následně s pomocí metody PEBS ani ověřit. To je také hlavní omezení, které ze zákona o zaměstnanosti vyplývá. Mimo to

[47] Bělina, M. a kol. Zákoník práce. Komentář. 2. vydání. Praha: C. H. Beck, 2010, s. 808.

[48] Viz rozhodnutí Nejvyššího soudu ze dne 20. 3. 2003, sp. zn. 21 Cdo 1491/2002.

v případě, že se zaměstnavatel bude při výběru budoucího zaměstnance chovat diskriminačně, lze mu uložit pokutu až do výše 1 milionu korun[49].

Vedle výše uvedených právních předpisů existují i další zákony, které mají pro použití metody PEBS spíše podpůrný charakter. Jedná se o zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdější předpisů, který upravuje vydávání výpisů z Rejstříku trestů a to pouze osobám, kterých se záznamy v něm vedené přímo dotýkají. Jak ale tento zákon dále v § 11 odst. 1 stanoví, je možno výpis vydat i na základě úředně ověřené plné moci zmocněnci této osoby nebo v rámci poskytování právní pomoci této osobě jejímu advokátovi. Výpis z rejstříku trestů pak slouží zaměstnavateli jako doklad o trestněprávní bezúhonnosti uchazeče o zaměstnání v případech, kdy je zvláštním právním předpisem tato vlastnost pro výkon určitých povolání vyžadována. Kromě informací o trestní minulosti budou mít svůj význam i údaje týkající se dosaženého stupně vzdělání, které může zaměstnavatel jakožto informace o kvalifikaci uchazeče rovněž požadovat. Jedná se zejména o originály nebo kopie vysokoškolského diplomu dle zákona č. 111/1998 Sb., o vysokých školách, ve znění pozdějších předpisů, který je dokladem o absolvování studijního programu v příslušném studijním oboru nebo se zaměstnavatel může, jestliže prokáže právní zájem, rovněž obrátit přímo na vysokou školu a ověřit, zda uchazeč danou školu skutečně studoval, případně za jakých okolností.

9.2.3 Shrnutí

Metoda Preemployment Background Screeningu má v pracovněprávních vztazích nesporně svoje opodstatnění. Jejím prostřednictvím je možno zabránit opakovanému hledání vhodných kandidátů na uvolněná pracovní místa nebo lze takto zmírnit ztráty způsobené nekvalifikovanými pracovníky. Současně by měla metoda PEBS napomáhat k vytvoření dobrých pracovních podmínek jak mezi jednotlivými zaměstnanci navzájem, tak i mezi zaměstnanci a vedením společnosti. Výběr spolehlivých zaměstnanců je základem pro eliminaci úniku důvěrných informací ze společnosti a v očích klientů pak zvedá její důvěryhodnost a míru spolehlivosti. Tím, že dojde k nepřijetí uchazečů s kriminální minulostí, zabrání zaměstnavatel případným škodám na svém movitém majetku a zároveň je zvýšena bezpečnost na pracovišti. Za

[49] Viz § 139 odst. 1 písm. a) ve spojení s § 139 odst. 3 písm. a) zákona o zaměstnanosti.

situace, kdy jsou za použití PEBS odhaleny nesrovnalosti v údajích uvedených uchazečem o zaměstnání, připadají v úvahu dvě možná východiska. Jedná-li se o osobní údaje, které na základě právního předpisu zaměstnavatel nesmí od uchazeče požadovat, nemá to vliv na platnost či neplatnost následně uzavřené pracovní smlouvy. Pokud je však zaměstnavatel oprávněn informace požadovat, mohou nepravdivé údaje v dotazníku nebo zfalšované dokumenty potvrzující dosaženou kvalifikaci vyvolat v zaměstnavateli omyl, na základě kterého byla pracovní smlouva uzavřena. Omyl má v pracovněprávních vztazích relevanci za předpokladu, že se týká skutečností, které jsou pro pracovněprávní úkon podstatné a bez nichž by k němu nedošlo v takové podobě, v jaké byl učiněn a zároveň druhý účastník omyl vyvolal nebo mu byl alespoň znám (druhý účastník o omylu věděl, ale neupozornil na něj)[50]. Uzavřel-li zaměstnavatel za těchto podmínek pracovní smlouvu, má možnost se u soudu dovolat její relativní neplatnosti dle § 49a občanského zákoníku ve spojení s § 20 zákoníku práce. Dovolání se relativní neplatnosti pracovní smlouvy způsobí, že na ni bude nahlíženo, jako by od počátku neexistovala. Z hlediska vzájemných nároků ze strany zaměstnavatele a zaměstnance bude výhodnější, pokud zaměstnavatel vznese námitku relativní neplatnosti pracovní smlouvy ještě před vznikem pracovního poměru a po jeho vzniku zvolí v případě odhalení nepravdivých údajů buďto ukončení ve zkušební době nebo cestu klasické výpovědi[51].

Přesto, že není Preemployment Background Screening v ČR legislativně zakotven, je možné ho v našich poměrech na základě existujících zákonů pro účely prověření minulosti uchazečů o zaměstnání využívat. Vyžaduje to především dobrou znalost právních předpisů v oblasti pracovního práva a zejména pak znalost zákona o ochraně osobních údajů. Pokud se zaměstnavatel rozhodne metodu PEBS provádět sám, je v první řadě potřeba splnit oznamovací povinnost dle § 16 zákona o ochraně osobních údajů týkající se shromažďování a další manipulace s osobními údaji uchazečů o zaměstnání, které naplňují definiční znaky zpracování. Jakmile ÚOOÚ prověří podané oznámení a nevznikne-li důvodná obava, že by zpracováním mohlo dojít k porušení zákona, zaregistruje úřad zaměstnavatele jako správce osobních údajů se všemi právními důsledky. K tomu je na místě opatřit si od uchazečů souhlas se zpracováním a

[50] Bělina, M. a kol. Zákoník práce. Komentář. 2. vydání. Praha: C. H. Beck, 2010, s. 98.

[51] Bezouška, P., Ivanco, G. Pracovní právo pro zaměstnavatele. Praha: Linde, 2010, s. 133.

ověřením jejich osobních údajů, přičemž samotným prověřením jejich minulosti může zaměstnavatel pověřit jak vlastní zaměstnance, tak i externí fyzické nebo právnické osoby coby zpracovatele. Je rovněž dobré si předem udělat podrobnou analýzu pracovních pozic, na jejichž obsazení bude metoda PEBS využita, aby zaměstnavatel věděl, které osobní údaje bude od zájemců o zaměstnání vyžadovat a neshromažďoval tak informace, které jsou bezpředmětné a vymykají se účelu, pro který mají být získány.

9.3 Využití kamerových systémů na pracovišti

Používání kamerových systému je velice diskutované téma. Při monitoringu osob může docházet k zásahům do jejich soukromí, a proto by měla být tomuto tématu věnována zvýšená pozornost. Rozhodne-li se zaměstnavatel monitorovat dění na pracovišti, má to především dva cíle. Tím prvním je předpoklad, že kamerový systém bude využit ke sledování plnění pracovních povinností zaměstnanci a současně se ohlídá důsledné dodržování pracovní doby. Druhým důvodem, proč jsou kamery na pracovišti instalovány, je pak ochrana majetku zaměstnavatele a to zejména s ohledem na možné krádeže. Problémem je, že právní předpisy drží jen stěží krok s reálným ekonomickým životem a pokrok v oblasti výpočetní techniky znamená stále nová rizika pro ochranu práv zaměstnanců i zaměstnavatelů. Pokud chce zaměstnavatel důsledně chránit své majetkové zájmy, nemůže tak činit neomezeně. Musí přitom respektovat právní předpisy chránící osobnostní práva zaměstnanců, jelikož jsou tato práva zvláště důležitá a mají v hierarchii lidských práv před právy majetkovými přednost.

Předpisů chránících osobnostní práva člověka je hned několik. Mimo článku 8 Úmluvy o ochraně lidských práv a základních svobod a článku 10 Listiny existuje úprava ochrany osobních práv týkající se zaměstnanců i v platném znění zákoníku páce. V hlavě osmé části třinácté zákoníku práce se dozvídáme z ustanovení § 316 odst. 1, že by zaměstnanci neměli bez svolení zaměstnavatele využívat ke svým osobním potřebám výrobní a pracovní prostředky zaměstnavatele, přičemž se toto omezení týká např. výpočetní nebo telekomunikační techniky. Zaměstnavatele přitom disponuje ze zákona oprávněním kontrolovat, zda jeho zaměstnanci tento zákaz dodržují, čímž je mu dána možnost přiměřeně chránit svůj majetek. Aby byl takovýto zásah do soukromé sféry zaměstnanců kompenzován, stanoví zákoník práce rovněž limity, které zaměstnavateli brání v přílišném zasahování do soukromí zaměstnanců. V § 316 odst. 2 je uvedeno, že

„*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*“. Pokud výše citované ustanovení rozebereme, zjistíme, že díky výjimce kdy zaměstnavatel může zasahovat do soukromí zaměstnanců z důvodu spočívajícího ve zvláštní povaze jeho činnosti, není soukromí na pracovišti zcela nedotknutelné. Jak ale interpretovat úmysl zákonodárce u spojení „zvláštní povaha činnosti zaměstnavatele“? Právní pojem „zvláštní povaha“ není dosud blíže specifikován a nezbývá než se přiklonit k názoru, že je jím myšlena činnost, kde jsou kladeny větší nároky na chování zaměstnanců (např. při manipulaci s utajovanými skutečnostmi, povinnosti zachovávat mlčenlivost nebo u manipulace s většími majetkovými hodnotami apod.)[52]. Pod otevřené nebo skryté sledování zaměstnanců zmíněné v § 316 odst. 2 je přitom možno podřadit s jistotou i nasazení kamerového systému. V souvislosti s tím se rovněž nabízí otázka, zda by byl právně relevantní souhlas zaměstnance s monitorováním pracoviště i mimo výjimku spočívající ve zvláštní povaze činnosti zaměstnavatele udělený např. v pracovní smlouvě a co by se stalo, pokud by tento souhlas vyslovili všichni zaměstnanci. Odpověď na otázku je jasná a zní nikoli. Základní lidská práva a tedy i právo na ochranu soukromí jsou konstruována jako nezcizitelná, což znamená, že jich jedinec nemůže být zbaven a to ani zákonem, ani se jich nelze vzdát projevem vůle jednotlivce nebo skupiny jednotlivců. Avšak i v případě, že by se zaměstnanec mohl svého práva vzdát, stále tu ještě existuje zákaz narušovat jeho soukromí vyplývající ze zákoníku práce. Kamery však nelze instalovat ani se souhlasem všech zaměstnanců, neboť jak vyplývá z § 2 odst. 1 zákoníku práce, odchýlení není možné od ustanovení ukládajících povinnost, leda že jde o odchýlení ve prospěch zaměstnance. Z toho plyne, že se v případě § 316 odst. 2 zákoníku práce jedná o kogentní ustanovení, které znamená pro zaměstnavatele jednoznačný zákaz. Ten tak nesmí své zaměstnance, vyjma závažného důvodu spočívajícího ve zvláštní povaze činnosti jím provozované, sledovat a jakékoliv jiné řešení spočívající v zapojení kamer by znamenalo obcházení zákona.

[52] Bártík, V., Janečková, E. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 2. vydání. Praha: Linde, 2009, s. 130.

9.3.1 Působnost zákona o ochraně osobních údajů

Pokud se zaměstnavatel rozhodne využít možnost instalovat kamerové systémy na pracovišti za podmínek § 316 odst. 2 zákoníku práce, vstupuje tímto do sféry působnosti zákona o ochraně osobních údajů. Je však nutné podotknout, že ne všechny kamerové systémy při své činnosti naplňují definiční znaky zpracování osobních údajů. V první řadě je nutné si uvědomit, že aby bylo možno hovořit o zpracování ve smyslu § 4 písm. e) zákona o ochraně osobních údajů, musí se jednat o činnost prováděnou systematicky, což znamená, že výstupy z kamerového systému musí být pravidelně zaznamenávány a k tomu musí být také kamerové zařízení technicky způsobilé. Provoz kamerového systému je tak zpracováním osobních údajů jen tehdy, pokud je vedle sledování určitého prostoru prováděn i záznam pořizovaných záběrů, nebo se tento záznam uchovává a to s konkrétním záměrem identifikovat fyzické osoby v souvislosti s určitým jednáním. Mimo tyto případy se bude jednat o nahodilou činnost zaměstnavatele, která pod režim zákona o ochraně osobních údajů nespadá. Tím ovšem není vyloučena aplikace jiných předpisů, zejména pak ustanovení občanského zákoníku upravující ochranu osobnosti.

Další otázkou je, zda je vůbec možno kamerový záznam považovat za osobní údaj či nikoli a v případě že ano, jakou má tento osobní údaj povahu. Dle ustanovení § 4 písm. a) zákona o ochraně osobních údajů je osobním údajem „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů*“, z čehož je nutno vycházet. Pokud je tedy na základě záznamu možno fyzickou osobu přímo nebo nepřímo identifikovat (např. v rámci určitého pracoviště) nebo je konkrétní osoba alespoň identifikovatelná, pokud jsou patrné její charakteristické rozpoznávací znaky (zejména obličej), lze záznam za osobní údaj považovat. V opačném případě můžeme prohlásit, že informace obsažená v záznamech z kamerových systémů „*nedosahuje kvality osobního údaje, neboť z pouhého obrazového záznamu fyzické osoby nelze tuto osobu bez použití dalších doprovodných údajů v záznamu neobsažených obecně ztotožnit*“[53]. Tímto tématem se ostatně zabýval i Městský soud v Praze, který posuzoval použití kamer v rámci hotelového komplexu, přičemž konstatoval, že „*záznam lidské podoby, respektive lidské tváře umožní jasně určit lidskou identitu na základě fyziologických*

[53] Bártík, V., Janečková, E. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 2. vydání. Praha: Linde, 2009, s. 134.

znaků, za tímto účelem se kamerový systém provozuje“ a dále dodává, že „*základním identifikačním znakem lidské bytosti je její vzhled*“[54]. Zjednodušeně řečeno, pokud lze zaměstnance nebo jinou fyzickou osobu na základě záznamu tváře identifikovat a to jak okamžitě po pořízení nahrávky tak i s odstupem času, jedná se o osobní údaje. Je logické se domnívat, že pokud by zaměstnavatel již dopředu vyloučil možnost, že bude někdo s použitím kamer identifikován, systém a jeho instalace by postrádal jakýkoli smysl.

Jestliže dospějeme na základě výše uvedeného k závěru, že zaměstnavatel s použitím kamerového systému na pracovišti skutečně zpracovává osobní údaje svých zaměstnanců, musíme z toho vyvodit patřičné důsledky. Tím nejpodstatnějším z našeho pohledu je fakt, že se takto zaměstnavatel dostává do pozice správce osobních údajů a má z toho plynoucí povinnosti, které mu zákon o ochraně osobních údajů ukládá. Je třeba se registrovat jako správce u ÚOOÚ, nejde-li o uplatnění některé z výjimek z oznamovací povinnosti a je také zapotřebí stanovit účel instalace kamerového systému, který bude korespondovat s důležitými a právem chráněnými zájmy správce (např. bude účelem ochrana majetku zaměstnavatele). Záznamy pak mohou sloužit pouze k takto vymezenému účelu. Dále je nutné, aby zaměstnavatel určil přiměřenou lhůtu, po kterou budou záznamy z kamerového systému uchovávány (jako hraniční se jeví doba v řádu dní[55]) a zajistil ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním. Zaměstnanci nebo i jiné osoby pohybující se v monitorovaných prostorách musí být též náležitě informovány (například nápisem na zdi nebo interním aktem zaměstnavatele) o tom, že je prostor, ve kterém se nachází, střežen kamerovým systémem. Tato povinnost vyplývá jak z ustanovení § 11 odst. 5 zákona o ochraně osobních údajů, tak ji zaměstnavateli ukládá i § 316 odst. 3 zákoníku práce. Pokud jde o souhlas subjektů údajů, není v případě použití kamerového systému zaměstnavatelem zapotřebí. Předmětné zpracování je možné realizovat za podmínek § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, který stanoví, že bez souhlasu subjektu údajů lze údaje zpracovávat „*pokud je to nezbytné pro ochranu práv a právem chráněných zájmů*

[54] Viz rozsudek Městského soudu v Praze sp. zn. 11 Ca 433/2008.

[55] Viz stanovisko ÚOOÚ č. 1/2006.

správce, příjemce nebo jiné dotčené osoby“ a ochrana majetku zaměstnavatele je jistě jedním z takových právem chráněných zájmů.

Pokud chce zaměstnavatel v prostoru pracoviště nainstalovat a provozovat kamerový systém obsahující rovněž i záznamové zařízení schopné nahrávat pořízené záběry, musí si uvědomit, že i když dodrží zákony stanovené podmínky, neměl by soukromí zaměstnanců omezovat nepřiměřeně. Ostatně existence pracovního poměru neznamená, že fyzická osoba bude naprosto oproštěna od svého osobního života, k čemuž dospěl i Evropský soud pro lidská práva. V rozsudku ve věci Niemietz v. Německo soud judikoval, že na základě výkladu čl. 8 Úmluvy o lidských právech a svobodách musí respektování soukromého života zahrnovat i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi. Dále soud uvedl, že neexistuje důvod, proč by měl způsob chápání pojmu „soukromý život“ vylučovat aktivity v rámci zaměstnání, protože i během pracovní činnosti má většina lidí příležitost rozvíjet vztahy s vnějším světem. Z toho důvodu by měl zaměstnavatel dbát na to, aby svým zaměstnancům zaručil dostatečnou míru soukromí v určitém prostoru, zejména na toaletách, v šatnách apod. Důležité je si uvědomit, že kamera sama o sobě nedokáže zabránit krádežím, stejně jako pomůže odhalit konzumaci alkoholu nebo drog na pracovišti jen v prostoru, který bezprostředně pokrývá její zorné pole. Dopad kamer na psychiku některých zaměstnanců stejně, jako na jejich pracovní výkonnost může být naopak negativní. Bude-li zaměstnanec pod stálým tlakem s vědomím, že je neustále kontrolován, nejspíš bude ve stresu a méně uvolněný. Proto by měla být instalace kamer na pracovišti prováděna s rozmyslem a mělo k tomu dojít na základě jistého konsenzu mezi zaměstnavatelem a zástupci zaměstnanců, který by zaručil, že jednotliví pracovníci mohou vyjádřit případné námitky k tomuto kroku.

9.4 Sledování elektronické pošty zaměstnavatelem

Jedné se o další žhavé téma, o kterém se v souvislosti s osobními údaji a ochranou soukromí v poslední době vede debata mezi laiky i odborníky, ale jednoznačného závěru zatím nebylo dosaženo. Současně se otázce sledování zaměstnaneckých internetových aktivit zaměstnavatelem naše legislativa věnuje jen poskrovnu, což jistě nepomáhá snadné aplikaci zákona a pochopení mantinelů, které platná právní úprava stanoví. Argumentem hovořícím ve prospěch zaměstnavatele a

práva monitorovat elektronickou poštu zaměstnanců bude především kontrola dodržování pracovní doby a její řádné využívání k plnění pracovních úkolů. Mimo to se ovšem monitorování elektronické pošty zaměřuje také na ochranu zaměstnanců před různými formami obtěžování, ochranu obchodního tajemství, ochranu před nedovoleným kopírováním dat, nebo lze tímto způsobem získat přístup k firemním informacím, je-li příslušný zaměstnanec např. na dovolené. Argumentem proti zavádění takovýchto kontrolních mechanismů zaměstnavatelem je pak požadavek, aby zaměstnavatel důsledně respektoval právo zaměstnanců na ochranu jejich soukromí a projevů osobní povahy, včetně ochrany korespondence a osobních údajů. Oba tyto názory jsou odůvodnitelné a jejich základ je třeba hledat napříč platnou legislativou v čele s ústavními předpisy.

Hovoříme-li o elektronické poště, kterou zaměstnanec obdrží do schránky počítače, který mu je svěřen k výkonu práce, považujeme takovou zprávu za písemnost, jako kteroukoli jinou. Přesto, že se ochrana listovního tajemství vztahuje zejména na písemnosti na hmotném nosiči informací jako je papír apod., je s ohledem na vývoj ve světě elektronických komunikací nutno zákony aplikovat přiměřeně aktuálním potřebám. Vycházet je potřeba především z čl. 13 Listiny, který stanoví, že „*nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením*“. Ústavní zásadu ochrany listovního tajemství dále rozpracovává jednak občanský zákoník, a to konkrétně § 12, kde je uvedeno, že písemnosti osobní povahy smějí být pořízeny nebo použity pouze se svolením fyzické osoby, jíž se týkají a dále i trestní zákoník, který v dílu 2 zvláštní části nazvaném Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství obsahuje v § 182 skutkovou podstatu trestného činu porušení tajemství dopravovaných zpráv. Z výše uvedeného tak lze usuzovat na značnou váhu, kterou Listina i ostatní právní předpisy ochraně listovního tajemství jako jednomu ze základních lidských práv přikládají. Na základě toho lze také s určitostí prohlásit, že povinnost respektovat takto ústavně formulované právo mají všichni, zaměstnavatele nevyjímaje. Pokud by se zaměstnavatel snažil argumentovat tím, že e-mail doručený na pracovní počítač již nemá charakter ryze soukromé zprávy, lze ho

odkázat na Směrnici Evropského parlamentu a Rady z roku 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Ta v bodu č. 24 úvodní části stanoví, že „*koncové zařízení uživatelů sítí elektronických komunikací a jakékoli informace uchovávané na takovém zařízení tvoří součást soukromí uživatelů, které vyžaduje ochranu v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod*“, kdy koncovým zařízením v našem případě bude počítačová stanice, na kterou elektronická pošta dochází.

S ohledem na to, že ani pracovněprávní vztah neodstraňuje právo na přiměřené soukromí zaměstnanců, jak již bylo v předešlé kapitole uvedeno, musí to zaměstnavatel respektovat a to i v případě, že se rozhodne využít svého práva a sledovat u svých zaměstnanců dodržování pracovní doby a jejího využití. Jak vyplývá ze stanoviska ÚOOÚ č. 2/2009, zaměstnavatel nemá právo monitorovat a dále zpracovávat obsah korespondence svých zaměstnanců. Dle názoru ÚOOÚ má zaměstnavatel možnost pouze sledovat počet e-mailů došlých a odeslaných z počítače zaměstnance a případně, považuje-li to za nutné z hlavičky e-mailu, zjistit, komu píší a od koho zprávy dostávají. Současně má zaměstnavatel také právo požadovat, aby si své soukromé záležitosti v pracovní době a na pracovišti vyřizovali pracovníci jen v nezbytné míře. Pro aplikaci zákona o ochraně osobních údajů bude přitom nutné, aby sledování elektronické pošty naplňovalo definiční znaky zpracování a s údaji takto získanými bylo dále manipulováno za určitým účelem. Nahodilé „prověrky“ e-mailů by zřejmě nebyly zpracováním, i když to neznamená, že by nepřiměřená manipulace se zprávami určenými zaměstnancům nemohla být považována za porušení listovního tajemství a osobnostního práva a za neoprávněný zásah do soukromí.

Situace je dnes taková, že u některých zaměstnavatelů panuje přesvědčení, že by z titulu svého postavení vůči zaměstnancům mohli kontrolovat kompletní elektronickou korespondenci a to jak pracovního tak i soukromého rázu. Je to dle mého názoru snaha o aplikaci rčení „můj dům, můj hrad“ na pracovněprávní vztahy, kdy se zaměstnavatelé považují za jakési panovníky a vše je jim v zájmu zajištění ochrany majetku a zajištění větší efektivity práce zaměstnanců - svých poddaných dovoleno. Osobně nemám pocit, že by kontrola soukromé korespondence zaměstnanců byla lékem na nízkou produktivitu práce a zřejmě bude pouze jedním ze způsobů, jak jí docílit. Pokud tedy zaměstnavatel chce zavést na pracovišti monitoring elektronické pošty a nechce

současně zasahovat v míře nepřiměřené do soukromí svých zaměstnanců, lze mu nabídnout následující řešení. Dle Jána Matějky z Ústavu státu a práva může zaměstnavatel kontrolovat elektronickou poštu svých zaměstnanců a dále s ní nakládat jen v těch případech, „*kdy lze důvodně předpokládat, že obsah zprávy je firemní*“. Jako vodítko pro určení o jakou poštu se jedná, pak Matějka využívá analogicky znění vyhlášky ministerstva dopravy a spojů č. 28/2001 Sb., která v § 5 odst. 7 stanoví, že „*je-li v adrese uvedena na prvém místě právnická osoba a na druhém místě fyzická osoba, za adresáta se považuje právnická osoba. Je-li v adrese uvedeno na prvém místě jméno a příjmení fyzické osoby, za adresáta se považuje fyzická osoba*“. Aplikace této vyhlášky je však pro tyto účely problematická, jelikož konstrukce e-mailové adresy vykazuje určitá specifika a od běžné doručovací adresy se tak v mnohém liší. Je ale možno říci, že pokud obsahuje e-mailová adresa označení zaměstnavatele (např. petr.novak@zaměstnavatel.cz), lze ji dle mého názoru důvodně považovat za firemní a jako takovou ji lze i namátkově kontrolovat. Na druhé straně se dá ale zároveň očekávat, že zaměstnanci budou firemní e-maily využívat také pro své soukromé účely, stejně jako je tomu u firemních telefonů. Z toho také vyplývá, že přímé zákazy využívání firemních adres elektronické pošty nejsou řešením a na místě bude zejména snaha zaměstnavatelů o rozumný kompromis. Především je zapotřebí zaměstnance o krocích směřujících ke kontrole elektronické pošty informovat a pokud možno tento postup zakotvit v interním aktu zaměstnavatele nebo s ním budoucí zaměstnance seznámit již v pracovní smlouvě. Budou-li zaměstnanci předem vědět, že firemní pošta může podléhat kontrole ze strany zaměstnavatele, jistě si rozmyslí, zda ji využijí také pro ryze soukromé účely a v případě, že tak i přes to učiní, budou podstupovat dobrovolné riziko.

Je možné, že se v blízké budoucnosti vytvoří pravidla pro kontrolu elektronické pošty zaměstnanců, která budou aplikovatelná obecně v rámci celých společností a pro tyto společnosti budou zároveň závazná. Přístup zaměstnavatelů by měl vycházet z toho, že se o určitý zásah do soukromí jedná a měl by tedy být především přiměřený a odpovídající rizikům. Zde se přitom nachází velká příležitost pro ÚOOÚ, aby k této problematice jako regulátor stanovoval podrobnější pravidla, která by byla vodítkem pro zaměstnavatele a pro systematickou rozhodovací činnost ÚOOÚ. Osobně se pak domnívám, že obsah elektronické pošty by neměl být soustavně monitorován bez

ohledu na její charakter. Namátkové kontroly by měly být směřovány výhradně na korespondenci firemní v případech, kdy vznikne podezření ze zneužití pracovních prostředků, resp. jejich využití k jiným než pracovním účelům. Dále by kontrola e-mailové korespondence připadala v úvahu v situacích, kdy tak zaměstnavatel učiní v zájmu ochrany svých práv a na základě důvodné obavy, že tato práva mohou být ohrožena.

10 Důsledky porušení povinností při zpracování osobních údajů

Ačkoliv je úprava ochrany osobních údajů zaměřena především na prevenci, kdy je primárním cílem zajistit, aby subjekt údajů neutrpěl na svých právech, obsahuje zákon o ochraně osobních údajů i další související postupy vedoucí k odstranění nežádoucího jednání a jeho důsledků. V úvahu tak připadají tři základní typy opatření (nápravná, sankční a satisfakční), z nichž poslední jmenované bylo podrobněji rozebráno v kapitole 7.2 týkající se možnosti subjektu údajů domáhat se ochrany svých práv. Jen připomenu, že pokud se subjekt údajů domnívá, že byla jeho práva poškozena, může se obrátit na správce nebo zpracovatele se žádostí o vysvětlení nebo je požádat, aby odstranili závadný stav. V případě vzniku škody v důsledku porušení povinností při zpracování osobních údajů má pak subjekt údajů možnost domáhat se svých nároků dle obecné úpravy náhrady škody obsažené v občanském zákoníku nebo, v záležitostech způsobení jiné než majetkové újmy, využít občanskoprávní úpravu ochrany osobnosti.

10.1 Kontrolní činnost ÚOOÚ

Mimo oprávnění daná zákonem fyzickým osobám má nepochybně v případě porušení povinností při manipulaci s osobními údaji podstatnou úlohu výkon dozorové činnosti Úřadu pro ochranu osobních údajů. Tu vykonává ÚOOÚ s použitím zákona č. 552/1991 Sb., o státní kontrole ve znění pozdějších předpisů a v tomto předpise obsažená pravidla jsou doplněna speciálními ustanoveními v zákoně o ochraně osobních údajů.

Kontrolu lze iniciovat mimo jiné na základě stížnosti nebo podnětu, přičemž mezi těmito instituty nelze najít podstatnější rozdíl a to zejména co se účinků jejich podání týče. Z literatury je možno pouze vyvodit, že stížnost by mohla být ve srovnání s podnětem formulována více konkrétně, kdežto podnět by mohl obsahovat i obecnější nástin řešení nevyhovující situace. Zákon o ochraně osobních údajů se o podnětu a stížnosti zmiňuje zejména v ustanovení § 31, kde je uvedeno, že „*kontrolní činnost Úřadu se provádí na základě kontrolního plánu nebo na základě podnětů a stížností*“ a také v § 29 odst. 1 písm. c), který říká, že ÚOOÚ „*přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení*“. Jak již bylo také v této práci uvedeno, může se subjekt údajů rovněž

obrátit na ÚOOÚ s žádostí, aby byl odstraněn závadný stav, pokud se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů v rozporu s ochranou soukromého a osobního života nebo v rozporu se zákonem, jak stanoví § 21 odst. 3 zákona o ochraně osobních údajů. Jedná-li se o okruh oprávněných subjektů k podání stížnosti nebo podnětu, jsou jimi kromě osob, jichž se zásah do soukromí přímo týká i další subjekty, které mají na nápravě závadného stavu zájem (např. občané cizího státu nebo novináři píšící o porušení zákona o ochraně osobních údajů). V souladu s tím by se mělo přihlížet i k anonymním podáním, ze kterých však musí být zřejmé, o jakou věc se jedná, protože žádost o jejich následné doplnění ze strany ÚOOÚ by logicky postrádala smysl. Stěžovatel může podání realizovat jak v běžné tak i v elektronické podobě a nemusí přitom splnit jakékoli formální náležitosti. Z důvodu dalšího postupu je ovšem žádoucí, aby bylo podání učiněno písemně. Z hlediska obsahu podání jsou pak klíčovými zejména jednoznačné určení subjektu, proti němuž směřuje, popsání toho, v čem je spatřováno porušení zákona o ochraně osobních údajů a připojení patřičných důkazů.

Oproti předchozímu znění zákona o ochraně osobních údajů je v současnosti možné, aby se stížnost netýkala primárně pouze zákona o ochraně osobních údajů, což lze dovodit z § 29 odst. 1, kdy je stanoveno, že dozorová pravomoc ÚOOÚ se vztahuje na „*dodržováním povinností stanovených zákonem při zpracování osobních údajů*“. Stížnosti tak mohou poukazovat na zpracování osobních údajů upravených i jinými zákony, které jsou vůči zákonu o ochraně osobních údajů zvláštní právní úpravou.

Důvody stížností jsou různé, ale v zásadě kopírují jednotlivé povinnosti, které má správce a zpracovatel při zpracování osobních údajů. Bude se jednat zejména o podání týkající se nejasně stanoveného účelu a rozsahu zpracování, s čímž souvisí i stížnosti směřující proti nadměrnému shromažďování osobních údajů bez stanovení odpovídajícího časového rámce předmětného zpracování. Dalším typem stížností jsou takové, které ukazují na užití osobních údajů pro jiné než původně stanovené účely a dále ty, jež napadají nedostatečné zabezpečení osobních údajů včetně nejrůznějších technických vad a komplikací. Konečně lze napadnout přesnost zpracovávaných údajů, chybějící informace o zpracování, formální nedostatky procesu zpracování (např. chybějící smlouva mezi správcem a zpracovatelem) a také vady poskytovaného souhlasu se zpracováním osobních údajů, kdy vadou nejzávažnější je jeho vynucení pod

určitou pohrůžkou. Je ovšem podstatné si uvědomit, že s podáním konkrétní stížnosti nejsou automaticky spojeny účinky zahájení správního řízení a ÚOOÚ není v žádném případě příslušným podáním vázán, z čehož plyne i to, že stěžovatel nemá postavení účastníka. Úřad má ale povinnost osobu podatele vyrozumět, jak s doručeným podáním naložil a rovněž musí zvážit, zda není dán v konkrétním případě důvod pro postoupení věci orgánům činným v trestním řízení, případně orgánům jiným. Současně je také nutno zmínit, že ÚOOÚ není v žádném případě oprávněn rozhodovat konkrétní spory o nároky stěžovatele, které nemají charakter nápravných opatření a směřují např. k vyslovení povinnosti zaplatit peněžitou náhradu. K tomuto závěru přispívá i ustanovení § 2 odst. 2 zákona o ochraně osobních údajů, které říká, že Úřadu pro ochranu osobních údajů jsou svěřeny kompetence v oblasti ochrany osobních údajů právě jen v rozsahu stanoveném tímto zákonem a dalšími relevantními předpisy.

Vlastní průběh kontroly zahájené ať již na základě stížnosti nebo z iniciativy ÚOOÚ je v zásadě v obou případech stejný. Kontroloři mohou vstupovat do příslušných objektů, požadovat potřebné dokumenty a informace, přičemž jsou povinni zachovávat mlčenlivost. Na závěr kontroly je vyhotoven protokol, který může mimo jiné obsahovat i uložení nápravných opatření, kterými dle konkrétních okolností mohou být: 1) likvidace osobních údajů, 2) upřesnění účelu zpracování osobních údajů, 3) upravení klauzule, jíž je dán subjektem údajů souhlas se zpracováním, 4) zastavení procesu předávání nebo zpřístupňování určitých údajů, jinými slovy jistý druh blokace, 5) uložení povinnosti poskytnout informace o zpracování, 6) uložení povinnosti osobní údaje aktualizovat a 7) přijetí dostatečných opatření k zabezpečení osobních údajů. Samotné nápravné opatření pak není sankcí. Jeho základním účelem je totiž pouze náprava závadného stavu a jeho opětovné navrácení do souladu s právními předpisy.

10.2 Sankce

Správní trestání v podobě uložení sankcí za porušení zákonných povinností nastupuje jako sekundární fáze prováděné dozorové činnosti a není vždy fází obligatorní. Navazuje na stádium prověřování a hodnocení zjištěných nedostatků a k jejímu uplatnění dochází pouze tam, kde „*je možno doložit nesoulad mezi skutečným stavem a právními normami požadovaným chováním kontrolovaného*“[56]. V zákoně o

[56] Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, s. 185.

ochraně osobních údajů jsou problematice sankcí věnovány §§ 44 až 46, kdy je dle těchto ustanovení možno sankcionovat přestupky až do výše 5 milionů Kč a jiné správní delikty až do výše 10 milionů Kč.

Přestupkem, za který lze potrestat fyzickou podnikající i nepodnikající osobu, která není v postavení správce nebo zpracovatele, je dle zákona o ochraně osobních údajů pouze porušení povinnosti mlčenlivosti. Tohoto přestupku se může dle § 44 odst. 1 zákona o ochraně osobních údajů dopustit fyzická osoba, která: „*a) je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru, b) vykonává pro správce nebo zpracovatele činnosti na základě dohody, nebo c) v rámci plnění zvláštním zákonem uložených oprávnění a povinností přichází u správce nebo zpracovatele do styku s osobními údaji*“. Ve výše uvedených případech je následkem takovéhoto jednání pokuta do výše 100 000 Kč, u nepodnikatelů v pozici správců a zpracovatelů je možno postihnout více typů jednání a jako trest v takovém případě připadá v úvahu pokuta až do výše 5 000 000 Kč. Za jiné správní delikty právnických a podnikajících fyzických osob v roli správců či zpracovatelů může ÚOOÚ udělit pokutu ve výši až 10 000 000 Kč. Zákon sám přitom mimo výčet jednotlivých sankčních opatření obsahuje i liberační ustanovení v § 46 odst. 1, podle kterého se právnická osoba zprostí odpovědnosti za správní delikt v případě, kdy prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. Při rozhodování o výši pokuty bude rozhodujícím měřítkem zejména závažnost, způsob, doba trvání a také následky protiprávního jednání a zvažovány budou rovněž i konkrétní okolnosti, za nichž bylo protiprávní jednání spácháno. V okamžiku, kdy protiprávní jednání dosáhne intenzity trestného činu, je pak sankční řízení vedené v prvním stupni Úřadem pro ochranu osobních údajů konzumováno případným řízením trestním.

Závěr

Cílem této práce byla analýza právní úpravy ochrany osobních údajů v pracovněprávních vztazích v České republice a snaha o jednotný pohled na tuto problematiku. I když byla práce zaměřena především na rozbor ustanovení zákona o ochraně osobních údajů, nebyly opomenuty ani klíčové předpisy pracovního práva, jako je zákon o zaměstnanosti či zákoník práce, přestože se platné znění těchto předpisů věnuje tématu ochraně osobnosti zaměstnanců a s tím i právnímu postavení zaměstnavatele jen okrajově, což je dle mého názoru škoda. O to více by měla být věnována pozornost aplikaci a výkladu zákona o ochraně osobních údajů jakožto i činnosti Úřadu pro ochranu osobních údajů, který k této problematice rovněž vyvíjí svou rozhodovací činnost jako hlavní orgán dozoru.

Z rozboru legislativních opatření směřujících k ochraně osobních údajů stejně jako i ze studia odborné literatury a dostupných zdrojů zabývajících se tímto tématem se domnívám, že by měla být věnována větší pozornost prevenci. Je sice pravdou, že zákon o ochraně osobních údajů ve svých ustanoveních klade na subjekty zpracovávající osobní údaje požadavky, které mají za cíl působit na samotný proces zpracování preventivně, a které vyjadřují záměr zákonodárce co nejvíce ochránit subjekt údajů před neoprávněným zásahem do jeho práv, ale pouze zákon mnohdy nestačí. Ačkoli je ochrana poskytována platným právem a důslednou aplikací základních zásad ochrany osobních údajů vyjádřených i v řadě evropských právních předpisů, na prvním místě, je nutné si uvědomit, že bez patřičné osvěty v podobě informovanosti veřejnosti nemá právní zakotvení práv a povinností takový účinek. Jak bylo v předešlých kapitolách popsáno, nemá běžný občan v zásadě právní povědomí o pravidlech, která musí dodržovat, a totéž platí i pro jeho práva vyplývající z ustanovení chránících jeho soukromí. Je jistě každému z nás jasné, že by nikdo neměl číst bez svolení naši osobní korespondenci nebo odposlouchávat soukromé telefonní hovory. To ovšem neznamená, že by současně každý dbal více na to, zda vlastním nevynuceným chováním neohrožuje svoje soukromí a neposkytuje zbytečně až příliš mnoho informací týkajících se jeho osobního života. Stejně tak zaměstnavatelé mohou podrobným studiem zákona dostát svých povinností. V běžném životě ovšem často není tak snadné zkombinovat přesné dodržení právních předpisů s reálnými ekonomickými potřebami. K tomu je totiž třeba nejen znalost platné legislativy, ale i řada jiných informací, které lze načerpat např. z

odborné literatury, veřejně přístupných zdrojů nebo i z činnosti vyvíjené zástupci médií. Pokud tedy hovořím o prevenci, myslím tím alespoň základní znalost právní úpravy ochrany osobních údajů dosaženou např. v rámci studia a k tomu, a to zejména u subjektů majících ze zákona především povinnosti (v našem případě jsou jimi zaměstnavatelé), i další vzdělávání v příslušné problematice např. častějšími konzultacemi s regulátorem v oblasti ochrany osobních údajů, kterým je u nás ÚOOÚ.

Z hlediska možných rizik ohrožení osobních údajů jsou z mého pohledu pracovněprávní vztahy méně exponovanou oblastí. Osobně se nedomnívám, že by bylo v zájmu zaměstnavatele přímo zneužívat osobní údaje svých zaměstnanců. V tomto směru je daleko ohroženější oblastí kupříkladu poskytování obchodních služeb nebo obecně poskytování informací klienty některých společností. Na druhou stranu je možno na základě této práce určit oblasti, které mohou z hlediska ochrany osobních údajů v pracovněprávních vztazích způsobovat problémy, a na které je třeba upozornit.

V kapitole třetí, které je věnována výkladu základních pojmů, je uvedeno, že osobní údaj lze charakterizovat jako jakoukoli informaci týkající se určeného nebo určitelného subjektu údajů. Právě tato základní definice obsažená v § 4 písm. a) zákona o ochraně osobních údajů je z pohledu jejího výkladu často obtížně pochopitelná. Myslím tím především interpretaci pojmu „určitelný“, kdy není na první pohled úplně zřejmé, kdy je ještě možno danou osobu považovat na základě jejích osobních údajů za skutečně určitelnou a kdy nikoli. Dle mého názoru není příliš vhodné, aby se nad míru rozšiřoval okruh případů, kdy jsou za osobní údaje považovány takové informace, které osoby identifikují pouze nepřímo a je k tomu navíc zapotřebí značného úsilí. Ztotožňuji se proto s názorem Richarda Otevřela, který na serveru jinepravo.blogspot.com rovněž poukazuje na praktickou nemožnost jasně pojem určitelnosti specifikovat. Přitom se jako možné řešení nabízí, s odkazem na stanovisko Pracovní skupiny WP 29 č. 4/2007, využití ceny (nákladů na identifikaci), jako měřítka pro určení, zda je pokus o identifikaci osoby ještě rozumný.

Z hlediska povinností, které dle zákona o ochraně osobních údajů dopadají na zaměstnavatele jako na správce osobních údajů, bych zdůraznil povinnost přijmout vhodná bezpečnostní opatření a také povinnost informační. V případě zabezpečení osobních údajů nejde jen o vhodný výběr technického vybavení, ale je také nutné zajistit, aby nedocházelo k neoprávněnému nebo nahodilému přístupu k osobním

údajům z důvodu selhání lidského faktoru, nebo aby byla tato možnost alespoň omezena na minimum. I když totiž zaměstnavatel dodrží důsledně všechny povinnosti, nelze s jistotou vyloučit, že se některý z jeho zaměstnanců bude chovat obdobně. Jak vyplývá z rozhodovací činnosti ÚOOÚ, lze se v praxi setkat s často velice laxním přístupem zaměstnavatelů k tomuto problému a to přesto, že v případě pochybení u jeho zaměstnanců odpovídá ze zákona za porušení povinností týkajících se ochrany osobních údajů právě zaměstnavatel. Zvýšená pozornost by pak měla být zejména věnována otázce náležité likvidaci nepotřebných osobních údajů. Jak bylo v této práci několikrát zmíněno, je nejlepší cestou, jak lze těmto komplikacím předcházet, vystavět ucelený systém vnitřních předpisů (např. provozní řády apod.). Ty mohou umožnit lepší vymahatelnost povinností, které jsou zaměstnancům na základě těchto předpisů uloženy a současně zaručí i jejich dostatečnou informovanost ohledně zpracování jejich osobních údajů. Poučení o tom, zda jsou zaměstnanci vůbec povinni své osobní údaje poskytovat a pokud ano, jaká jsou jejich práva v souvislosti s procesem zpracování takto nashromážděných údajů, je informací základní a subjektu údajů by nemělo být rozhodně odpíráno. Přitom je nutné, aby byly informace v jasné a srozumitelné formě zaměstnancům poskytnuty na počátku procesu zpracování, případně aby byly doplňovány i v jeho průběhu. Není potřeba se více pozastavovat nad tím, že jsou-li poskytované informace spojeny se souhlasem ke zpracování osobních údajů, musí být tento souhlas nevynucený a svobodný.

Co se týče nejvíce diskutovaných oblastí v souvislosti s problematikou ochrany osobních údajů v pracovněprávních vztazích, lze odkázat na kapitolu devátou této práce. Na tomto místě se však pokusím tyto problémy stručně zrekapitulovat a navrhnout jejich možná řešení. Pokud se bavíme o osobních údajích sdělovaných a zpracovávaných před vznikem pracovního poměru, je současná legislativa poměrně strohá. Úprava je obsažena v §§ 30 a 316 zákoníku práce spolu s § 12 zákona o zaměstnanosti. Tato úprava je sama o sobě relativně jasná, ale ucelenější popis osobních údajů a informací, které zaměstnavatel může či nemůže po uchazečích o zaměstnání vyžadovat, by dle mého názoru nebyl od věci. Pouhé konstatování, že sdělovány by měly být obecně jen údaje bezprostředně související s výkonem práce, je s ohledem na různorodost a specifika určitých povolání dosti strohé. Zohledněny by tak měly být více potřeby zaměstnavatele při výběru budoucích pracovníků. Na druhou stranu by měl

zaměstnavatel postupovat více než obezřetně a vyžadovat po uchazečích o zaměstnání skutečně jen ty informace, které jsou pro něj rozhodující. Jako vhodné řešení by mohly posloužit např. předtištěné formuláře, které by byly uchazeči poskytnuty při vstupním pohovoru a obsahovaly by pouze klíčové údaje. Takto by se zároveň i eliminovala možnost, aby sám uchazeč sděloval osobní údaje, které postrádají pro zaměstnavatele jakékoliv praktické využití.

V práci byla nastíněna také otázka využití metody Preemployment Background Screeningu v České republice. Jak již bylo výše konstatováno, naše právní předpisy s touto metodou přímo nepočítají, ale současně zákoník práce, zákon o zaměstnanosti a zákon o ochraně osobních údajů obsahují vodítka, s jejichž pomocí je metodu PEBS možno praktikovat i v našich podmínkách. Není proto dle mého názoru třeba přijmout právní úpravu novou. Je ale nutno doporučit těm zaměstnavatelům, kteří se s pomocí metody PEBS rozhodnou prověřit minulost budoucích nebo stávajících zaměstnanců, aby svůj postup raději předem konzultovali s odborníky na toto téma, nebo se obrátili přímo na ÚOOÚ. V případě, kdy v rámci PEBS dochází dle zákona o ochraně osobních údajů k jejich zpracování, musí totiž zaměstnavatel dodržet všechny povinnosti, které mu zákon ukládá, což nemusí být vždy snadno realizovatelné.

Posledními a z mého pohledu problematickými oblastmi, které v závěru krátce připomenu, jsou využití kamerových systémů na pracovišti a sledování elektronické pošty zaměstnanců. U nasazení kamer se zdá být jasné znění § 316 zákoníku práce, který v odstavci 2 zakazuje nepřiměřené zasahování do soukromí zaměstnanců. Komplikace ovšem mohou nastat v okamžiku, kdy je třeba správně interpretovat výjimku z tohoto zákazu obsaženou v § 316 odst. 3 zákoníku práce. Není totiž zcela jasné, co mínil zákonodárce spojením "zvláštní povaha činnosti zaměstnavatele". Zákon sám tak umožňuje neurčitý výklad, což nevede z mého pohledu k dosažení přiměřeného stupně právní jistoty. Jedná-li se o případy, kdy zaměstnavatel smí kontrolovat e-maily svých zaměstnanců, je situace ještě nejasnější a osobně bych přivítal intervenci ze strany ÚOOÚ. Úřad pro ochranu osobních údajů v rámci své činnosti vydává stanoviska a rozhodnutí, která jsou vhodným interpretačním vodítkem k platné legislativě, ovšem řada těchto jeho vyjádření je přímo odvislá od konkrétních stížností a podnětů reagujících na porušení zákona. Tím vznikají prázdná místa všude tam, kde dosud ÚOOÚ nemusel zasahovat a v některých oblastech, jako je právě kamerové sledování

nebo kontrola elektronické pošty zaměstnanců dosud logicky dostatečně jasné a přesvědčivé názory chybí. S ohledem na množství diskuzí na toto téma lze usuzovat, že by pružnější reakce ze strany ÚOOÚ, která by odrážela vývoj technických prostředků a hlavně ekonomickou realitu dneška, nebyla od věci.

Je více než zřejmé, že u pracovněprávních vztahů nestačí pouze důsledně aplikovat zákony mající za cíl chránit osobní informace zaměstnanců. Je současně třeba přijmou i řadu jiných opatření samotnými zaměstnavateli, bez nichž by bylo prosazování principů ochrany osobních údajů v pracovněprávních vztazích oslabeno. Považuji také za vhodné, aby byl mezi zaměstnavateli a zaměstnanci veden průběžný dialog na toto téma a panovala vzájemná snaha o nastolení konsenzu, který by vedl k udržení dobrých pracovních podmínek a zajistil by také zachování práv subjektů na obou stranách.

Na úplný závěr mohu prohlásit, že neshledávám současnou situaci z hlediska ochrany osobních údajů v pracovněprávních vztazích za špatnou. Úroveň ochrany garantovaná platnými právními předpisy je v České republice dostačující, což ovšem neznamená, že ji shledávám bezchybnou. V některých případech je míra ochrany ve prospěch subjektu údajů z mého pohledu dokonce vyšší, než bych považoval za vhodné. Jde ale především o oblast dosud ne tolik prozkoumanou a řada konkrétních řešení bude jistě otázkou budoucí praxe a zejména, a v to pevně doufám, další a ještě intenzivnější osvětové a interpretační činnosti Úřadu pro ochranu osobních údajů.

Abstrakt

Ochrana osobních údajů v pracovněprávních vztazích je téma v České republice aktuální. Jako jedno ze základních lidských práv, je právo na ochranu soukromí jednotlivce a s tím i spojená ochrana osobních údajů garantována ústavními předpisy a dále je pak rozvedena v několika zákonech a předpisech nižší právní síly.

Úkol, jehož splnění si tato práce klade za svůj cíl, je především podrobná analýza platné právní úpravy v České republice i předpisů Evropské unie, které problematiku ochrany osobních údajů postihují. Zároveň práce obsahuje i nástin konkrétních problémů, které se v souvislosti s ochranou osobních údajů v pracovněprávních vztazích vyskytují, a předkládá jejich možná řešení.

Text práce je členěn do celkem 10 kapitol a podkapitol, které se zabývají jednotlivými aspekty daného tématu a podrobněji je rozvádějí. V prvních dvou kapitolách je nastíněna právní úprava ochrany soukromí a ochrany osobních údajů u nás i v rámci předpisů Evropské unie.

Třetí a čtvrtá kapitola se věnuje výkladu a definici základních pojmů, kterými jsou „osobní údaj“ a „zpracování“ osobních údajů. V jednotlivých podkapitolách je pak stručně popsán obsah těchto pojmů a uvedeny příklady jejich možného výkladu.

Kapitola pátá je věnována subjektům, jichž se osobní údaje týkají a také těm, které se podílejí na jejich zpracování. Pokud se jedná o pracovněprávní vztahy, bude se výklad týkat především zaměstnavatelů a jejich zaměstnanců.

Následující část, tedy kapitola šestá, pojednává o jednotlivých povinnostech zaměstnavatele, které doprovázejí proces zpracování osobních údajů jeho zaměstnanců při jeho zahájení, průběhu a následně i ukončení.

Sedmá kapitola pak uvádí v návaznosti na kapitolu předešlou výčet práv, která mají zaměstnanci v případě zpracování jejich osobních údajů stejně jako i v případě, kdy je porušením povinností ze strany jejich zaměstnavatele nebo i jiných subjektů neoprávněně zasaženo do jejich soukromého a osobního života.

Kapitola osmá rozvádí podrobněji téma předávání osobních údajů do zahraničí. Jsou zde uvedeny jak podmínky samotného procesu předávání, tak i instituty, které ho ulehčují.

V předposlední části nazvané Praktické problémy je věnována pozornost oblastem pracovněprávních vztahů, kde je s osobními údaji nejvíce manipulováno a

s tím souvisí i možnost jejich zneužití nebo jiného zásahu do práv jejich nositele – zaměstnance.

Poslední desátá kapitola, která předchází samotnému závěru, popisuje důsledky porušení povinností plynoucích z předpisů týkajících se ochrany osobních údajů a uvádí i sankce, které za tato porušení přicházejí v úvahu.

Závěrem je konstatováno, že z hlediska právní garance ochrany osobních údajů v České republice je situace dostačující. Je ale zároveň nutné dodat, že by bylo v budoucnu vhodné platnou legislativu doplnit především s ohledem na aktuální technický a ekonomický vývoj. V úvahu připadá také ještě intenzivnější činnost vyvíjená Úřadem pro ochranu osobních údajů v oblasti prevence a interpretace.

Klíčová slova: osobní údaj, zpracování, správce

Abstract

Personal data protection in employment relations is an up-to-date subject in the Czech Republic. It is one of the fundamental human rights. Right for privacy and its protection are guaranteed by constitutional law and then elaborated in several statutes and executive regulations.

The goal of the thesis is to analyze legal regulation of the matter in the Czech Republic and European Union. At the same time there is mentioned particular problems that arise in relation to personal data protection in employment relations and their possible solutions.

The thesis is divided into 10 chapters that consists of subsections. The subsections deal with particular aspects of the topic and analyze them more closely. First two chapters describe legislation that is dealing with privacy protection and personal data protection in the Czech Republic and European Union.

The third and fourth chapters focuse on interpretation and definition of basic terms that are „personal data“ and „personal data processing“. In the subsections there is briefly described the substance of the terms and there are given examples of their possible interpretations.

The fifth chapter is dedicated to the subjects of personal data and those that participate in personal data processing. As to employment relations those are mostly employers and their employees.

Next part, the sixth chapter, concerns itself with particular duties that the employer has. Those are essential for the whole personal data processing all the way from the beginning to the end.

The seventh chapter enumerates rights of employees when their personal data are being processed and also their rights arising from the situation when the employer or some other subject of the process breach their duties and this unlawful breach disturbs personal life of the employee.

The eights chapter closely looks at the matter of passing personal data abroad. In this chapter you can find the conditions under which is this possible and institutes developed to make the process easier.

The ninth chapter called Practical issues describes areas of employment relations where the manipulation wiht personal data is most frequent. In relation to this there is the biggest possibility of abuse or some other violation of rights of the employee.

At last, the tenth chapter deals with consequences of infringment of the law and describes penalties for the violations.

In the end it needs to be said the level of personal data legal protection in the Czech Republic is sufficient. Nevertheless in the future it would be useful to improve the legislation so that it would keep up with the technological and economical progress. There is also possible more intensive effort of the Office for Personal Data Protection especially in the area of prevention and interpretation.

Key words: personal data**,** personal data processing, personal data administrator

Seznam zkratek

BCR- Binding Corporate Rules („závazná podniková pravidla“)

Evropská úmluva - Evropská úmluva o ochraně lidských práv a svobod, vyhlášena jako č. 209/1992 Sb., ve znění pozdějších předpisů

Listina - Listina základních práv a svobod, vyhlášena ústavním zákonem č. 23/1991 Sb. a republikována usnesením předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku ČR, ve znění zákona č. 162/1998 Sb.

Občanský zákoník - zákon č. 40/1964 SB., občanský zákoník, ve znění pozdějších předpisů

PEBS - Preemployment Background Screening

Pracovní skupina WP 29 - pracovní skupina zřízená podle čl. 29 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů

Protokol - Dodatkový protokol k Úmluvě Rady Evropy č. 108/1981, o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva č. 108)

Směrnice 95/46/ES - Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů

Úmluva č. 108 - Úmluva rady Evropy č. 108/1981, o ochraně osob se zřetelem na automatizované zpracování osobních dat

Ústava - ústavní zákon č. 1/1993 Sb., Ústava České Republiky, ve znění pozdějších ústavních předpisů

ÚOOÚ - Úřad pro ochranu osobních údajů

Zákon o elektronických komunikacích - zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů

Zákon o evidenci obyvatel - zákon č. 133/2000 Sb., o evidenci obyvatel a rodných čísel, ve znění pozdějších předpisů

Zákon o ochraně osobních údajů - zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

Zákon o svobodném přístupu k informacím - zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Zákon o zaměstnanosti - zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů

Zákoník práce - zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

Seznam použité literatury

Monografické publikace

- Bártík, V., Janečková, E. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 2. vydání. Praha: Linde, 2009
- Bezouška, P., Ivanko, G. Pracovní právo pro zaměstnavatele. Praha: Linde 2010
- Bělina, M. a kol. Zákoník práce. Komentář. 2. vydání. Praha: C. H. Beck, 2010
- König, P., Lacina, L., Přenosil, J. Učebnice evropské integrace. 2. vydání. Brno: Barrister & Principal, 2007
- Maštalka, J. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008
- Mates, P. Ochrana osobních údajů. 1 vydání. Praha: Karolinum, 2002
- Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer, 2008
- Řezníček, P. redaktor. Personalistika 2009-2010. Praha: ASPI, Wolters Kluwer, 2009

Článek z periodika

- Géblová, A. Češi, nenechte si šacovat soukromí!. Podnikání v praxi, 2003, č. 28, s. 4.

Materiály Úřadu pro ochranu osobních údajů

- www.uoou.cz, Judikatura
- www.uoou.cz, Média, Ochrana osobních údajů v českých médiích, Sledování zaměstnanců přes počítač? Nelze nyní, tím méně v budoucnu
- www.uoou.cz, K problémům z praxe č. 1/2001, Úřad pro ochranu osobních údajů, K pojmu osobní údaj
- www.uoou.cz, K problémům z praxe č. 2/2005, Úřad pro ochranu osobních údajů, Zpracování osobních údajů zaměstnanců vzhledem k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů
- www.uoou.cz, Předávání osobních údajů do zahraničí, K problémům z praxe, Předávání osobních údajů zaměstnanců do zahraničí

- www.uoou.cz, Předávání osobních údajů do zahraničí, K problémům z praxe, Přehled případů předávání osobních údajů do zahraničí, u nichž není nutno žádat Úřad o povolení
- www.uoou.cz, Předávání osobních údajů do zahraničí, K problémům z praxe, Závazná podniková pravidla (Binding Corporate Rules) jako nástroj běžného předávání osobních údajů do třetích zemí
- www.uoou.cz, Stanovisko Úřadu pro ochranu osobních údajů č. 1/2006, „Provozování kamerového systému z hlediska zákona o ochraně osobních údajů“
- www.uoou.cz, Stanovisko Úřadu pro ochranu osobních údajů č. 2/2008, „Souhlas se zpracováním osobních údajů“
- www.uoou.cz, Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009, „Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště“
- www.uoou.cz, Stanovisko Úřadu pro ochranu osobních údajů č. 2/2010, „Předání osobních údajů do jiných států“
- www.uoou.cz, Z rozhodovací činnosti Úřadu, K dodržování povinností přijmout a provést bezpečnostní opatření k ochraně osobních údajů v soukromoprávní sféře
- www.uoou.cz, Z rozhodovací činnosti Úřadu, K souhlasu se zpracováním citlivých osobních údajů
- www.uoou.cz, Z rozhodovací činnosti Úřadu, K provozování kamerového systému
- www.uoou.cz, Z rozhodovací činnosti Úřadu, Povinnost zabezpečit osobní údaje
- www.uoou.cz, Z rozhodovací činnosti Úřadu, K zabezpečení osobních údajů
- www.uoou.cz, Z rozhodovací činnosti Úřadu, Ke zpracování osobních údajů bývalých zaměstnanců

Odkazy na webové stránky

- www.asisonline.org
- jinepravo.blogspot.com, Otevřel, R. Soumrak užitečného internetu? (Díl I)
- www.cak.cz, Jouza, L. Ochrana osobních práv zaměstnance. Bulletin advokacie, 2008, č. 6, s. 34-38
- www.epravo.cz, Loebl, Z., Hajný, F., Fryntová, J. Monitorování e-mailů zaměstnanců

- www.itpravo.cz, Matějka, J. Ochrana soukromí na pracovišti dle zákona č. 262/2006 Sb. (nového zákoníku práce)
- www.odbory-online.cz, Právní ochrana zaměstnance, Pracovní poměr, Předsmluvní vztahy
- pravniradce.ihned.cz, Správní právo, Bártík, V., Janečková, E. Likvidace osobních údajů jako součást zpracování