

TRNAVSKÁ UNIVERZITA V TRNAVE



Vzor citácie: SISKOVIČOVÁ, K. *Ochrana súkromia a osobných údajov zamestnanca*, Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, xxx s. ISBN 978-80-8082-932-2

RECENZENTI:

prof. JUDr. Petr Tröster, CSc.
doc. JUDr. Mgr. Andrea Olšovská, PhD.
JUDr. Mikuláš Füleky, PhD.

KATARÍNA SISKOVIČOVÁ

**OCHRANA SÚKROMIA
A OSOBNÝCH ÚDAJOV
ZAMESTNANCA**



TRNAVA 2015

© Katarína Siskovičová, 2015

ISBN 978-80-8082-932-2

OBSAH

Predhovor	3
1. Právo na ochranu osobnosti a súkromia (teoretické východiská)	3
1.1 Právo na ochranu osobnosti	3
1.2 Právo na súkromie	3
1.2.1 Historický exkurz k vymedzeniu pojmu súkromie	3
1.2.2 Pojem súkromie v súčasnej právnej teórii a judikatúre súdov ..	3
1.2.3 Vzájomný vzťah práva na súkromie a vlastníckeho práva	3
2. Pramene právnej úpravy ochrany súkromia a osobných údajov zamestnanca	3
2.1 Pramene medzinárodnej a európskej právnej úpravy	3
2.2 Pramene slovenskej právnej úpravy	3
3. Ochrana súkromia zamestnanca	3
3.1 Základné spôsoby výkonu kontroly a zásahov do súkromia zamestnanca	3
3.2 Monitorovanie zamestnancov na pracovisku	3
3.2.1 Všeobecný právny rámec monitorovania zamestnancov na pracovisku	3
3.2.2 Monitorovanie zamestnancov prostredníctvom kamerových systémov	3
3.2.3 Monitorovanie elektronickej pošty zamestnancov	3
3.2.4 Sledovanie pohybu zamestnancov na internete	3
3.2.5 Monitorovanie telefonických hovorov zamestnancov	3
3.2.6 Osobná kontrola vecí a osobné prehliadky zamestnancov	3
3.2.7 Sledovanie pohybu zamestnancov prostredníctvom systému GPS	3
4. Ochrana osobných údajov zamestnanca	3
4.1 Osobný údaj	3
4.2 Osobitné kategórie osobných údajov	3
4.3 Spracúvanie osobných údajov	3
4.4 Subjekty oprávnené na spracúvanie osobných údajov	3

4.4.1	Prevádzkovateľ	3
4.4.2	Zástupca prevádzkovateľa a sprostredkovateľ	3
4.4.3	Príjemca	3
4.5	Povinnosti zamestnávateľa ako prevádzkovateľa osobných údajov	3
4.5.1	Oznamovacia povinnosť a osobitná registračná povinnosť	3
4.5.2	Informačná povinnosť	3
4.5.3	Povinnosť vyžiadať súhlas dotknutej osoby	3
4.5.4	Povinnosť prijať bezpečnostné opatrenia	3
4.5.5	Povinnosť likvidácie osobných údajov	3
4.6	Práva zamestnanca ako dotknutej osoby	3
4.7	Spracúvanie osobných údajov na pracovisku	3
4.7.1	Osobné údaje pred vznikom pracovného pomeru	3
4.7.2	Osobné údaje zamestnanca počas trvania pracovného pomeru	3
4.7.3	Osobné údaje zamestnanca po skončení pracovného pomeru	3
4.8	Prostriedky ochrany osobných údajov zamestnanca v Slovenskej republike	3
4.9	Ochrana osobných údajov v Európskej únii z hľadiska empirického výskumu	3
	Zoznam použitej literatúry	3
	Prílohy	3
	O autorke	3

PREDHOVOR

Charakteristickou črtou dnešnej doby je neustály pohyb prejavujúci sa intenzívnym technologickým a technickým pokrokom, ktorý so sebou prináša prevertné zmeny. Inovatívne informačné technológie poskytujú ich používateľom nové komunikačné možnosti, uľahčujú im prístup k realizácii obchodov a poskytovaniu služieb a prinášajú im výrazné ekonomické a časové úspory. V pracovnej sfére vznikajú v dôsledku rýchleho rozvoja technických monitorovacích zariadení nové spôsoby a formy kontroly výkonu práce, ktoré slúžia na zistenie miery využívania pracovného času, úrovne dodržiavania pracovnej disciplíny a efektivity vykonávanej práce. Najčastejším dôvodom zavádzania uvedených opatrení je predchádzanie škodám na majetku zamestnávateľa a zabránenie úniku informácií v prospech tretích subjektov.

V každom pracovnoprávnom vzťahu sú zamestnanci nútení poskytovať určité osobné údaje zamestnávateľovi ako subjektu, pre ktorého vykonávajú záväznú prácu, čo tiež znamená, že sú voči nemu v podriadenom vzťahu a sú od neho ekonomicky závislí. Na druhej strane sú zamestnávateľia povinní v rámci plnenia zákonných povinností voči rozličným štátnym orgánom a ďalším subjektom spracúvať osobné údaje zamestnancov. Často však dochádza k situácii, že zhromažďujú a spracúvajú osobné údaje vo väčšom rozsahu, než ustanovuje zákon, pretože sa domnievajú, že to zvýši celkovú efektivitu práce alebo motiváciu zamestnancov pri dosahovaní lepších pracovných výsledkov. Je bežnou praxou, že veľké obchodné korporácie poskytujú osobné údaje o svojich zamestnancoch aj rôznym subjektom v zahraničí v rámci vlastnej organizačnej štruktúry i mimo nej. Zamestnanec preto v komplikovanej sieti získavania a prenosu informácií prestáva mať často prehľad, aké druhy údajov o jeho osobe spracúva jeho zamestnávateľ, prípadne ktorým tretím subjektom tieto údaje poskytuje a či nedochádza k ich cezhraničnému prenosu.

Vzhladom na to, že zamestnanec je slabšou stranou v pracovnoprávnom vzťahu a je v nevýhodnejšom postavení, je úlohou štátu zabezpečovať nevyhnutnú ochranu jeho súkromia (vrátane osobných údajov), pretože to je jedno z najdôležitejších základných ľudských práv. Treba, aby štát zabezpečil okrem prehľadnej právnej úpravy aj náležitú súdnu ochranu a efektívnu kontrolu od príslušných správnych orgánov, hlavne Úradu na ochranu osobných údajov Slovenskej republiky.

Pri monitorovaní zamestnávateľa využívajú rôzne prostriedky a postupy, ktoré považujú z rozličných dôvodov za prínosné pri dosahovaní ich trvalého rozvoja a podnikateľského úspechu. Moderné monitorovacie prostriedky však so sebou prinášajú aj veľké riziká obmedzenia súkromia zamestnancov, vyrovnania sa s nimi, na ktoré nie je väčšina ich používateľov pripravená. V súvislosti s rôznymi spôsobmi monitorovania a formami kontroly na pracovisku sa vynára otázka, do akej miery možno konanie zamestnávateľa považovať za oprávnené a naopak, kedy už možno hovoriť o zásahu do základných práv a slobôd zamestnanca, najmä do jeho osobnej integrity. Definovanie hraníc oprávnených záujmov oboch strán a hľadanie prijateľného riešenia vo vzťahu k rozsahu nevyhnutnej ochrany súkromia a osobných údajov zamestnanca sa v dnešnom pracovnom a právnom prostredí ešte viac komplikuje. Na jednej strane zamestnávateľa poskytujú zamestnancom na výkon práce prostriedky, ktorých hodnota v mnohých prípadoch prekračuje niekoľkomesačnú mzdu zamestnanca (napr. výrobné strojové zariadenia, služobné motorové vozidlá). Nebolo by preto spravodlivé, ak by zamestnávateľa nemohli nakladanie s týmito predmetmi žiadnym spôsobom kontrolovať. Zamestnanec sa totiž zdržiava na pracovisku zamestnávateľa v podstate len z jedného jediného dôvodu, a tým je výkon práce. Je preto samozrejmé, že právo na súkromie zamestnancov sa v pracovnoprávných vzťahoch nemôže uplatňovať neobmedzene a má svoje hranice. Na druhej strane však aj právo zamestnávateľa zasahovať do osobnostných práv zamestnanca a jeho súkromia nie je neobmedzené a tiež má svoje hodnotové, ale aj zákonné limity.

Uvedený konflikt záujmov, ktorý predstavuje hlavný spor riešený v predloženej monografii, sa pokúsime vysvetliť prostredníctvom právnej filozofie a teórie, ale aj aplikačnej praxe najvyšších súdnych inštitúcií. Spolupráca členov spoločnosti vytvára priestor, v ktorom dochádza k vzájomnému prekryvaniu sa jednotlivých záujmov. Ochrana práva jedného tak logicky musí pôsobiť obmedzenie práva druhého subjektu. Špecifickým prípadom uvedeného rozporu je konflikt dvoch základných práv. Podľa Dworkina v pozadí každého takéhoto konfliktu stoja súperiace právne princípy. Jeho argument je totiž založený na predstave, že ľudské práva majú povahu právnych princípov, ktorých morálny obsah pôsobí ako „*politický triumf v rukách jednotlivcov. Jednotlivci majú práva vo chvíli, keď kolektívny cieľ nie je z nejakého dôvodu dostatočným ospravedlnením, aby sa im upieralo to, čo ako jednotlivci chcú mať alebo konať, alebo keď nie je dostatočným ospravedlnením toho, aby sa im pôsobila nejaká škoda alebo ujma*“.¹ Dworkin sa vo svojej teórii v podstate snaží ukázať, že hierarchia právnych princípov, a teda aj riešenie napätia medzi jednotlivými základnými právami je možné iba na apli-

¹ DWORKIN, R. Law as Interpretation. In: *Texas Law Review*, vol. 60, 1981 – 1982, p. 543.

kačnej úrovni.² Jeho teória nám teda umožňuje pochopiť, v akom vzťahu je právo zamestnanca na súkromie a vlastnícke právo zamestnávateľa. Je zrejmé, že s rozvojom informačných technológií zamestnávateľa získali nové možnosti kontroly svojich zamestnancov. Právny poriadok, ale aj aplikačná prax preto nanovo stanovujú obsah oprávnených záujmov zamestnávateľa a zamestnanca v oblasti ochrany osobných údajov, čím sa v podstate snažia vyvážiť vzniknuté napätie medzi právom zamestnanca na súkromie a vlastníckym právom zamestnávateľa v oblasti pracovnoprávných vzťahov.

Doterajšia judikatúra nám ponúka odpovede na viaceré súvisiace problémy. Napríklad Ústavný súd Slovenskej republiky vo viacerých svojich rozhodnutiach (napr. aj v náleze z 27. februára 1997 sp. zn. PL. ÚS 7/96) vyslovil právny názor, podľa ktorého sa všetky základné práva a slobody chránia len v takej miere a rozsahu, dokiaľ uplatnením jedného práva alebo slobody nedôjde k neprimeranému obmedzeniu či dokonca popretiu iného práva alebo slobody. Rovnováha verejného a súkromného záujmu je dôležitým kritériom určovania primeranosti obmedzenia každého základného práva a slobody. Podobný názor vyslovil aj Najvyšší súd Slovenskej republiky v rozsudku z 19. mája 2010 sp. zn. 5 Cdo 108/2009, v ktorom judikoval, že „okrem práv spätých s ochranou osobnosti v čl. 19 Ústava Slovenskej republiky zaručuje aj iné základné práva a slobody, napr. právo na súdnu a inú ochranu (čl. 46 až 50) a slobodu prejavu (čl. 26). Uplatňovanie týchto základných práv a slobôd a ich právna ochrana musia byť proporcionálne a vzájomne vyvážené tak, aby sa nadmernou ochranou jedného práva nad únosnú mieru nepotlačila ochrana iného práva. To znamená, že ani existencia zásahu do osobnostných práv nemusí nevyhnutne viesť k záveru o neoprávnenosti takéhoto zásahu, ak bol dôsledkom uplatňovania iného základného práva a vzhľadom na okolnosti uplatňovania iného základného práva nepresiahol hranice primeranosti“.

Zdá sa, že postoj najvyšších súdnych inšancií na Slovensku nie je ničím výnimočný. Vo väčšine ústavných systémov európskych krajín sa z materiálneho hľadiska ustálila trojica kritérií, podľa ktorých určujeme opodstatnenosť obmedzení základných práv a slobôd. Sú nimi **princípy legality, legitimacy a proporcionality**.³ Vo vzťahu k právu na súkromie to znamená, že jeho obmedzenie je možné

² Nedostatkem Dworkinovej teórie je nemožnosť vopred vymedziť obsah základných práv a slobôd, čím sa zároveň oslabuje aj právna istota, pretože rozhodovanie súdov sa stáva nepredvídateľným. ONDŘEJKA, P. *Princíp proporcionality a jeho role při interpretaci základních práv a svobod*. Praha: Leges, 2012, s. 61.

³ „**Legalita** zásahu do práva na súkromie znamená, že štát môže do práva na súkromie zasiahnuť iba na základe zákona. Preto v rámci legality zásahu sa skúma, či k nemu došlo v súlade s platnými právnymi predpismi, pričom sa prihliada aj na to, či právny predpis bol verejne publikovaný a teda dostupný, a či jeho následky boli predvídateľné. Skúma sa teda aj kvalita zákonnej úpravy, ktorá je základom zásahu do práva na súkromie.

iba v prípade, ak „daný skutkový stav možno *ratione materiae* považovať za súčasť práva na súkromie. Po kladnej odpovedi na túto otázku treba skúmať, či zásah bol legálny. V ďalšom sa potom skúma, či bol zásah legitímny a napokon, či bol proporcionálny. Ak sa dospeje k negatívnej odpovedi pri niektorej z týchto otázok, ďalej sa už v skúmaní problematiky nepokračuje“.⁴ Z dikcie uvedenej právnej vety je zrejmé, že medzi princípom legitimacy, legality a proporcionality je určitá logická nadväznosť a že testu proporcionality predchádza test legality a legitimacy obmedzení základných práv. Napokon línií trichotómie legitimacy, legality a proporcionality zodpovedá aj článok 52 ods. 1 Charty základných práv Európskej únie, ktorý stanovuje, že „akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných“.

Podľa európskej judikatúry test proporcionality vo všeobecnosti spočíva v troch nasledujúcich krokoch. V prvom rade sa zisťuje vhodnosť, v druhom rade potrebnosť a až nakoniec sa skúma proporcionality v užšom zmysle slova, keď sa porovnáva závažnosť obmedzení v kolízii stojacich základných práv. Práve spôsobom uplatňovania proporcionality v užšom zmysle slova, teda otázkou vyvažovania práva na súkromie zamestnanca (vrátane práva na ochranu jeho osobných údajov) a vlastníckeho práva zamestnávateľa, sa budeme v práci zaoberať.⁵

Problematika ochrany súkromia v pracovnom práve je v súčasnosti veľmi diskutovanou a prerokovanou témou v právnej teórii v Slovenskej republike. Koncepcia štruktúry predloženej monografie je preto prispôbena naplneniu základného cieľa práce, ktorým je snaha autorky prispieť k lepšiemu pochopeniu

Legitimita zásahu do práva na súkromie vyplýva z čl. 8 ods. 2 dohovoru a znamená, že do práva na súkromie možno zasiahnuť len vtedy, keď je to v záujme štátu z dôvodov ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojov a zločinnosti, v záujme spoločnosti z dôvodu ochrany zdravia a morálky, zabezpečenia hospodárskeho blahobytu krajiny a v záujme jednotlivcov z dôvodu ochrany ich práv a slobôd.

Proporcionality zásahu znamená, že k zásahu možno prikočiť len vtedy, keď je to nevyhnutné (sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami) a iba v duchu požiadaviek kladených na demokratickú spoločnosť vyznačujúcu sa pluralizmom, toleranciou a voľným duchom.“ Pozri bližšie nálezy Ústavného súdu Slovenskej republiky zo 4. februára 2009 sp. zn. I. ÚS 117/07 alebo zo 14. júna 2006 sp. zn. I. ÚS 274/05.

⁴ Nález Ústavného súdu Slovenskej republiky zo 14. júna 2006 sp. zn. I. ÚS 274/05.

⁵ Pozri Rozhodnutie SD EÚ z 20. mája 2003 v spojených právnych veciach Österreichischer Rundfunk, veci C-465/00, C-38/01 a C-139/01 alebo Rozhodnutie SD EÚ z 9. novembra 2010 v spojených právnych veciach Volker und Markus Schecke GbR a Hartmut Eifert v. Hessensko, veci C-92/09, C-93/09. FOLDOVÁ, V. – NONNEMANN, F. Zverejňovanie platů zamestnanců veřejné sféry ve světle aktuálního rozsudku Nejvyššího správního soudu. In: *Právní rozhledy*, 2015, č. 2, s. 66.

podstaty ochrany súkromia a osobných údajov zamestnanca s prihliadnutím na rozmanité možnosti a osobitosti využívania moderných technických monitorovacích prostriedkov, a to tak z hľadiska zamestnanca, ako aj zamestnávateľa. Venujeme sa komplexnému posúdeniu prínosov a rizík nových informačných technológií vo vzťahu k viacerým dôležitým právnym aspektom ochrany osobnosti a ochrany súkromia zamestnanca. Cieľ práce sa pokúsime dosiahnuť aj vymedzením hraníc medzi právami a povinnosťami zamestnávateľa a zamestnanca, ako aj porovnávaním ich oprávnených záujmov v oblasti ochrany súkromia a osobných údajov. Je nepochybné, že už zo samej podstaty akéhokoľvek základného práva a slobody vyplýva, že musí byť limitované do tej miery, aby nedochádzalo jeho uplatňovaním k neprimeraným zásahom do základných práv a slobôd iných osôb. Z uvedených dôvodov je dôležité dôsledne uplatňovať spomenutú zásadu proporcionality vo vzťahu k ochrane súkromia zamestnanca.

Text monografie je rozdelený do štyroch kapitol.

V úvode priblížujeme podstatu problému konfliktu osobnostných práv zamestnanca a majetkových práv zamestnávateľa, čo vytvára ďalej priestor, v ktorom budeme schopní z rôznych hľadísk určovať a porovnávať oprávnené a neoprávnené zásahy do súkromia a ostatných osobnostných práv zamestnanca.

V prvej kapitole sa venujeme výkladu pojmov a teoretickým východiskám práva na ochranu osobnosti a ochranu súkromia. Nedielnou súčasťou analýzy pojmu súkromie je tiež historický exkurz do jeho vývoja, ktorý nám dovoľuje vidieť danú problematiku v širšom dejinnom kontexte.

Dôsledné predstavenie širokej pramennej základne ochrany súkromia a osobných údajov na medzinárodnej, ako aj európskej úrovni je nevyhnutným predpokladom kvalitnej interpretácie vnútroštátnej právnej úpravy. Preto práve pramene medzinárodnej, európskej a vnútroštátnej právnej úpravy ochrany súkromia a osobných údajov zamestnanca tvoria obsah druhej kapitoly. V monografii sa nezameriavame iba na výklad všeobecne záväznej právnej úpravy (*law in books*), ale vo významnej miere ho doplníme aj prameňmi z oblasti aplikačnej praxe súdov (*law in action*), najmä súdnymi rozhodnutiami Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie, ostatných všeobecných súdov Slovenskej republiky i Ústavného súdu Slovenskej republiky.

Obsahom tretej kapitoly je všeobecný právny rámec monitorovania zamestnancov na pracovisku vyplývajúci zo slovenskej právnej úpravy. Jej významnou súčasťou je priblíženie v praxi najčastejšie využívaných spôsobov výkonu kontroly zamestnancov na pracovisku zamestnávateľmi pomocou špeciálnych monitorovacích systémov (od monitorovania kamerovými systémami cez sledovanie elektronickej pošty, pohybu na internete a telefonických hovorov až po osobné prehliadky, kontrolu vecí či sledovanie pohybu zamestnancov pomocou GPS). Spomenieme tiež vybrané problémy obmedzenia týkajúce sa jednotlivých spô-

sobov monitorovania, ktoré vyplývajú z aktuálnej judikatúry najmä európskych súdnych inštitúcií.

Štvrtá kapitola predloženej monografie je z hľadiska rozsahu najväčšia. Je zameraná na rozbor relevantnej slovenskej právnej úpravy ochrany súkromia a osobných údajov zamestnanca v pracovnoprávných vzťahoch, ktorej presahy môžeme pozorovať aj v ostatných kapitolách práce. Uvádzame v nej základné pojmové definície vymedzené v zákone o ochrane osobných údajov, ako napríklad osobný údaj, spracúvanie osobných údajov a subjekty oprávnené na spracúvanie osobných údajov. Ďalšiu časť tvorí rozbor jednotlivých povinností zamestnávateľa ako prevádzkovateľa osobných údajov, ale aj analýza práv zamestnanca ako príslušnej osoby pri spracúvaní osobných údajov. Ako prínos tejto kapitoly považujeme jej záverečnú časť, v ktorej sa zaoberáme rôznymi aspektmi spracúvania osobných údajov v pracovnoprávných vzťahoch, ktoré sú systematicky rozčlenené podľa jednotlivých štádií trvania pracovného pomeru (pred vznikom, počas trvania a po jeho skončení). Na získanie uceleného pohľadu uvádzame aj konkrétne príklady z rozhodovacej činnosti slovenských súdov a kontrolnej činnosti Úradu na ochranu osobných údajov Slovenskej republiky. Súčasťou kapitoly sú aj prostriedky ochrany osobných údajov zamestnanca, najmä z hľadiska občianskoprávnej a pracovnoprávnej úpravy, ale tiež úpravy podľa osobitných predpisov, ktoré môže zamestnanec využiť v prípade, že dochádza k neoprávneným zásahom do jeho práv. Osobitnú pozornosť venujeme aj úvahám o aktuálnej kvalitatívnej úrovni slovenskej právnej úpravy i aplikačnej praxe vo vzťahu k ochrane osobných údajov zamestnanca, vychádzajúc pritom z výsledkov výskumu zameraného na úroveň ochrany osobných údajov a realizovaného v niektorých členských štátoch Európskej únie v roku 2012.

V závere monografie je zhrnutie zistení a výsledkov vo vzťahu k stanoveným cieľom práce, ktoré sú základom prezentácie našich názorov, návrhov a úvah o možnostiach skvalitnenia právnej úpravy de lege ferenda. Kvalitná právna úprava je totiž základným predpokladom zvýšenia celkovej úrovne ochrany súkromia a osobných údajov zamestnanca aj v aplikačnej praxi.

Vzhľadom na rozsah tejto témy sme postupovali pri tvorbe a výbere jednotlivých kapitol od všeobecného ku konkrétnemu a snažili sme sa výkladovú teoretickú časť prepojiť s judikatúrou a konkrétnymi príkladmi z aktuálnej praxe. V monografii využívame všeobecné logické metódy, najmä deskripciu, komparáciu, dedukciu, indukciu, analýzu a syntézu. Naším cieľom nebolo len deskriptívne zhrnúť súčasný právny stav, ale skôr predstaviť realitu ochrany osobných údajov v praxi. V rámci nášho výskumu sme sa pritom nesnažili empiricky pochopiť čo najväčšiu vzorku judikátov týkajúcich sa ochrany osobných údajov a súkromia. Pracovali sme skôr s vybranými rozsudkami a prípadmi z praxe, ktoré boli schopné zastúpiť dáta, s ktorými sme neprišli do styku. Z tohto hľadiska má mono-

grafia skôr charakter typologickej než taxonomickej práce. Z metodologického hľadiska je predložená monografia viac sociologickou než dogmatickou štúdiou. V každej kapitole sa snažíme priblížiť, akým spôsobom sa súvisiaca právna úprava aplikuje v praxi, čo nám umožnilo poukázať na jej medzery a nedostatky a v závere následne navrhnúť žiadané zmeny.

Samotnému spracovaniu problematiky v monografickej podobe tiež predchádzala kvalitná heuristika relevantnej literatúry. Medzi základné informačné zdroje, využívané v monografii, patria najmä odborné publikácie, články zo slovenských i zahraničných odborných právnických časopisov, legislatívne dokumenty, súdne rozhodnutia a internetové zdroje.

1. PRÁVO NA OCHRANU OSOBNOSTI A SÚKROMIA (teoretické východiská)

Každý zamestnanec je v prvom rade fyzickou osobou disponujúcou osobnostnými právami z hľadiska občianskeho práva a právo na ochranu jeho ľudskej dôstojnosti mu patrí tak na pracovisku ako aj mimo neho. Je nepochybné, že právo na ochranu osobnosti a súkromia úzko súvisí s ochranou osobných údajov aj v pracovnoprávných vzťahoch, pretože v rámci nich sa nevyhnutne, rovnako ako v ostatných súkromnoprávných zmluvných vzťahoch, spracúvajú osobné údaje ich účastníkov.

Pracovnoprávne predpisy *ex lege* vyžadujú od zamestnávateľov spracovanie osobných údajov zamestnanca už pred vznikom, počas trvania i po skončení pracovnoprávneho vzťahu, čo im umožňuje disponovať s veľkým rozsahom informácií o osobnosti každého zamestnanca a otvára sa im priestor pre rôzne nedovolené zásahy do jeho osobnej integrity. Zamestnávateľ je na jednej strane oprávnený požadovať od zamestnanca rôzne osobné údaje, ktoré sú dôležité pre výkon jeho práce, je však aj povinný rešpektovať jeho osobnostné práva a nezasahovať nepriemeraným spôsobom do jeho súkromia.

Predtým než pristúpime ku hľadaniu a definovaniu hraníc medzi právami a povinnosťami zamestnávateľa a zamestnanca, ako aj porovnávaníu ich oprávnených záujmov, v prvom rade treba vysvetliť podstatu osobnostných práv. V úvodnej kapitole sa preto venujeme definovaniu základných pojmov a určeniu teoretických východísk práva na ochranu osobnosti a jej súkromia.

1.1 Právo na ochranu osobnosti

Definíciu všeobecného osobnostného práva⁶ v objektívnom zmysle sa snažili sformulovať viacerí právni vedci. Z hľadiska právnej teórie nájdeme výstižnú

⁶ V právnej teórii sa používa aj pojem osobnostné právo alebo právo späté s osobnosťou človeka, pretože ide výsostne o osobnostné stránky patriace každej fyzickej osobe. Pozri VOJČÍK, P. a kol. *Občiansky zákonník. Stručný komentár*. Bratislava: Iura Edition, 2008, s. 54.

definíciu u Knappa, ktorý osobnostné práva vníma ako „*súhrn právnych noriem, ktoré upravujú právo, resp. jednotlivé čiastkové práva, ktorých predmetom je osobnosť fyzickej osoby ako celku, resp. jednotlivé hodnoty tvoriace súčasť celkovej fyzickej a morálnej integrity osobnosti každej fyzickej osoby ako individuality a suveréna, a ktorých subjekty majú voči ostatným subjektom (fyzickým či právnickým osobám) rovné právne postavenie a zásadnú autonómiu vôle*“.⁷

Právnym základom súkromnoprávnej ochrany osobnosti (osobnostných práv) sú nepochybne právne predpisy občianskeho práva hmotného. Pri interpretácii právnej úpravy, ktorá zakotvuje právo na ochranu osobnosti, je preto potrebné brať do úvahy viaceré základné súkromnoprávne zásady ako napríklad:

- a) zásady v pochybnostiach v prospech života,
- b) zásady prednosti ľudskej bytosti pred záujmami spoločnosti alebo vedy,
- c) zásady nedotknuteľnosti osobnosti,
- d) zásady odvolateľnosti súhlasu,
- e) zásady zákazu získania finančného prospechu z ľudského tela alebo jeho častí,
- f) zásady posmrtnej ochrany.⁸

Špecifická povaha osobnostných práv spočíva v ich osobitnom objekte, na ktorý sa viažu, resp. ktorý je ich nositeľom, t. j. na človeka a jeho osobnosť. Sú chránené Občianskym zákonníkom spolu s ďalšími právnymi normami nášho právneho systému. Ustanovenie § 1 ods. 1 Občianskeho zákonníka je jedným z pilierov občianskeho, resp. súkromného práva, ktoré do popredia občianskych práv a slobôd aj z hľadiska štruktúry samotného Občianskeho zákonníka výslovne kladie najmä ochranu osobnosti, no zároveň aj nedotknuteľnosť vlastníctva (s týmto právom sa osobnostné práva dostávajú často do kolízie v právnej teórii i v praxi).

Základom súkromnoprávnej ochrany osobnostných práv sú ustanovenia § 11 až 16 Občianskeho zákonníka. Z hľadiska systematiky je v § 11 obsiahnutá generálna klauzula, ktorá pod ochranou osobnosti každej fyzickej osoby rozumie na prvom mieste ochranu života a zdravia človeka, po ktorej nasleduje občianska česť a ľudská dôstojnosť, súkromie, meno a v neposlednom rade všetky prejavy osobnej povahy. Už samotné znenie ustanovenia naznačuje, že uvedené zložky osobnosti človeka nie sú navzájom nezávislé a ich postavenie nie je možné vnímať bez analýzy ich vzájomných vzťahov. Rozsah ochrany života a zdravia človeka sa totiž často prekrýva s ďalšími uvedenými zložkami osobnostných práv v tom

⁷ KNAP, K., ŠVESTKA, J., JEHLIČKA, O., PAVLÍK, P., PLECITÝ, V. 2004. *Ochrana osobnosti podľa občianskeho práva*. 4. podstatne přepracované a doplněné vyd. Praha: Linde, 2004, s. 57.

⁸ ELIÁŠ, K. a kol. *Občianský zákoník: velký akademický komentář. 1. svazek*. Praha: Linde Praha, a. s., 2008, s. 109.-

zmysle, že ochranou jednej zložky sa chránia aj ostatné.⁹ Osobnostné práva sú prejavom potreby chrániť osobnosť človeka ako celku. Všetky čiastkové osobnostné práva preto navonok z hľadiska objektívneho vytvárajú jednotu, ktorá je základom komplexného, tzv. všeobecného osobnostného práva. Všetky čiastkové osobnostné práva sú vo svojej podstate ideálne statky, ktoré sú jeho súčasťou, pričom platí, že prislúchajú každej fyzickej osobe ako subjektu práva. Sú teda neprenosné a majú výlučne osobný charakter.¹⁰

V súlade s § 11 Občianskeho zákonníka právna teória medzi jednotlivé aspekty občianskoprávnej ochrany osobnosti fyzickej osoby zaraďuje právo na telesnú integritu, právo na meno, právo na občiansku česť a ľudskú dôstojnosť, právo na ochranu prejavov osobnej povahy zachytené na hmotnom substráte (napr. podobizne a zvukové záznamy) a právo na súkromie.¹¹ Výpočet čiastkových osobnostných práv uvedených v § 11 Občianskeho zákonníka však nemá taxatívny charakter. Z obsahu jeho znenia, a to slova „najmä“, je zrejmé, že zákonodarca predpokladal, že zákon v otázke takého komplexného problému, akým je ochrana osobnosti jednotlivca, nesmie zostať významovo uzavretý. Pozitívny demonštratívny výpočet § 11 Občianskeho zákonníka je ďalej konkretizovaný v § 12, pričom prostriedky ochrany ako aj spôsob domáhania sa nárokov vzniknutých z neoprávneného zásahu do osobnostných práv je upravený v § 13 až 16.

Na tomto mieste je nevyhnutné zdôrazniť, že ochrana osobnosti sa rozširuje v súkromnom práve aj na ochranu mortis causa, t. j. postmortálnu ochranu osobnosti zomrelého i pozostalých osôb v zmysle ustanovení § 11 až § 13 a § 15 Občianskeho zákonníka. V uznesení z 13. októbra 2011 sp. zn. 3 Cdo 84/2011 (R 38/2012) dospel Najvyšší súd Slovenskej republiky k presvedčeniu, že „*ak tým istým konaním, ktoré po smrti fyzickej osoby neoprávnené zasiahlo do osobnosti zomrelého (napríklad jeho cti a dobrého mena), došlo zároveň k zásahu aj do osobnosti pozostalej osoby (napríklad do jej práva na súkromie)*“. Vzhľadom na okolnosti, za ktorých k takému konaniu došlo, judikatúra pripustila možnosť tzv. postmor-

⁹ Ochrana občianskej cti je preto často spojená s ochranou dobrého a mena a pod. Ochrana osobnosti sa však dostáva do konfliktu aj s principiálne odlišnými hodnotami, akou je napr. sloboda prejavu alebo právo na informácie. V tom prípade sa spor medzi jednotlivými hodnotami a princípmi rieši na základe ich vyvažovania. Tým sa hľadá optimálne riešenie, ktoré by vyhovovalo zásadám proporcionality a zároveň by bolo v súlade s Ústavou Slovenskej republiky. K problémom spojeným s aplikáciou ochrany niektorých osobnostných práv pozri bližšie TELEČ, I. Chránené statky osobnosti. In: *Právni rozhledy*. ISSN 1210-6410, 2007, roč. 15, č. 8, s. 271.

¹⁰ Pozri rozsudok Najvyššieho súdu Slovenskej republiky z 31. januára 1996 sp. zn. 3 Cdo 98/95 (R 53/1996).

¹¹ Porovnaj KIRSTOVÁ, K. Ochrana osobnosti fyzickej osoby. In: LAZAR, J. a kol. *Občianske právo hmotné*. I. diel. Bratislava: Iura Edition, 2010, s. 185 a ďalej VOJČÍK, P. a kol. *Občiansky zákonník. Stručný komentár*. Bratislava: Iura Edition, 2008, s. 54.

tálnej ochrany osobnosti.¹² Na druhej strane právnickým osobám osobnostné práva právny poriadok nepriznáva. Patria jej však práva obdobné právam osobnostným. Podľa § 19b sa právnické osoby môžu domáhať ochrany svojho mena alebo dobrej povesti (reputácie) a pod.

Hoci je úprava ochrany osobnosti v Občianskom zákonníku tradičná a relatívne samostatná, nemôžeme tvrdiť, že je vyčerpávajúca a komplexná. Ochrana osobnosti, ako aj problematika integrity fyzickej osobnosti je spojená a súvisí s celým radom iných právnych odvetví, a to tak súkromnoprávnej povahy – napr. pracovného práva (Zákonník práce), ale aj verejnoprávnej povahy – napr. ústavného práva (Ústava Slovenskej republiky a Listina základných práv a slobôd), trestného (Trestný zákon) a správneho (Zákon o priestupkoch). Z toho vyplýva, že osobnosť fyzickej osoby je chránená celým právnym poriadkom a nielen Občianskym zákonníkom. Často sa preto stáva, že nároky vzniknuté z nedovoleného zásahu do osobnostných práv podľa Občianskeho zákonníka, budú v súbehu so vznikom trestnoprávnej zodpovednosti osoby, ktorá sa dopustila takéhoto zásahu. Napríklad nedovolený zásah do osobnostných práv zamestnanca podľa Zákonníka práce sa často dostáva do súbehu s porušením ochrany čiastkových osobnostných práv podľa občianskeho, správneho alebo trestného práva.

Na základe uvedeného môžeme dospieť k záveru, že osobnosť človeka je komplexným pojmom a chráni sa ako celok. To znamená, že právny poriadok garantuje ochranu všetkých čiastkových osobnostných práv každej fyzickej osobe počas aj po jej smrti. Občiansky zákonník v § 11 vymenúva čiastkové osobnostné práva, ktoré sú predmetom ochrany psychickej ale aj fyzickej nedotknuteľnosti človeka. Demonstratívny výpočet čiastkových osobnostných práv v tomto ustanovení umožňuje zaradiť pod ochranu osobnosti aj ďalšie významné statky, ktorými sú v súvislosti s ústavno-konformným výkladom právo na ochranu života a zdravia, ochranu občianskej cti a ľudskej dôstojnosti, osobnej slobody, právo na meno a dobrú povesť, právo na ochranu súkromia a mnohé ďalšie. Vzhľadom na uvedené je nepochybné, že zamestnanec je tiež fyzickou osobou, ktorá má počas trvania pracovnoprávneho vzťahu a v odôvodnených prípadoch aj po jeho skončení nárok na ochranu všetkých vymenovaných čiastkových osobnostných práv.

Ochrana života a zdravia je na prvom mieste z hľadiska umiestnenia v rámci demonstratívneho výpočtu zložiek osobnostných práv v § 11 Občianskeho zá-

¹² Porovnaj tiež rozsudok Najvyššieho súdu Slovenskej republiky z 31. januára 1996 sp. zn. 3 Cdo 98/95 (R 53/1996), v ktorom sa uvádza, že „právo na ochranu osobnosti je právo osobnej povahy, ktoré zaniká smrťou fyzickej osoby a neprechádza na dedičov. Preto ak žalobca v priebehu konania zomrie, súd konanie zastaví... Osobám uvedeným v ustanovení § 15 Občianskeho zákonníka vzniká originálne právo na ochranu osobnosti smrťou fyzickej osoby, do práv ktorej bolo zasiahnuté“.

konníka.¹³ Ochrana života a zdravia človeka sa neviaže len na jeho fyzickú, ale aj psychickú nedotknuteľnosť, čím sa zabezpečuje integrita človeka ako celku.

Z povahy tejto ochrany potom vyplýva, že ochrana života sa nedá oddeliť od ochrany zdravia a naopak. Fyzická a psychická nedotknuteľnosť je všeobecne spájaná s ďalšími čiastkovými právami, a to hlavne s právom:

- a) na ochranu života vrátane ochrany života ešte pred narodením,
- b) na život v zdravom životnom prostredí,
- c) na dôstojný život,
- d) na informácie o vlastnom zdravotnom stave,
- e) na vlastné telo a jeho časti.¹⁴

Tento výpočet nás privádza k záveru, že obsah ochrany života a zdravia je široký. Tým, že sa neobmedzuje iba na fyzickú, ale aj psychickú integritu človeka, predpokladá sa, že každý zásah (porušenie alebo jej obmedzenie) si vyžaduje slobodný informovaný súhlas nielen o samotnom realizovanom zásahu, ale aj o jeho možných rizikách. Kým do fyzickej integrity možno zasiahnuť predovšetkým prostredníctvom poskytovania zdravotnej starostlivosti, do psychickej integrity možno v dnešnej informačnej dobe zasiahnuť bez existencie akéhokoľvek fyzického kontaktu, napr. aj zásahmi do osobnostných práv. Napríklad sociálne siete, ale aj verejné blogy sú priestorom na šírenie nepravdivých a zavádzajúcich informácií, ktorými sa môže veľmi jednoducho narušiť psychická nedotknuteľnosť človeka. V súčasnosti nie sú zriedkavé aj prípady tzv. krádeží identity.

Medzi ďalšie čiastkové osobnostné práva patrí **ochrana občianskej cti a ľudskej dôstojnosti**. Tie sa v podstate výsostne orientujú na zachovanie nedotknuteľnosti psychickej integrity človeka. Tak občianska česť, ako aj dôstojnosť sa považujú za vysoko subjektívne kategórie, ktoré súvisia s postavením jednotlivca a jeho vážnosťou v spoločnosti. Ľudská dôstojnosť sa pritom viaže na symetriu interpersonálnych vzťahov, čo sa prejavuje v podobe očakávaného správania adresátov práv a povinností podľa noriem, ktoré spoločenstvo prijalo.¹⁵ V podstate je ochrana ľudskej dôstojnosti prejavom vzájomnej rovnosti osôb, ktoré si v spoločnosti adresujú príkazy, zákazy a dovolenia.

Nedeliteľnou súčasťou sociálneho života človeka je jeho **meno**, ktoré považujeme za identifikačný, ale zároveň aj individualizačný znak každej fyzickej osoby. Ochrana mena sa vzťahuje nielen na krstné meno s priezviskom, ale tiež aj na prezývku, pseudonym, iniciály či monogram. Podrobnosti verejnoprávnej

¹³ Podobne ako v zákone č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov je život a zdravie z hľadiska systematiky prvou a najdôležitejšou zložkou človeka, ktorú treba chrániť.

¹⁴ MATEJKA, J. *Internet jako objekt práva: Hledání rovnováhy autonomie a soukromí*. 1. vyd. Praha: CZ.NIC, 2013, s. 139.

¹⁵ HABERMAS, J. *Budoucnost lidské přirozenosti. Na cestě k liberální eugenicé?* 1. české vyd. Praha: FILOSOFIA, 2003, s. 43.

ochrany mena sú obsiahnuté v zákone o matrikách.¹⁶ Súkromnoprávna úprava je o niečo nejednoduchšia, pretože ochrana mena fyzickej osoby nie je upravená len v rámci jedného predpisu. Základom je síce Občiansky zákonník, no určité aspekty ochrany mena môžeme nájsť aj v oblasti autorského práva, konkrétne v autorskom zákone,¹⁷ ktorý chráni predovšetkým duševné vlastníctvo autora, ale aj pseudonym. S autorským zákonom a jeho ochranou sú spojené aj akékoľvek prejavy osobnej povahy, pričom nezáleží na tom, či boli vyjadrené ústne, písmom, zvukom, obrazom, prípadne zachytené v audiovizuálnej podobe. Rozhodujúcim kritériom, podľa ktorého posudzujeme, či si takéto prejavy zaslúžia ochranu alebo nie, je ich vzťah k fyzickej osobe, resp. ich osobná povaha a nie forma ich vyjadrenia. Ochrana sa preto poskytuje všetkým formám vyjadrenia prejavov osobnej povahy bez ohľadu na nosič, ktorý umožňuje ich uchovanie.¹⁸

Právo na súkromie sa stalo jedným z najrozsiahlejších osobnostných práv, pretože pri zásahu do súkromia neoddeliteľne dochádza aj k zásahu do všetkých ostatných osobnostných práv (života a zdravia, občianskej cti a ľudskej dôstojnosti či rodinného života).¹⁹ Práve tomuto právu a jeho ochrane sa budeme primárne venovať, pričom sa zameriame na jeho význam v oblasti pracovnoprávných vzťahov.

1.2 Právo na súkromie

Hlavným dôvodom, pre ktorý sme v predchádzajúcej podkapitole venovali pozornosť významu a postaveniu osobnostného práva v našom právnom poriadku, je zaradenie práva na súkromie medzi najvýznamnejšie čiastkové osobnostné práva, ktoré súvisia aj s výkonom závislej práce zamestnanca pre zamestnávateľa. Zamestnávateľ si často nárokuje neoprávnene zasahovať do jeho osobnostných práv, čím môže získať informácie o rôznych aspektoch súkromného života zamestnanca práve kvôli ochrane jeho vlastných záujmov (najmä ochrany majetku). Zamestnanec vykonávajúci prácu v súkromných priestoroch zamestnávateľa pomocou jeho výrobných prostriedkov sa dostáva do nevýhodnejšej pozície. Konflikt týchto dvoch záujmov – záujem na ochrane (vlastníctva) majetku a zá-

¹⁶ Zákon č. 420/2006 Z. z. o matrikách v znení neskorších predpisov.

¹⁷ Zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov.

¹⁸ Osobná povaha prejavov sa pritom posudzuje vždy vzhľadom na konkrétny prípad, pričom každý takýto prejav sa stáva osobným, keď umožňuje identifikáciu osoby podľa špecifik zachytených na nosiči. V prípade písomnosti pôjde napríklad o denníky, pri zvukovom zázname o zachytenie prednesu na diktafóne, pri obrazovom zázname o osobné fotografie a podobne.

¹⁹ MATES, P. *Ochrana osobných údajů*. 1. vyd. Praha: Karolinum, 2002, s. 37.

ujem na ochrane súkromia – nás núti definovať pojem „súkromie“, ktorý sa stáva ústredným pojmom v snahe o vymedzenie hraníc odôvodnených zásahov do tohto základného práva zamestnanca zo strany zamestnávateľa.

1.2.1 Historický exkurz k vymedzeniu pojmu súkromie

Historický posun pri vnímaní súkromia nastal na prelome 19. a 20. storočia v Spojených štátoch amerických. V jednom z najvplyvnejších článkov v histórii amerického práva s názvom „The Right to Privacy“ (prekl. „Právo na súkromie“) autori Louis D. Brandeis a Samuel D. Warren spojili ochranu súkromnej sféry so slobodou jednotlivca v moderných dejinách. Základné myšlienky formulované v článku rozvinul Brandeis už ako člen Najvyššieho súdu v rokoch 1916 až 1939 v známom disente v právnej veci *Olmstead v. Spojené štáty americké* v roku 1928. Výsledkom bolo z dnešného hľadiska výrazne reštriktívne vnímanie pojmu súkromia, ktoré bolo chápané ako „právo byť ponechaný osamote“, t. j. právo na pokoj a ochranu pred vonkajšími zásahmi predovšetkým vo svojom obydlí.²⁰ Napriek tomu sa Brandeis spolu s Warrenom zaslúžili o to, že sa v USA pojem súkromia oddelil od vlastníctva. Súkromie sa stalo základom pre tzv. všeobecné právo na súkromie („*general right to privacy*“), ktorého sa bolo možné dovolať priamo a nielen sprostredkované.²¹ Až neskôr sa začalo právo na súkromie považovať za obsahovú súčasť širšieho práva na vlastnú osobnosť, pričom bolo relatívne nezávislé od iných práv a slobôd.

V Európe sa súkromiu venovala výraznejšia pozornosť až po druhej svetovej vojne, keď boli podpísané viaceré medzinárodné zmluvy a dohovory, ako sú Všeobecná deklarácia ľudských práv z roku 1948, Európsky dohovor o ochrane ľudských práv a základných slobôd z roku 1950 alebo Medzinárodný pakt o občianskych a politických právach z roku 1966. Pojem súkromia sa v nich spájal s rodinným a súkromným životom. S masívnym nástupom informačných technológií v 80. a 90. rokoch 20. storočia sa pojem súkromia obsiahnutý v čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd opätovne stal stredobodom verejnej diskusie.²² V informačnej spoločnosti totiž ochrana

²⁰ WARREN, D. S., BRANDEIS, L. D. The Right to Privacy. In: *Harvard Law Review*, 1890, vol. 4, no. 5. (online). (cit. 2014-12-13). Dostupné z: (<http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>).

²¹ Právo na súkromie bolo spájané s vlastníckym právom. Súkromie tak bolo niečo, čoho sa mohol domáhať iba vlastník. MATEJKA, J. *Internet jako objekt práva: Hledání rovnováhy autonomie a soukromí*. 1. vyd. Praha: CZ.NIC, 2013, s. 35.

²² Dá sa povedať, že v aplikačnej praxi sú obmedzenia, ale aj realizácia práva na súkromie v medziach, ktoré dnes považujeme za tradičné (napr. domové prehliadky), pomerne jednoznačnou

práva na súkromie získavala celkom nové rozmery a špecifiká a bolo by naivné myslieť si, že miera súkromia zostala technickým pokrokom nedotknutá. Postupne sa stierali rozdiely medzi tým, čo považujeme za súkromné a verejné informácie a zákony chrániace súkromie sa ukázali ako nedostatočné kvôli zastaraným koncepciám.

O vytvorenie aplikovateľnej definície práva na súkromie v podmienkach meniacej sa spoločnosti sa snažila už Younger komisia.²³ Z jej správy z roku 1972 vyplýva, že súkromie je vo všeobecnosti právom na nedotknuteľnosť vlastnej osoby, domova, rodiny a vzťahov, ale na druhej strane aj právom na určenie, akým spôsobom a v akom rozsahu sa budú informácie o určitej osobe poskytovať druhým. Problémom je, že z tejto definície nie sme schopní presne určiť, v akom rozsahu máme právo na nedotknuteľnosť osoby, domova, rodiny a podobne, pretože z nej nie je zrejmé, ktoré formy zásahu je možné považovať za porušenie práva na súkromie.

Napriek snahe sa ani Calcuttskej komisii²⁴ nepodarilo spresniť nejasný rozsah čl. 8 Európskeho Dohovoru, čo viedlo k odmietnutiu možnosti formulovať obsah pojmu práva na súkromie. V druhej polovičke deväťdesiatych rokov sa však objavuje inkluzívny prístup k právu na súkromie. Jeho súčasťou sa stalo právo na anonymitu, samotu a diskretnosť, ktoré môžeme považovať za prejavy ochrany osobnosti jednotlivca, jeho nezávislosti, integrity a dôstojnosti.²⁵

1.2.2 Pojem súkromie v súčasnej právnej teórii a judikatúre súdov

Pojem „súkromie“ v súčasnosti nemá explicitnú definíciu,²⁶ o ktorej by v našom právno-kultúrnom prostredí panovala zhoda. V právnej teórii je „súkromie“ významovo otvoreným pojmom. Dôvodom je skutočnosť, že tento pojem je podobný iným právnym pojmom, ako napríklad pojmu spravodlivosti, dôstojnosti a podobne, ktorých spoločným znakom je, že každý pokus o ich jasné a presné vymedzenie sa nevyhne vzniku anomálií. Každá zásada má totiž nejakú výnimku, čo znamená, že pri takých všeobecných právnych pojmoch, medzi ktoré môžeme zaradiť aj súkromie, a ktorých obsah sa zároveň týka hodnotového naladenia na-

záležitosťou. Svedčí o tom aj pomerne stabilná a jednotná prax súdov, ako aj ďalších orgánov aplikačnej praxe.

²³ Report of the Younger Committee on Privacy (1972), Cmnd 5012, s. 10.

²⁴ Report of the Committee on Privacy and Related Matters (1990), Cmnd 1102, s. 7.

²⁵ FORD, M. Two conceptions of Worker Privacy. In: *Industrial Law Journal*, 2002, vol. 31, no. 2, p. 136.

²⁶ KNAPP, V. *Vědecká propedeutika pro právníky*. Praha: Eurolex Bohemia, 2003, s. 178.

šej právnej kultúry, nie je vytvorenie vyčerpávajúcej definície súkromia až takým žiaducim cieľom. Podľa nášho názoru preto určitá časť pojmu súkromia zostane nevyhnutne skrytá a súkromie tak v budúcnosti bude aj naďalej významovo otvoreným pojmom.

Súkromie môžeme chápať v dvojakom zmysle slova. „*V užšom ponímaní ako ochranu subjektívne vytvorenej predstavy o súkromnom živote človeka, v širšom zmysle môže zahŕňať aj ochranu širšieho okolia bezprostredne nadväzujúceho na životné potreby a záujmy danej osoby, ktoré sú spojené s rodinou, priateľmi a pod.*“²⁷

Podľa niektorých názorov tvorí obsah práva na súkromie osoby pozitívna a negatívna zložka. Právo fyzickej osoby rozhodnúť sa podľa vlastného uváženia, či, v akom rozsahu a akým spôsobom majú byť skutočnosti jeho osobného súkromia sprístupnené iným, tvorí pozitívnu zložku. Negatívna zložka pritom zahŕňa právo brániť sa proti neoprávneným zásahom do tejto sféry zo strany iných osôb.²⁸

Z pozitívnej definície vychádza aj Vojčík, keď uvádza, že právo na súkromie spočíva v práve fyzickej osoby rozhodnúť podľa vlastného uváženia, či a v akom rozsahu majú byť skutočnosti z jeho súkromného života sprístupnené iným. Podľa jeho názoru ochrana práva na súkromie zahŕňa sféru súkromného života osobnosti človeka a zároveň jeho intímnej sféry a vnútorného myšlienkového či citového života.²⁹ Postupným vývojom judikatúry ESLP sa pojem súkromie rozširuje z oblasti rodinných a citových vzťahov jednotlivcov až do oblasti pracovnoprávných vzťahov, t. j. na pracoviská, a v súčasnosti pod pojmom súkromie možno chápať aj nedotknuteľnosť obydli, ktoré slúži ako súkromné pracovisko, ochranu listového tajomstva, ale napr. aj profesionálneho tajomstva.

Právo na súkromie sa garantuje len fyzickým osobám a nie právnickým osobám, u ktorých o súkromí či súkromnom živote nemôžeme polemizovať. Z povahy tohto pojmu totiž vyplýva, že napr. v rámci domových prehliadok, v zásade sa môžu týkať iba základné práva a slobody osôb fyzických, nie právnických osôb, hoci môže ísť o ich obchodné aktivity. U právnických osôb by v tejto súvislosti mohlo ísť len o ochranu hospodárskej súťaže či obchodného tajomstva. Tieto práva však nepatria pod ochranu súkromia v zmysle čl. 8 Dohovoru.³⁰

Pojem súkromie sa pokúsili definovať a interpretovať aj vnútroštátne súdy. V uznesení Najvyššieho súdu Slovenskej republiky z 18. februára 2010 sp. zn. 3

²⁷ KLÍMA, K. a kol. *Komentár k Ústavě a Listině*. 2. díl. 2. vyd. Plzeň: Aleš Čeněk, 2009. s. 982.

²⁸ KNAP, K., ŠVESTKA, J., JEHLIČKA, O., PAVLÍK, P., PLECITÝ, V. 2004. *Ochrana osobnosti podle občanského práva*. 4. podstatně přepracované a doplněné vyd. Praha: Linde, 2004. s. 335.

²⁹ VOJČÍK, P. a kol. *Občiansky zákonník. Stručný komentár*. Bratislava: Iura Edition, 2008, s. 56.

³⁰ MATES, P. *Ochrana soukromí ve správním právu*. 2. vyd. Praha: Linde, 2006, s. 21. Porovnaj tiež rozhodnutie Ústavního soudu ČR z 22. marca 1999 sp. zn. IV. ÚS 528/98.

Cdo 137/2008, R 53/2010 sa uvádza, že „právo na súkromie spočíva v práve fyzickej osoby samostatne sa rozhodnúť podľa vlastného uváženia, či a v akom rozsahu majú byť skutočnosti z jej súkromného života prístupné iným alebo zverejnené“. Krajský súd v Trnave v rozhodnutí z 21. mája 2013 sp. zn. 24 Co 101/2013 konštatoval, že „súčasťou súkromného života je nepochybne tiež rodinný život zahrňujúci vzťahy medzi blízkymi príbuznými a rešpektovanie súkromného, teda i rodinného života musí zahrňovať do určitej miery právo na vytváranie a rozvíjanie vzťahov s ďalšími ľudskými bytosťami, aby tak bolo možné, okrem iného, tiež rozvíjať a naplňovať vlastnú osobnosť“. Ústavný súd Slovenskej republiky (ďalej len Ústavný súd SR) v rozhodnutí zo 4. decembra 2007 sp. zn. PL. ÚS. 12/01 dospel k rovnakému názoru, pričom doplnil, že „s takto vymedzenými právami bezprostredne súvisí všeobecný ústavný princíp slobody (čl. 2 ods. 3 ústavy), ktorý, ako už bolo uvedené, je jednou zo základných hodnôt demokratického a právneho štátu a ktorý spočíva v povinnosti štátu rešpektovať a chrániť sféru osobnej autonómie jednotlivca.... Vo vzájomnej spojitosti tak predmetné práva a princípy garantujú istú ‚vnútornú sféru‘, v ktorej môže jednotlivec žiť podľa vlastných predstáv a vylúčiť z nej ‚vonkajší svet‘, a sféru, v ktorej sa môže jednotlivec slobodne rozvíjať, realizovať svoju osobnosť a vstupovať do vzťahov, ako aj rozvíjať vzťahy s inými osobami. Právo na súkromie a na ochranu súkromného života v spojení s princípom slobody, tak v tom najzákladnejšom vymedzení, opierajúc sa aj o základné právo na ľudskú dôstojnosť, garantuje jednotlivcovi možnosť autonómneho sebaurčenia“. Môžeme konštatovať, že v rámci judikatúry slovenských všeobecných súdov a Ústavného súdu SR sú limity a obmedzenia súkromia stanovené tým, že do súkromia patrí všetko to, čo nie je človek povinný sprístupniť alebo prezradiť inému. Právo na súkromie je preto sférou, v ktorej sa jednotlivec na základe vlastného slobodného uváženia môže rozhodnúť, ktoré informácie sprístupní inému buď fyzicky (resp. priamo), alebo ho o tom informuje (resp. informáciu sprostredkuje).³¹

Otázkou ochrany súkromia vo vzťahu k rodinným príslušníkom v spojení s ochranou osobnosti fyzickej osoby (aj po smrti) a práva na život sa zaoberal aj Ústavní soud České republiky (ďalej len „Ústavní soud ČR“) vo svojom náleze z 20. mája 2002 sp. zn. IV ÚS 315/01, keď riešil súbeh trestnoprávnej zodpovednosti s občianskoprávnou zodpovednosťou za porušenie práva na ochranu osobnosti, pričom vymedzil aj rozsah pojmu „súkromie“. Dospel pritom k záveru, že v tomto prípade bola jednak zo strany sťažovateľa (žalovaného) naplnená skutková podstata trestného činu ublíženia na zdraví s následkom smrti syna žalobcov a taktiež došlo k neoprávnenému zásahu do práva žalobcov ako vedľajších účastníkov konania na ochranu osobnosti pred ústavným súdom.

³¹ PAVLÍČEK, V. a kol. Ústava a ústavní řád České republiky: komentář. 2. vyd. Praha: Linde, 1999, s. 112.

Ústavní soud ČR v tomto zmysle konštatoval, že „*súkromie osoby nemožno obmedziť iba na slobodné rozhodovanie fyzickej osoby o sprístupňovaní skutočností týkajúcich sa jej súkromia iným osobám na ochranu proti neoprávneným zásahom do tohto oprávnenia*“. Z citovaných dokumentov je zrejmé, že Ústavní soud ČR s odkazom na judikatúru ESLP a na jeho interpretáciu čl. 8 Dohovoru dospel k obdobnému záveru ako slovenské súdy. Pojem súkromie a súkromný život osoby nie je možné odtrhnúť od vzťahov, ktoré si jednotlivec vytvára s ďalšími ľudskými bytosťami. Pojem súkromie preto zahŕňa aj rodinný život a vzťahy s blízkymi príbuznými.

Na druhej strane môžeme v rozhodovacej činnosti súdov pozorovať pokusy o negatívne vymedzenie pojmu súkromie, t. j. čo sa za súkromie nepovažuje. V tejto súvislosti možno spomenúť rozhodnutie Ústavního soudu ČR z 31. marca 2009 sp. zn. I. ÚS. 452/09, ktorého obsahom je práve negatívne definovanie pojmu „súkromia“ a je zaujímavé v tom, že sa týka pracovnoprávných vzťahov. V predmetnej rozhodovanej veci dospel k záveru, že nemožno z práva na ochranu súkromia v osobnej a rodinnej sfére odvodzovať automaticky aj právo na ochranu súkromia vo sfére pracovnej. V odôvodnení uviedol, že „*právo na ochranu pred neoprávnenými zásahmi do súkromia sa spravidla vzťahuje na prípady zásahov do súkromnej a rodinnej sféry, v ktorých jednotlivec prejavuje svoju osobnosť slobodne a autonómne. V tejto sfére sa však neocitá v situácii, kedy v prostredí zamestnávateľa vystupuje a plní funkcie pracovného charakteru. Rovnako potom listové tajomstvo, tajomstvo iných písomností a záznamov, tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením nemožno vzťahovať na činnosť, ktorá má byť svojou povahou činnosťou pracovnou*“.

Základom obsahového vymedzenia pojmu „právo na súkromie“ v právnej teórii, ale aj právnej praxi na medzinárodnej i vnútroštátnej, je najčastejšie judikatúra ESLP. V rozhodovacej činnosti ESLP možno pozorovať tri roviny chápania predmetného pojmu, ktoré sú prejavom tzv. súkromného života jednotlivca:

Prvou rovinou je sloboda rozhodovať sa o svojom vlastnom tele. Sem patrí napr. právo na zmenu pohlavia.³²

Druhou rovinou je ochrana súkromnej sféry. Podľa Barancovej sa práve táto rovina najviac týka pracovnoprávných vzťahov,³³ pretože sem zaraďujeme najmä ochranu jednotlivcov pri ich individuálnej komunikácii s inými.³⁴

³² Rozhodnutie ESLP z 11. júla 2002 v právnej veci Goodwin v. Spojené kráľovstvo, sťažnosť č. 28957/95.

³³ BARANCOVÁ, H. Monitorovanie zamestnancov a ochrana súkromného života v judikatúre európskych súdov. In: BARANCOVÁ, H. a kol. *Monitorovanie zamestnancov a právo na súkromný život*. Bratislava: Sprint dva, 2010, s. 19.

³⁴ Rozsudok ESLP zo 6. septembra 1978 v právnej veci Klass a i. v. Nemecko, sťažnosť č. 5029/71.

Tretou rovinou je právo na slobodný životný štýl,³⁵ ktoré súvisí s povinnosťou zamestnávateľa rešpektovať prejavy zamestnancov v obliekaní, v úprave vzhľadu či také prejavy zamestnancov, ktoré vyplývajú z ich náboženského presvedčenia alebo z ich príslušnosti k etnickej alebo národnostnej skupine.

Právom na súkromný život sa zaoberal EŠLP v rozhodnutí zo 16. decembra 1992 v právnej veci **Niemietz v. Nemecko**³⁶, v ktorom dospel k záveru, že **nie je možné, ani nevyhnutné pokúšať sa o vyčerpávajúcu definíciu pojmu „súkromný život“**. Dôvodil, že by bolo *príliš reštriktívne obmedzovať tento pojem na „vnútorný kruh“, v rámci ktorého môže jednotlivec žiť svoj vlastný osobný život podľa svojej vôle a úplne z neho vylúčiť vonkajší svet nezahrnutý do tohto kruhu. Rešpektovanie súkromného života do určitej miery zahŕňa právo na vytváranie a rozvíjanie vzťahov s ďalšími ľudskými bytosťami. Potom tiež neexistuje dôvod pre to, aby z pojmu „súkromný život“ bola vylúčená aktivita profesijnej alebo obchodnej povahy, pretože práve počas svojej pracovnej činnosti má väčšina ľudí značnú, ak nie najväčšiu príležitosť rozvíjať vzťahy s vonkajším svetom*.

Zo skutkových okolností prípadu ďalej vyplýva, že sťažovateľ Niemietz namietal, že bolo porušené jeho právo na rešpektovanie nedotknuteľnosti obydľia a korešpondencie v zmysle čl. 8 Dohovoru a bolo taktiež poškodené dobré meno jeho advokátskej kancelárie, aj jeho povest' ako advokáta. Nemecká vláda na druhej strane tvrdila, že čl. 8 Dohovoru neposkytuje aj ochranu kancelárskym priestorom pred prehliadkou. Argumentovala ďalej, že je nevyhnutné rozlišovať na jednej strane medzi súkromným životom a obydľím a na druhej strane profesijným alebo obchodným životom a miestnosťami, kde sa činnosti tejto povahy uskutočňujú. V tomto rozhodnutí EŠLP extenzívnym výkladom dospel k záveru, že právo na súkromie v sebe zahŕňa aj právo na vytvorenie a rozvíjanie vzťahov s inými ľuďmi na pracovisku, ktoré tvoria profesionálny život jednotlivca. Zároveň konštatoval porušenie čl. 8 Dohovoru, ku ktorému došlo neoprávneným zásahom do súkromného života sťažovateľa vykonaním prehliadky jeho advokátskej kancelárie. Z koncepcie súkromia, ktorá bola sformulovaná v prípade Niemietz v. Nemecko, ako aj ďalších podobných rozhodnutiach EŠLP, vyplýva, že pracovný život je dôležitým a centrálnym aspektom súkromného života a patrí pod pojem súkromia ako takého.³⁷ Tento názor zaujal z pochopiteľných dôvodov. Môžu totiž celkom ľahko vzniknúť situácie, v ktorých by sme nedokázali rozlíšiť, ktoré

³⁵ BARANCOVÁ, H. a kol. *Základné práva a slobody v pracovnom práve*. Plzeň: Aleš Čeněk, 2012, s. 107.

³⁶ Rozsudok EŠLP zo 16. decembra 1992 v právnej veci Niemietz v. Nemecko, sťažnosť č. 13710/88.

³⁷ Obdobne v rozsudku zo 16. februára 2000 v právnej veci Amann v. Švajčiarsko, sťažnosť č. 27798/95, EŠLP uviedol pri definovaní tohto pojmu, že „neexistuje žiadny zásadný dôvod na ospravedlnenie vylúčenia činnosti profesijnej alebo obchodnej povahy z pojmu súkromný život“.

činnosti jednotlivca tvoria jeho súkromný a ktoré profesijný život, pretože činnosť spojená s povoláním či obchodovaním sa môže vykonávať aj v súkromnom obydľí. Ak by teda súd nepristúpil ku komplexnému chápaniu pojmu súkromie a jeho rozšíreniu aj na aspekty jeho profesijného či obchodného života, mohlo by to viesť k nerovnakému zaobchádzaniu. Ochrana súkromného života v najširšom význame, t. j. aj vrátane ochrany súkromia v súvislosti s profesionálnou činnosťou, by sa potom neposkytovala v zmysle Dohovoru tým fyzickým osobám, ktorých profesionálne a súkromné činnosti by boli vzájomne previazané do takej miery, že by neexistoval reálny spôsob, ako ich diferencovať (t. j. určiť hranice medzi súkromným a pracovným životom).

ESLP vo veci **X. a Y. v. Holandsko** zaujal aj postoj vo vzťahu k právu jednotlivca voliť si jemu vyhovujúci spôsob sexuálneho života. ESLP sa jasne vyjadril, že právo na slobodu sexuálneho života je dôležitou súčasťou práva na súkromie, pretože je neodmysliteľnou súčasťou nadväzovania a rozvíjania vzťahov s inými jednotlivcami.³⁸

Ďalším zaujímavým rozhodnutím týkajúcim sa ochrany súkromia je **Halford v. Spojené kráľovstvo**.³⁹ Sťažovateľka, ktorá pracovala ako asistentka policajného riaditeľa, v sťažnosti namietala, že jej telefonické hovory uskutočnené z domáceho i pracovného telefónu boli odpočúvané. Informácie získané odpočúvaním oboch telefonických zariadení mali byť podľa jej presvedčenia použité proti nej v prebiehajúcom pracovnoprávnom spore so zamestnávateľom. ESLP v tejto veci dospel k názoru, že telefonické hovory sťažovateľky z jej domácnosti aj zo zamestnania možno podriaďiť pod pojem „súkromný život“ a „korešpondencia“ v súlade s čl. 8 Dohovoru. Záverom ESLP konštatoval, že vzhľadom na to, že sťažovateľku zamestnávateľ neupozornil na možnosť odpočúvania telefonických hovorov, išlo vzhľadom na jej legitímne očakávania nepochybné o neoprávnený zásah do jej súkromného života.

Súkromie bolo aj ústrednou témou rozhodnutia ESLP vo veci **Copland v. Spojené Kráľovstvo**,⁴⁰ pričom jeho postoj ku chápaniu tohto pojmu už nevyznel jednoznačne v prospech zamestnanca. Zo skutkových okolností prípadu je zrejmé, že zamestnávateľ nariadil monitorovanie telefonických hovorov sťažovateľky, ktorá bola zamestnaná ako asistentka riaditeľa vzdelávacej inštitúcie. Okrem toho nariadil aj sledovanie jej elektronickej pošty a pohybu na internete. Nesledoval však obsah komunikácie, ale záznamy o komunikácii uskutočnené prostredníc-

³⁸ Rozsudok ESLP z 26. marca 1985 v právnej veci X. a Y. v. Holandsko, sťažnosť č. 8978/80.

³⁹ Rozsudok ESLP z 25. júna 1997 v právnej veci Halford v. Spojené kráľovstvo, sťažnosť č. 20605/92.

⁴⁰ Rozsudok ESLP z 3. apríla 2007 v právnej veci Copland v. Spojené kráľovstvo, sťažnosť č. 62617/00.

tvom telekomunikačných zariadení (výpisy volaných čísel, odosielateľov e-mailov). EŠLP po preskúmaní danej veci konštatoval, že pod pojem súkromný život a korešpondencia v zmysle čl. 8 ods. 1 Dohovoru možno subsumovať okrem telefonických hovorov aj používanie elektronickej pošty a internetu. Uviedol, že hoci zhromaždené údaje sa ďalej nevyužívali, už samo zhromažďovanie dát môže byť kvalifikované ako zásah do súkromného života. Podľa jeho názoru v čase zásahu do súkromia sťažovateľky neboli u zamestnávateľa právne zakotvené podmienky legálneho monitorovania telefonických hovorov a využívania internetu interným predpisom alebo všeobecne záväzným predpisom, preto došlo k porušeniu práva garantovaného čl. 8 Dohovoru. Pripustil však, že v niektorých špecifických situáciách, najmä ak je to nevyhnutné na dosiahnutie legitímnych cieľov, môže byť zásah do súkromia akceptovateľný.

Zásah do súkromia sťažovateľa prostredníctvom kamerového systému s vyhotovením záznamu prešetroval EŠLP v právnej veci **Perry v. Spojené kráľovstvo**.⁴¹ Policajný orgán vyhotovil záznam sťažovateľa počas jeho pobytu na policajnej stanici s cieľom uskutočniť rekogníciu v trestnom konaní, na základe ktorej sťažovateľa svedkovia identifikovali. Súd rozhodnutie založil na názore, že sledovanie osoby na verejnom mieste (akým je napr. nákupné centrum alebo aj policajná stanica) použitím vizuálneho zariadenia, ktoré nevyhotovuje záznam, nie je zásahom do súkromia v zmysle čl. 8 Dohovoru, na rozdiel od nepretržitého či systematického vyhotovovania záznamu umožňujúceho úplnú identifikáciu sledovanej osoby. EŠLP v danej veci dospel k záveru, že policajný orgán nepostupoval v súlade s vnútroštátnou právnou úpravou, keď vyhotovil záznam a použil ho na účely rekognície bez toho, aby získal predchádzajúci súhlas sledovaného alebo ho informoval o vytvorení a použití záznamu a poučil ho o jeho právach.

V prípade **Uzun v. Nemecko**⁴² bol predmetom skúmania zásah do práva na súkromie sledovaním pohybu a aktuálnej polohy fyzickej osoby. Sťažovateľ ako podozrivý z páchania teroristickej trestnej činnosti bol monitorovaný okrem bežných sledovacích zariadení (kamier, telefónov, elektronickej pošty) aj prostredníctvom zariadenia GPS (Global Positioning System). Keďže informácie získané z dôkazných prostriedkov boli použité proti nemu v trestnom konaní, sťažovateľ namietal porušenie jeho práva na rešpektovanie súkromného života v zmysle čl. 8 Dohovoru. EŠLP síce konštatoval, že uvedeným postupom bolo porušené jeho právo na súkromie, ale s poukazom na čl. 8 ods. 2 Dohovoru argumentoval odôvodnením, že sledovanie pomocou GPS, aj vzhľadom na charakter pácha-

⁴¹ Rozsudok EŠLP zo 17. júla 2003 v právnej veci Perry v. Spojené kráľovstvo, sťažnosť č. 63737/00.

⁴² Rozsudok EŠLP z 2. septembra 2010 v právnej veci Uzun v. Nemecko, sťažnosť č. 35623/05.

nej trestnej činnosti bolo nevyhnutné v demokratickej spoločnosti a primerané sledovaným legitímnym cieľom.

Podľa judikatúry ESLP je právo na ochranu osobných údajov obsahovou súčasťou práva na súkromný život (práva na ochranu súkromnej sféry).⁴³ V rozhodnutí ESLP v právnej veci **Rotaru v. Rumunsko** sa sťažovateľ domáhal náhrady nemajetkovej ujmy spôsobenej nepravdivými informáciami⁴⁴ o členstve sťažovateľa v politickom fašistickom hnutí z tajného spisu Rumunskej spravodajskej služby (ďalej len „RIS“). Aj keď vnútroštátny odvolací súd dospel k záveru, že uvedené údaje o sťažovateľovi nie sú pravdivé, nepovažoval jeho uplatnený nárok za dôvodný, keďže zo strany RIS podľa jeho názoru nedošlo k zásahu do práva sťažovateľa na súkromie. Dôvodil, že táto inštitúcia je len subjektom uchovávajúcim nepravdivé osobné údaje. Napokon v konaní pred ESLP sťažovateľ namietal, že RIS môže kedykoľvek použiť informácie o jeho súkromnom živote, ktoré sú nepravdivé a hanlivé, a domáhal sa uznania a vyslovenia porušenia čl. 8 Dohovoru. Rumunská vláda poprela možnosť aplikácie uvedeného článku s odôvodnením, že informácie v spise RIS sa netýkajú sťažovateľovho súkromného života, ale jeho verejného života s prihliadnutím na jeho rozhodnutie angažovať sa v politickom živote. ESLP s poukazom na závery zaujaté v rozhodnutí v právnej veci *Niemietz v. Nemecko* uviedol, že spis RIS obsahoval rôzne informácie o živote sťažovateľa, hlavne o jeho štúdiu, politickej činnosti a záznamoch v registri trestov. Konštatoval, že ak sa tieto informácie (resp. osobné údaje) systematicky zhromažďujú a uchovávajú v spise vedenom štátnymi agentmi, patria pod rozsah pojmu súkromný život v zmyslu čl. 8 Dohovoru, a hoci boli v tomto prípade niektoré z nich oficiálne uznané za nepravdivé, mohli poškodiť dobrú povesť sťažovateľa. Dospel k názoru, že štát porušil čl. 6, 8 aj 13 Dohovoru najmä tým, že vnútroštátna právna úprava dostatočne neupravovala rozsah a spôsob výkonu moci verejnými orgánmi (RIS) a neumožňovala napadnúť zhromažďovanie ani nepravdivosť takýchto informácií patriacich do sféry súkromného života jednotlivca. Obsahu pojmu osobný údaj sa budeme venovať v ďalších častiach práce.

Z hľadiska judikatúry štrasburských orgánov ochrany práva patrí pod právo na súkromný život najmä:

- a) zákaz zhromažďovania a úschovy osobných údajov,
- b) práva spojené s menšinovou sexuálnou orientáciou,
- c) právo na ochranu obydlia a domová sloboda,⁴⁵

⁴³ Rozsudok ESLP zo 16. februára 2000 v právnej veci *Amann v. Švajčiarsko*, sťažnosť č. 27798/95, rozsudok ESLP zo 4. mája 2000 v právnej veci *Rotaru v. Rumunsko*, sťažnosť č. 28341/95, Rozsudok ESLP z 2. augusta 1984 v právnej veci *Malone v. Spojené Kráľovstvo*, sťažnosť č. 8691/79.

⁴⁴ V rozhodnutí namiesto pojmu „osobný údaj“ používa ESLP pojem „informácie“.

⁴⁵ Pojmy súkromný život a obydlie podľa čl. 8 ods. 1 Dohovoru treba vykladať ako miesta zahŕňajúce

- d) právo na ochranu korešpondencie a tajomstva dopravovaných správ,
- e) právo na ochranu životného prostredia.⁴⁶

Vzhľadom na vyššie uvedené rozhodnutia ESĽP možno zhrnúť, že vytvorenie vyčerpávajúcej definície „súkromia“ na základe tejto judikatúry sa dá len veľmi ťažko realizovať, ak nie je celkom nereálne. Hoci sme si stanovili najskôr cieľ definovať pojem „súkromie“, dospeli sme k záveru, že sa môžeme pokúsiť len o priblíženie charakteru tohto osobnostného práva. Právo na súkromný život totiž zahŕňa širokú oblasť záujmov jednotlivca a prakticky neobmedzenú škálu možných zásahov do tohto práva. Celú situáciu pritom komplikuje ešte aj fakt, že spoločnosť sa neustále vyvíja. V informačnom veku sa objavujú nové možnosti otvárajúce cesty novým spôsobom, ako sa dá zasiahnuť do súkromia jednotlivca. V súčasnosti preto môžeme pozorovať skôr tendencie tento pojem rozširovať a vyladať extenzívne, tak aby obsiahol čo najviac prípadov, keď dochádza k zásahom do súkromnej sféry jednotlivcov. Považujeme to za správne, hoci si myslíme, že ochrana nesmie byť neprimeraná a v každom jednotlivom prípade treba starostlivo skúmať a definovať jej medze, aby nedochádzalo k poškodzovaniu a porušovaniu základných práv iných osôb. ESĽP preto vo svojich rozhodnutiach pripúšťa aj opatrenia nevyhnutné na bránenie ich majetkových práv, ktoré je zamestnávateľ oprávnený vykonať, rešpektujúc zásadu legality a legitimacy.

1.2.3 Vzájomný vzťah práva na súkromie a vlastníckeho práva

Pri skúmaní problematiky pojmu súkromie sa stretávame z historického hľadiska často s otázkami a úvahami, či má byť súkromie jedného človeka chránené menej alebo rovnako ako vlastnícke právo iného človeka, s ktorým sa ocitá právo na súkromie v kolízii. Analogicky sa táto kontroverzná otázka vynára aj v prostredí pracovnoprávných vzťahov. Preto považujeme za potrebné načrtnúť v práci aj túto problematiku, s ktorou je spojených viacero kontroverzných otázok a snažíme sa aj pomocou historických súvislostí hľadať riešenie sporu, ak dochádza ku kolízii práva na súkromie zamestnanca s vlastníckym právom zamestnávateľa.

Historicky bolo právo na súkromie vždy spojené s ochranou súkromného vlastníctva. Ich vzájomnosť položila základy toho, čo dnes vnímame ako rozdiel medzi súkromným a verejným priestorom. Vlastníctvo bolo dokonca dôvodom,

ňajúce aj miesta profesijnej či komerčnej aktivity. Pozri ČAPEK, J. *Evropská úmluva o ochraně lidských práv a základních svobod*. I. část. Linde, 2010, s. 283.

⁴⁶ SVÁK, J. *Ochrana ľudských práv. Z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práv*. II. rozšírené vydanie. Bratislava: Eurokódex, 2006, s. 592.

prečo sa sféra ochrany súkromia, a v jej rámci právo na súkromný a rodinný život ocitli za akousi bariérou, pretože súkromie začalo byť vnímané ako priestor, do ktorého štát nemohol svojvoľne zasahovať. Problém sa však objavil vtedy, keď právo na súkromie kolidovalo s vlastníckym právom, keď sa hodnoty a princíp nedotknuteľnosti vlastníctva dostali do sporu s hodnotami a princípom nedotknuteľnosti súkromia.

Uvedený spor sa nepochybne týka aj oblasti pracovnoprávných vzťahov. Extrémnym príkladom je obdobie 19. storočia vo Veľkej Británii, keď zamestnávateľia hrubým spôsobom zasahovali do života svojich zamestnancov tým, že sa snažili kontrolovať ich súkromie.⁴⁷ Išlo predovšetkým o sluhov v domácnosti, resp. v prostredí strednej Európy o čeladníkov, ktorí sa nemohli bez povolenia gazdu (zamestnávateľa) vzdialiť z domu alebo pozemku alebo prijímať návštevy.⁴⁸ Súkromie čelade tak na pozemku a v dome gazdu prakticky neexistovalo, pretože súkromné záujmy čelade boli takmer úplne podrobené vôli ich zamestnávateľa. Tento stav bol spôsobený hlavne tým, že právo gazdu kontrolovať život svojich zamestnancov bolo odvodené z jeho vlastníckeho práva domu alebo pozemku, na ktorom čelad' vykonávala prácu. V podstate to znamenalo, že právo na súkromie mal v tom období len ten, kto bol zároveň aj vlastníkom, keďže vtedajšia právna úprava nepamätala pri ochrane súkromia aj na nevlastníkov.

Od 19. storočia nastal výrazný posun v oblasti ochrany súkromia zamestnanca. V európskych podmienkach právna úprava osciluje medzi dvoma základnými koncepciami. Prvá je založená na názore, že právo vlastníť súkromný majetok je pojmom širším, základnejším a originálnejším, z ktorého je právo na súkromie len odvodené. Opačný názor predstavuje koncepcia, že právo na súkromie je rovnako ako vlastnícke právo neodňateľným základným ľudským právom a slobodou, dokonca má silnejšie postavenie. K druhej spomenutej koncepcii sa prikláňa aj väčšina názorov súčasnej slovenskej a českej právnej teórie. Podľa niektorých názorov právnych vedcov je právo na ochranu súkromia z hľadiska štruktúry právneho systému právom vyššie postaveným než právo na ochranu majetku (vlastníctva).⁴⁹

Úprava vzťahu ochrany osobnosti a vlastníctva v Slovenskej republike je v Občianskom zákonníku konformná s Ústavou Slovenskej republiky aj medzinárod-

⁴⁷ PROST, A., VINCENT, G. *History of Private Life Volume V: Riddles of Identity in Modern Times*. Cambridge: Harvard University Press, 1991, s. 31 – 36.

⁴⁸ Pozri k tomu bližšie MOSNÝ, P. a kol. *Právno-historická realita sociálnej doktríny 20. storočia*. Kraków: Spolok Slovákov v Poľsku – Towarzystwo Słowaków w Polsce, 2014, s. 76 – 77.

⁴⁹ Porovnaj napr. MORÁVEK, J. Možnosti monitorování zaměstnanců na pracovišti v právním řádu České republiky. In: BARANCOVÁ, H. a kol. *Monitorovanie zamestnancov a právo na súkromný život*, Bratislava: Sprint dva, 2010, s. 45. Tiež ELIÁŠ, K. a kol. *Občianský zákonník – Veľký akademický komentár*. Praha: Linde, 2008, s. 92.

nými dokumentmi. Z ustanovenia § 1 ods. 1 platného Občianskeho zákonníka vyplýva, že „*úprava občianskoprávných vzťahov prispieva k napĺňaniu občianskych práv a slobôd, najmä ochrany osobnosti a nedotknuteľnosti vlastníctva*“. Z hľadiska gramatického i systematického výkladu citovaného ustanovenia ochrana osobnosti predchádza ochrane vlastníckeho práva, preto by sa mala chrániť vždy na prvom mieste. Ochrana osobnosti je pritom spojená s vymedzením pojmu súkromie, a tým aj s právom na súkromie.

Nadradenosť práva na súkromie je viditeľná predovšetkým v pracovnoprávnej úprave, kde sa najmä pod vplyvom európskeho práva dostáva do popredia ochrana práva na súkromie zamestnanca pred ochranu vlastníckeho práva zamestnávateľa. V praxi sa však objavujú tendencie, ktorých cieľom je dosiahnuť čo najväčšiu možnú ochranu vlastníckeho práva zamestnávateľa. Môžeme sa stretnúť s tým, že zamestnávateľa prostredníctvom „individuálne dohodnutých“ podmienok v pracovnoprávnej zmluve využívajú postavenie zamestnanca, ktorý je pri vyjednávani slabšou zmluvnou stranou v pracovnoprávnom vzťahu. Ich konanie pritom často vychádza z nesprávnej analýzy a interpretácie občianskoprávných a pracovnoprávných noriem o ochrane súkromia zamestnanca.

Relevantnej právnej úprave ochrany súkromia sa síce venujeme až v druhej kapitole práce, no na základe predchádzajúceho výkladu sa prikláňame ku koncepcii, ktorá považuje právo na ochranu osobnosti a súkromia každej fyzickej osoby, t. j. aj zamestnanca, za osobitné ústavné a občianske právo, ktoré je aj v pracovnoprávných vzťahoch nadradené ochrane vlastníckeho práva zamestnávateľa. Zastávame názor, že právo na súkromie je najrozsiahljším a aj najuniverzálnejším osobnostným právom, pretože v prípade zásahov do práva na súkromie dochádza k zásahom aj do ostatných osobnostných práv. Ak chceme teda chrániť osobnosť jednotlivca, musíme chrániť aj jeho súkromie. Jedno bez druhého nemôže existovať.

Vzhľadom na uvedené sa právo na súkromie osoby môže ľahko ocitnúť v kolízii s vlastníckym právom inej osoby. Ak vznikne takáto situácia, pri hľadaní jej optimálneho riešenia nesmieme zabúdať na prísne dodržanie zásady legality, legitimity i proporcionality, čo by v konečnom dôsledku malo nastoliť dlhodobo udržateľný stav aspoň čiastočnej rovnováhy medzi ochranou súkromia a vlastníctva. Proporcionality nám totiž znemožňuje, aby sme pri hľadaní konečnej odpovede na otázku, ktoré z dvoch práv si zasluhuje väčšiu ochranu, uprednostnili iba jedno z nich.

2. PRAMENE PRÁVNEJ ÚPRAVY OCHRANY SÚKROMIA A OSOBNÝCH ÚDAJOV ZAMESTNANCA

Princíp ochrany osobnosti, jej súkromia a osobných údajov je zakotvený v medzinárodných zmluvách a im zodpovedajúcich právnych aktoch na európskej úrovni, ktoré tvoria ideový a normatívny základ každej vnútroštátnej právnej úpravy. Sú vyjadrením prirodzene právnych hodnôt medzinárodného spoločenstva, ktoré sa zohľadňujú pri tvorbe, aplikácii a výklade právnych predpisov s cieľom zachovania zmyslu a účelu tohto hodnotového rámca.

2.1 Pramene medzinárodnej a európskej právnej úpravy

Za základný dokument medzinárodnej ochrany súkromia a osobných údajov sa považuje **Všeobecná deklarácia ľudských práv** (ďalej len „Deklarácia“), ktorá je pre členov medzinárodného spoločenstva záväzná ako súčasť obyčajového všeobecne platného medzinárodného práva.⁵⁰ Bola prijatá 10. decembra 1948 v New Yorku. Z jej obsahového znenia, vo vzťahu k ochrane súkromia a osobných údajov, sú podstatné najmä ustanovenia, týkajúce sa ochrany ľudskej dôstojnosti, ochrany osobnosti a práva na uspokojivé pracovné podmienky. Okrem záväzných ustanovení, ktoré majú normatívny význam, je z hľadiska interpretácie a lepšieho chápania dôvodov a cieľov tohto aktu dôležité spomenúť aj Preambulu Deklarácie. Valné zhromaždenie Organizácie spojených národov v nej vyhlásilo, že *„uznanie prirodzenej dôstojnosti a rovných a neodňateľných práv všetkých členov ľudskej rodiny je základom slobody, spravodlivosti a mieru vo svete... a „národy Organizácie Spojených národov znovu potvrdili v Charte svoju vieru v základné ľudské práva, v dôstojnosť a hodnotu ľudskej osobnosti, ako aj v rovné práva žien a mužov a rozhodli sa podporovať sociálny rozvoj a lepšie životné podmienky vo väčšej slobode“*. V rámci normatívnej časti možno nadviazať na preambulu priamo prostredníctvom čl. 12 Deklarácie, ktorý ustanovuje, že *„nikto nesmie byť vystavený svojvoľ-*

⁵⁰ ŠTURMA, P. *Mezinárodní a evropské kontrolní mechanismy v oblasti lidských práv*, 3. vydanie, Praha: C. H. Beck, 2011, s. 27.

nému zasahovaniu do súkromia, rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na právnu ochranu proti takýmto zásahom alebo útokom“. Toto ustanovenie súvisí aj s čl. 3, v ktorom sa uvádza, že „každý má právo na život, slobodu a osobnú bezpečnosť“, pretože vo vzájomnom spojení vytvárajú obsahový rámec práva každého jednotlivca žiť život, podľa vlastných predstáv bez zásahov do jeho súkromia s výnimkou prípadov, ktoré odôvodňujú uprednostnenie silného verejného záujmu vyjadreného právnymi predpismi na úrovni zákona. Vo vzťahu k ochrane vlastníckeho práva zamestnávateľa ustanovuje čl. 17, že „každý má právo na vlastný majetok tak sám, ako aj v spoločnosti s inými a nikto nesmie byť svojvoľne zbavený vlastného majetku“. Významné je vyhlásenie v čl. 29 Deklarácie, vyjadrujúce podstatu slobody moderného človeka⁵¹ „každý má povinnosti voči spoločnosti, v ktorej jedine môže slobodne a plne rozvinúť svoju osobnosť“ a v ďalšom odseku „pri výkone vlastných práv a slobôd môže byť každý podrobený iba takým obmedzeniam, ktoré sú zákonom stanovené výhradne na to, aby bolo zabezpečené plné uznanie a rešpektovanie práv a slobôd iných a aby bolo vyhovené spravodlivým požiadavkám morálky, verejného poriadku a všeobecného blaha v demokratickej spoločnosti“.

Z prameňov medzinárodného práva zohráva dôležitú úlohu **Medzinárodný pakt o občianskych a politických právach** (ďalej len „prvý Pakt“) a **Medzinárodný pakt o hospodárskych, sociálnych a kultúrnych právach** (ďalej len „druhý Pakt“), ktoré boli prijaté Valným zhromaždením Organizácie spojených národov 16. decembra 1966 a podpísané Československou socialistickou republikou 7. októbra 1976.⁵² Vychádzajú a zároveň konkretizujú ustanovenia Všeobecnej deklarácie ľudských práv, preto je nevyhnutné chápať ich obsahový význam v spojení so Všeobecnou deklaráciou ľudských práv a Chartou OSN. Ide o zmluvy vytvárajúce spektrum základných ľudských práv a slobôd na medzinárodnej úrovni, pretože ich obsahom je právne zakotvenie občianskych, politických, hospodárskych, sociálnych a kultúrnych práv, ktoré uznalo medzinárodné spoločenstvo a majú relevanciu aj k analyzovanej problematike ochrany súkromia a osobných údajov. Spoločnou črtou oboch paktov je v preambulách obsiahnutá deklarácia, že pôvod všetkých v nich uvedených práv sa odvodzuje od prirodzenej dôstojnosti ľudskej bytosti.

V ustanovení čl. 16 Medzinárodný pakt o občianskych a politických právach zakotvuje právo každého jednotlivca na uznanie jeho právnej osobnosti.⁵³ Zo

⁵¹ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 85.

⁵² Oznámenie Ministerstva zahraničných vecí ČSSR č. 120/1976 Zb.

⁵³ Čl. 16 Medzinárodného paktu o občianskych a politických právach: „Každý má právo na to, aby bola všade uznávaná jeho právna osobnosť.“

znenia čl. 12 Deklarácie vychádza aj čl. 17 prvého Paktu, ktorý je takmer identický.⁵⁴ Právo na osobnosť nie je priamo v tomto medzinárodnom dokumente zakotvené, ale prostredníctvom čl. 16 a čl. 17 garantuje ochranu osobnosti vo všetkých právnych vzťahoch. Ochrana je zabezpečená však len vo vzťahu k tzv. právnej osobnosti, čo znamená, že musí ísť o fyzickú osobu, ktorej právny poriadok priznáva spôsobilosť na práva a povinnosti, a teda disponuje právnou subjektivitou.⁵⁵ Keďže právnická osoba nemá osobnosť, je zrejme, že pod pojem právna osobnosť v zmysle tohto ustanovenia nespadá aj právnická osoba, hoci aj táto môže disponovať právami obdobnými osobnostným právam (napr. právom na dobrú povesť alebo právom na názov) a môže sa domáhať ich ochrany.⁵⁶ V oboch paktoch sú práva zodpovedajúce jednotlivým stránkam osobnosti jednotlivca zakotvené v samostatných článkoch bez určitej nadväznosti, čo vedie k záveru, že osobnostné práva sú svojou povahou samostatnými osobnostnými právami, ktoré navzájom prispievajú k ochrane jednotlivých stránok osobnosti.

S cieľom zabezpečiť medzinárodnú ochranu osobných údajov zamestnancov vydala Medzinárodná organizácia práce, ktorej snahou je vo všeobecnosti zlepšenie pracovných podmienok a sociálneho zabezpečenia pre jednotlivcov, zamestnávajúcich na celom svete, **Kódex ochrany osobných údajov zamestnancov** (ďalej len „Kódex“), ktorý v čl. 1 „*upravuje využívanie osobných údajov zamestnancov za účelom ochrany dôstojnosti zamestnancov a ochrany ich súkromia*“. Pritom za zamestnanca považuje aj bývalého zamestnanca a uchádzača o zamestnanie (čl. 3 Kódexu). Kódex zakotvuje aj zásady, ktoré sčasti korešpondujú s ustanoveniami čl. 6 Smernice č. 95/46/ES. Zakazuje, aby výkonnosť zamestnanca bola hodnotená len na základe osobných údajov zhromaždených prostredníctvom elektronického sledovania (čl. 5 ods. 6) alebo, aby sa zamestnanci vzdali práv na ochranu súkromia (čl. 13). Ustanovuje, že zamestnanec nie je povinný uvádzať pravdivé údaje, ak zamestnávateľ zisťuje citlivé údaje alebo kladie otázky, ktoré sú v rozpore s niektorými zásadami uvedenými v Kódexe (čl. 6 ods. 8).⁵⁷

V európskom priestore zohráva dôležitú ak nie významnejšiu úlohu medzinárodný právny akt prijatý na pôde Rady Európy. Je ním **Dohovor o ochrane**

⁵⁴ Čl. 17 Medzinárodného paktu o občianskych a politických právach: „*Nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromného života, do rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na zákonnú ochranu proti takýmto zásahom alebo útokom.*“

⁵⁵ K pojmu právna subjektivita bližšie pozri DULAKOVÁ JAKÚBEKOVÁ, D. Subjektívne práva a povinnosti In: LAZAR, J. a kol. *Občianske právo hmotné. I. diel.* Bratislava: Iura Edition, 2010, s. 152 – 153.

⁵⁶ KIRSTOVÁ, K. Ochrana osobnosti fyzickej osoby. In: LAZAR, J. a kol. *Občianske právo hmotné. I. diel.* Bratislava: Iura Edition, 2010, s. 190.

⁵⁷ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích.* Praha: Wolters Kluwer ČR, 2013, s. 94.

ľudských práv a základných slobôd (ďalej len „Dohovor“ alebo „Európsky dohovor“)⁵⁸ s platnosťou od 3. septembra 1953, ku ktorému pristúpila Česká a Slovenská federatívna republika podpísaním 21. februára 1991. Hoci sa Dohovor sociálnych práv týka len marginálne,⁵⁹ jeho význam pre oblasť pracovnoprávných vzťahov a pracovného práva sa prejavuje v špecifických, z hľadiska dôležitosti nemenej významných súvislostiach **právnej ochrany súkromia zamestnanca**. Chráni právo jednotlivca na súkromný život v najširšom kontexte a predstavuje právny základ národných úprav v pracovnoprávných kódexoch európskych krajín.

Osobitnú pozornosť si vyžaduje čl. 8 Dohovoru, ktorý je dôležitý vo vzťahu k ochrane osobných údajov a jeho dôležitosť často zvýraznil vo svojej rozhodovacej činnosti aj ESĽP. Čl. 8 ods. 1 Dohovoru chránené predovšetkým základné „právo na rešpektovanie súkromného a rodinného života, obydlika a korešpondencie“ (čl. 8 ods. 1).⁶⁰ V zmysle čl. 8 ods. 2 Dohovoru „*štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných*“. V citovanom článku 8 ods. 2 je teda povinnosť štátu formulovaná pasívne, t. j. štát sa musí zdržať zásahov do práva na súkromný a rodinný života, obydlie a korešpondenciu a toto obmedzenie je štát, resp. zákonodarná moc povinná rešpektovať pri tvorbe národnej legislatívy. Obmedzená je aj výkonná moc v zásahoch do práva na súkromie len v medziach platnej právnej úpravy. Judikatúra ESĽP sa vyvinula tak, že doplnila túto pasívnu zložku právnej povinnosti nezasahovať do práva na súkromie zložkou aktívnou v tom zmysle, že v určitých prípadoch je štát dokonca povinný konať na ochranu porušeného práva.⁶¹ Práve test proporcionality nám slúži na skúmanie splnenia podmienok podľa čl. 8 ods. 2 Dohovoru.

Ako sme už uviedli, ESĽP v judikatúre nepovažoval za možné (ale ani nevyhnutné) vyčerpávajúcim spôsobom definovať pojem „súkromný život“,⁶² ktorému ochranu poskytuje čl. 8 Dohovoru. Uviedol, že pod týmto pojmom podľa citovaného článku Dohovoru sa rozumie jednak osobné súkromie človeka (osobná sféra jednotlivca, teda napr. údaje týkajúce sa mena, pohlavia, sexuálnej orien-

⁵⁸ Súčasťou Dohovoru je aj a jeho 14 dodatkových (opčných) protokolov.

⁵⁹ Predovšetkým pokiaľ ide o zákaz nútenej práce (čl. 4), koalíčnú slobodu (čl. 11), zákaz diskriminácie (čl. 14).

⁶⁰ Podľa čl. 8 Dohovoru predmetom ochrany aj korešpondencia, v písomnej aj elektronickej podobe. Pozri rozsudok ESĽP zo 6. septembra 1978 v právnej veci Klass a i. v. Nemecko, sťažnosť č. 5029/71, § 55.

⁶¹ ESĽP rozsudok Marckx 1979, A-31, § 31, ČAPEK, J. *Evropská úmluva o ochraně lidských práv a základních svobod. I. část – Úmluva*. Praha: Linde, 2010, s. 286.

⁶² Rozsudok ESĽP zo 16. decembra 1992 v právnej veci Niemietz v. Nemecko.

tácie), ale aj právo každého človeka na vytváranie a rozvíjanie vzťahov s ďalšími ľudskými bytosťami (súkromnej, profesijnej či komerčnej povahy).⁶³ Vo vzťahu k uvedenému vyjadril presvedčenie, že ochranu súkromia jednotlivcovi nemožno odoprieť v zmysle čl. 8 ods. 1 Dohovoru len preto, že napadnuté opatrenie sa vzťahuje len na jeho profesionálnu činnosť.⁶⁴

Na rešpektovanie vlastníckeho práva a ochranu majetku je zameraný čl. 1 Dodatkového protokolu č. 1 k Dohovoru, ktorý ustanovuje, že „každá fyzická alebo právnická osoba má právo pokojne užívať svoj majetok. Nikoho nemožno pozbaviť jeho majetku s výnimkou verejného záujmu a za podmienok, ktoré ustanoví zákon a všeobecné zásady medzinárodného práva“.

Popri Dohovore si zaslúži spomenúť aj iné významné dokumenty Rady Európy, určené na ochranu osobných údajov. Nepochybne k nim možno zaradiť aj **Dohovor Rady Európy o ochrane jednotlivca pri automatizovanom spracovaní osobných údajov č. 108/1981 z 28. januára 1981** s dodatkami k tomuto dohovoru (ďalej len „Dohovor č. 108“), ktoré nadobudli pre Slovenskú republiku platnosť 1. januára 2001.⁶⁵ Význam Dohovoru č. 108 spočíva najmä v tom, že predstavuje základ pre vnútroštátne normy upravujúce ochranu osobných údajov (aj slovenského ZOOÚ), nakoľko obsahuje v čl. 2 definície pojmov, akými sú „osobný údaj“, „subjekt osobných údajov“, „správca osobných údajov“ a „automatizované spracúvanie osobných údajov“ alebo v čl. 6 vymenúva osobitné kategórie údajov, ako sú rasový pôvod, náboženské presvedčenie, či sexuálna orientácia, označované aj ako tzv. „citlivé údaje“.⁶⁶ Okrem základných teoretických pojmov sa v ňom nachádzajú princípy a zásady ochrany osobných údajov, ktoré sa premietli do Smernice č. 95/46/ES a jej prostredníctvom do pôvodného zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov. Zastrešuje navyše spoluprácu zmluvných strán nielen pri spracúvaní, ale aj pri odovzdávaní a prenose osobných údajov do tretích krajín. Podľa tohto medzinárodného dokumentu, ktorý Morávek definuje ako „hard law“ či „self-executing“, sa má postupovať priamo, v prípade ak vnútroštátny právny predpis nepokrýva jeho pôsobnosť, t. j. ak poskytuje menšiu garanciu ochrany práv jednotlivcovi vo vzťahu k ochrane osobných údajov, ku ktorých spracúvaniu dochádza.⁶⁷ Toto

⁶³ ŠTEFKO, M. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In *Jurisprudence*, 2012, č. 7/8, s. 18.

⁶⁴ Rozsudok ESEP z 24. apríla 1990 v právnej veci Huvig v. Francúzsko, § 8 a § 25 a zo 16. februára 2000 v právnej veci Amann v. Švajčiarsko.

⁶⁵ Oznámenie Ministerstva zahraničných vecí SR publikované pod č. 49/2001 Z. z.

⁶⁶ Bližšie pozri MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 104 a 106.

⁶⁷ MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 100.

však nie je prípad ZOOÚ, ktorého právna úprava je ucelenejšia a konzistentnejšia. Rada Európy pravidelne monitoruje proces pristupovania jednotlivých zmluvných strán k Dohovoru č. 108 a kontrolujú úroveň ochrany osobných údajov.

Dokumentom, ktorý je integrálnou súčasťou primárneho práva Európskej únie a ktorý si zaslúži osobitnú pozornosť je **Charta základných práv Európskej únie** (ďalej len „Charta“).⁶⁸ V ustanovení čl. 1 Hlavy I. je zakotvený právny základ ochrany súkromia, osobnostných práv a ochrany osobných údajov, v ktorom sa uvádza, že: „*Ludská dôstojnosť je nedotknuteľná. Musí byť rešpektovaná a chránená.*“ Čl. 1 ďalej rozvíja čl. 3 ods. 1 Charty v znení: „*Každý má právo na to, aby bola rešpektovaná jeho fyzická a duševná nedotknuteľnosť.*“ Špeciálnym ustanovením k čl. 1 je čl. 7 Charty (zodpovedajúci tiež ustanoveniu čl. 8 ods. 1 Dohovoru), ktorý zakotvuje, že „*každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie.*“ Oproti ostatným spomínaným medzinárodným aktom Charta výslovne garantuje ochranu osobných údajov v článku 8: „*Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom (t. j. legitímnom) základe ustanovenom zákonom.*“ Z citovaného ustanovenia taktiež vyplýva, že „*každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a má právo na ich opravu. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.*“ Zo znenia Charty základných práv EÚ je zrejmé zdôraznenie zásady legality spracúvania osobných údajov na základe legitímneho, legálneho a presne stanoveného účelu a len s predchádzajúcim súhlasom príslušných osôb. Zároveň definuje ich subjektívne práva na prístup k údajom a právo na ich opravu, ak sú nepresné, a nevyhnutnosť existencie nezávislého orgánu dozoru. Súdny dvor EÚ v tejto súvislosti vyslovil právny názor, že prejavom všeobecného právneho princípu nedotknuteľnosti súkromia je aj ochrana osobných údajov, ktorú môžeme považovať za čiastkové právo súvisiace s ochrannou súkromnej sféry jednotlivca.⁶⁹ K uvedenej problematike má pre komplexné posúdenie význam spomenúť aj čl. 17 ods. 1 Charty: „*Každý má právo vlastniť svoj oprávnené nadobudnutý majetok, užívať ho, nakladať s ním a odkázať ho. Nikoho nemožno zbaviť jeho majetku, s výnimkou verejného záujmu, v prípadoch a za podmienok, ktoré ustanovuje zákon, pričom musí byť včas vyplatená spravodlivá ná-*

⁶⁸ Charta základných práv EÚ priznáva občanom EÚ a osobám s trvalým pobytom v EÚ isté osobné, občianske, politické, hospodárske a sociálne práva, ktoré tým zakotvuje v práve EÚ. Z obsahového hľadiska ju tvorí 6. kapitol a a 50 článkov. Platnosťou Lisabonskej zmluvy 1. decembra 2009 sa stala Charta základných práv EÚ formálne právne záväznou pre všetky členské štáty EÚ. Pozri (http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/133501_sk.htm).

⁶⁹ C-101/01 zo 6. novembra 2004 v právnej veci Lindqvist.

hrada. Užívanie majetku môže byť upravené zákonom v nevyhnutnej miere v súlade so všeobecným záujmom.“

Z oblasti komunitárnych prameňov práva upravujúcich ochranu osobných údajov je nepochybne najvýznamnejšou **smernica Európskeho parlamentu a Rady č. 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov** (ďalej len „smernica č. 95/46/ES“). Uvedená smernica predstavuje lex generalis a slúži ako základný právny nástroj, ktorý vymedzuje základné princípy a pravidlá spracúvania osobných údajov v Európskej únii, preto sa často označuje ako „všeobecná smernica“. ⁷⁰ Jej ideový a normatívny základ vychádza zo Zmluvy o fungovaní Európskej únie, v ktorej čl. 16 (bývalom čl. 286 Zmluvy o Európskom spoločenstve) ustanovuje, že *„každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. Európsky parlament a Rada v súlade s riadnym legislatívnym postupom ustanovia pravidlá, ktoré sa vzťahujú na ochranu fyzických osôb, pokiaľ ide o spracúvanie osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie, ako aj členskými štátmi pri výkone činností, ktoré patria do rozsahu pôsobnosti práva Únie, a pravidlá, ktoré sa vzťahujú na voľný pohyb takýchto údajov. Dodržiavanie týchto pravidiel podlieha kontrole nezávislých orgánov. Pravidlami prijatými na základe tohto článku nie sú dotknuté osobitné pravidlá ustanovené v článku 39 Zmluvy o Európskej únii“*. Odkazuje a nadväzuje pritom na súkromie, tak ako je chránené v čl. 8 Dohovoru. Ešte pred samotným vstupom do Európskej únie Slovenská republika bola povinná prijať osobitný zákon na ochranu osobných údajov v súlade so štandardmi tejto Smernice a harmonizovať ďalšie právne akty (napr. vyhlášky), ktoré sa tejto problematiky dotýkali. Predmet smernice č. 95/46/ES je vymedzený v čl. 1, pričom ukladá členským štátom povinnosť *„chrániť základné práva a slobody fyzických osôb, a najmä ich právo na súkromie v súvislosti so spracovaním osobných údajov“*. Zakazuje im tiež v ods. 2 *„obmedzovanie alebo bránenie voľnému toku osobných údajov medzi členskými štátmi z dôvodov spojených s ochranou poskytnutou podľa odseku 1“*. Definuje základné pojmy v čl. 2, pričom niektoré pojmy napr. „osobný údaj“ vymedzuje obdobne ako Dohovor č. 108, ale niektoré aj pozmeňuje ako „spracúvanie osobných údajov“ alebo dopĺňa úplne nové pojmy, ako napr. „súhlas subjektu údajov“. ⁷¹ Treba spomenúť aj čl. 8 smernice č. 95/46/ES, ktorý vymedzuje aj „osobitné kategórie osobných údajov,“ ktoré je možné spracúvať len za podmienky výslovného a informovaného

⁷⁰ Obsahuje 72 recitálov a 34 článkov. Recitály predstavujú zdôvodnenie jeho samotnej normatívnej časti, avšak majú dôležitú interpretačnú a aplikačnú funkciu. MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 121.

⁷¹ Základné pojmy vychádzajú zo stanovísk Pracovnej skupiny 29 (WP 29): WP 29 č. 4/2007 k pojmu osobné údaje, WP 29 č. 1/2010 k pojmu správca a spracovateľ, WP 29 č. 15/2011 k definícii súhlasu.

ho súhlasu subjektu údajov, alebo ktorých spracúvanie je bez výnimky zakázané, ak to ustanoví vnútroštátny predpis.

Na základe čl. 29 smernice č. 95/46/ES bola zriadená **Pracovná skupina pre ochranu jednotlivcov so zreteľom na spracúvanie osobných údajov**, ktorá je však bežne známa pod skratkou „WP 29“, z anglického slovného spojenia „working party“ (ďalej len „Pracovná skupina 29“). Jej úlohou je zjednocovanie právnej úpravy smernice č. 95/46/ES na úrovni jej interpretácie a aplikácie v členských štátoch EÚ. Má poradnú funkciu a pri svojej činnosti je nezávislá. Je zložená zo zástupcov národných orgánov dozoru alebo orgánov dozoru určených jednotlivými členskými štátmi, zástupcov orgánov alebo orgánov vytvorených pre orgány a inštitúcie EÚ a zástupcov Komisie. Dôležitá je jej povinnosť upovedomiť Komisiu o nesúlade medzi národnými právnymi úpravami na ochranu osobných údajov a praxou členských štátov, ak hrozí narušenie rovnosti ochrany osôb v súvislosti so spracúvaním osobných údajov v rámci EÚ. Predkladá stanoviská a odporúčania Komisii a jej pomocnému orgánu Výboru v zmysle čl. 31 a vypracováva správy a výročnú správu o stave ochrany osobných údajov jednotlivcov v súvislosti so spracúvaním osobných údajov v EÚ a tretích štátoch, ktorú predkladá Komisii, Európskemu parlamentu s Rade. Správy a výročná správa podliehajú povinnému zverejňovaniu. Podľa čl. 30 má Pracovná skupina 29 všeobecne tieto povinnosti: „a) skúmať každú otázku pokrývajúcu uplatniteľnosť vnútroštátnych opatrení prijatých podľa tejto smernice, aby sa prispelo k jednotnej uplatniteľnosti takýchto opatrení; b) predkladať Komisii stanovisko o úrovni ochrany v spoločenstve a v tretích krajinách; c) radiť Komisii o akejkoľvek navrhnutej zmene tejto smernice, o akýchkoľvek ďalších alebo špecifických opatreniach, aby sa zabezpečili osobné práva a slobody fyzických osôb vzhľadom na spracovanie osobných údajov a o akýchkoľvek iných navrhnutých opatreniach spoločenstva, ovplyvňujúce tieto práva a slobody; d) poskytovať stanovisko k zákonným predpisom navrhnutým na úrovni spoločenstva.“⁷²

Pracovná skupina 29 sa aktuálne zaoberá aj diskusiami o ďalšom smerovaní legislatívy EÚ v oblasti ochrany osobných údajov. Smernica č. 95/46/ES je podľa niektorých názorov zastaraná a nedostatočná z hľadiska potrieb aplikačnej praxe, keďže bola vytvorená a prijatá v čase, keď internet a technické prostriedky určené na komunikáciu a monitorovanie neboli na takej vyspelej úrovni a neboli využívané tak masovo ako v súčasnosti. Z uvedeného dôvodu sa príslušné európske orgány zaoberajú niekoľko posledných rokov otázkou, či vôbec a akým spôsobom pripraviť nový harmonizovaný a jednotný právny rámec ochrany osobných údajov, ktorý by umožňoval kontinuálny prenos osobných údajov do iných člen-

⁷² MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 151 – 152.

ských krajín EÚ a zabezpečoval efektívnu ochranu všetkým fyzickým osobám v rámci EÚ. Pritom odborná verejnosť nedospela k jednotnému právnenému názoru o potrebe či priam nevyhnutnosti reformy a je rozdelená do troch názorových táborov.⁷³

Správy z činnosti Európskej komisie vydané počas posledných dvoch rokov informujú o tejto najnovšej iniciatíve v oblasti ochrany osobných údajov. Novú európsku legislatívu, resp. nový právny rámec ochrany osobných údajov tvoria dva návrhy:

- Návrh nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „všeobecné nariadenie o ochrane osobných údajov“). Toto nariadenie má nahradiť smernicu Európskeho parlamentu a Rady č. 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracúvaní osobných údajov a voľnom pohybe týchto údajov,
- Návrh smernice o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov.⁷⁴

Detailnejšie informácie, argumentáciu i odôvodnenie potreby prijatia nového právneho rámca ochrany osobných údajov je možné nájsť napríklad v Pracovnom dokumente útvarov Komisie o posúdení vplyvu nového právneho rámca.⁷⁵ Analytické hodnotenie nového právneho rámca je možné nájsť v Stanovisku Pracovnej skupiny 29 č. 1/2012,⁷⁶ ako aj v stanovisku Európskeho dozorného úradníka pre ochranu osobných údajov o reforme ochrany osobných údajov.⁷⁷

V januári 2012 predložila Európska komisia návrh komplexnej reformy pravidiel ochrany údajov v EÚ z roku 1995 (95/46/ES) vo forme vyššie uvedeného

⁷³ Bližšie pozri MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 153.

⁷⁴ Táto smernica má nahradiť rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach. Vzhľadom na riešenie problematiky práce sa jej obsahu a významu nebudeme v práci bližšie venovať.

⁷⁵ *Pracovný dokument útvarov Komisie. Zhrnutie posúdenia vplyvu*. (online). Brusel: Európska komisia, 2012. (cit. 2014-12-07). Dostupné z: (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2012:0073:FIN:SK:PDF>).

⁷⁶ Stanovisko Pracovnej skupiny 29 č. 1/2012 k návrhom týkajúcim sa reformy v oblasti ochrany údajov z 23. marca 2012, WP 191.

⁷⁷ *Opinion of the European Data Protection Supervisor on the data protection reform package*. (online). Brusel: EDPS, 2012. (cit. 2014-12-07). Dostupné z: (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf).

všeobecného nariadenia o ochrane osobných údajov s cieľom posilniť právo na súkromie v on-line prostredí. Medzi hlavné prínosy, ktoré v ňom Európska komisia deklaruje patrí:⁷⁸

- zavedenie jediného súboru pravidiel, ktorý bude platiť v celej EÚ a jeho cieľom je odstrániť zbytočné administratívne zaťaženie, akým je aj oznamovacia povinnosť podnikov o činnostiach spojených so spracúvaním a ochranou osobných údajov (predpokladaným prínosom pre podniky je výrazné šetrenie nákladov prostredníctvom vytvorenia priestoru pre tvorbu a zachovanie pracovných miest),
- zriadenie Európskej rady pre ochranu osobných údajov, ktorá by mala prevziať a kontinuálne nahradiť činnosť Pracovnej skupiny 29,
- posilnenie zodpovednosti a nezávislosti tých, ktorí údaje spracúvajú (t. j. „zodpovedných osôb“),⁷⁹
- posilnenie postavenia a rozšírenie právomocí nezávislých národných orgánov pre ochranu údajov (napr. právo uložiť pokutu tým podnikom, ktoré porušia pravidlá EÚ v oblasti ochrany údajov až do výšky 1 milióna eur alebo až do 2 % celkového ročného obratu podniku),
- garanciu tzv. „práva byť zabudnutý“, t. j. práva na opravu a úplnú likvidáciu osobných údajov, v prípadoch, ak nebudú existovať žiadne zákonné dôvody a nebude daný účel na ich ďalšie uchovávanie (zhromažďovanie) a spracúvanie alebo bude odvolaný súhlas so spracúvaním alebo ak dotknutá osoba vznesie námietku proti spracúvaniu.

Návrh tohto jednotného právneho nástroja Európskej Komisie bol postúpený v priebehu roka 2013 parlamentným výborom Európskeho parlamentu a Rade ministrov EÚ na diskusiu a prerokovanie. Niektoré výkonné či zákonodarné orgány členských štátov (napr. Spolkovej republiky Nemecka, Belgicka, Francúzska či Švédska)⁸⁰ však vzniesli zásadné pripomienky, spochybňujúce právnu reguláciu navrhovaného všeobecného nariadenia o ochrane osobných údajov v tom zmysle, že je v rozpore so zásadou subsidiarity uvedenou v čl. 5 Zmluvy o Európskej únii. K uvedenému názoru o nerešpektovaní zásady subsidiarity sa priklonil aj Morávek.⁸¹ Rokovania o reforme ochrany údajov prebiehajú už viac ako tri roky

⁷⁸ Stanovisko Pracovnej skupiny 29 č. 1/2012 k návrhom týkajúcim sa reformy v oblasti ochrany údajov z 23. marca 2012, WP 191.

⁷⁹ Slovenský ZOOÚ na rozdiel od českého zákona č. 101/2000 Zb. o ochrane osobných údajů pozná inštitút zodpovednej osoby.

⁸⁰ Pozri napr. *Stanovisko Spolkovej rady SRN*. (online). 2014. (cit. 2014-12-07). Dostupné z: (http://www.europarl.europa.eu/RegData/commissions/juri/communication/2012/487796/JURI_CM%282012%29487796_CS.pdf).

⁸¹ Podľa zásady subsidiarity uvedenej v čl. 5 ods. 3 Zmluvy o Európskej únii: „*koná Európska únia v oblastiach, ktoré nepatria do jej výlučnej právomoci, len v takom rozsahu a vtedy, ak ciele*

a aj keď sa v rámci rokovaní zaznamenal pokrok, stále zostáva reforma len v štádiu prípravy. Hlavy členských štátov a vlády EÚ sa pritom zaviazali niekoľkokrát k rýchlemu uzavretiu rokovaní. Európska rada⁸² sa na konci júna 2014 na svojom zasadnutí uzniesla na odporúčaní, že je dôležité prijať všeobecný právny rámec ochrany osobných údajov do roku 2015.⁸³

Európska komisia sa v rôznych správach snaží informovať členské štáty o nevyhnutnosti a prínose tohto právneho nástroja, ale z výsledkov niektorých štatistík a prieskumov uskutočnených nezávislými inštitúciami zameranými na ochranu osobných údajov (napr. organizácie European Digital Rights) sú jasné kritické postoje k jednotnému právnemu nástroju, ktorý považujú skôr za politický dokument ako za dokument založený na overených vedeckých poznatkoch a serióznom výskume. Podľa ich názoru pôjde skôr o prepojenie viacerých vnútroštátnych právnych úprav, a v konečnom dôsledku tento nástroj zneprehľadní ešte viac už aj tak rozsiahle a zložité európske normy o ochrane osobných údajov. Kritika je založená najmä na problematickej oblasti bezpečnosti takto uchovávaných osobných údajov, ktoré musia prevádzkovatelia, t. j. aj zamestnávateľia garantovať.

Prameňom európskeho práva z oblasti ochrany osobných údajov je aj **smernica Európskeho parlamentu a Rady č. 2002/58/ES z 12. júla 2002 o spracovaní osobných údajov a ochrane súkromia v sektore elektronických komunikácií** [smernica o súkromí a elektronických komunikáciách (ďalej len „smernica č. 2002/58/ES“)], ktorou došlo k nahradeniu predchádzajúcej smernice č. 97/66/ES z 15. decembra 1997 o spracovaní osobných údajov a ochrane súkromia v telekomunikačnom sektore. Obe uvedené smernice garantujú dôvernú osobných údajov a ochranu súkromia pri komunikácii prostredníctvom elektronických prostriedkov (e-mail). Účel smernice č. 2002/58/ES spočíva v prispôbení sa novým digitálnym technológiám, ktoré so sebou prinášajú zvláštne požiadavky na ochranu osobných údajov a súkromia ich používateľov.⁸⁴ Kľúčovú technológiu predsta-

zamýšľané touto činnosťou nemôžu členské štáty uspokojivo dosiahnuť na ústrednej úrovni alebo na regionálnej a miestnej úrovni, ale z dôvodov rozsahu alebo účinkov navrhovanej činnosti ich možno lepšie dosiahnuť na úrovni Únie.“ Pozri MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 155.

⁸² Európska rada poskytuje Európskej únii potrebné podnety na jej rozvoj a stanovuje jej všeobecné politické smerovanie a priority. Nevykonáva však legislatívnu funkciu. Po nadobudnutí platnosti Lisabonskej zmluvy 1. decembra 2009 sa z nej stala oficiálna inštitúcia.

⁸³ REICHERTS, M. *The right to be forgotten and the EU data protection reform: Why we must see through a distorted debate and adopt strong new rules soon.* (online). 2014. (cit. 2014-12-07). Dostupné z: (http://europa.eu/rapid/press-release_SPEECH-14-568_en.htm).

⁸⁴ Článok 1 smernice č. 2002/58/ES stanovuje jej pôsobnosť a cieľ tým, že uvádza, že „*touto smernicou sa harmonizujú predpisy členských štátov, nevyhnutné pre zabezpečenie rovnocennej úrovne ochrany základných práv a slobôd, najmä práva na súkromie, so zreteľom na spracovanie osobných*

vuje v rámci tejto smernice internet, ktorý poskytuje priestor na prevádzkovanie množstva elektronických komunikačných služieb, čo so sebou prináša v praxi veľké množstvo nových možností pre používateľov, ale aj nových rizík vo vzťahu k ich súkromiu a osobným údajom. Prínosom smernice je rozšírenie ochrany súkromia aj na právnické osoby (pretože používa neutrálny pojem „účastníci“). Smernica ďalej upravuje citlivé otázky, ako je uchovávanie údajov na účely trestného konania, rozosielanie nevyžiadaných správ, využívanie „cookies“ a ukladanie osobných údajov do verejných adresárov. Tiež upravuje špiónážny softvér a iné podobné nástroje, ktoré sú schopné preniknúť do koncového zariadenia používateľa bez jeho vedomia s cieľom získať prístup k informáciám, uchovávať skryté informácie alebo sledovať činnosť používateľa a sú schopné vážne narušiť jeho súkromie.

Cieľom **Nariadenia Európskeho parlamentu a Rady (ES) č. 45/2001 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov orgánmi a inštitúciami Spoločenstva a o voľnom pohybe týchto údajov** prijatého 18. decembra 2000 je uľahčenie voľného pohybu informácií, ktorý má zabezpečiť práva osôb na rešpektovanie ich súkromného života. Týka sa spracúvania osobných údajov vo všetkých orgánoch a inštitúciách Európskej únie, ak sa toto spracovanie uskutočňuje v rámci výkonu činností spadajúcich pod pôsobnosť práva Európskej únie. Význam spočíva v zabezpečení jednotného uplatňovania pravidiel ochrany základných práv a slobôd fyzických osôb v súvislosti so spracovaním ich osobných údajov na území všetkých členských štátov Európskej únie. Ústrednou témou smernice je aj právne zakotvenie voľného pohybu osobných údajov nielen medzi jednotlivými členskými štátmi, ale aj medzi inštitúciami a orgánmi Európskej únie pri výkone ich právomocí. Za osobitný prínos tejto smernice možno považovať zriadenie nezávislého orgánu dozoru, ktorý je poverený dohľadom nad spracúvaním osobných údajov orgánmi a inštitúciami Európskej únie. Ide o špeciálny orgán ochrany práva osobných údajov s názvom Európsky dozorný úradník pre ochranu osobných údajov („European Data Protection Supervisor“),⁸⁵ ktorý má zabezpečovať ochranu tohto práva v členských štátoch. Ide o jednu z najmladších inštitúcií EÚ.⁸⁶ Smernica právne zakotvuje aj zásady

údajov v odvetví elektronických komunikácií a na zaistenie voľného pohybu týchto údajov a elektronických komunikačných zariadení a služieb Spoločenstva“.

⁸⁵ Do funkcie bol vymenovaný Giovanni Buttarelli (Taliano) so začiatkom funkčného obdobia od 4. decembra 2014. Tlačová správa. *Giovanni Buttarelli named new data protection watchdog*. (online). 2014. (cit. 2015-01-01). Dostupné z (<http://www.europarl.europa.eu/news/en/news-room/content/20141127IPR81016/html/Giovanni-Buttarelli-named-new-data-protection-watchdog>).

⁸⁶ FRIDRICH, B., MIHÁLIKOVÁ, S., MOKRÁ, L., SIMAN, M. *Ochrana ľudských práv v Európskej únii*. Bratislava: Univerzita Komenského, 2008, s. 197. Tiež pozri (<http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=sk>).

ochrany osobných údajov a súkromia v rámci telekomunikačných sietí a opravné prostriedky (žalobu na Súdny dvor Európskej únie a sťažnosť Európskemu dozornému úradníkovi).⁸⁷

Do skupiny predpisov práva Európskej únie z oblasti ochrany súkromia patríla donedávna tiež **smernica Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES** (ďalej len „smernica č. 2006/24/ES“), známa pod medzinárodným názvom „Data Retention Directive“. Z dôvodovej správy k tejto smernici vyplýva, že bola prijatá najmä so zámerom získať prístup k prevádzkovým a lokalizačným údajom, ktoré sú dôležité na účely súvisiace s uplatňovaním práva a zaistením bezpečnosti, napríklad z hľadiska prevencie, vyšetrovania, odhaľovania a stíhania závažných trestných činov, akými je organizovaný zločin a terorizmus. Jedným z kľúčových rozhodnutí Súdneho dvora Európskej únie vo vzťahu k ochrane osobných údajov, ktoré má priamy dopad na uvedenú smernicu, je rozhodnutie z 8. apríla 2014 v spojených právnych veciach Digital Rights Ireland Ltd. a Kärntner Landesregierung, veci C-293/12 a C-594/12. Súdny dvor EÚ v ňom skúmal súlad smernice č. 2006/24/ES s Chartou základných práv EÚ. Výsledkom bolo vyhlásenie uvedenej smernice ako celku za neplatnú, nakoľko došiel k záveru, že jej prijatím porušil zákonodarca zásadu proporcionality v zmysle článkov 7 a 8 a čl. 52 ods. 1 Charty základných práv EÚ.⁸⁸ V bode 57 uviedol, že *„smernica všeobecne zahŕňa akúkoľvek osobu a všetky spôsoby elektronickej komunikácie, ako aj všetky prevádzkové údaje bez toho, aby stanovovala akékoľvek rozlíšenie, obmedzenie alebo výnimku na základe cieľa, ktorým je boj proti závažnej trestnej činnosti“*. Hlavný nedostatok smernice podľa názoru Súdneho dvora EÚ predstavoval najmä princíp uchovávania osobných údajov založený na plošnosti a všeobecnej platnosti, ktorý vyhlásil za neprijateľný, v dôsledku čoho napokon zrušil uvedenú smernicu s účinkami ex tunc, teda s platnosťou k dátumu nadobudnutia jej platnosti.⁸⁹

⁸⁷ HRADÍLOVÁ, J. *Ochrana osobných údajů v Evropské unii*. Ikaros (online). 2008, roč. 12, č. 2. (cit. 2014-12-18). Dostupné z: (<http://www.ikaros.cz/ochrana-osobnich-udaju-v-evropske-unii>).

⁸⁸ VOBOŘIL, J. *Jaké budou dopady zrušení směrnice o data retention?* (online). 2014. (cit. 2014-12-17). Dostupné z: (<http://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html>).

⁸⁹ Rozhodnutie SD EÚ z 8. apríla 2014 v spojených právnych veciach Digital Rights Ireland Ltd. a Kärntner Landesregierung, veci C-293/12 a C-594/12.

2.2 Pramene slovenskej právnej úpravy

Súkromný život každej fyzickej osoby, t. j. aj zamestnanca sa týka viacerých sfér spoločenského života (jeho osobnosti, osobných údajov, zdravia), čo sa prejavuje aj v tom, že právna úprava danej problematiky nie je komplexne zahrnutá v jednom predpise. Ochrana osobnosti je predmetom právnej úpravy viacerých právnych odvetví súkromného i verejného práva (občianskeho, správneho, trestného práva) v Slovenskej republike, ktoré vytvárajú jej komplexný rámec. Ústavným rámcom ochrany osobnostných práv a ochrany súkromia človeka je čl. 19 Ústavného zákona č. 460/1992 Zb. Ústavy Slovenskej republiky (ďalej len „Ústavy Slovenskej republiky“), v zmysle ktorého *„každý má právo na zachovanie ľudskej dôstojnosti, osobnej cti, dobrej povesti, na ochranu mena, ochranu pred neoprávneným zasahovaním do súkromného a rodinného života, ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe“*.

Občianskoprávna úprava ochrany osobnosti je založená na ustanoveniach druhej hlavy Ústavy Slovenskej republiky, a to konkrétne čl. 14 až 16 a čl. 19 až 21. V slovenskom právnom poriadku všeobecné osobnostné právo netvorí samostatné odvetvie súkromného práva, ale tvorí neoddeliteľnú súčasť občianskeho práva (hmotného) a jeho právne základy sú zakotvené v ustanoveniach § 11 až 16 zákona č. 40/1964 Zb. Občianskeho zákonníka v znení neskorších predpisov (ďalej len „**Občianskeho zákonníka**“).

Generálnu klauzulu ochrany osobnosti predstavuje § 11 Občianskeho zákonníka, podľa ktorého *„fyzická osoba má právo na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy“*. Zákon v tomto ustanovení výpočet konkrétnych zásahov do osobnostných práv fyzickej osoby nevymenúva. Ustanovuje len znaky, pri danosti ktorých treba určité konanie považovať za zásah do osobnosti občana. Hoci zákon nedefinuje pojem „zásah“ a ani nepodáva výpočet konkrétnych foriem zásahov, ktorými môžu byť porušené osobnostné práva jednotlivca, je ním však bezpochyby jednak aktívne konanie, ako aj pasívne správanie (zdržanie sa konania alebo jeho opomenutie), ktoré má v zákone uvedené znaky. Týmito znakmi sú predovšetkým neoprávnenosť zásahu⁹⁰ a tiež jeho objektívna spôsobilosť negatívne pôsobiť na osobnosť fyzickej osoby.

Na základe uvedeného možno dospieť k záveru, že *„o neoprávnený zásah do osobnosti fyzickej osoby nepôjde, ak existujú okolnosti vylučujúce neoprávnenosť“*

⁹⁰ „Neoprávneným zásahom“ nie je zásah do osobnostnej sféry jednotlivca, ak sú dané okolnosti vylučujúce protiprávnosť konania, napr. výkon práva, plnenie povinnosti, svojpomoc, nutná obrana či krajná núdza.

*zásahu. Jednou z takých okolností môže byť aj výkon zo zákona vyplývajúceho práva alebo plnenie zákonom uložennej povinnosti. Takýmito prípadmi sú najmä zákonné licencie v zmysle § 12 ods. 2 a 3 Občianskeho zákonníka⁹¹ tak ako licencie stanovené inými osobitnými zákonmi (napr. Zákonom o rodine, Trestným zákonom, Trestným poriadkom a pod.), avšak za predpokladu, že takto vykonané zásahy sú uskutočnené v rámci a v medziach týchto zákonov. Je pritom vždy na pôvodcovi zásahu do práva na ochranu osobnosti, aby preukázal, že existoval konkrétny dôvod, ktorý podľa platnej právnej úpravy neoprávnenosť zásahu vylučuje“.*⁹² V súlade s uvedeným Ústavný súd Slovenskej republiky v náleze z 29. novembra 1995 sp. zn. I. ÚS 33/95 z vyslovil názor, že „ústavné právo na rešpektovanie súkromného života vrátane práva na ochranu osobných údajov nemá absolútnu povahu v tom zmysle, že by vylučovalo všetky zásahy orgánov štátu. Štátne orgány majú oprávnenie na zásah do práva na ochranu osobných údajov za predpokladu, že tento zásah možno považovať za oprávnený podľa čl. 19 ods. 3 Ústavy Slovenskej republiky“.

Pokiaľ ide o subjektívnu stránku, resp. subjekt zásahu, je ním primárne fyzická osoba, ale z aktuálnej rozhodovacej činnosti súdov vyplýva, že subjektom zásahu môže byť aj právnická osoba. Na podporu tohto tvrdenia možno uviesť zaujímavé rozhodnutie Najvyššieho súdu Slovenskej republiky z 26. septembra 2013 sp. zn. 3 Cdo 228/2012, ktoré hovorí o tom, že zodpovednosť za neoprávnený zásah do osobnostných práv v zmysle § 11 a nasl. Občianskeho zákonníka nesie aj **právnická osoba**, hoci bol zásah spôsobený konkrétnou fyzickou osobou, avšak za podmienky, že táto fyzická osoba bola použitá zodpovednou právnickou osobou ako realizátor jej vlastnej činnosti. Za určujúce kritériá na posúdenie „činnosti realizovanej pre právnickú osobu“ pritom Najvyšší súd Slovenskej republiky považoval miestny, časový a vecný vzťah k plneniu danej činnosti.

Ak určité konanie má zákonné znaky zásahu do chránených osobnostných práv, má fyzická osoba, do ktorej práv sa zasiahlo, v zmysle občianskoprávnej úpravy právo najmä domáhať sa, aby sa upustilo od neoprávnených zásahov a aby sa jej poskytlo primerané zadosťučinenie (§ 13 ods. 1 Občianskeho zákonníka). Pokiaľ by sa nezdalo postačujúce takéto zadosťučinenie najmä preto, že bola v značnej miere znížená dôstojnosť fyzickej osoby alebo jej vážnosť v spoločnosti, má fyzická osoba tiež právo na náhradu nemajetkovej ujmy v peniazoch (§ 13 ods. 2 Občianskeho zákonníka). Zodpovednosť za neoprávnený zásah do osobnostných práv fyzickej osoby je založená primárne na objektívnom princípe (ak

⁹¹ Z ustanovenia § 12 ods. 2 Občianskeho zákonníka vyplýva, že v prípade, ak zamestnávateľovi vyplýva povinnosť zverejniť napr. fotografiu zamestnanca zo zákona, súhlas zamestnanca so zverejnením sa nepovažuje za potrebný.

⁹² Pozri rozsudok Najvyššieho súdu Slovenskej republiky z 19. mája 2010 sp. zn. 5 Cdo 108/2009.

vznikne nemajetková ujma), to znamená, že sa nevyžaduje zavinenie pôvodcu tohto neoprávneného zásahu.⁹³

Právo na súkromie je aj imanentnou súčasťou pracovnoprávných vzťahov s tým, že jeho limity predstavujú práva a oprávnené záujmy zamestnávateľa, medzi ktoré patrí aj právo na ochranu vlastníctva a ústavné právo na podnikanie. V Slovenskej republike zákonnú úpravu ochrany súkromia v pracovnoprávných vzťahoch predstavuje zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov (ďalej len „**Zákonník práce**“). Precíznejšiu úpravu monitoringu zamestnancov zaviedla posledná novela Zákonníka práce zákonom č. 361/2012 Z. z. účinná od 1. januára 2013. Podmienky monitoringu zamestnancov pôvodne upravené v článku 11 Základných zásad Zákonníka práce sa presunuli do normatívnej časti s cieľom dodať tomuto aspektu pracovnoprávných vzťahov potrebnú váhu a dôležitosť.

Ako vyplýva z ďalšieho výkladu Zákonník práce, právo na súkromie nepovažuje za úplne nedotknuteľné. Aktuálna úprava ochrany súkromia zamestnancov upravená v § 13 ods. 4 Zákonníka práce⁹⁴ definuje časové, vecné a priestorové podmienky, za ktorých môže zamestnávateľ zamestnanca kontrolovať. Výkon kontroly môže uskutočniť len

1. na pracovisku a v spoločných priestoroch zamestnávateľa,
2. v prípade vážnych dôvodov,
3. ak vážne dôvody spočívajú v osobitej povahe činností zamestnávateľa,
4. len dovoľeným spôsobom, tzn. monitorovaním (napríklad videokamerou), záznamom telefonických hovorov uskutočňovaných pracovnými technickými zariadeniami zamestnávateľa a kontrolou elektronickej pošty odoslanej z pracovnej elektronickej adresy a doručenej na túto adresu,⁹⁵

⁹³ Pozri bližšie kapitolu 4.8 Prostriedky ochrany osobných údajov zamestnanca v Slovenskej republike.

⁹⁴ § 13 ods. 4 Zákonníka práce: „zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitej povahe činností zamestnávateľa narušať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronicкую poštu odoslanú z pracovnej elektronickej adresy a doručení na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.“

⁹⁵ Z uvedeného aktuálneho znenia zákona vyplýva, že listové zásielky adresované zamestnancovi ako súkromnej osobe zamestnávateľ nemôže kontrolovať vôbec. Z pôvodného obsahu čl. 11 Základných zásad Zákonníka práce sa vypustila kontrola listových zásielok adresovaných zamestnancovi ako súkromnej osobe v dôsledku zákazu takejto kontroly vyformovaného judikatúrou Európskeho súdu pre ľudské práva, pretože súkromná pošta zamestnanca obsahovo prislúcha do práva na osobné súkromie. Výnimka z toho práva nie je možná pri akomkoľvek vážnom dôvode na strane zamestnávateľa vyplývajúceho z osobitej povahy jeho činnosti.

5. po predchádzajúcom upozornení zamestnanca, že výkon kontroly uskutoční,
6. pri zavedení kontrolného mechanizmu musí výkonu kontroly predchádzať prerokovanie so zástupcami zamestnancov a informovanie zamestnancov, predmetom prerokovania a poskytnutých informácií musí byť rozsah kontroly, spôsob jej uskutočnenia, ako aj dĺžka jej trvania.

Barancová uvádza, že osobitná povaha činnosti zamestnávateľa predstavuje právny základ, z ktorého možno následne odvodiť vážne dôvody zamestnávateľa. V tejto súvislosti odporúča, aby zamestnávateľa vykonávajúci zásahy do súkromia vymedzili vážne dôvody vo svojom vnútornom predpise, hoci v prípade vzniku súdneho sporu v konečnom dôsledku je len v právomoci príslušného súdu rozhodnúť, či vymedzenie pojmu „vážne dôvody“ zodpovedá zásade proporcionality tak, ako to vyžadujú európske pramene práva, ale aj aktuálna judikatúra Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie. Za užitočné tiež považuje vymedzenie pojmov „pracovisko“ a „spoločné priestory zamestnávateľa“.⁹⁶

V praxi sa tiež odporúča, aby zamestnávateľ splnenie povinnosti prerokovať zavádzanú kontrolu a informovať zamestnancov zachytil v písomnej forme, napríklad formou zápisnice zo stretnutia so zamestnaneckým dôverníkom alebo so zástupcami zamestnancov. Výber vhodnej formy na informovanie zamestnanca závisí od potreby zavádzanej kontroly. Ak má zamestnávateľ vážny dôvod na sústavnú kontrolu zamestnanca, napríklad v obchodných priestoroch, je vhodné výkon kontroly upraviť priamo v pracovnej zmluve alebo v internom predpise. V prípade potreby kontroly ad hoc, napríklad v rámci kontroly e-mailovej komunikácie zamestnanca, ktorý spracúva objednávky klientov, vykonávanej iba počas jeho práceneschopnosti, postačuje forma písomného oznámenia.

Podľa čl. 11 Základných zásad⁹⁷ v znení poslednej novely Zákonníka práce zamestnávateľ môže zhromažďovať len také osobné údaje o zamestnancovi, ktoré súvisia s jeho kvalifikáciou, profesionálnymi skúsenosťami a údaje, ktoré môžu byť významné z hľadiska práce, ktorú má vykonávať, vykonáva alebo vykonával.

Ak sa zamestnanec domnieva, že zamestnávateľ porušil podmienky výkonu kontroly, môže sa v zmysle § 13 ods. 5 Zákonníka práce⁹⁸ brániť podaním

Pozri Dôvodovú správu k novele Zákonníka práce zákonom č. 361/2012 Z. z. – osobitná časť, k bodom 7 až 9.

⁹⁶ BARANCOVÁ, H. a kol. *Základné práva a slobody v pracovnom práve*. Plzeň: Aleš Čeněk, 2012, s. 106.

⁹⁷ Čl. 11 Základných zásad Zákonníka práce: „Zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s jeho kvalifikáciou a profesionálnymi skúsenosťami a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával.“

⁹⁸ § 13 ods. 5 Zákonníka práce: „Zamestnanec má právo podať zamestnávateľovi sťažnosť v súvislosti s porušením zásady rovnakého zaobchádzania podľa odsekov 1 a 2 a nedodržaním podmienok

sťažnosti zamestnávateľovi alebo sa môže podľa ods. 7 citovaného ustanovenia⁹⁹ obrátiť na súd a domáhať sa právnej ochrany. Zamestnanec sa môže sám rozhodnúť, ktorú možnosť si zvolí. V prípade, ak je sťažnosť zamestnanca opodstatnená, zamestnávateľ je povinný na sťažnosť zamestnanca odpovedať bez zbytočného odkladu, prípadne aj vykonať nápravu, upustiť od protiprávneho konania a odstrániť jeho následky. Na podanie žaloby nie je prechádzajúce upozornenie zamestnávateľa potrebné.

Prísnejšie kritériá uplatňovania ochrany osobnosti zamestnanca súvisia aj s ustanovením § 81 Zákonníka práce, podľa ktorého sa má zamestnanec na pracovisku zdržiavať výlučne len kvôli výkonu práce, nie na iné účely, ktoré sú v rozpore s oprávnenými záujmami zamestnávateľa. Zároveň je povinný podľa § 81 písm. e/ Zákonníka práce riadne hospodáriť s prostriedkami, zverenými zamestnávateľom a chrániť jeho majetok pred poškodením, zničením alebo stratou.

Právna úprava v Zákonníku práce je len čiastkovou právnou úpravou, ďalšie obmedzenia vyplývajú zo zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o ochrane osobných údajov**“ alebo „ZOOÚ“). Zákon o ochrane osobných údajov je presným príkladom právneho predpisu, ktorý obsahuje ustanovenia ako verejného, tak aj súkromného práva. Verejnoprávny prvok je zastúpený napr. v ustanoveniach, ktoré upravujú konanie pred Úradom na ochranu osobných údajov. Z hľadiska súkromného práva upravuje zároveň občianskoprávne záväzkové vzťahy medzi prevádzkovateľom (zamestnávateľom) a príslušnou osobou (zamestnancom).

Právnu úpravu ochrany osobných údajov v pracovnoprávných vzťahoch tvorí viacero vzájomne významovo previazaných právnych predpisov. Ich vzájomný vzťah možno definovať nasledovne. ZOOÚ je lex generalis pre oblasť ochrany osobných údajov, pričom jeho ustanovenia treba vykladať v súlade s účelom smernice č. 95/46/ES, v ktorej má tento zákon svoj pôvod. Zákonník práce je vo vzťahu k ZOOÚ rovnako ako k Občianskemu zákonníku lex specialis. Priznáva totiž zamestnávateľovi práva a ukladá mu povinnosti vo vzťahu k spracúvaniu osobných údajov zamestnancov. Ďalším osobitným právnym predpisom, ktorý je vo vzťahu špeciality k ZOOÚ, je napr. zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov, ktorý dopĺňa zásady a princípy vyplývajúce zo ZOOÚ. Vzájomný vzťah Občianskeho zákonníka a ZOOÚ

podľa odsekov 3 a 4; zamestnávateľ je povinný na sťažnosť zamestnanca bez zbytočného odkladu odpovedať, vykonať nápravu, upustiť od takého konania a odstrániť jeho následky.“

⁹⁹ § 13 ods. 7 Zákonníka práce: „Zamestnanec, ktorý sa domnieva, že jeho súkromie na pracovisku alebo v spoločných priestoroch bolo narušené nedodržaním podmienok podľa odseku 4, môže sa obrátiť na súd a domáhať sa právnej ochrany.“

spočíva na princípe špeciality, t. j. *lex generalis* ku *lex specialis*. Prikláňame sa k názoru, že Občiansky zákonník poskytuje (resp. poisťuje) ochranu osobnostných práv zamestnanca, ak by došlo k prekročeniu prípustných limitov spracovania osobných údajov stanovených vo vyššie uvedených predpisoch. V literatúre sa však už objavil aj názor, že, ide o dve právne úpravy, ktoré existujú súbežne a zároveň samostatne a nezávisle.¹⁰⁰ Uvedené závery o vzťahu porovnávaných základných právnych predpisov o ochrane súkromia a osobných údajov zamestnanca sme zhrnuli v prehľadnej Tabuľke č. 1 uvedenej v prílohách tejto monografie.

Medzi pramene práva na ochranu súkromia a osobných údajov zamestnanca v Slovenskej republike zaraďujeme aj ďalšie právne normy zákonného charakteru, ako napríklad: zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov, zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov, zákon č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov, zákon č. 351/2011 Z. z. o elektronických komunikáciách, zákon č. 171/1993 Z. z. o Policajnom zbore Slovenskej republiky, zákon č. 154/1994 Z. z. o matrikách v znení neskorších predpisov, zákon č. 301/1995 Z. z. o rodnom čísle, zákon č. 162/1995 Z. z. o katastri nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam (katastrálny zákon), zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním), zákon č. 576/2004 Z. z. o zdravotnej starostlivosti a o zmene niektorých zákonov.

¹⁰⁰ VETERNÍKOVÁ, M. *Právna ochrana osobnosti*. Bratislava: Procom, 2003, s. 150.

3. OCHRANA SÚKROMIA ZAMESTNANCA

3.1 Základné spôsoby výkonu kontroly a zásahov do súkromia zamestnanca

Zamestnávateľia môžu zasahovať do súkromia svojich zamestnancov vykonávaním sofistikovanej kontroly. Na kontrolu svojich zamestnancov môžu využívať najrôznejšie spôsoby kontroly pomocou monitorovacích zariadení a opatrení na sledovanie obmedzujúcich osobné (fyzické a psychické) charakteristiky zamestnancov. Spôsoby vykonávania kontroly obmedzujúce, resp. zasahujúce široké spektrum oblastí súkromného života zamestnancov môžeme rozdeliť prehľadne do dvoch kategórií.¹⁰¹

Prvou kategóriou sú prostriedky kontroly, medzi ktoré zaraďujeme monitorovacie zariadenia a opatrenia na sledovanie zamestnancov:

- monitorovanie prostredníctvom kamerových systémov
- monitorovanie e-mailovej komunikácie
- sledovanie telefonických hovorov
- sledovanie využívania počítača a pohybu na internete
- sledovanie pohybu pomocou GPS
- kontrola užívania alkoholu, omamných a psychotropných látok
- osobnostný profil
- majetkový profil

Druhú kategóriu tvoria osobné (behaviorálne) obmedzenia a požiadavky na zamestnancov:

- zákaz fajčenia
- obmedzenia telesnej hmotnosti
- požiadavky na fyzickú kondíciu

¹⁰¹ COHEN, C. F., COHEN, M. E. On-duty and Off-duty: Employee Right to Privacy and Employer's Right to Control the Private Sector. In: *Employee Responsibilities and Rights Journal*, 11/2007. (online). 2007. (cit. 2015-01-26). Dostupné z: (http://www.researchgate.net/publication/225629872_On-duty_and_Off-duty_Employee_Right_to_Privacy_and_Employers_Right_to_Control_in_the_Private_Sector), s. 236-237.

- obmedzenia osobného vzhľadu (kódex obliekania, viditeľné tetovania, piercing, účes, brada a iná úprava zovňajšku)
- zákaz citových či intímnych vzťahov na pracovisku

V ďalšej podkapitole sa zameriame výlučne na prvú uvedenú kategóriu prostriedkov kontroly, a to na spôsoby monitorovania zamestnancov na pracovisku pomocou technických zariadení.

3.2 Monitorovanie zamestnancov na pracovisku

Jednou zo základných povinností zamestnancov je podľa § 81 písm. a/ až písm. c/ a písm. e/ Zákonníka práce pracovať zodpovedne a riadne, plniť pokyny nadriadených, ktoré sú vydané v súlade s právnymi predpismi na využívanie pracovného času na prácu. Zamestnancom sa tiež ukladá povinnosť dodržiavať právne predpisy a ostatné predpisy vzťahujúce sa na nimi vykonávanú prácu, ak boli s nimi riadne oboznámení. Okrem toho sú povinní riadne hospodáriť s prostriedkami, ktoré im zveril zamestnávateľ, chrániť majetok zamestnávateľa a nekonať v rozpore s jeho oprávnenými záujmami. Uvedeným povinnostiam zodpovedá právo zamestnávateľa primeraným spôsobom kontrolovať, či nedochádza k ich porušovaniu.

V súčasnosti môžeme zaznamenať trend, kedy zamestnávateľ zavádza na pracovisku¹⁰² opatrenia na sledovanie zamestnancov z dôvodu kontroly plnenia vyššie uvedených základných povinností. Za týmto účelom využíva zamestnávateľ rozličné monitorovacie zariadenia, ktoré majú predovšetkým chrániť jeho vlastnícke právo, život a zdravie zamestnancov, kolegov a iných osôb, ktoré sa v kontrolovanom priestore zdržujú. Ako prevádzkovateľ monitorovacieho zariadenia je oprávnený chrániť svoje práva, ale je zároveň povinný rešpektovať práva a oprávnené záujmy iných. Musí stále dohliadať na to, či je prevádzka monitorovacieho zariadenia nevyhnutná a či je akceptovateľným a primeraným zásahom do osobnostných práv, pretože k zásahom do osobnostných práv zamestnanca kvôli ochrane majetku alebo iných oprávnených záujmov zamestnávateľa by malo dochádzať len v odôvodnených prípadoch a pri dodržaní všetkých podmienok ustanovených Občianskym zákonníkom, Zákonníkom práce a ZOOÚ.

¹⁰² Pracovisko vymedzuje právna teória ako určitý priestor, v ktorom má zamestnanec vykonávať svoju prácu (napr. kancelária, dielňa, stavenisko), a pričom ide o pojem užší než miesto výkonu práce, ktoré si účastníci pracovnoprávneho vzťahu dohodli v pracovnej zmluve v zmysle § 43 ods. 1 písm. b/ Zákonníka práce. BARANCOVÁ, H., SCHRONK, R. *Pracovné právo*. Bratislava: SPRINT, 2007, s. 397.

3.2.1 Všeobecný právny rámec monitorovania zamestnancov na pracovisku

Legislatívny rámec monitorovania na pracovisku je v Slovenskej republike obsiahnutý v troch právnych normách: Zákonníku práce, Občianskom zákonníku a ZOOÚ, ktorého ustanovenia vo významnej miere dopĺňajú právnu úpravu v Zákonníku práce.

Primárna právna úprava monitorovania zamestnancov vyplýva z § 13 ods. 4 Zákonníka práce, v ktorom sa uvádza, že zamestnávateľ nemôže bez **vážnych dôvodov**¹⁰³ spočívajúcich v osobitnej povahe činnosti zamestnávateľa narušovať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa (okrem iného) aj tým, že ho monitoruje. Uvedené ustanovenie tak predstavuje jedinú zákonom (resp. Zákonníkom práce) povolenú výnimku prevádzkovania monitorovacieho zariadenia na pracovisku. V opačnom prípade, t. j. ak by nebola splnená materiálna podmienka existencie „vážnych dôvodov spočívajúcich v osobitnej povahe činnosti zamestnávateľa“, zamestnávateľ by nebol oprávnený monitorovať zamestnancov prostredníctvom sledovacieho systému a to ani v prípade, ak by ho na také monitorovanie inak oprávňoval súhlas zamestnanca.

Zo Zákonníka práce ani z osobitných pracovnoprávných predpisov však nevyplýva, na aké konkrétne druhy zamestnávateľov sa bude tento pojem vzťahovať a vysvetlenia nám neponúka ani doterajšia judikatúra súdov. V Dôvodovej správe k novele Zákonníka práce zákonom č. 316/2012 Z. z., ktorý nadobudol účinnosť 1. januára 2013 (k bodom 7 až 9) zákonodarca uviedol len jediný príklad takéhto vážneho dôvodu, a to prevenciu pred krádežou majetku. Zamestnávateľa majú prirodzene tendenciu presadzovať názor, že práve činnosť, ktorú vykonávajú, má „osobitnú povahu“.

Na základe uvedených dôvodov sme dospeli k záveru, že výklad tohto pojmu preto v aplikačnej praxi zostáva problematický. Uvažujúc o tomto z nášho hľadiska všeobecnom právnom pojme sme aj v súvislosti s predchádzajúcim výkladom o povahe súkromia dospeli k interpretácii, ktorá pod „osobitnou povahou činnosti zamestnávateľa“ rozumie v prvom rade rizikové pracoviská, kde môže dochádzať k nebezpečným situáciám (jadrové elektrárne, banky a pod.),¹⁰⁴ ale zároveň sa vzťahuje sa aj na iných „bežných“ zamestnávateľov, ak to odôvodňujú okolnosti konkrétneho prípadu. Pod „osobitnou povahou činnosti zamestnáva-

¹⁰³ Stačí, aby bol prítomný jediný dôvod, aj keď to nevyplýva priamo zo znenia citovaného ustanovenia, ale z príslušnej dôvodovej správy. Pozri Dôvodová správa k novele Zákonníka práce zákonom č. 361/2012 Z. z. – osobitná časť, k bodom 7 až 9.

¹⁰⁴ JANEČKOVÁ, E., BARTÍK, V. *Kamerové systémy v praxi. Právni režim z pohľadu ochrany osobných údajů a ochrany osobnosti*. Praha: Linde Praha, a.s., 2011, s. 68.

teľa“ treba podľa nášho názoru tiež rozumieť najmä takú činnosť zamestnávateľa, s ktorou sú spojené zvýšené nároky na správanie zamestnancov (napr. povinnosť mlčanlivosti, ochrana utajovaných skutočností, ochrana obchodného tajomstva alebo know how). Stotožňujeme sa s názorom Morávka, podľa ktorého vážny dôvod spočívajúci v osobitnej povahe činnosti zamestnávateľa treba vykladať vo vzťahu k činnosti zamestnávateľa v užšom zmysle (napr. zásobovanie, obsluha zákazníkov), teda ku konkrétnej práci a nie k činnosti v širšom zmysle (napr. podľa predmetu činnosti uvedenom v živnostenskom oprávnení a obchodnom registri), keďže môže nastať situácia, kedy pri činnosti v širšom zmysle, ktorá nemá taký charakter, že by mohla ospravedlniť zásah do súkromia zamestnancov, existuje úsek činnosti zamestnávateľa v užšom zmysle, kde taký dôvod daný je.¹⁰⁵

Ak sa na zamestnávateľa vzťahuje výnimka uvedená v § 13 ods. 4 Zákonníka práce, musí vykonať všetky opatrenia, aby zaistil, že nedôjde k neprimeranému zásahu do práva na súkromie zamestnancov. V praxi sa to prejavuje napríklad takým spôsobom, že ak zamestnávateľ nainštaluje monitorovací systém v šatniach na snímanie priestoru úložných (odkladacích) skriniek z dôvodu prevencie krádeží, má zároveň povinnosť zabezpečiť nejaký priestor – prezliakareň, na ktorý monitorovacie zariadenie nebude mať dosah. Zamestnávateľ musí pritom splniť ďalšie nevyhnutné podmienky stanovené v osobitných predpisoch. Špecifické povinnosti vyplývajú zamestnávateľovi nielen zo Zákonníka práce ale aj zo ZOOÚ, ktorý obsahuje podrobnejšiu právnu úpravu práv, povinností a jeho zodpovednosti pri spracúvaní osobných údajov (§ 5 ods. 1 a § 6 a nasl. ZOOÚ).¹⁰⁶

Z ustanovenia § 13 ods. 4 Zákonníka práce v platnom a účinnom znení oproti predošlej právnej úprave účinnej do 31. decembra 2012 vyplýva povinnosť zamestnávateľa **prerokovať so zástupcami zamestnancov** spôsob zavedenia vybraných prostriedkov určených na sledovanie a kontrolu, rozsah a čas ich vykonávania. Zamestnávateľ je tiež povinný **o kontrole vopred informovať** aj svojich zamestnancov vrátane skutočností týkajúcich sa spôsobu, rozsahu a času, ale tiež aj o dôvodoch kontroly. Najčastejšie sa v súvislosti s uvedenou kontrolou zamestnanca odporúča rozmiestniť informačné tabuľky na pracovisku (v znení napr. „tento priestor je monitorovaný kamerovým systémom“), ale tiež podrobne upraviť vo vnútornom predpise (pracovnom poriadku) či

¹⁰⁵ MORÁVEK, J. Možnosti monitorování zaměstnanců na pracovišti v právním řádu České republiky. In: BARANCOVÁ, H. a kol. *Monitorovanie zamestnancov a právo na súkromný život*, Bratislava: Sprint dva, 2010, s. 38 – 68.

¹⁰⁶ Povinnosti zamestnávateľa ako prevádzkovateľa informačného systému pri spracúvaní osobných údajov rozdeľujú autori Komentára k ZOOÚ s ohľadom na jednotlivé štádiá procesu spracúvania. Pozri kapitolu 4.5 Povinnosti zamestnávateľa ako prevádzkovateľa osobných údajov alebo VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 72 – 75.

kolektívnej zmluve rozsah, spôsob a čas kontroly zamestnancov monitorovacím systémom. S týmito dokumentmi musia byť riadne a preukázateľne oboznámení všetci zamestnanci.

Dôvod, pre ktorý sa zamestnávateľ rozhodne zaviesť na pracovisku monitorovacie zariadenia, definuje a do značnej miery limituje spôsob vykonania kontroly. Uvedenému dôvodu kontroly musí zamestnávateľ prispôbiť použité sledovacie zariadenia z organizačného i technického hľadiska. Tomu zodpovedá aj zámer zákonodarcu vyjadrený v dôvodovej správe k citovanej právnej úprave, kde zdôraznil, že monitorovanie zamestnancov by malo byť účelné, transparentné a primerané a zásahy do súkromia musia spĺňať podmienky dodržania zásady legality, legitimity a proporcionality v súlade s judikatúrou Európskeho súdu pre ľudské práva.¹⁰⁷ Povinnosť zamestnávateľa informovať o rozsahu kontroly sa viaže na druh zhromažďovaných údajov. O spôsobe kontroly v tomto prípade zamestnávateľ musí informovať o vymedzenom monitorovanom priestore, prípadne umiestnení kamier, o stanovenom spôsobe vyhotovovania záznamov a ich využívaní, tiež musí stanoviť, po aký čas budú takto zhromaždené údaje uchovávané, resp. dlhodobo archivované, a tiež aké osoby budú oprávnené na výkon kontroly, ku ktorým údajom budú mať prístup a na akej úrovni sú bezpečnostné opatrenia na zabránenie neoprávnenému prístupu k nim. Vnútorný predpis môže tiež upravovať disciplinárne konanie pre prípad porušenia bezpečnostných predpisov.

Medzi ustanovenia upravujúce možnosť vykonávania monitorovania na pracovisku patria napr. aj § 177, § 147 a § 82 Zákonníka práce. Podľa § 177 ods. 1 Zákonníka práce je zamestnávateľ povinný zabezpečovať pracovné podmienky, ktoré umožnia zamestnancom riadne plnenie pracovných úloh bez ohrozenia života, zdravia a majetku. Ak sa zistia nejaké nedostatky, je povinný urobiť opatrenia na ich odstránenie. Na ochranu majetku je zamestnávateľ podľa § 177 ods. 2 Zákonníka práce oprávnený vykonávať v nevyhnutnom rozsahu kontrolu vecí, ktoré zamestnanci vnášajú na pracovisko alebo odnášajú z pracoviska. Podmienky výkonu sledovania určí zamestnávateľ v pracovnom poriadku.

Možno podotknúť, že povinnosť riadiť a kontrolovať prácu zamestnancov prináleží predovšetkým vedúcemu zamestnancovi v súlade s § 82 písm. a/ Zákonníka práce. Zároveň je jeho kompetenciou i povinnosťou podľa písm. e/ a f/ citovaného ustanovenia zabezpečiť, aby nedochádzalo k porušovaniu pracovnej disciplíny a zabezpečiť, aby prijatie opatrení na ochranu majetku zamestnávateľa bolo efektívne a včasné. Z uvedeného vyplýva, že tento vedúci zamestnanec by mal byť sústavne prítomný na pracovisku a pravidelne sledovať výkonnosť práce vykonávanej jeho podriadenými.

¹⁰⁷ Dôvodová správa k novele Zákonníka práce zákonom č. 361/2012 Z. z. – osobitná časť, k bodom 7 až 9.

V rámci ochrany práce v zmysle § 147 ods. 1 Zákonníka práce je jeho povinnosťou zabezpečovať bezpečnosť a ochranu zdravia zamestnancov pri práci a vykonávať opatrenia vrátane zabezpečenia prevencie, prostriedkov a vhodného systému na riadenie ochrany práce. Podľa nášho názoru do rámca povinností zabezpečiť bezpečnosť, ochranu a prevenciu patrí aj povinnosť monitorovať dianie na pracovisku primeraným spôsobom.¹⁰⁸ Hranice (limity) takejto primeranej kontroly ustanovuje § 13 ods. 4 Zákonníka práce najmä v prípadoch, v ktorých dochádza ku kolízii s právom na ochranu súkromia.

3.2.2 Monitorovanie zamestnancov prostredníctvom kamerových systémov

Druhy kamerových systémov

Pri zavedení a prevádzkovaní kamerového systému je nevyhnutné z hľadiska definovania pôsobnosti relevantných právnych noriem a nimi určených povinností zamestnávateľa rozlišovať, či ide o **kamerový systém bez záznamu (tzv. on-line kamerový systém)** alebo **kamerový systém so záznamom**.

Za predpokladu, že zábery nie sú uchovávané na zariadení vyhotovujúcom záznam, ale obraz zachytený kamerovým systémom je len prenášaný on-line a kontrolovaný určenou osobou (zamestnancom), nedochádza k aplikácii ZOOÚ, pretože chýba naplnenie podmienky „spracúvania“ osobných údajov v zmysle § 4 ods. 3 písm. a/ ZOOÚ (t. j. nejde vôbec o spracúvanie osobných údajov). Aj v takom prípade však zamestnávateľ nesmie dohľad vykonávať v rozpore s ustanoveniami na ochranu ústavou garantovaných základných práv a slobôd alebo osobnostných práv v zmysle Občianskeho zákonníka.

V prípade, že sa záznamy z kamier uchovávajú na záznamovom zariadení a umožňujú identifikáciu fyzických osôb (tie môžu byť identifikované alebo identifikovateľné, buď priamo alebo nepriamo), môžeme hovoriť o spracúvaní osobných údajov v zmysle ZOOÚ. Monitorovaním priestoru pracoviska so záznamom totiž vzniká informačný systém, ktorého prevádzkovanie podlieha ZOOÚ a zamestnávateľ, ako jeho prevádzkovateľ, je tak povinný si splniť zákonné povin-

¹⁰⁸ V slovenskej právnej úprave nemáme ustanovenie, ktoré by zodpovedalo § 316 ods. 1 českého Zákonníka práce, ktoré zakotvuje zákaz zamestnancovi bez súhlasu zamestnávateľa používať na svoju osobnú potrebu výrobné a pracovné prostriedky zamestnávateľa vrátane výpočtovej techniky ani jeho telekomunikačné zariadenia, pričom dodržiavanie tohto zákazu je zamestnávateľ oprávnený primeraným spôsobom kontrolovať.

nosti, ktoré mu z neho vyplývajú.¹⁰⁹

Vychádzajúc z českej právnej úpravy ochrany osobných údajov v zákone č. 101/2000 Sb. o ochrane osobných údajů (ďalej len „český ZOOÚ“) má podobný názor aj Morávek, keď uvádza, že povinnosti vyplývajúce z českého ZOOÚ sa na zamestnávateľa budú vzťahovať len vtedy, pokiaľ bude využívať monitorovacie zariadenie – kamerový systém, ktorý uchováva záznam zachytených snímok či informácií za účelom ich využitia na identifikáciu fyzických osôb v súvislosti s určitým konaním.¹¹⁰ Podobne aj Štefko konštatuje, že sledovací systém, ktorý zachytáva a sprostredkúva len aktuálny snímok sledovaného priestoru bez následnej archivácie, nemožno považovať za monitorovacie zariadenie, ktoré podlieha právnej úprave ZOOÚ, pretože osobné údaje nespracováva. V prípade kamerového systému pritom zdôraznil, že musí ísť o systém, ktorý bude sledovať uzavreté priestory, kde sa predpokladá pohyb osôb.¹¹¹ Zamestnávateľ musí zabezpečiť a zamedziť po organizačnej a technickej stránke neoprávnený prístup k archivovaným záznamom – osobným údajom (prostredníctvom elektronického hesla, kódovaním údajov v prípade prenosu inému subjektu).

Dôvody zavedenia kamerových systémov

Dôvod zavedenia kamerových systémov úzko súvisí s typom zamestnávateľa a pracoviska, kde monitorovanie prebieha. K priestorom najčastejšie monitorovaným zamestnávateľmi patria výrobné haly, sklady, vstupné chodby (vrátnice a recepcie) a priestory bankových a úradných priehradiek, kde sa predpokladá manipulácia s finančnou hotovosťou, ktorá si vyžaduje zvýšenú ochranu. Na druhej strane medzi monitorované priestory, v ktorých zamestnanci môžu prirodzene očakávať, naopak, zvýšenú úroveň ochrany ich súkromia, patria kancelárie. Podľa nášho názoru sem však patria aj kancelárie pre dvoch alebo väčší počet zamestnancov typu „open-space office“. Ďalej sú to rôzne druhy priestorov slúžiacich u zamestnávateľa na stravovanie (jedálne, bary, kuchyne, bufety) a samozrejme aj sprchy, toalety, šatne, ale aj čakárne či oddychové miestnosti.¹¹²

¹⁰⁹ Pozri bližšie kapitolu 4.5 Povinnosti zamestnávateľa ako prevádzkovateľa osobných údajov.

¹¹⁰ Na tomto mieste treba podotknúť, že pokiaľ zo snímky zaznamenananej kamerovým systémom nie je možné identifikovať fyzickú osobu z dôvodu jej nízkej kvality alebo nemožnosti optického priblíženia či digitálneho zväčšenia, nemožno hovoriť o spracúvaní osobných údajov, pretože nie je naplnená jedna zo základných podmienok pôsobnosti ZOOÚ. Pozri Metodické usmernenie ÚOOÚ č. 1/2014, Monitorovanie priestoru prístupného verejnosti kamerovým systémom, s. 2.

¹¹¹ ŠTEFKO, M. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In: *Jurisprudence*, 2012, č. 7/8, s. 19.

¹¹² Obdobný názor zastáva vo svojom stanovisku aj Európsky dozorný úradník. EDPS. *European data protection supervisor video-surveillance guidelines*. (online). 2010, (cit. 2015-01-10),

Najčastejšie uvádzané „vážne dôvody“, ktorými zamestnávateľa odôvodňujú zavedenie kamerového systému, možno rozdeliť do dvoch skupín podľa cieľov, ktoré sa monitorovaním snažia dosiahnuť. Do prvej skupiny zaraďujeme kontrolu, či zamestnanci plnia svoje pracovné povinnosti a využívajú pracovný čas efektívne na dôsledné plnenie pracovných úloh (ide o sledovanie výkonnosti zamestnancov a efektivity práce) a či nedochádza na pracovisku prípadne k porušovaniu zákazu fajčenia, užívania alkoholu alebo omamných látok. Do druhej skupiny patria dôvody súvisiace s ochranou majetku zamestnávateľa prostredníctvom kontroly správnosti používania zariadení, prevencie krádeží a sledovania návštev na pracovisku.

Primeranosťou a oprávnenosťou zavádzaných sledovacích zariadení na pracoviskách, ktoré tiež úzko súvisia s dôvodmi monitorovania, sa zaoberajú aj príslušné inštitúcie na úrovni Európskej únie. Európsky dozorný úradník na ochranu osobných údajov (ďalej len „Európsky dozorný úradník“) vo svojej príručke k problematike videodohľadu (kamerovými systémami) na pracovisku konštatoval, že ciele monitorovania, ako napr. kontrola efektivity výkonu práce, kontrola požadovanej úrovne kvality (výrobných a služieb), dodržiavanie interných predpisov alebo snaha o získanie spoľahlivých a usvedčujúcich dôkazov pre prípad súdneho sporu so zamestnancom, nemôžu nikdy vystupovať ako samostatné dôvody na legitímne uskutočňovanie monitorovania na pracovisku. Vyjadril zároveň presvedčenie, že neprimerané kontrolné opatrenia môžu spôsobiť zamestnancom zbytočný stres s následkom narušenia dôvery k zamestnávateľovi, čo môže dokonca znížiť jeho motivácie a produktivity.¹¹³ Sledovanie na pracovisku pomocou kamerových systémov len na účel kontroly efektívnosti výkonu práce zamestnancov nepovažujeme v súlade s názorom Európskeho dozorného úradníka za prípustné. V diskusnej rovine akceptovanie takej situácie by podľa nášho názoru prichádzalo do úvahy len v krajnom prípade, ak by bol daný závažný dôvod zamestnávateľa, ktorý by vyhovoval striktným podmienkam testu proporcionality.¹¹⁴

Riešenie oprávnenosti zavádzania kamerových systémov na pracovisku spočíva v legálnosti a legitímnosti jeho samotnej inštalácie súvisiacej aj s množstvom a umiestnením kamier a jeho vplyvmi na súkromie zamestnanca. S poukazom na

Dostupné z: (https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf), s. 29.

¹¹³ EDPS. *European data protection supervisor video-surveillance guidelines*. (online). 2010, (cit. 2015-01-10). Dostupné z: (https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf), s. 22.

¹¹⁴ Ak je účelom kontroly (iba) efektívnosť výkonu práce zamestnanca a obsahom záznamu kamerového systému sú osobné údaje zamestnanca, zamestnávateľ by mal v súlade so zásadou transparentnosti minimálne umožniť, aby si zamestnanec mohol pozrieť vyhotovený záznam na jeho žiadosť.

názory Ústavného súdu Slovenskej republiky vyjadrené v náleze zo 4. februára 2009 sp. zn. I.ÚS 117/07¹¹⁵ sme dospeli k záveru, že ak je dôvodom inštalovania kamerového systému v priestoroch pracoviska predchádzanie krádežiam alebo odhalenie predaja či užívania alkoholických, omamných alebo psychotropných látok, pretože sa už v minulosti takéto prípady reálne vyskytli a zamestnávateľ v ich dôsledku utrpel majetkovú škodu, pričom nainštalovanie kamerového systému ich výrazne redukovalo, prípadne jeho pomocou bola odhalená osoba porušujúca normy pracovnoprávne alebo trestnoprávne, potom je prirodzené a zároveň právne prípustné očakávať, že zamestnávateľ bude chcieť nainštalovať kamerový systém na pracovisku s cieľom využiť ho v prípade pracovnoprávneho sporu, napr. o neplatné skončenie pracovného pomeru.

V súvislosti s vymedzením dôvodu monitorovania sa objavuje zaujímavá otázka vyplývajúca z praxe, či je prípustný dôkaz získaný monitorovaním z iného dôvodu (napr. kvôli získania dôkazov o spáchaní trestného činu krádeže tovaru zamestnancom zo skladu zamestnávateľa), ak bol pôvodný dôvod monitorovania na pracovisku vymedzený odlišne (napr. kontrola dodržiavania pracovnej disciplíny). Vo všeobecnosti platí, že iba dôkaz, ktorý je vyhotovený v súlade so zákonom, môže použiť účastník konania alebo orgán činný v trestnom konaní v rámci príslušného sporu, inak je jeho prípustnosť prinajmenšom pochybná.

Z toho vyplýva, že ak zamestnávateľ zavedie monitorovanie z iného dôvodu a zároveň zistí, že na pracovisku sa pácha trestná činnosť, vyhotovený záznam ako dôkaz podľa nášho právneho názoru nie je v zásade možné použiť v rámci žiadneho súdneho konania. V rámci trestného konania si myslíme, že každý dôkaz (aj napr. dôkaz v podobe videozáznamu vyhotovenom kamerovým systémom zamestnávateľa usvedčujúci zamestnanca zo spáchania trestného činu krádeže), ktorý nebol získaný orgánmi činnými v trestnom konaní, je nepoužiteľný proti zamestnancovi, ak sa má ním preukázať jeho vina.

Súd je však oprávnený voľne hodnotiť každý dôkaz, ktorý je mu predložený. Preto sa domnievame, že hoci súd je povinný nepripustiť nezákonne získaný dôkaz, ak to odôvodňujú výnimočné okolnosti, ktoré treba hodnotiť ad hoc, je možné takýto dôkaz pripustiť v rámci občianskoprávných sporov (napr. o neplatné skončenie pracovného pomeru). V takom prípade by dôkazy získané pomocou kamerového systému nemali byť odmietnuté a rozhodnutie súdu by malo na základe nimi preukázaných skutočností znieť v prospech zamestnávateľa. Ak by

¹¹⁵ Ústavný súd Slovenskej republiky v náleze zo 4. februára 2009 sp. zn. I.ÚS 117/07 vyjadril názor, že „zásah do práva na súkromie je prípustný, len ak je to v demokratickej spoločnosti nevyhnutné v záujme dosiahnutia legitímneho cieľa. Nevyhnutnosť potom musí skúmať všeobecný súd s ohľadom na konkrétne okolnosti prípadu s dôrazom na skutočnosť, či tieto neumožňujú dosiahnuť stanovený cieľ (predchádzanie zločinnosti) inak, ako zásahom do práva na rešpektovanie súkromného života a korešpondencie“.

však šlo o situáciu, keď by bol kamerový systém inštalovaný do priestorov toaliet alebo spích alebo prezliekarní na pracovisku a najmä bez toho, aby to odôvodňovali predchádzajúce okolnosti a vážne dôvody zamestnávateľa, dalo by sa očakávať rozhodnutie súdu vyznievajúce v prospech zamestnanca, ktorý by sa bránil na súde žalobou proti uvedeným zásahom do súkromia. Opäť však vyjadrujeme presvedčenie, že výsledok sporu bude závisieť od okolností konkrétneho prípadu.

Podmienky zavedenia kamerového systému

Pri spracúvaní vizuálneho (či audiovizuálneho) záznamu dochádza k zachytávaniu jednotlivých charakteristík a údajov dotknutej fyzickej osoby (resp. na získavanie a spracúvanie jeho osobných údajov), na základe ktorých ju možno pri istej minimálnej úrovni kvality záznamu identifikovať (t. j. ak je zo záznamu nepriamym alebo priamym spôsobom možné rozpoznať jej charakteristické znaky, najmä črty tváre).¹¹⁶ Týmto spôsobom monitorovania teda nepochybne dochádza aj k spracúvaniu osobných údajov zamestnancov.

Kontrola a sledovanie prostredníctvom kamerových systémov nie je podmienená získaním predchádzajúceho súhlasu zamestnancov podrobených monitorovaniu, pokiaľ sú splnené podmienky vyplývajúce zo znenia ustanovenia § 13 ods. 4 Zákonníka práce. V porovnaní s pracovnoprávnou úpravou, ktorá je k úprave v Občianskom zákonníku vo vzťahu špeciality, je podľa Vojčíka predchádzajúci súhlas zamestnanca nevyhnutným v zmysle § 12 ods. 1 Občianskeho zákonníka v prípade, ak zamestnávateľ používa na sledovanie prostriedky, prostredníctvom ktorých je možné vyhotoviť obrazové snímky, zvukové alebo obrazovo-zvukové záznamy.¹¹⁷ Takýto záznam môže obsahovať osobné údaje, ktoré podliehajú ochrane aj v zmysle § 4 ods. 1 ZOOÚ, pretože proces zachytenia, resp. uchovávanie záznamu hlasu, výzoru zamestnanca alebo jeho pracovného výkonu je spracúvaním osobných údajov podľa § 4 ods. 3 písm. a/ ZOOÚ, ktoré si vyžaduje jeho súhlas. Z uvedeného vyplýva, že súhlas zamestnanca ako fyzickej osoby s monitorovaním sa v zmysle Zákonníka práce v zásade nevyžaduje, ale vyžaduje sa v zmysle občianskoprávnej úpravy podľa Občianskeho zákonníka prípadne aj ZOOÚ.

Na základe tohto výkladu sme dospeli k názoru, že monitorovanie na pracovisku prostredníctvom kamerového systému so záznamom, ktorým dochádza k spracúvaniu osobných údajov zamestnancov, je prípustné:

¹¹⁶ BARTÍK, V., JANEČKOVÁ, E. Kamery se záznamovým zařízením na pracovišti. In. *Práce a mzda*, ISSN 0032-6208. 2010, roč. 58, č. 3, s. 30.

¹¹⁷ Súhlas zamestnanca je nevyhnutné získať ešte pred vyhotovením záznamu a nie je možné ho nahradiť súhlasom, ktorý oprávňuje nakladať s už vyhotovenými záznamami. Pozri bližšie VOJČÍK, P. a kol. *Občiansky zákonník. Stručný komentár*. Bratislava: Iura Edition, 2008, s. 64.

- **bez súhlasu dotknutých osôb**, ak sa na daný prípad vzťahuje výnimka v zmysle § 10 ods. 1 až 4 ZOOÚ, najmä **ak je to nevyhnutné plniť úlohy stanovené osobitným zákonom** (napr. aj Zákonníkom práce, zákonom č. 171/1993 Z. z. o Policajnom zbore¹¹⁸ a zákonom č. 1/2014 Z. z. o organizovaní verejných športových podujatí a o zmene a doplnení niektorých zákonov),¹¹⁹
- **inak len so súhlasom dotknutých osôb.**¹²⁰

Zdôrazňujeme, že zamestnávateľ nemôže inštalovať kamerový systém v prípade, ak získa, resp. si „vynúti“ súhlas všetkých zamestnancov na monitorovanie v pracovnej zmluve. Zamestnanec sa totiž nemôže vzdať svojho práva na ochranu súkromia na pracovisku, pretože základné ľudské práva a slobody sú neodňateľné, neodcudziteľné, nepremlčateľné a nezrušiteľné. Zároveň z § 17 ods. 1 Zákonníka práce vyplýva, že právny úkon, ktorým sa zamestnanec vopred vzdáva svojich práv, je neplatný. Aj v prípade, že by sa zamestnanec vzdal svojho práva, nemôže zamestnávateľ zaviesť na kontrolné účely žiadne opatrenia.¹²¹ Platí tiež, že od kogentného ustanovenia § 13 ods. 4 Zákonníka práce sa zamestnávateľ nemôže odchýliť, keďže podľa § 1 ods. 6 Zákonníka práce možno upraviť pracovné podmienky zamestnania a zamestnanca len výhodnejšie, ako to upravuje Zákonník práce alebo iný pracovnoprávny predpis, ak to výslovne nezakazujú alebo ak z ich povahy nevyplýva, že sa od nich nemožno odchýliť.

Treba sa zaoberať aj okruhom potenciálne monitorovaných osôb, keďže pomocou inštalovaného kamerového systému celkom bežne dochádza k spracúvaniu nielen osobných údajov zamestnancov, ale aj ďalších osôb, ktoré sa objavujú v monitorovaných priestoroch pracoviska náhodne (klienti, osobné návštevy). Aj voči takýmto skupinám osôb treba, aby si zamestnávateľ splnil minimálne informačnú povinnosť o monitorovaní (o monitorovanom priestore a subjekte

¹¹⁸ § 69 ods. 2 zákona č. 171/1993 Z. z.: „*Policajný zbor je oprávnený, ak je to potrebné na plnenie jeho úloh, vyhotovovať zvukové, obrazové alebo iné záznamy z miest verejne prístupných a zvukové, obrazové alebo iné záznamy o priebehu služobnej činnosti alebo služobného zákroku.*“

¹¹⁹ § 21 ods. 1 a 2 zákona č. 1/2014 Z. z.: „(1) *Pri organizovaní rizikového podujatia je organizátor podujatia povinný zriadiť pri vchodoch a východoch športového zariadenia a v priestoroch športového zariadenia kamerový systém, ktorý umožní v čase konania podujatia nepretržité monitorovanie uvedených priestorov a identifikáciu fyzickej osoby alebo iného predmetu a zabezpečí záznam v digitálnej forme. Túto povinnosť má organizátor podujatia na futbalovom podujatí a hokejovom podujatí najvyššej celoštátnej súťaže v kategórii dospelých, a ak to ustanovujú požiadavky medzinárodnej športovej organizácie alebo národného športového zväzu. (2) Kamerový systém musí byť zriadený tak, aby nezasahoval do súkromia fyzických osôb, ktoré nie sú účastníkmi podujatia.*“

¹²⁰ Splnenie tejto požiadavky sa môže v praxi ťažko dosiahnuť, pretože ako uvádzajú niektorí autori, je často nemožné vopred a celkom presne určiť okruh osôb, na ktoré bude mať kamerové zariadenie dosah. Pozri BARTÍK, V., JANEČKOVÁ, E. Kamery se záznamovým zařízením na pracovišti. In. *Práce a mzda*, ISSN 0032-6208. 2010, roč. 58, č. 3, s. 30.

¹²¹ JANEČKOVÁ, E., BARTÍK, V. *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde Praha, a.s., 2011, s. 55.

vykonávajúcom monitorovanie). Z uvedeného vyplýva, že všetky osoby, ktorých údaje sa v priestoroch pracoviska spracúvajú (stáli zamestnanci i náhodní návštevníci), musia mať príležitosť vopred sa oboznámiť s možnosťou, že sú, resp. budú, monitorovaní. V zmysle stanoviska Európskeho dozorného úradníka na ochranu osobných údajov by informácia (oznámenie) o monitorovaní, spĺňajúca požadované základné kritériá, mohla znieť aj nasledujúco: „*Kvôli vašej bezpečnosti sa táto budova a jej bezprostredné okolie monitoruje kamerovým systémom. Záznam je uchovávaný 48 hodín. Bližšie informácie nájdete na www.web.sk alebo na telefónnom čísle + 421912 345 678.*“¹²²

Uvedené teoretické závery demonštrujeme na nasledujúcich dvoch príkladoch z praxe. Cieľom prvého príkladu je poukázať na to, za akých skutkových okolností dochádza k porušeniu ZOOÚ, a naopak druhý reprezentuje príklad, kedy k jeho porušeniu nedochádza.

ZOOÚ sa bude vzťahovať aj na prípady, keď zamestnávateľ nainštaluje prostredníctvom externej firmy kamerový systém, napr. na pracovisku výrobnjej činnosti, ktorý bude nielen vyhotovovať, ale po istý čas aj uchovávať vyhotovené záznamy a na základe toho bude vyvodzovať následky za porušovanie pracovnej disciplíny. Ak sa zamestnávateľ domnieva, že ide iba o bežné monitorovanie jeho súkromného priestoru, zamestnancov informuje len prostredníctvom informačnej tabule. Obdobný prípad mal v Českej republike takú dohru, že ÚOOÚ ČR a príslušný inšpektorát práce považovali sťažnosť jedného zamestnanca firmy za porušenie práva na súkromie za dôvodnú. Konštatovali, že keďže šlo o vyhotovenie videozáznamu, ktoré patrí pod pojem spracovanie osobných údajov, a ktoré zároveň podlieha registrácii na ÚOOÚ ČR (a táto podmienka nebola splnená), zamestnávateľ porušil nielen český ZOOÚ, ale aj český Zákoník práce.¹²³ V Slovenskej republike máme obdobnú právnu úpravu, v zmysle ktorej takýto monitorovací systém by ako informačný systém rovnako podliehal za daných okolností registrácii na Úrade na ochranu osobných údajov podľa § 33 a nasl. ZOOÚ. Vzhľadom na uvedené si myslíme, že ak by si zamestnávateľ nespĺnil všetky podmienky stanovené ZOOÚ, mohlo by byť v prípade sporu jeho konanie kvalifikované ako nezákonné (aj v rozpore s § 13 ods. 4 Zákoníka práce).

Českí autori, ktorí vychádzajú z českej právnej úpravy, uvádzajú ako opačný príklad, že ak zamestnávateľ nainštaluje kamerový systém v obmedzenom a uzamknutom priestore pracoviska pre, resp. kvôli prevencii krádeží a ak tento

¹²² EDPS. *European data protection supervisor video-surveillance guidelines*. (online). 2010, (cit. 2015-01-10). Dostupné z: (https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf). s. 64.

¹²³ JANEČKOVÁ, E., BARTÍK, V. *Kamerové systémy v praxi. Právní režim z pohľadu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde Praha, a.s., 2011, s. 76.

systém pomôže odhaliť (resp. identifikovať) páchatela trestného činu krádeže alebo lúpeže v uzamknutom a zaistenom priestore, bez možnosti prístupu ďalších osôb, nepôjde o porušenie českého ZOOÚ ani Zákonníka práce.¹²⁴ Vzhľadom na predchádzajúci výklad vo vzťahu k dôvodom a podmienkam zavedenia monitorovacieho systému na pracovisku si myslíme, že rovnaký záver možno konštatovať aj v podmienkach slovenskej právnej úpravy.

Monitorovanie verejných priestorov zamestnávateľom

Na posúdenie pôsobnosti relevantných právnych predpisov pri zavedení akéhokoľvek systému na sledovanie zamestnancov, t. j. aj kamerového systému, je dôležitým ukazovateľom hlavne povaha prostredia, v ktorom sa bude tento systém využívať. Preto treba rozlišovať **priestor prístupný verejnosti (verejný) a neverejný (súkromný) priestor**.

Kamerové systémy inštalované na sledovanie priestorov prístupných verejnosti predstavujú nepochybne najmenšiu intenzitu zásahu do súkromia. Kvôli zvyšovaniu úrovne informovanosti prevádzkovateľov informačných systémov osobných údajov o zákonom stanovených podmienkach a predpokladoch, ktoré sa na nich kladú, vydal ÚOOÚ v auguste roku 2014 Metodické usmernenie č. 1/2014. Metodické usmernenie sa zameriava na základné povinnosti prevádzkovateľa kamerového systému, čiže aj na každého zamestnávateľa monitorujúceho verejnú priestranosť. Z obsahu usmernenia vyplýva, že pri posúdení opodstatnenosti a legálnosti kamerového systému treba citlivo hodnotiť všetky okolnosti, ktoré majú pozitívny či negatívny vplyv na práva a právom chránené záujmy prevádzkovateľa aj dotknutých osôb, najmä ak prevádzkovateľ vykonáva v rámci monitorovania pracoviska aj monitorovanie priestorov prístupných verejnosti.¹²⁵

Kamerový systém, ktorý monitoruje priestoru prístupného verejnosti, v ktorom sa pohybujú dotknuté fyzické osoby a kvalita snímania obrazu je dostatočná na určenie ich charakteristických, resp. identifikujúcich črt, je totiž tiež považovaný za informačný systém spracúvajúci osobné údaje.¹²⁶ Každý zamestnávateľ ako

¹²⁴ JANEČKOVÁ, E., BARTÍK, V. *Kamerové systémy v praxi. Právni režim z pohľadu ochrany osobných údajů a ochrany osobnosti*. Praha: Linde Praha, a. s., 2011, s. 76 – 77.

¹²⁵ Význam usmernenia spočíva v obmedzení porušovania ZOOÚ prevádzkovateľmi kamerových systémov monitorujúcich verejnú priestranosť tým, že im poskytuje informácie o skutočnostiach, akými sú: vymedzenie účelu spracúvania osobných údajov (§ 15 ods. 7 prvá veta ZOOÚ) a oprávnených dôvodov monitorovania, splnenie požiadaviek primeranosti a nevyhnutnosti monitorovania kamerovým systémom a využitia záznamu iba za účelom uplatňovania právnej zodpovednosti v rámci priestupkového alebo trestného konania, ak osobitný zákon neustanovuje inak. Obsahom sú aj povinnosti vo vzťahu k dodržiavaniu lehoty stanovenej na uchovávanie záznamu z kamerového systému a spôsob označenia monitorovaného priestoru.

¹²⁶ V tejto súvislosti je zaujímavé aj pomerne nové rozhodnutie Súdneho dvora Európskej únie

prevádzkovateľ zariadenia monitorujúceho (aj) priestor prístupný verejnosti musí preto rešpektovať ustanovenia ZOOÚ. Predmetný zákon pritom nerozlišuje medzi prevádzkovateľom kamerového systému so záznamom a prevádzkovateľom kamerového systému, ktorý záznam nevyhotovuje, ak obidva systémy umožňujú identifikáciu osôb. Zároveň je z hľadiska ZOOÚ irelevantné, či pri monitorovaní určeného priestoru sa vyhotovuje záznam a ukladanie na nosič informácií, alebo ide len o priamy prenos z monitorovaného priestoru na zobrazovaciu jednotku pomocou kamery (tzv. streaming). Pre pôsobnosť zákona taktiež nie je podstatné, či prevádzkovateľ má kamerový systém, z ktorého sú výstupy spracovávané napr. prostredníctvom internetu (prenášanie obrazu v režime OCTV¹²⁷) alebo iba v rámci uzatvoreného televízneho okruhu (režim CCTV¹²⁸).¹²⁹

3.2.3 Monitorovanie elektronickej pošty zamestnancov

Občiansky zákonník chráni súkromie zamestnancov vo vzťahu k písomnostiam osobnej povahy (§ 12). Vojčík uvádza, že písomnosti osobnej povahy sú písomnosti vytvorené a určené na súkromné účely, pričom písomnosť definuje ako „*písomne zachytený prejav patriaci do súkromnej, intímnej sféry občana, týkajúcej sa najmä jeho predstáv, myšlienok, názorov, pocitov*“. Ďalej uvádza, že z obsahového rámca tohto pojmu sú prirodzene „*vylúčené písomnosti, ktoré majú úradný charakter (týkajúce sa hospodárskej činnosti a výkonu povolania, úradné spisy i rozhodnutia orgánov a pod.)*“.¹³⁰ Z uvedenej definície možno dospieť k záveru, že aj elektronic-
ká pošta sa považuje za písomnosť a jej obsah podlieha ochrane listového tajom-

z 11. decembra 2014 v právnej veci František Ryněš v. Úřad pro ochranu osobních údajů České republiky, vec C-212/13, v ktorom konštatoval, že „*článok 3 ods. 2 druhá zarážka smernice Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov sa má vykladať v tom zmysle, že prevádzkovanie kamerového systému umiestneného fyzickou osobou na jej rodinnom dome na účely ochrany majetku, zdravia a života majiteľov domu, ktorý umožňuje obrazový záznam osôb ukladaný do nahrávacieho zariadenia, na ktorom sa záznam priebežne nahráva na harddisk, pričom ten systém sníma tiež verejné priestranstvo, nepredstavuje spracovanie údajov na výkon výlučne osobných alebo domácich činností v zmysle tohto ustanovenia*“.

¹²⁷ OCTV je skratkou z angl. pojmu „opened-circuit television“ a znamená otvorený televízny okruh, čiže bežné širokopásmové vysielanie dostupné prakticky každému.

¹²⁸ CCTV je skratkou z angl. pojmu „closed-circuit television“ a znamená uzavretý televízny okruh, v ktorom sa signál z kamier prenáša na uzavretý, resp. významne obmedzený počet používateľov. Zábery z CCTV systému vidí iba ten, kto má na to oprávnenie.

¹²⁹ Metodické usmernenie ÚOOÚ č. 1/2014, Monitorovanie priestoru prístupného verejnosti kamerovým systémom, s. 2.

¹³⁰ VOJČÍK, P. a kol. *Občiansky zákonník. Stručný komentár*. Bratislava: Iura Edition, 2008, s. 56 a 57.

stva a tajomstva prepravovaných správ. Ochranu listového tajomstva a tajomstva prepravovaných správ zaručuje článok 22 Ústavy Slovenskej republiky. Zároveň je obsiahnutá v § 8 zákona č. 507/2001 Z. z. o poštových službách (ako poštové tajomstvo)¹³¹ a v zákone č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov.¹³² Ochrane v zmysle uvedených právnych noriem nepodliehajú písomnosti a správy už doručené.

Tajomstvo písomností a prepravovaných správ je v zmysle trestnoprávnej úpravy chránené len od okamihu odovzdania na prepravu (t. j. ich podania) až do okamihu ich dodania príjemcovi (napr. dodaním na odovzdávacom mieste, ktorým je byt, domová schránka, poštová priehradka a podobne, prípadne podaním správy prostredníctvom elektronickej komunikačnej služby do konkrétneho počítača, resp. do počítačovej siete).¹³³ Ak zamestnávateľ poruší tajomstvo prepravovaných správ a nejde o oprávnený zásah do listového tajomstva a tajomstva prepravovaných správ napr. v zmysle § 108 až 110 zákona č. 301/2005 Z. z. Trestného poriadku, vzniká mu trestnoprávna zodpovednosť za úmyselný trestný čin podľa § 196 zákona č. 300/2005 Z. z. Trestného zákona,¹³⁴ ktorý možno kvalifikovať z hľadiska závažnosti a nebezpečnosti ako prečin.

Kontrolou na pracovisku nesmie dochádzať k zásahom do osobnostných práv zamestnanca podľa § 11 Občianskeho zákonníka, len ak by bol daný závažný dôvod spočívajúci v osobitnej povahe činnosti zamestnávateľa v zmysle § 13 ods. 4 Zákonníka práce, ktorý by oprávňoval zamestnávateľa na monitorovanie

¹³¹ Ustanovenie § 8 zákona o poštových službách zakotvuje predmet poštového tajomstva ako informácie a údaje o poštových zásielkach, obsah korešpondencie (listové tajomstvo) a obsah ostatných poštových zásielok.

¹³² Ustanovenie § 4 a 5 zákona o elektronických komunikáciách chráni listové tajomstvo pred vyzvedaním alebo otvorením uzavretého listu alebo inej prepravovanej písomnosti, tajomstvo informácie prenášanej prostredníctvom elektronickej komunikačnej služby, alebo tajomstvo verejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci a ďalšie technické systémy.

¹³³ Komentár ASPI k § 196 Trestného zákona.

¹³⁴ Podľa § 196 ods. 1 Trestného zákona „*kto úmyselne poruší a) listové tajomstvo vyzvedaním alebo otvorením uzavretého listu alebo inej písomnosti prepravovanej poštovým podnikom alebo iným obvyklým spôsobom, b) tajomstvo informácie prenášanej prostredníctvom elektronickej komunikačnej služby, alebo c) tajomstvo verejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci, vrátane elektromagnetického vyžarovania z počítačového systému, prenášajúceho takéto počítačové dáta, potrestá sa odňatím slobody až na tri roky*“. Komentár ASPI k § 196 Trestného zákona uvádza, že „*porušením tajomstva vyzvedaním sa rozumie predovšetkým otvorenie uzavretého listu bez ohľadu na to, či bol jeho obsah niekomu oznámený, ďalej prezradenie správy podanej v otvorenom liste (korešpondenčnom lístku, pohľadnici, v otvorenej listovej zásielke a pod.), ako aj náhodné vypočutie a následné prezradenie správy pri telefonickom alebo telegrafickom styku atď. Analogicky pôjde aj o porušenie tajomstva informácie prenášanej prostredníctvom elektronickej komunikačnej služby, verejným prenosom počítačových dát, resp. elektromagnetickým vyžarovaním z počítačového systému, ktorý prenáša takéto počítačové dáta*“.

hospodárenia so zverenými prostriedkami, t. j. aj formou kontroly elektronickej pošty a pohybu na internetových stránkach. V spojitosti s rozvojom technológií a informatizáciou spoločnosti majú zamestnávateľa potrebu čoraz dôslednejšie kontrolovať svojich zamestnancov v súvislosti s dodržiavaním pracovnej disciplíny a využívaním pracovného času a pracovných prostriedkov výlučne na výkon práce pre zamestnávateľa. Ako sme už v práci uviedli medzi oprávnenia zamestnávateľa patrí právo primeraným spôsobom kontrolovať, ako zamestnanci hospodária s hodnotami zverenými na výkon práce. Medzi základné povinnosti zamestnanca totiž patrí podľa § 81 písm. e/ *Zákonníka práce* „*povinnosť hospodáriť riadne s prostriedkami, ktoré mu zveril zamestnávateľ, a chrániť jeho majetok pred poškodením, stratou, zničením a zneužitím a nekonať v rozpore s oprávnenými záujmami zamestnávateľa*“.

Najbežnejšou formou zneužívania elektronických pracovných prostriedkov zamestnancami je používanie pracovného e-mailu na súkromné účely, on-line nákupy, alebo surfovanie na internete a sociálnych sieťach počas pracovného času. V prvom rade treba uviesť, že zverené prostriedky nie je zamestnanec oprávnený na pracovisku využívať na súkromnú listinnú korešpondenciu či e-mailovú komunikáciu. V zásade platí, že pracovná e-mailová schránka sa má používať výlučne na pracovné účely, len ak by zamestnávateľ výslovne dovolil používanie pracovnej e-mailovej adresy aj na súkromné účely. Možno dokonca vysloviť domnienku, že ak sú korešpondencia, resp. e-mail, doručené na pracovisko, považujú sa za pracovné a nepodliehajú ochrane súkromia zamestnanca, ak okolnosti nenasvedčujú, že platí opak.¹³⁵

Pracovnú elektronickej poštu treba striktne odlišovať od súkromnej elektronickej pošty. Z uvedeného možno dospieť k záveru, že obsah pracovných e-mailov môže zamestnávateľ, resp. nadriadený legálne otvoriť a kontrolovať kedykoľvek. Stretli sme sa však aj s názorom, že zamestnávateľ môže otvárať súkromné e-maily doručené do pracovnej e-mailovej schránky iba vtedy, keď zamestnanca vopred upozornil, že jeho pracovná e-mailová schránka je monitorovaná.¹³⁶ Ak však výslovne zamestnávateľ povolí používanie pracovného e-mailu aj na súkromné účely a z identifikačných znakov správy, akými sú odosielateľ, predmet správy či oslovenie príjemcu je evidentné, že ide o súkromný e-mail, v tom prípade nie je zamestnávateľ oprávnený za žiadnych okolností otvoriť a zisťovať obsah takej komunikácie.

¹³⁵ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 406.

¹³⁶ HVOZDOVIČOVÁ, J. *Sledovanie v práci je na dennom poriadku*. Sme (online). 2011. (cit. 2015-02-10). Dostupné z: (<http://ekonomika.sme.sk/c/6129902/sledovanie-v-praci-je-na-dennom-poriadku.html#ixzz1dEZACiRX>).

Diametrálne odlišná situácia nastáva vtedy, keď zamestnanec nie je na pracovisku a kvôli hrozbe zásahu do majetkovej sféry zamestnávateľa treba urobiť neodkladné úkony spočívajúce v získaní informácií z pracovného e-mailu tohto zamestnanca. Počas neprítomnosti zamestnanca na pracovisku za uvedených okolností možno pripustiť, že zamestnávateľ bude oprávnený otvoriť a čítať pracovnú korešpondenciu. Súhlasíme však s názorom, že pokiaľ zistí, že obsah korešpondencie, ktorú nemohol pred otvorením identifikovať ako súkromnú, má súkromný charakter, je povinný jej čítanie bezodkladne ukončiť, pretože akékoľvek ďalšie pokusy o zistenie obsahu tejto komunikácie môžu byť kvalifikované ako porušenie listového tajomstva.¹³⁷

K oprávnenosti zamestnávateľa kedykoľvek monitorovať obsah pracovnej elektronickej pošty a použiť informácie získané takým spôsobom ako dôkaz v súdnom konaní, možno uviesť zaujímavý prípad z praxe. Zo skutkových okolností vybraného prípadu vyplýva, že zamestnávateľ sledovaním obsahu doručených a odoslaných e-mailov na pracovnú e-mailovú adresu zamestnanca s prístupom k obchodnému alebo bankovému tajomstvu odhalil jeho závažné protiprávne konanie, spočívajúce v skopírovaní a odoslaní množstva údajov zamestnávateľa o klientoch a zamestnancoch, pracovných postupoch, hodnoteniach, projektoch, prezentáciách a know-how na inú súkromnú adresu. Na základe ustálenej judikatúry súdov je v takom prípade tzv. „krádeže údajov“ akceptovateľné zo strany zamestnávateľa aj okamžité skončenie pracovného pomeru pre závažné porušenie pracovnej disciplíny, lebo ide o situáciu, keď nie je možné od zamestnávateľa spravodlivo požadovať, aby zamestnanca zamestnával až do uplynutia výpovednej lehoty. Možno sa totiž dôvodne domnievať, že v dôsledku predmetného konania zamestnanca bola vážne narušená dôvera medzi účastníkmi pracovnoprávneho vzťahu a zamestnávateľovi hrozí alebo bola spôsobená väčšia škoda. Takto získaný dôkaz preto môže podľa nášho názoru zamestnávateľ použiť v prípade pracovnoprávneho sporu, pretože aby zamestnávateľ mohol skončiť pracovný pomer (či už výpoveďou alebo okamžite), musí disponovať dôkazmi, na základe ktorých bude mať súd za dostatočne preukázané, že zamestnanec zavinene porušil pracovnú disciplínu (resp. svoje pracovné povinnosti).¹³⁸

¹³⁷ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 406.

¹³⁸ Na skončenie pracovného pomeru pre porušenie pracovnej disciplíny je preto dôležité, aby zamestnávateľ preukázal zavinenie zamestnanca (úmysel alebo aspoň nedbanlivosť). Pretože pojem „zavinenie“ Zákonník práce ani iný pracovnoprávny predpis nedefinuje, treba vychádzať pri výklade tohto pojmu zo „zavinenia“, upraveného v Trestnom zákone. Pozri OLŠOVSKÁ, A. *Skončenie pracovného pomeru z dôvodu porušenia pracovnej disciplíny*. e-pravo (online). 2014. (cit. 2015-03-09). Dostupné z: (<http://www.epravo.sk/top/clanky/skoncenie-pracovneho-pomeru-z-dvodu-porusenja-pracovnej-discipliny-1796.html>).

Doteraz ESLP vo viacerých rozhodovaných právnych veciach akceptoval, že zamestnávateľ môže legitímne kontrolovať, či zamestnanec nevyužíva služobný telefón, elektronickú poštu alebo internet v rozpore s oprávnenými záujmami zamestnávateľa. Z jeho doterajšej judikatúry však tiež vyplýva, že zamestnávateľ nesmie sledovať a spracovávať obsah telefonickej, e-mailovej a listinnej komunikácie svojich zamestnancov, pričom ale zatiaľ nevydal rozhodnutie, v ktorom by zakázal zamestnávateľom monitorovanie počtu doručených a odoslaných e-mailových správ na pracovnú e-mailovú adresu, a to vrátane údajov o odosielateľoch a adresátoch správ.¹³⁹

Monitorovanie elektronickej pošty bolo ústrednou témou aj rozhodnutia ESLP vo veci *Copland v. Spojené kráľovstvo*,¹⁴⁰ pričom jeho postoj ku chápaniu pojmu „súkromie“ už na rozdiel od dovtedajšej judikatúry nevyznel jednoznačne a bezpodmienečne v prospech zamestnanca. Zo skutkových okolností daného prípadu je zrejmé, že zamestnávateľ nariadil monitorovanie telefonických hovorov sťažovateľky, ktorá bola zamestnaná ako asistentka riaditeľa štátnej vzdelávacej inštitúcie. Okrem toho nariadil aj sledovanie jej elektronickej pošty a zároveň pohyb na internete. Nesledoval však obsah komunikácie, ale záznamy o komunikácii uskutočnené cez telekomunikačné zariadenia (výpisy volaných čísel, odosielateľov e-mailov). Britská vláda pred ESLP tvrdila, že monitorovanie prebehlo kvôli zisteniu, či žalobkyňa nadmerne nepoužívala telekomunikačné zariadenia školy na osobné účely. Vláda ďalej uvádzala, že monitorovanie telefónnych hovorov sa skladalo len z analýzy telefónnych účtov vysokej školy, na ktorých boli zobrazené volané čísla, dátumy, čas volaní, rovnako ako aj dĺžka a cena hovorov. Žalobkyňa však tvrdila, že došlo k detailnému a podrobnému zaznamenávaniu dĺžky a počtu hovorov, ktoré prijala alebo volala a zaznamenávali sa aj telefónne čísla súkromných osôb, ktoré jej volali. Ďalej uviedla, že aspoň pri jednej príležitosti sa zamestnávateľ dozvedel meno fyzickej osoby, s ktorou telefonovala. Pani Copland si myslela, že monitoringu podliehala aj jej e-mailová korešpondencia v práci, keďže zamestnávateľ od jej rodinného príslušníka žiadal, aby poskytol informácie o e-mailoch, ktoré jej poslal.

Po preskúmaní danej veci ESLP v súlade so svojou predchádzajúcou rozhodovacou činnosťou¹⁴¹ konštatoval, že pod pojem súkromný život a korešpondencia

¹³⁹ ŠTEFKO, M. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In: *Jurisprudence*, 2012, č. 7/8, s. 20. Porovnaj tiež Stanovisko ÚOOÚ ČR, č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelom k monitoringu pracoviště.

¹⁴⁰ Rozsudok ESEP z 3. apríla 2007 v právnej veci *Copland v. Spojené kráľovstvo*, sťažnosť č. 62617/00.

¹⁴¹ Napr. rozsudok ESEP z 25. júna 1997 v právnej veci *Halford v. Spojené kráľovstvo* a rozsudok zo 16. februára 2000 v právnej veci *Amann v. Švajčiarsko*.

v zmysle čl. 8 ods. 1 Dohovoru možno subsumovať okrem telefonických hovorov aj používanie elektronickej pošty a internetu. Zároveň uviedol, že aj keď zhromaždené údaje sa ďalej nevyužívali, už samotné zhromažďovanie dát môže byť kvalifikované ako zásah do súkromného života. ESLP nakoniec dospel k záveru, že monitorovanie činnosti konkrétneho zamestnanca na pracovisku nebolo vopred ohlásené a v čase zásahu do súkromia sťažovateľky neboli u zamestnávateľa právne zakotvené podmienky legálneho monitorovania telefonických hovorov a využívania internetu interným predpisom alebo všeobecne záväzným predpisom, preto došlo k porušeniu práva garantovaného čl. 8 Dohovoru. Pripustil však, že v niektorých špecifických situáciách, najmä ak je to nevyhnutné na dosiahnutie legitímnych cieľov, môže byť zásah do súkromia akceptovateľný.¹⁴² ESLP týmto rozhodnutím v podstate otvoril cestu diskusii o tom, aké kritériá si treba zvoliť, aby sme boli schopní posúdiť legitimitu, ale aj akceptovateľnosť zásahu do súkromia monitorovaním elektronickej pošty zamestnancov. Zdôraznil nielen dôležitosť súdnej interpretácie existujúcich všeobecných noriem na ochranu súkromia, ale aj význam presnej špecifikácie spôsobov prípustnej kontroly vo vnútornom predpise zamestnávateľa.

Medzi najrozšírenejšie spôsoby kontrolovania elektronickej pošty zamestnancov patrí skenovanie elektronickej pošty s cieľom detekovať vírusy alebo odfiltrovať spamy, skríning elektronickej pošty na účely detekcie vopred určeného obsahu a služba na detekciu prečítania e-mailu („Did they read it“).

Skenovanie elektronickej pošty s cieľom detekovať vírusy

Chrániť technické pracovné zariadenia, napr. počítače pred vírusmi, ktoré môžu závažným spôsobom poškodiť, resp. zničiť ich programové vybavenie, sú povinní poskytovatelia elektronickej komunikačnej služby (t. j. buď priamo zamestnávateľa, ktorí zodpovedajú za poskytovanie služieb elektronickej pošty na pracovisku, alebo zamestnávateľa prostredníctvom dodávateľa tejto služby na základe zmluvy). Na jej výkon musia uskutočniť podľa čl. 4 smernice č. 2002/58/ES vhodné technické a organizačné opatrenia tak, aby zaručili bezpečnosť svojich služieb. V prípade, ak je to z hľadiska bezpečnosti siete nevyhnutné, môžu tak urobiť aj v spolupráci s poskytovateľom verejnej komunikačnej siete.

Barancová definuje skríning elektronickej pošty ako bezpečnostné opatrenie, ktoré je zamerané na bezpečnosť a ochranu systému správcu údajov. V praxi totiž v prípade doručenia e-mailu obsahujúceho vírus na e-mailovú adresu zamestnanca, sa môžu poškodiť ďalšie dokumenty alebo softvér uchovávaného v koncovom

¹⁴² Rozsudok ESLP z 3. apríla 2007 v právnej veci Copland v. Spojené kráľovstvo, sťažnosť č. 62617/00.

zariadení používateľa a spôsobiť tak výpadok systému poskytovateľa elektronickej pošty. To môže v konečnom dôsledku až narušiť prenos ďalšej e-mailovej komunikácie.¹⁴³

Pri skríningu e-mailov poskytovateľa služieb elektronickej pošty musia zabezpečiť,

- aby obsah e-mailov a príloh zostal v tajnosti pred tretími osobami okrem príjemcu,
- v prípade detekcie vírusu musí nainštalovaný softvér poskytovať dostatočné záruky zachovania dôvernosti korešpondencie,
- ak sa antivírusové opatrenie uskutočňuje formou skenovania obsahu, malo by sa spúšťať automaticky a výlučne na tento účel, pretože sa nesmie analyzovať obsah e-mailov zo žiadneho iného dôvodu.¹⁴⁴

Skenovanie (skríning) elektronickej pošty s cieľom odfiltrovať spam

Uvedené opatrenie by malo zamestnancov chrániť pred nevyžiadanou poštou, ktorú systém automaticky vyhodnotí ako „spam“. Zo stanoviska Pracovnej skupiny 29 č. 2/2006 vyplýva, že spam vo svojej podstate ohrozuje skôr celkovú výkonnosť siete a najmä služby elektronickej pošty než bezpečnosť služieb poskytovateľa služby elektronickej pošty. Jeho výskyt môže spôsobiť, že poskytovateľ stratí schopnosť poskytovať túto službu. Uvedený spôsob skenovania e-mailov je rizikový v tom, že pri filtrovaní spamu sa môže aj zabrániť doručenie žiadanej, legálnej pošty, čo môže byť za istých okolností neoprávnený zásah do súkromnej komunikácie a porušenie čl. 10 Dohovoru. Preto by bolo podľa názoru Pracovnej skupiny 29 vhodnejším riešením, ak by používateľom elektronickej pošty (zamestnancom) zostala zachovaná možnosť kontroly všetkých doručených e-mailov, t. j. vrátane e-mailov odfiltrovaných automaticky do osobitnej kategórie „spam“ a sami zamestnanci by sa rozhodli, či ide skutočne o nevyžiadajú poшту a či má byť odfiltrovaná.¹⁴⁵

¹⁴³ BARANCOVÁ, H. a kol. *Základné práva a slobody v pracovnom práve*. Plzeň: Aleš Čeněk, 2012, s. 118 – 119.

¹⁴⁴ Stanovisko Pracovnej skupiny 29 č. 2/2006, ktorá sa zaoberá problematikou ochrany súkromia v kontexte poskytovania služieb spočívajúcich v skríningu elektronickej pošty z 21. februára 2006, WP 118, s. 6. Tiež BARANCOVÁ, H. a kol. *Základné práva a slobody v pracovnom práve*. Plzeň: Aleš Čeněk, 2012, s. 119.

¹⁴⁵ Stanovisko Pracovnej skupiny 29 č. 2/2006, ktoré sa zaoberá problematikou ochrany súkromia v kontexte poskytovania služieb spočívajúcich v skríningu elektronickej pošty z 21. februára 2006, WP 118, s. 8.

Skríning elektronickej pošty na účely detekcie vopred určeného obsahu

Pri uskutočňovaní tohto typu filtrovania dochádza k cenzúre súkromnej e-mailovej komunikácie poskytovateľmi služieb elektronickej pošty napr. preto, že obsah komunikácie nie je v súlade so zákonom. Pracovná skupina 29 dospela k názoru, že poskytovatelia služieb elektronickej pošty nielenže nemajú povinnosť monitorovať vopred určený obsah alebo obsah, pri ktorom existuje podozrenie zo škodlivého charakteru, ale že v zmysle článku 5 ods. 1 smernice č. 2002/58/ES nemajú oprávnenie filtrovať, uchovávať alebo uskutočňovať iné druhy zachytávania komunikácie alebo súvisiacich prevádzkových údajov na účely detekcie vopred určeného obsahu bez súhlasu používateľov služby. Jediná výnimka, oprávňujúca uskutočniť takýto skríning, len ak to ustanovuje zákon, je obsiahnutá v článku 15 smernice č. 2002/58/ES implementovanej prostredníctvom právnych predpisov členských štátov.¹⁴⁶

Služba na detekciu prečítania e-mailu („Did they read it“)

Ide o osobitný typ služby, ktorý sprostredkúva používateľovi služby elektronickej pošty možnosť zistiť, či ním odoslaný e-mail a) adresát, resp. adresáti prečítali, b) kedy bol prečítaný, c) koľkokrát bol prečítaný (alebo prinajmenšom koľkokrát došlo k jeho otvoreniu), d) či bol odoslaný ďalším osobám a e) na ktorý e-mailový server bol odposlaný a kde sa tento server nachádza. Služba napokon umožňuje aj zistiť, ktorý typ internetového prehliadača a operačného systému príjemca e-mailu používa. To znamená, že o spracúvaní takých údajov nie sú poskytnuté príjemcom e-mailov, od ktorých sa tieto údaje získavajú, žiadne informácie. Príjemcom navyše nie je daná na výber možnosť odsúhlasiť, resp. nepovoliť, používateľovi systému spracovanie informácií súvisiacich s potvrdením prijatia e-mailov. Pracovná skupina 29 videla problém v realizácii a využívaní tejto služby skrytou formou. Podľa jej názoru skryté spracovanie predmetných informácií odporuje zásadám ochrany údajov obsiahnutým v článku 7 a 10 smernice č. 95/46/EHS, keďže na také spracovanie údajov musí poskytovateľ služby najprv získať od príjemcu e-mailu výslovný a jednoznačný súhlas.¹⁴⁷

¹⁴⁶ Stanovisko Pracovnej skupiny 29 č. 2/2006, ktoré sa zaoberá problematikou ochrany súkromia v kontexte poskytovania služieb spočívajúcich v skríningu elektronickej pošty z 21. februára 2006, WP 118, s. 9.

¹⁴⁷ Stanovisko Pracovnej skupiny 29 č. 2/2006, ktoré sa zaoberá problematikou ochrany súkromia v kontexte poskytovania služieb spočívajúcich v skríningu elektronickej pošty z 21. februára 2006, WP 118, s. 10.

Sociálne a psychologické dôsledky využívania e-mailovej komunikácie medzi zamestnancami

Komunikácia výhradne prostredníctvom počítačov, internetu a mobilných zariadení v posledných rokoch spôsobuje, že ľudia vo firmách vzájomne osobne komunikujú čoraz menej. Tento trend sa vyvinul až do tej miery, že aj kolegovia sediaci pár metrov od seba uprednostňujú na komunikáciu chatom alebo e-mailom. Z nedávnej tlačovej správy prevzatej z britskej televíznej a rozhlasovej stanice BBC vyplýva, že vedenie britskej firmy Procure Plus si všimlo negatívny vplyv tohto novodobého fenoménu na zamestnancov i chod celej firmy a pokúsilo sa o istý druh sociologického a psychologického experimentu. Priamo nariadilo svojim 40 zamestnancom, že každá interná komunikácia musí prebiehať akýmkoľvek iným spôsobom než cez elektronickú poštu a boli teda povinní uprednostniť telefóny, mítingy či osobný kontakt. Zamestnanci si spočiatku po rozpačitej adaptácii na nové podmienky na pracovisku po veľmi krátkom čase zvykli na firemné nariadenia hraničiace so sociologickým výskumom. Výsledkom zavedeného opatrenia bola redukcia e-mailov o 50 percent a zlepšila sa vzájomná osobná interakcia v pracovnom prostredí. Spokojnosť s výsledkom viedla k tomu, že pri nariadeniach firma zotrvala.¹⁴⁸ Na základe uvedeného možno dospieť k záveru, že priama osobná komunikácia je veľmi dôležitá aj na pracovisku a prispieva aj k vyššej produktivite zamestnancov.

3.2.4 Sledovanie pohybu zamestnancov na internete

Ustanovenie § 13 ods. 4 Zákonníka práce obsahuje základnú právnu úpravu ochrany súkromia zamestnanca a zakotvuje obmedzenie zamestnávateľa pri výkone sústavnej, systematickej a mimoriadne intenzívnej kontroly zamestnanca, ktorú je oprávnený realizovať len v otvorenej forme,¹⁴⁹ keďže v súlade s judikatúrou EŠLP nie je prípustné, aby zamestnávateľ vykonával tajné sledovanie.¹⁵⁰ Aj keď

¹⁴⁸ BEREČZ, A. *Boj so zdegenerovanou komunikáciou: Firma ľuďom zatrhla e-maily*. (online). 2014. (cit. 2014-12-02). Dostupné z: (<http://podnikanie.etrend.sk/podnikanie-riadenie/boj-so-zdegenerovanou-komunikaciou-firma-ludom-zatrhla-e-maily.html>).

¹⁴⁹ Uvedený záver vyplýva aj z judikatúry EŠLP, porovnaj napr. rozsudok z 2. septembra 2010 v právnej veci *Uzun v. Nemecko*, sťažnosť č. 35623/05 alebo zo 17. júla 2003 v právnej veci *Perry v. Spojené kráľovstvo*, sťažnosť č. 63737/00. Pozri ŠTEFKO, M. Ochrana súkromia zamestnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In *Jurisprudence*, 2012, č. 7-8, s.19.

¹⁵⁰ Rozsudok EŠLP zo 6. septembra 1978 v právnej veci *Klass a i. v. Nemecko*, sťažnosť č. 5029/71, § 55, Rozsudok EŠLP z 2. augusta 1984 v právnej veci *Malone v. Spojené Kráľovstvo*, sťažnosť č. 8691/79, § 68.

sa v právnej teórii môžu vyskytnúť právne názory pripúšťajúce skryté sledovanie, v rámci výskumu problematiky ochrany súkromia sme sa nestretli s presvedčivým súdnym rozhodnutím ani relevantnou argumentáciou, ktorá by odôvodňovala jeho prípustnosť a oprávnenosť.

Zamestnávateľ, ktorý na pracovisku monitoruje využívanie internetu, celkom legitímne a legálne realizuje svoje právo kontrolovať, či si zamestnanec riadne plní svoje povinnosti vyplývajúce z pracovného pomeru. Pri zavedení sledovania by mal však uprednostniť v prvom rade také opatrenia a prostriedky, aby zamestnancom zamedzil prístup na stránky a k aplikáciám, ktoré nepotrebujú na výkon svojej práce. Za vhodné riešenie sa považuje, ak zároveň jasne vymedzí interným predpisom (pracovným poriadkom) pravidlá využívania internetu pri práci, napr. výslovne uvedie, že nie je dovolené ho používať na súkromné účely, resp. vymedzí prípady, keď je jeho využívanie na súkromné účely dovolené a stanoví jeho rozsah.¹⁵¹

Zamestnávateľ môže priamo v pracovnej zmluve alebo internom predpise povoliť používanie zverených prostriedkov pre osobnú potrebu, t. j. používať internetové pripojenie neobmedzene alebo len na návštevu vybraných web stránok v priebehu pracovného času (celého alebo jeho časti) alebo až po jej skončení. V takom prípade možno logicky dospieť k záveru, že sledovanie zo strany zamestnávateľa nebude v rozsahu zasahujúcom do súkromnej sféry zamestnanca prípustné.¹⁵²

Zásadný význam má aj ekonomické hľadisko spomenutých opatrení. Ak by malo byť zavádzané opatrenie spojené s neprimeranými nákladmi či úsilím, nemožno na ňom trvať. K tejto situácii dochádza hlavne vtedy, keď zamestnanec pri svojej práci bežne využíva internet a nie je vopred zrejmé, aké webové stránky sú pre jeho prácu nevyhnutné, t. j. nemožno vopred určiť stránky, ktoré zamestnávateľ považuje za povolené. V týchto prípadoch je totiž veľmi náročné blokovat prístup na konkrétne stránky alebo skupiny stránok. Po splnení informačnej povinnosti môže však v rámci sledovania aktivity pohybu zamestnanca na internete spracovávať osobné údaje v rozsahu dátumu, hodiny a dĺžky času stráveného prehliadaním určitých webových stránok, a to výlučne vo vzťahu k tým, ktoré zamestnanec primárne nepotrebuje na výkon práce, pričom aj táto podmienka v prípade neprimeraných nákladov odpadá.¹⁵³

Pri akomkoľvek preukázaní porušenia pracovnej zmluvy či pracovného poriadku môže zamestnávateľ ukladať sankcie za ich porušenie, ktoré mu poskytuje

¹⁵¹ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 404. Tiež MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. In: *Právní rozhledy*. ISSN 1210-6410. 2012, roč. 20, č. 5, s. 175.

¹⁵² Primerane sa uvedené vzťahuje aj na používanie e-mailovej pošty na súkromné účely.

¹⁵³ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 405.

najmä Zákonník práce (napr. upozornenie na menej závažné porušenie pracovnej disciplíny a možnosť výpovede v zmysle § 63 ods. 1 písm. d/ bod 4 Zákonníka práce). Nie je však vylúčené ani okamžité skončenie pracovného pomeru vzhľadom na závažnosť porušenia povinností, ktoré sa odvíja od času stráveného inou činnosťou než výkonom práce a od miery nákladov a rizík vzniknutých zamestnávateľovi v súvislosti s touto nelegálnou a nedovolenou činnosťou na pracovisku.¹⁵⁴

Monitorovaním pohybu zamestnanca na internete zo strany zamestnávateľa sa zaoberal Najvyšší súd Českej republiky v rozhodnutí zo 16. augusta 2012, sp. zn. 21 Cdo 1771/2011. Z jeho odôvodnenia vyplýva, že súd prvého stupňa zamietol žalobu žalobcu (bývalého zamestnanca) o určenie neplatnosti okamžitého skončenia pracovného pomeru, ku ktorému pristúpil zamestnávateľ potom, ako preukázateľne zistil, že zamestnanec strávil v sledovanom období viac ako polovicu riadneho pracovného času (podľa počtu hodín takmer 103 hodín, čo v prepočte na pracovné dni predstavuje 13 z celkového počtu 21 pracovných dní) neefektívne, napr. prehliadaním rôznych internetových stránok, hraním on-line hier a vybavovaním súkromných záležitostí prostredníctvom internetu (odosiadaním SMS a MMS). Aj keď zamestnávateľ pripustil, že sledoval pohyb zamestnanca na internete počas pracovnej zmeny bez jeho súhlasu, svoju argumentáciu založil na závere, že žalobca porušil zákaz používať na súkromné účely výrobné a pracovné prostriedky zamestnávateľa a týmto konaním zamestnanec porušil pracovný poriadok, ktorý ustanovoval povinnosť nepoužívať internetové stránky, ktoré nesúvisia s výkonom práce. Prepustený zamestnanec namietal, že zamestnávateľ ho sledoval tajne, a preto podľa jeho názoru nebol prípustný dôkaz vo forme výpisu ním navštívených internetových stránok počas pracovného času. Z uvedených dôvodov napadol rozhodnutie odvolacieho súdu, ktorým rozhodnutie súdu prvého stupňa potvrdil. Najvyšší súd dovolanie podané zo strany zamestnanca zamietol. Z odôvodnenia rozsudku vyplýva, že účelom kontroly vykonávanej zamestnávateľom nebolo zistenie obsahu korešpondencie zamestnanca (e-mail, SMS, a pod.) ale zistenie, či zamestnanec rešpektuje zákaz používať pre svoju vlastnú potrebu výpočtovú techniku zamestnávateľa vrátane telekomunikačných zariadení a či dodržiava pravidlá stanovené v internom predpise (resp. pracovnom poriadku) zamestnávateľa. Dovolací súd dospel k záveru, že cieľom kontroly bola výlučne ochrana majetku zamestnávateľa a nebola neoprávneným zásahom do súkromia zamestnanca. Súd skonštatoval, že zámer monitorovania zamestnávateľa bol legitímny, a preto výpis navštívených internetových stránok považoval za prípustný dôkaz. Predmetnú právnu vec prejednával následne Ústavný súd Českej republiky, ktorý odmietol ústavnú sťažnosť žalobcu (zamestnanca) ako

¹⁵⁴ MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. In: *Právní rozhledy*. ISSN 1210-6410. 2012, roč. 20, č. 5, s. 177 – 178.

zjavne neopodstatnenú a vyslovil, že nezistil porušenie základných práv sťažovateľa garantovaných ústavnými zákonmi alebo medzinárodnými zmluvami, ktorými je Česká republika viazaná.

Obdobný prípad sa podľa našich informácií zatiaľ na Slovensku neriešil, ale bolo by zaujímavé porovnať, k akému názoru by v obdobnom prípade dospeli slovenské súdy. Aj keď právna úprava je v danej pracovnoprávnej oblasti podobná v oboch štátoch, vieme si predstaviť aj odlišnú právnu argumentáciu.

3.2.5 Monitorovanie telefonických hovorov zamestnancov

Ochrana súkromia je širšou kategóriou, ktorej obsahovou súčasťou je aj ochrana tajomstva správ podávaných telefónom. Ako sme už viackrát v našej práci uviedli, ochrana súkromia je zakotvená vo viacerých ustanoveniach Ústavy Slovenskej republiky vrátane čl. 22 a čl. 13 Listiny základných práv a slobôd a v Dohovore o ochrane ľudských práv a základných slobôd je sústredená v článku 8. Aj Ústavný súd Slovenskej republiky často vo svojej rozhodovacej činnosti judikuje, že základné práva obsiahnuté v Ústave Slovenskej republiky sa snaží vykladať v intenciách Dohovoru, teda v intenciách judikatúry Európskeho súdu pre ľudské práva v Štrasburgu. V náleze zo 14. júna 2006 sp. zn. I. ÚS 274/05 sledujúc názorovú líniu ESĽP¹⁵⁵ vyjadril, že aj odpočúvanie telefonických hovorov je zásahom do práva na súkromie podľa čl. 22 Ústavy a čl. 13 Listiny ako aj podľa čl. 8 Dohovoru. Vo vzťahu ku kontrole telefonických hovorov na pracovisku platia rovnaké zásady ako pri kontrole elektronickej pošty. Určujúcimi kritériami miery ochrany súkromia zamestnanca sú vo všeobecnosti priestor, v ktorom sa nachádza a čas, počas ktorého sa v ňom nachádza. Dôležitú úlohu zohráva aj jeho vzťah k danému miestu a legitímne očakávania vzhľadom na tieto faktory.¹⁵⁶ V judikatúre ESĽP sa vyskytuje názor, že ak zamestnanec vedie rozhovor so súkromnou osobou, oprávnené očakáva, že hovorí len s touto osobou a nie so svojím zamestnávateľom, resp. oddelením pre vnútorné záležitosti.¹⁵⁷ Odpočúvaním súkromných i obchodných rozhovorov uskutočnených prostredníctvom telefonického zariadenia môže dochádzať k vážnemu ohrozeniu či narušeniu súkromia všetkých na hovore zúčastnených osôb, preto ESĽP priznáva nárok na ochranu

¹⁵⁵ Porovnaj rozsudok ESĽP zo 6. septembra 1978 v právnej veci Klass a ostatní v. Nemecko, sťažnosť č. 5029/71 alebo Rozsudok ESĽP z 25. júna 1997 v právnej veci Halford v. Spojené kráľovstvo, sťažnosť č. 20605/92.

¹⁵⁶ ŠTEFKO, M. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In: *Jurisprudence*, 2012, č. 7/8, s. 18.

¹⁵⁷ Rozsudok ESĽP z 25. októbra 2007 v právnej veci Van Vondel v. Holandsko, sťažnosť č. 38258/03.

pred neoprávneným zásahom do práva na súkromie nielen držiteľovi odpočívajúcej telefónnej linky, ale aj tretím osobám, ktorým sa z tejto linky volá, resp. ktoré na túto linku volajú.¹⁵⁸

ESLP v rozsudku z 25. júna 1997 v právnej veci Halford v. Spojené kráľovstvo¹⁵⁹ založil legitímnosť očakávaní zamestnankyne o súkromnej povahe jej telefonických hovorov na tom, že v rámci jej pracovnej pozície generálneho kontrolóra mala k dispozícii vlastnú miestnosť vybavenú dvoma telefónnymi zariadeniami. Jedno z nich bolo určené na súkromné účely, pričom zamestnávateľ sťažovateľku vopred výslovne nepoučil o možnosti odpočívania telefonických hovorov uskutočnených z tohto zariadenia a nevyžiadal si jej súhlas. Na základe uvedených dôvodov dospel k záveru, že všetky hovory uskutočnené sťažovateľkou z pracoviska prostredníctvom telefonického zariadenia určeného na súkromné účely patria pod pojem „súkromný život“ a „korešpondencia“ a možno na ne aplikovať čl. 8 Dohovoru.¹⁶⁰

Z uvedeného vyplýva, že odpočúvanie a zaznamenávanie obsahu telefonických hovorov na pracovisku medzi zamestnancami alebo medzi zamestnancami a tretími osobami je v zásade podmienené súhlasom zamestnanca a možno ho realizovať len vo výnimočných a odôvodnených prípadoch (napr. ak je zamestnanec obchodným zástupcom a kvôli uzatváraniu kúpnych zmlúv telefonicky komunikuje so zákazníkmi). Bez súhlasu a vedomia zamestnanca preto zamestnávateľ nie je oprávnený kontrolovať obsah jeho telefonických hovorov, aj keby sa obsah hovoru mal významne týkať jeho záujmov. K spomenutému názoru sa prikláňa aj Barancová, ktorá v tejto súvislosti uvádza, že tajné odpočúvanie telefonických hovorov bez ohľadu na to, či majú súkromnú alebo služobnú (obchodnú) povahu, je striktné neprípustné, pretože by sa uskutočnilo v rozpore s čl. 8 Dohovoru aj čl. 7 a 8 Charty základných práv Európskej únie. Ak chce teda zamestnávateľ uskutočňovať legálne odpočúvanie telefonických hovorov na pracovisku, je jeho povinnosťou zabezpečiť nielen súhlas zamestnanca, ale aj súhlas tretej osoby, s ktorou zamestnanec telefonuje.¹⁶¹

Zamestnávateľ teda nie je oprávnený bez legitímneho dôvodu a za splnenia zákonných podmienok odpočúvať súkromné telefonické hovory zamestnancov uskutočnené na pracovisku v pracovnom čase. Na druhej strane sa stretávame

¹⁵⁸ Porovnaj Rozsudok ESLP z 24. apríla 1990 v právnej veci Krusslin v. Francúzsko, sťažnosť č. 11801/85.

¹⁵⁹ Rozsudok ESEP z 25. júna 1997 v právnej veci Halford v. Spojené kráľovstvo, sťažnosť č. 20605/92.

¹⁶⁰ ŠTEFKO, M. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod. In: *Jurisprudence*, 2012, č. 7/8, s. 18.

¹⁶¹ BARANCOVÁ, H. a kol. *Základné práva a slobody v pracovnom práve*. Plzeň: Aleš Čeněk, 2012, s. 116.

v odbornej verejnosti s vysokou mierou tolerancie pri monitorovaní odchádzajúcich a prichádzajúcich hovorov na pracovisku, najmä ich početnosti a zisteniu identity volaných osôb. Súvisí to so skutočnosťou, že ak zamestnanec použije telekomunikačné zariadenie, ktoré mu zveril zamestnávateľ na účely, ktoré nesúvisia s výkonom práce, a to bez jeho vedomia a povolenia, zamestnávateľ vzhľadom na jeho právo na ochranu majetku si môže uplatňovať voči zamestnancovi náhradu škody, ktorá mu týmto protiprávnym konaním vznikla.

Preto využívajú zamestnávatelia výpisy telefonických hovorov a využívajú ich v rámci vykonávania dohľadu nad využívaním pracovného času a zverených pracovných prostriedkov (služobných pevných liniek a mobilných zariadení) zamestnancami. Tvrdíme, že aj v takýchto prípadoch by mal byť zamestnanec o monitorovaní a jeho pravidlách informovaný vnútorným predpisom alebo iným primeraným spôsobom. Ak zamestnávateľ povolí využívanie služobných telefonických zariadení aj na súkromné účely, mal by stanoviť jasné pravidlá, ktoré by v prípade porušenia mohol klasifikovať ako porušenie pracovnej povinnosti, resp. pracovnej disciplíny, vyplývajúcej najmä z pracovnej zmluvy a náležitým spôsobom zamestnanca sankcionovať.¹⁶²

Na sledovanie a rozlíšenie uskutočnených súkromných hovorov od ostatných, ktoré nevyhnutne súvisia s výkonom práce zamestnanca pre zamestnávateľa slúžia v praxi rôzne predvoľby, ktoré musí zamestnanec zadať pri vytočení čísla. Zamestnávateľ na základe osobitne označených súkromných telefonických hovorov dokáže následne z výpisu všetkých uskutočnených hovorov vyčleniť tie, ktoré zamestnancovi môže dať k náhrade, resp. ktoré mu strhne zo mzdy. Problematickým je z nášho hľadiska monitorovanie odoslaných SMS a MMS správ. Je totiž mimoriadne náročné rozlíšiť tie SMS a MMS, ktoré majú súkromnú povahu od ostatných správ, ktoré sú nevyhnutne odosielané v súvislosti s výkonom práce. Jedným z možných riešení, ktorým by mohol zamestnávateľ zamedziť neželanému zasielaniu správ na jeho účet zo služobných telefónov, je stanovenie napr. mesačného limitu, ak by ho zamestnanec prekročil, musel by zvýšené náklady odôvodniť alebo priamo nahradiť.

Na záver dodávame, že zhromažďovanie údajov o počte uskutočnených telefonických hovorov alebo odoslaných správ týkajúcich sa konkrétneho zamestnanca spadá podľa nášho názoru do obsahového rámca pojmu spracúvanie osobných údajov definovaného v § 4 ods. 3 písm. a/ ZOOÚ, preto musí zamestnávateľ dbať na splnenie všetkých povinností z tohto osobitného zákona vyplývajúcich. Ich konkretizácii sa venujeme bližšie v štvrtej kapitole Ochrana osobných údajov zamestnanca.

¹⁶² BARTÍK, V. – JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. 2. vyd. Praha: Linde, 2010, s. 151.

3.2.6 Osobná kontrola vecí a osobné prehliadky zamestnancov

Otázku vykonávania kontroly vecí a osobných prehliadok zamestnancov zamestnávateľom rieši ustanovenie § 177 ods. 2 Zákonníka práce. Zamestnávateľia môžu vykonávať v zmysle tohto ustanovenia kontrolu zamestnancov kvôli predchádzaniu škôd na ich majetku. Môžu však vykonávať len kontrolu vecí, ktoré zamestnanci vnášajú na pracovisko alebo odnášajú z pracoviska a to len v nevyhnutnom rozsahu. Ide teda nielen o kontrolu tašiek, ale aj odevu zamestnancov (vreciek), ich osobných dopravných prostriedkov, prípadne aj odkladacích priestorov (šatní) či dokonca ich kancelárií.¹⁶³

Zamestnávateľia môžu vykonávať kontrolu prostredníctvom kontrolných mechanizmov len zo závažných zákonom stanovených dôvodov, akým je ochrana majetku zamestnávateľa a predchádzanie škodám na tomto majetku. Pripomíname, že nejde len o oprávnenie zamestnávateľa, aby vykonával kontrolu kvôli ochrane svojho majetku, ale súčasne je to aj jeho povinnosť. Musí však zvoliť taký spôsob a formu kontroly, aby v čo najširšej možnej miere zabránil vzniku škôd alebo ich vznik aspoň obmedzil.¹⁶⁴ Ak ide o spôsob vykonávania osobnej kontroly, zamestnávateľia ju nemusia vykonávať len prostredníctvom svojich zamestnancov. V praxi je zaužívaná spolupráca so súkromnými bezpečnostnými agentúrami, ktorá je založená na podklade zmluvného vzťahu a splnomocnenia udeleného zamestnávateľom. Existencia tohto zmluvného vzťahu je však nevyhnutná.¹⁶⁵

Výkon kontroly musí byť primeraný (t. j. len v rozsahu nevyhnutnom na dosiahnutie cieľa) a zamestnávateľ ju môže uskutočniť len za podmienky, že vopred písomne informuje zamestnanca o spôsoboch a rozsahu výkonu kontroly (napr. v tomto prípade v pracovnom poriadku). Štefko vychádzajúc z judikatúry ESĽP¹⁶⁶ uvádza, že za neprimeraný zásah do súkromia zamestnanca by mohla byť

¹⁶³ Pre porovnanie v ustanovení § 248 ods. 2 zákon č. 262/2006 Sb. Zákonník práce navyše zakotvuje striktný zákaz vykonávania osobnej prehliadky fyzickou osobou opačného pohlavia. V praxi sa nám to javí ako komplikované riešenie, keďže potom zamestnávateľ vykonávajúci osobné prehliadky a zamestnávajúci aj mužov aj ženy musí zabezpečiť, aby kontrola bola vykonávaná aspoň jedným zástupcom mužského a jedným zo ženského pohlavia.

¹⁶⁴ Z rozhodnutia českého Nejvyššího soudu zo 7. mája 2003, sp. zn. 21 Cdo 2172/2002 vyplýva obdobný názor, že „povinnosť soustavně kontrolovat, zda zaměstnanci plní své pracovní úkoly tak, aby nedocházelo ke škodám, ukládá zaměstnavateli přijmout a soustavně uplatňovat takový soubhrn způsobů a forem kontroly plnění pracovních úkolů zaměstnanci, který lze po něm vzhledem ke konkrétní časové a místní situaci rozumně požadovat a který je způsobit co nejvíce omezit a snížit riziko vzniku škod“.

¹⁶⁵ JAKUBKA, J. Ochrana osobních a osobnostních práv zaměstnanců, 1. část. In: *Práce a mzda*, 2005, č. 12, s. 29.

¹⁶⁶ Rozsudok ESĽP z 26. júla 2007 v právnej veci *Peev v. Bulharsko*, sťažnosť č. 64209/01.

považovaná aj prehliadka písacieho stola a skriň na spisy zamestnanca uskutočnená v jeho neprítomnosti zamestnávateľom, keďže zamestnanec môže oprávnené predpokladať, že jeho písací stôl aj skrine na spisy sú považované za súkromný majetok, pretože v nich má uložené aj veci a predmety osobnej potreby.¹⁶⁷

S odkazom na ustanovenie § 11 Občianskeho zákonníka, ktorý okrem iného upravuje právo fyzickej osoby na ochranu zdravia, si myslíme, že zamestnanec môže zo zdravotných dôvodov odmietnuť špecifický druh osobnej kontroly (napr. kontrolu pomocou detektorov kovov), ak by mohla znamenať ohrozenie alebo až poškodenie jeho zdravia a zdravotného stavu. Musel by sa však podrobiť osobnej prehliadke vykonanej štandardným spôsobom. Podmienky výkonu kontroly určí zamestnávateľ v pracovnom poriadku, pričom pri osobnej kontrole zamestnanca platia rovnako záväzné predpisy o ochrane osobnosti, osobnej slobody a ľudskej dôstojnosti.

3.2.7 Sledovanie pohybu zamestnancov prostredníctvom systému GPS

Rýchly technologický vývoj v oblasti sledovacích zariadení umožňuje zamestnávateľom kontrolovať pohyb zamestnancov aj prostredníctvom Globálneho polohového systému, z anglického pojmu Global Positioning System (ďalej v texte ako „GPS“), inštalovaného v motorových vozidlách alebo iných mobilných zariadeniach, ktoré využívajú zamestnanci pri výkone práce. V rámci pracovnoprávných vzťahov sa využíva systém GPS na monitorovanie zamestnancov využívajúcich najmä počas pracovnej zmeny ako výrobné prostriedky zamestnávateľa služobné motorové vozidlá. Záujem zamestnávateľa na takomto monitorovaní je omnoho vyšší, ako napr. pri služobných mobilných telefónoch, pretože prevádzka služobných motorových vozidiel je pre neho neporovnateľne nákladnejšia. Kvôli absencii menej invazívneho prostriedku do súkromia jednotlivca, ktoré by umožňovalo obdobným spôsobom kontrolovať využívanie týchto výrobných prostriedkov pri výkone jeho práce mimo pracoviska, nemožno spochybníť, že monitorovanie pomocou systému GPS je preto v zásade prípustným a primeraným spôsobom kontroly zamestnancov.

Odôvodnený záujem zamestnávateľa na získaní presných informácií o pohybe služobných motorových vozidiel v priebehu pracovného času je logický a nespochybniteľný najmä v prípadoch výkonu povolání, akými sú profesionálni vodiči, obchodní zástupcovia či servisní technici. Pri týchto osobitných kategóriách

¹⁶⁷ ŠTEFKO, M. Ochrana súkromia zamestnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In: *Jurisprudence*, 2012, č. 7/8, s. 19.

zamestnancov nemá totiž zamestnávateľ možnosť iným spôsobom kontrolovať riadne využívanie zverených pracovných prostriedkov a plnenie pracovných úloh, pretože sa nezdržujú na jednom stálom pracovisku. V súlade s právnym názorom vyjadreným v rozsudku Krajského súdu v Bratislave zo 16. januára 2013 sp. zn. 4 CoPr 1/2012 a 4 CoPr 2/2012 považujeme za dôležité zdôrazniť, že údaje získané na základe záznamov GPS sú len údajmi o pohybe motorového vozidla, ktoré zamestnanec používal. Nemôžu byť v súdnom spore, napr. o neplatné skončenie pracovného pomeru, použité ako dôkazy preukazujúce využívanie fondu pracovného času zamestnancom, resp. nedodržanie týždenného pracovného času, v rozpore so záujmami zamestnávateľa, navyše ak zamestnávateľ neeviduje dochádzku zamestnancov, t. j. konkrétny čas, ktorý by mali stráviť na pracovisku. Preto odvolací súd potvrdil rozhodnutie súdu prvého stupňa, ktoré založil na závere, že okamžité skončenie pracovného pomeru je neplatné, pretože na základe predložených dôkazov nemal za preukázané, že by došlo k závažnému porušeniu pracovnej disciplíny.¹⁶⁸

Ako hlavný dôvod využívania GPS monitoringu zamestnancov zamestnávateľia uvádzajú najmä úsporu nákladov. Na určenie konkrétnej polohy zamestnanca, resp. služobného motorového vozidla, sa využíva systém prijímačov signálov GPS vo vozidle alebo mobilnom zariadení (notebook, mobilný telefón), ktorý ukladá aktuálne informácie o polohe vozidla či pohybe osoby zamestnanca do internej pamäte. Pomocou technológie GPS tak môže zamestnávateľ sledovať rýchlosť a smer vozidla, čas strávený na jednom mieste a čas, kedy zamestnanec konkrétne miesto opustí. Potom získané údaje spracuje počítačový program, ktorý dokáže vyhodnotiť aj počet najazdených kilometrov a vyhotoviť ročné alebo mesačné zúčtovanie pohonných hmôt.¹⁶⁹

Ďalším legitímnym účelom kontroly pohybu zamestnancov môže byť aj zvýšenie bezpečnosti zamestnancov, ktorí pracujú v rizikových oblastiach či ťažko dostupnom teréne (baníci, pracovníci záchranej služby a iní terénni pracovníci) alebo predchádzanie trestnej činnosti (krádeže služobných vozidiel alebo prepravovaného tovaru či peňazí). Prikláňame sa k názoru, že ak to odôvodňujú okolnosti konkrétneho prípadu a sú splnené podmienky v zmysle § 13 ods. 4 Zákonníka práce (napr. sú pre monitorovanie vážne dôvody spočívajúce v opakovaných krádežoch alebo hrozí zamestnávateľovi väčšia škoda), zamestnávateľ je oprávnený využívať na sledovanie pohybu zamestnancov systém GPS aj

¹⁶⁸ Predmetný rozsudok potvrdzujúci určujúci výrok prvostupňového súdu o neplatnosti okamžitého skončenia pracovného pomeru bol aj predmetom prieskumu pred dovolacím súdom, ktorý dovolanie zamestnávateľa odmietol. Pozri bližšie rozhodnutie Najvyššieho súdu Slovenskej republiky z 24. septembra 2014 sp. zn. 5 Cdo 248/2013.

¹⁶⁹ Pozri BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobných údajů v aplikační praxi*. 2. vyd. Praha: Linde, 2010, s. 153.

mimo pracoviska alebo mimo riadneho pracovného času (napr. cez víkend) kvôli odhaleniu páchania trestnej činnosti (krádeže). V súlade s názormi uvedenými k prípustnosti dôkazu v trestnom konaní, získaného monitorovaním pracoviska kamerovým systémom, zastávame rovnaký názor, že v trestnom konaní by bol dôkaz o páchaní trestnej činnosti na základe záznamov z GPS neprípustný, avšak v občianskoprávnom spore si vieme predstaviť, že by súdy taký dôkaz pripustili, pretože je povinnosťou zamestnávateľa v sporovom konaní preukázať porušenie pracovných povinností (pracovnej disciplíny).

Ak je zariadenie na určenie polohy využívajúce systém GPS inštalované v inom mobilnom zariadení než automobile (napr. smartfone), môže byť zásah do súkromia v prípade sledovania pohybu zamestnanca ďaleko závažnejší. Podľa stanoviska Pracovnej skupiny 29 nie je správne zariadenia na sledovanie vozidiel klásť na jednu úroveň so zariadeniami na sledovanie zamestnancov vzhľadom na ich rozdielnu funkciu. Funkcia zariadení na sledovanie vozidiel spočíva v sledovaní alebo monitorovaní polohy vozidiel, v ktorých sú inštalované. Zamestnávateľia by ich preto zároveň nemali využívať na sledovanie alebo monitorovanie správania alebo miesta pobytu vodičov alebo iných zamestnancov, napríklad vysielaním výstrah v súvislosti s rýchlosťou vozidla.¹⁷⁰

Prikláňame sa k názoru, že nielen zamestnávateľ, ale všetky subjekty, ktoré získajú prístup k informáciám o polohe z inteligentných mobilných zariadení (napr. služobných notebookov alebo rôznych aplikácií cez služobné smartfony) a ktoré ďalej aktívne spracúvajú geolokačné údaje, musia žiadať o predchádzajúci súhlas sledované osoby. Ak sú podmienky udelenia súhlasu splnené automaticky prostredníctvom povinnej akceptácie všeobecných podmienok alebo prostredníctvom potreby vyjadriť nesúhlas so spracúvaním uvedených informácií, nemožno taký súhlas považovať za slobodný. V tejto súvislosti poukazujeme na skutočnosť, že zamestnávateľia by sa namiesto získania súhlasu mali skôr zamerať na skúmanie, či je vo vzťahu k základným právam a slobodám zamestnancov nevyhnutné, aby vykonávali dohľad nad presnou polohou zamestnancov vzhľadom na legitímny účel, ktorý musí byť zároveň preukázateľný.

Problematika monitorovania pohybu pomocou systému GPS je na verejnosti predmetom rozsiahlych diskusií a to predovšetkým pri hľadaní optimálnej hranice medzi ochranou „vyšších záujmov“ na monitorovaní osôb a neprimeraným zásahom do ich ľudských práv, najmä práva na ľudskú dôstojnosť. V roku 2010 vôbec po prvýkrát sudcovia EŠLP v prípade *Uzun v. Nemecko* rozhodovali spor v rámci, ktorého boli za účelom sledovania fyzickej osoby v trestnom konaní podozrivej zo spoluúčasti na teroristických útokoch využité dáta získané pro-

¹⁷⁰ Stanovisko Pracovnej skupiny 29 č. 13/2011 ku geolokačným službám inteligentných mobilných zariadení zo 16. mája 2011, WP 185, s. 15.

stredníctvom systému GPS.¹⁷¹ Ide teda o prelomové rozhodnutie, v ktorom sa EStLP stotožnil s názorom nemeckého ústavného súdu, že zásah do práva sťažovateľa na súkromie a práva na spravodlivý súdny proces bol primeraný vzhľadom na závažnosť zločinov, z ktorých bol podozrivý. V odôvodnení vysvetlil, že toto podozrenie zo zločinov vraždy v štádiu pokusu a teroristických útokov bolo také závažné, že sledovanie sťažovateľa pomocou GPS považoval za primerané vzhľadom na ochranu národnej bezpečnosti a verejného poriadku. Konštatoval, že sledovanie pohybu prebiehalo v súlade s nemeckým osobitným zákonom, ktorý je dostatočnou zárukou proti svojvoľnému nezákonnému získavaniu dôkazov, a napadnutým postupom vnútroštátnych orgánov preto nedošlo k porušeniu článku 8 Dohovoru. EStLP dokonca vyjadril názor, že sledovanie pomocou GPS je menším zásahom do práva na súkromný život ako odpočúvanie telefonických hovorov.¹⁷²

Zaujímavé postrehy uverejnili v odbornom článku americkí advokáti, ktorí na niekoľkých prípadoch zo súdnych siení, v ktorých boli zamestnávateľia obvinení z porušenia súkromia zamestnancov, demonštrovali, že súdy pred súkromím zamestnancov uprednostnili vo väčšine prípadov záujem zamestnávateľa na monitorovaní pomocou GPS v služobných vozidlách. Svoj postoj odôvodňovali najmä tým, že informácia o polohe služobného vozidla je v podstate informáciou verejne prístupnou.

Autori článku na základe vlastných postrehov sformulovali nasledujúce odporúčania pre zamestnávateľov, ak sa rozhodnú zaviesť technológiu GPS na pracovisku. Odporúčajú pritom:¹⁷³

- integrovať monitorovanie do vnútornej politiky zamestnávateľa – stanoviť a zverejniť presné pravidlá využívania majetku a výrobných prostriedkov zamestnávateľa vrátane počítačov, pracovných e-mailov a služobných telefónov a vozidiel. Vymedziť ich využívanie len na pracovné účely a v prospech zamestnávateľa, prípadne vymedziť prípady, ktoré bude zamestnávateľ považovať za porušenie stanovených pravidiel,
- vyhradiť si právo na monitorovanie využívania výrobných prostriedkov vo vlastníctve zamestnávateľa a informovať zamestnancov o tom, aké druhy výrobných prostriedkov budú vybavené GPS systémom, aké druhy informácií

¹⁷¹ Rozsudok EStLP z 2. septembra 2010 v právnej veci *Uzun v. Nemecko*, sťažnosť č. 35623/05.

¹⁷² Vzhľadom na to, že každý jednotlivý prípad treba posudzovať samostatne a s prihliadnutím na primeranosť zásahu do práva na súkromný život pri sledovaní pomocou systému GPS, nemožno vylúčiť, že v budúcnosti bude obdobný prípad vyriešený iným spôsobom.

¹⁷³ TOWNS, D. M., COBB, L. M. Notes on: GPS technology; Employee monitoring enters a new area. In: *Labor Law Journal*, vol. 63, issue 3, p. 203 – 208. (online). 2012. (cit 2015-01-30). Dostupné z: (<http://connection.ebscohost.com/c/articles/80170931/notes-on-gps-technology-employee-monitoring-enters-new-era>).

budú prostredníctvom nich získavané, na aké účely a akým spôsobom budú ďalej získané informácie spracovávané a v akom čase bude monitorovanie prebiehať,

- obmedziť monitorovanie výhradne počas stanoveného pracovného času a zabezpečiť možnosť vypnutia systému GPS počas prestávok a po pracovnom čase,
- zabezpečiť pravidelné kontroly technických prístrojov a zariadení využívajúcich systém GPS (kalibrácia, úprava presnosti prístrojov),
- zabezpečiť dôveryhodnosť zaznamenaných informácií a ochranu súkromia zamestnancov (najmä v rámci dohôd medzi zamestnávateľmi a prevádzkovateľmi GPS služieb).

Na základe uvedeného sme dospeli k záveru, že zamestnávateľ by pri zavedení systému sledovania pomocou GPS mal vziať do úvahy, či získané benefity vyššej efektívnosti v rámci využívania výrobných prostriedkov zamestnancami naozaj prevážia nad rizikom porušenia práv zamestnancov a potenciálnym súdnym sporom rozhodnutým v prospech zamestnanca. Zamestnávateľ by mal teda vždy predovšetkým využívať na monitorovanie pohybu najmenej rušivé prostriedky, sústavnému monitorovaniu by sa mal vyhnúť úplne a mal by uprednostňovať systémy, ktoré vyšlú výstražný signál v okamihu, keď zamestnanec prekročí určenú virtuálnu hranicu.

Za štandardné riešenie sa preto vo všeobecnosti odporúča, aby mal zamestnanec zachovanú možnosť vypnúť akékoľvek monitorovacie zariadenie poskytujúce lokalizačné služby mimo pracovného času a aby bol o tejto možnosti a postupe (spôsobe) aj zrozumiteľne informovaný. Používateľom lokalizačných služieb by malo zostať výhradné právo jednotlivito súhlasiť so zapnutím konkrétnych aplikácií, ktoré monitorujú ich pohyb.¹⁷⁴ V prípadoch terénnych pracovníkov, kde sa prihliada najmä na ich bezpečnosť a prevenciu trestnej činnosti, je podľa nášho názoru prípustné vykonávať kontrolu len po predchádzajúcom informovaní, resp. upozornení v súlade s § 13 ods. 4 Zákonníka práce.

Treba však prihliadať na to, že aj v prípade monitorovania pohybu zamestnancov môže zamestnávateľ spracúvať získané osobné údaje len po obmedzený čas, ktorý môže byť stanovený rôzne na základe odlišných aspektov a potrieb zamestnávateľa. Čas, počas ktorého sa údaje budú vyhodnocovať, nesmie byť neprimerane dlhý. Po získaní súhrnných údajov v stanovenom období a ich dôkladnej analýze (uskutočnenej v krátkom čase po ich získaní) by sa mali údaje trvalo zlikvidovať, s výnimkou nevyhnutného zachovania údajov pre prípad uplatnenia oprávnených záujmov zamestnávateľa (ak môžu slúžiť ako dôkazný prostriedok

¹⁷⁴ Stanovisko Pracovnej skupiny 29 č. 13/2011 ku geolokačným službám inteligentných mobilných zariadení zo 16. mája 2011, WP 185, s. 14.

v prípadnom budúcom spore so zamestnancom). Zároveň pripomíname, že ak sa kontroly polohy zamestnancov nevykonávajú dlhodobo, systematicky a pravidelne, nemožno považovať také monitorovanie za spracúvanie osobných údajov monitorovaných osôb v zmysle § 4 ods. 3 písm. a/ ZOOÚ.

4. OCHRANA OSOBNÝCH ÚDAJOV ZAMESTNANCA

Osobné údaje sú vstupnou bránou do súkromia každého jednotlivca. Stali sa súčasťou každodennej reality v oblasti rôznych spoločenských vzťahov nielen pracovnoprávných vzťahov. Pravdepodobne práve táto skutočnosť spôsobila, že dnes nie sme schopní celkom jasne vymedziť význam právneho pojmu osobný údaj. Za súčasného trendu vývoja informačných technológií je totiž z praktického hľadiska takmer nemožné určiť, čo všetko patrí k pojmu osobný údaj. Na jeho zrozumiteľnosti mu nepridáva ani pomerne rozsiahla a neustále sa vyvíjajúca právna úprava a stále vzácna judikatúra súdov. Pri aplikácii právnych noriem súvisiacich s ochranou osobných údajov preto stále narážame na nové prípady, ktoré dokážu spochybniť našu doterajšiu predstavu o tom, čo rozumieme pod právnym pojmom osobný údaj. Napriek tomu nie je snaha o definovanie a presné určenie osobných údajov márna. Ak vychádzame z predpokladu, že akýkoľvek právny predpis musí na národnej i nadnárodnej úrovni poskytovať náležitú ochranu právam fyzických osôb pred neoprávneným zasahovaním do ich súkromného života, je našou povinnosťou pokúšať sa v zatiaľ neprehľadnom svete osobných údajov hľadať určitý systém.

4.1 Osobný údaj

Odborným termínom „osobný údaj“ rozumieme v zmysle § 4 ods. 1 ZOOÚ „údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu“. Definícia osobného údaju bola prevzatá z čl. 2 písm. a/ smernice č. 95/46/ES¹⁷⁵ s tým rozdielom, že smernica používa namiesto termínu

¹⁷⁵ Podľa čl. 2 písm. a/ smernice č. 95/46/ES osobné údaje „znamenajú akúkoľvek informáciu, ktorá sa týka identifikovanej alebo identifikovateľnej fyzickej osoby; identifikovateľná osoba je osoba, ktorú možno identifikovať, priamo alebo nepriamo, najmä pomocou overenia identifikačného čísla alebo jedného alebo viacerých faktorov špecifických pre jeho fyzickú, fyziologickú, duševnú, hospodársku, kultúrnu alebo sociálnu identitu“.

„osobný údaj“ termín „informácia“ a v podstate zodpovedá z obsahového hľadiska vymedzeniu pojmu v čl. 2 Dohovoru č. 108.¹⁷⁶ Z uvedenej definície vychádza v rozhodovacej činnosti aj Súdny dvor Európskej únie, ktorý v rozsudku zo 6. novembra 2003 v právnej veci Bodil Lindqvist, vec C-101/2001 v § 24 doplnil, že do jej obsahového rámca patrí aj „meno osoby v spojitosti s jej telefónnym číslom alebo informáciami o jej pracovných podmienkach alebo záľubách“.

Zákon neobsahuje uzavretý výpočet osobných údajov podliehajúcich právnej ochrane. Právny pojem osobný údaj je preto rovnako ako súkromie významovo otvorený. Rozhodujúce sú preto kritériá, podľa ktorých posudzujeme či informácia, s ktorou sme prišli do kontaktu, má alebo nemá povahu osobného údaju. V zásade však platí, že o osobný údaj ide v prípadoch, ak máme k dispozícii informáciu, ktorá má osobnú povahu. Schopnosť rozlišovať informáciu s osobnou povahou od akejkoľvek inej informácie získame až v okamihu posúdenia všetkých do toho okamihu dostupných údajov, ktoré možno k fyzickej osobe priradiť a na základe ktorých možno dospieť k jej jednoznačnej identifikácii.

Všeobecným materiálnym prameňom právnej úpravy osobných údajov sa stalo Stanovisko č. 4/2007, ktoré 20. júna 2007 prijala Pracovná skupina na ochranu osobných údajov zriadená podľa čl. 29 smernice č. 95/46/ES pod číslom WP 136. Podľa uvedeného stanoviska legálna definícia osobného údaju sa skladá zo štyroch identifikačných znakov:¹⁷⁷

1. akýkoľvek údaj, resp. charakteristika (pričom zákon neustanovuje, že musí ísť o objektívny a pravdivý údaj),
2. týkajúci sa,
3. určenej alebo určiteľnej (identifikovanej alebo identifikovateľnej),
4. fyzickej osoby.

Ak podrobíme dostupné informácie o fyzickej osobe uvedeným štyrom kritériám, tak zistíme, že osobnými údajmi sú nielen titul, meno, priezvisko, adresa a ďalšie kontaktné údaje, dátum narodenia, rodné číslo, ale aj údaje o správaní alebo konaní osoby, biometrické údaje a akékoľvek informácie o osobných vlastnostiach, pomeroch alebo iných špecifických znakoch, ktoré charakterizujú alebo odhaľujú fyzickú (muž, žena), fyziologickú (hlas, chôdza), psychickú (návyky), ekonomickú (výška mzdy), kultúrnu (materinský jazyk) alebo sociálnu (určité postavenie v spoločnosti) identitu fyzickej osoby.¹⁷⁸ V právnej vede sa vyskytujú

¹⁷⁶ Podľa nášho názoru je pojem „informácia“ výrazovo výstižnejší a bolo by vhodné de lege ferenda uvažovať o jeho zosúladení so smernicou č. 95/46/ES (osobný údaj je napr. v jej anglickom znení definovaný pojmom information, v nemeckom znení pojmom die Information, vo francúzskom znení pojmom l'information). Tento výraz je použitý i v českom ZOOÚ.

¹⁷⁷ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 44.

¹⁷⁸ ÚOOÚ, Metodické usmernenie č. 1/2013 k pojmu osobné údaje z 1. júla 2013. (online).

názory, že medzi osobné údaje patria aj informácie ako napríklad, že určitá osoba sa pohybuje na určitom mieste v určitý čas, že tam vykonávala nejakú činnosť, alebo že má alebo mala pri sebe určitý predmet.¹⁷⁹

Treba zdôrazniť, že osobné údaje sa viažu výhradne k fyzickej osobe – jednotlivcovi (v prípadoch *inter vivos* i *mortis causa*). V tejto súvislosti sa dostáva do popredia ďalší dôležitý pojem a ním je **dotknutá osoba**. Jej charakteristickou črtou je, že ide vždy o „osobu, ktorej sa osobné údaje týkajú“. Za takú osobu naša právna úprava nepovažuje právnickú osobu ani fyzickú osobu – podnikateľa.¹⁸⁰ Považuje za ňu však osobu, ktorá už nežije (pozri § 12 ods. 7 ZOOÚ), avšak právna veda v súlade s čl. 7 ods. 1 Dohovoru o právach dieťaťa nepriznáva takú ochranu narodenému (t. j. počatému a ešte nenarodenému dieťaťu).¹⁸¹ Zároveň však niektoré názory poukazujú na skutočnosť, že by mu mohla byť ochrana priznaná v zmysle § 7 ods. 1 Občianskeho zákonníka.¹⁸²

Aby bol naplnený charakteristický znak „týkajúci sa“, musí osobný údaj obsahovať aspoň jeden z nasledujúcich prvkov. Buď pôjde o informáciu, ktorá zachytáva údaje o konkrétnej osobe (údaj o obsahu) alebo informáciu, ktorej cieľom je posúdiť konkrétnu osobu a jej správanie (údaj o účele), prípadne informáciu, ktorá má dosah na práva a záujmy konkrétnej osoby (údaje o výsledku).¹⁸³

Kritérium určitosti, resp. určiteľnosti, je založené na povahe charakteristických znakov, tzv. identifikátorov, ktoré sa týkajú a určujú konkrétnu osobu alebo sú spôsobilé určiť aj inú osobu. Fyzickú osobu možno považovať za identifikovanú vtedy, keď je v rámci skupiny osôb odlišená od všetkých ostatných príslušníkov skupiny, čiže dôjde k jednoznačnému určeniu jej identity.¹⁸⁴ Rozdiel medzi týmito dvomi kategóriami spočíva v tom, že ak možno fyzickú osobu identifikovať

Dostupné z: (http://www.dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmerzenie_c_1_2013_k_pojmu_osobne_udaje.pdf).

¹⁷⁹ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávní agendě*. Praha: BMSS Start, 2010, s. 26.

¹⁸⁰ ÚOOÚ, Metodické usmernenie č. 2/2013 k základným pojmom – osoby pri spracúvaní osobných údajov z 1. júla 2013. (online). Dostupné z http://www.dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmerzenie_c_2_2013_k_zakladnym_pojmom-osoby_pri_spracuvani_osobnych_udaj_ov_aktualpw.pdf.

¹⁸¹ Pozri bližšie VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 50.

¹⁸² Podľa § 7 ods. 1 Občianskeho zákonníka „spôsobilosť fyzickej osoby mať práva a povinnosti vzniká narodením. Túto spôsobilosť má aj počaté dieťa, ak sa narodí živé.“ Pozri bližšie VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 49.

¹⁸³ Pozri bližšie VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 47.

¹⁸⁴ Pozri tiež rozhodnutie Najvyššieho súdu Slovenskej republiky z 25. novembra 2009 sp. zn. 6 Sžo 250/2008.

vať prakticky bez vynaloženia námahy, považuje sa za subjekt určený. Ak možno osobu určiť len pri vynaložení určitého úsilia, hovoríme o subjekte určiteľnom.¹⁸⁵

Na základe uvedeného sme dospeli k záveru, že pod pojem osobný údaj môžeme subsumovať „akýkoľvek druh údajov a charakteristík, ktoré je možné priradiť ku konkrétnej fyzickej osobe“. Má relatívnu povahu, pretože to, či ide o osobný údaj, závisí od komplexného posúdenia dostupných údajov v ich vzájomnej súvislosti a zároveň od celkovej situácie.¹⁸⁶ Ako príklad nám môže poslúžiť nasledujúce porovnanie. E-mailovú adresu v tvare napr. nick@gmail.com bez ďalších charakteristík nemožno považovať za osobný údaj, avšak ak sa už nachádza v tvare napr. meno.priezvisko@firma.sk, tak ju môžeme jednoznačne považovať za osobný údaj, pretože z takej adresy možno poznať meno, priezvisko, kontaktný údaj a údaj o zamestnávateľovi.¹⁸⁷ Pri posudzovaní osobného charakteru dostupných informácií o konkrétnej osobe je pritom potrebné zohľadňovať aj geografický faktor.¹⁸⁸

Okrem pojmu osobný údaj ZOOÚ zakotvuje v ustanovení § 4 ods. 3 písm. i/ aj pojem „**anonymizovaný údaj**“, ktorý predstavuje v istom zmysle protiklad pojmu osobný údaj. Je špecifickým „osobným údajom, upraveným do takej formy, v ktorej ho nemožno priradiť ku konkrétnej fyzickej osobe, ktorej sa týka, s prihliadnutím na všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich iná osoba využije na identifikáciu danej fyzickej osoby“.¹⁸⁹ Procesom anonymizácie sa stáva konkrétna osoba neidentifikovateľnou a osobný údaj sa mení na anonymný. Anonymizácia však nie je proces, ktorého výsledkom je komplexná a „dokonalá“ anonymita subjektu. Prevádzkovateľ, ktorý vykonáva a zodpovedá za anonymizáciu, má totiž stále možnosť identifikácie osoby, ktorej údaje už raz boli anonymizované.

¹⁸⁵ Za osobný údaj, na základe ktorého je osoba určiteľná sa považuje v praxi aj číslo mobilného telefónu. Pozri rozhodnutie Nejvyššího správného soudu České republiky z 12. februára 2009 sp. zn. 9 As 34/2008.

¹⁸⁶ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 45.

¹⁸⁷ Opačný názor je vyjadrený napr. v rozsudku Krajského súdu v Bratislave z 15. februára 2006 sp. zn. 2S 94/05, ale nemožno ho považovať za vecne správny.

¹⁸⁸ Informácia alebo súbor informácií, ktoré sú osobným údajom na úrovni jednej obce, nemusí automaticky znamenať, že sú osobným údajom aj na regionálnej úrovni. Pozri bližšie ÚOOÚ, Metodické usmernenie č. 1/2013 k pojmu osobné údaje z 1. júla 2013. (online). Dostupné z: (http://www.dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmerne_nie_c_1_2013_k_pojmu_osobne_udaje.pdf).

¹⁸⁹ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 62.

4.2 Osobitné kategórie osobných údajov

ZOOÚ v § 13 medzi osobitné kategórie osobných údajov¹⁹⁰ zaraďuje osobné údaje o rasovom a etnickom pôvode, politických názoroch, náboženskej viere a svetonázore, členstve v politických stranách a hnutiach alebo v odborových organizáciách a tiež údaje o fyzickom a psychickom zdravotnom stave a zdravotnej spôsobilosti a údaje o pohlavnom (sexuálnom) živote.¹⁹¹ Osobitne tiež vymedzuje rodné číslo, ktoré je všeobecne použiteľným identifikátorom,¹⁹² biometrické údaje a údaje o porušení ustanovení zakladajúcich trestnú alebo administratívno-právnu zodpovednosť. V porovnaní s ostatnými kategóriami pre spracúvanie osobitných kategórií osobných údajov platia striktnjšie podmienky. Zároveň to platí aj vtedy, ak sa pri spracúvaní osobných údajov vyskytne len jeden citlivý osobný údaj. Zákaz ich spracúvania však nie je absolútny, pretože výnimky z obmedzenia ustanovuje § 14 ZOOÚ.

4.3 Spracúvanie osobných údajov

Na súčasnú medzinárodnú aj európsku právnu úpravu v oblasti ochrany osobných údajov reflektuje aj platný ZOOÚ, v ktorého ustanoveniach sa premietajú základné zásady pri spracúvaní osobných údajov (napr. zásada konečnosti, transparentnosti, dôvernosti a bezpečnosti, kontroly a mnohé iné).¹⁹³ Za spracúvanie osobných údajov a dodržiavanie jednotlivých zásad nesie podľa slovenskej právnej úpravy zodpovednosť prevádzkovateľ, v pracovnoprávných vzťahoch zamestnávateľ.

¹⁹⁰ V porovnaní s českou právnou úpravou v ustanoveniach § 4 písm. b/ a § 9 zákona č. 101/2000 Sb. o ochrane osobných údajů slovenský ZOOÚ nepoužíva pojem „citlivé údaje“, ale namiesto toho používa pojem „osobitné kategórie osobných údajov“ a rozdielne od českej úpravy nezaraďuje medzi ne napr. aj genetické údaje alebo údaje odhaľujúce národnostný pôvod.

¹⁹¹ Podľa § 13 ods. 1 ZOOÚ „spracúvať osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách a údaje týkajúce sa zdravia alebo pohlavného života, sa zakazuje“.

¹⁹² Podľa zákona č. 301/1995 Z. z. o rodnom čísle v znení neskorších predpisov. V zmysle § 13 ods. 1 ZOOÚ „pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor ustanovený osobitným zákonom len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Spracúvať iný identifikátor, ktorý v sebe skrýva charakteristiky dotknutej osoby, alebo zverejňovať všeobecne použiteľný identifikátor sa zakazuje“.

¹⁹³ Pozri bližšie KUNER, CH. *European data privacy law and online business*. Oxford: University Press, 2003, p. 17 alebo tiež ÚOOÚ, *Zásady pri spracúvaní osobných údajov*. (online). Dostupné z: (<https://dataprotection.gov.sk/uouu/sk/content/zasady-pri-spracuvani-osobnych-udajov>).

Obsah pojmu spracúvanie osobných údajov vymedzuje ustanovenie § 4 ods. 3 písm. a) ZOOÚ ako „*vykonávanie operácií alebo súboru operácií s osobnými údajmi*“. Ďalej demonštratívne uvádza, že tento pojem v sebe zahŕňa činnosti ako: získavanie, zhromažďovanie, uchovávanie, blokovanie, likvidáciu, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie a podobne. V bodoch 1 až 6 tohto ustanovenia sú konkrétnejšie vysvetlené niektoré z vymenovaných operácií. Pritom za spracúvanie osobných údajov možno považovať aj jediný samostatný úkon, ktorý sa týka osobných údajov. Pri spracúvaní osobných údajov nezáleží na tom, či dochádza k získaniu a spracúvaniu osobných údajov manuálne (v listinnej podobe) alebo prostredníctvom automatizovaných prostriedkov spracúvania.¹⁹⁴

Pri spracúvaní osobných údajov musí ísť o operácie vykonávané systematicky a je povinnosťou prevádzkovateľa spracovávať len presné a aktualizované údaje. ZOOÚ nenormuje vykonávanie aktualizácií, ale naopak ponecháva ich na uvážení samotného prevádzkovateľa. Splnenie požiadavky aktuálnych osobných údajov zamestnancov môže realizovať zamestnávateľ tak, že raz do roka poskytne prehľad spracovávaných údajov zamestnancom na kontrolu ich presnosti a pravdivosti.¹⁹⁵ Ak dospeje následne k záveru, že spracovávané údaje sú nepresné alebo neaktuálne, má povinnosť ich podľa konkrétnej situácie blokovať, opraviť alebo zlikvidovať. Zákonnou výnimkou, keď sa môžu spracúvať osobné údaje bez ohľadu na splnenie kritérií presnosti a pravdivosti osobných údajov, je ustanovenie § 3 ods. 1 ZOOÚ, ak je to nevyhnutné na zabezpečenie verejného záujmu a prevádzkovateľ plní povinnosti ustanovené osobitným zákonom na zaistenie verejného poriadku a bezpečnosti, ochrany dotknutých osôb alebo práv a slobôd iných a podobne. Aktualizácia osobných údajov sa môže vykonať z iniciatívy prevádzkovateľa aj z podnetu dotknutého subjektu, napr. zamestnanca, ktorého právo domáhať sa opravy, prípadne až likvidácie nesprávnych údajov vyplýva z ustanovenia § 28 ods. 1 ZOOÚ.

Medzi spracovateľské operácie osobných údajov sa najčastejšie zaraďuje ich poskytovanie, sprístupňovanie a zverejňovanie, ktorému predchádza, samozrejme, ich získanie a zhromažďovanie. Už v štádiu zhromažďovania osobných údajov musí mať prevádzkovateľ definovaný účel, ktorému má spracúvanie slúžiť, pretože už v tomto štádiu sa uchovávajú na určitý nosič informácií, ktorý umožňuje ich ďalšie spracúvanie. Poskytovanie osobných údajov sa chápe vo význame odovzdávania osobných údajov z informačného systému na spracovanie inému

¹⁹⁴ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 54.

¹⁹⁵ Stanovisko Pracovnej skupiny 29 č. 8/2001 k spracúvaniu osobných údajov v rámci pracovného pomeru z 13. septembra 2001, WP 48, s. 22.

prevádzkovateľovi, jeho zástupcovi, sprostredkovateľovi alebo iným oprávneným osobám, t. j. predpokladá sa ďalšie nakladanie s osobnými údajmi treťou stranou. Sprístupňovaním je oznámenie alebo umožnenie prístupu k osobným údajom príjemcovi s tým rozdielom, že oproti poskytovaniu sprístupnené osobné údaje nie sú predmetom ďalšieho spracovania. Zverejňovanie osobných údajov sa odlišuje od sprístupňovania v tom, že ide o publikovanie, vystavenie, umiestnenie na verejne prístupnom mieste najmä prostredníctvom masovokomunikačných prostriedkov.¹⁹⁶

Zamestnávateľa nemôžu dosiahnuť legitímne spracovanie osobných údajov, ktorých spracúvanie je zakázané zákonom, získaním súhlasu zamestnanca so spracúvaním.¹⁹⁷

4.4 Subjekty oprávnené na spracúvanie osobných údajov

4.4.1 Prevádzkovateľ

Pri spracúvaní osobných údajov je prevádzkovateľ najdôležitejším subjektom, nakoľko je aj najčastejším adresátom povinností ustanovených ZOOÚ. Jeho definíciu zakotvuje ustanovenie § 4 ods. 2 písm. b/ ZOOÚ, podľa ktorého je prevádzkovateľom „každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracováva osobné údaje vo vlastnom mene; ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto splňa zákonom, priamo vykonateľným právne záväzným aktom Európskej únie alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ustanovené podmienky“.

Tento pojem možno vymedziť z pozitívneho i negatívneho hľadiska.¹⁹⁸

Pozitívna definícia prevádzkovateľa je založená na výklade, že sám alebo spoločne s inými určuje účel a podmienky spracúvania osobných údajov fyzických osôb. Prevádzkovateľom teda nie je osoba, ktorá zbiera akékoľvek údaje o akej-

¹⁹⁶ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 54 až 55.

¹⁹⁷ Stanovisko Pracovnej skupiny 29 č. 8/2001 k spracúvaniu osobných údajov v rámci pracovného pomeru z 13. septembra 2001, WP 48, s. 22.

¹⁹⁸ ÚOOÚ, Metodické usmernenie č. 2/2013 k základným pojmom – osoby pri spracúvaní osobných údajov z 1. júla 2013. (online). Dostupné z: (http://www.dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmernenie_c_2_2013_k_zakladnym_pojmom-osoby_pri_spracuvani_osobnych_udaj_ov_aktualpw.pdf).

koľvek osobe. Spracúvanie osobných údajov prevádzkovateľ vykonáva vždy vo vlastnom mene, systematicky (pravidelne a opakovane), hoci aj nelegálne, a nesie zaň zodpovednosť. Jeho ďalším charakteristickým znakom je, že sa buď pre spracúvanie osobných údajov fyzických osôb rozhodne sám, alebo mu táto povinnosť vyplýva priamo zo zákona, ale za splnenia podmienky, že nespracováva údaje na vlastnú potrebu. Prevádzkovateľom tak môže byť akýkoľvek subjekt, spracúvajúci osobné údaje bez ohľadu na to, či ide o fyzickú osobu, právnickú osobu alebo orgán verejnej moci. Je ním vždy subjekt ako celok a nie jeho organizačná časť (napr. pobočka).¹⁹⁹ Negatívne vymedzenie pojmu prevádzkovateľ zaň nepovažuje toho, kto spracováva osobné údaje na vlastnú potrebu v rámci osobných alebo domácich činností (adresár, fotoalbum) alebo spracováva náhodne získané osobné údaje (bez predchádzajúceho určenia účelu a podmienok spracúvania).

4.4.2 Zástupca prevádzkovateľa a sprostredkovateľ

Spracúvanie osobných údajov môže prevádzkovateľ vykonávať sám alebo ním poverí svojho zástupcu alebo ho vykonáva sprostredkovateľ na základe zmluvy uzavretej s prevádzkovateľom. Zástupca prevádzkovateľa²⁰⁰ disponuje rovnakými právami a povinnosťami pri spracúvaní osobných údajov ako prevádzkovateľ, dokonca má rovnakú zodpovednosť. Zástupca však na rozdiel od sprostredkovateľa spracováva osobné údaje vo vlastnom mene. Zástupca prevádzkovateľa je preto vždy osobou odlišnou od samotného prevádzkovateľa. Na základe písomného poverenia disponuje oprávneniami vykonávať samostatne celé spracúvanie osobných údajov alebo len jeho časť. Prevádzkovateľ môže zástupcu splnomocniť, aby spracúvanie vykonal prostredníctvom tretieho subjektu (tzv. subdodávateľa). Samotné spracúvanie musí zástupca vykonávať v súlade s pokynmi prevádzkovateľa, pretože sa na oboch vzťahujú rovnaké povinnosti. Príkladom je informačná povinnosť zástupcu, ktorú si musí za prevádzkovateľa splniť v zmysle § 8 ods. 7 ZOOÚ. Na druhej strane niektoré povinnosti, akou je aj povinnosť vymedziť účel spracúvania osobných údajov, prináležia výlučne prevádzkovateľovi. Musí tak urobiť v písomnej zmluve, a to pred začatím alebo najneskôr v deň začatia spracúvania osobných údajov.

Sprostredkovateľ je osobou, na ktorú prevádzkovateľ prenesie právomoc

¹⁹⁹ Prevádzkovateľom nie je ani zamestnanec zabezpečujúci z technickej stránky spracúvanie osobných údajov (napr. správca siete). MATES, P. *Ochrana osobných údajů*. 1. vyd. Praha: Karolinum, 2002, s. 44.

²⁰⁰ Podľa § 4 ods. 2 písm. c/ ZOOÚ je zástupcom prevádzkovateľa „každý, kto na území Slovenskej republiky zastupuje prevádzkovateľa so sídlom, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v tretej krajine“.

spracovávať osobné údaje na základe poverenia v písomnej zmluve (najčastejšie mandátnej zmluve).²⁰¹ Sprostredkovateľ je preto osobou, ktorá je oprávnená vykonávať spracúvanie osobných údajov v mene prevádzkovateľa. V zmysle § 8 ZOOÚ zodpovedá sprostredkovateľ za plnenie zákonom vymedzených povinností prevádzkovateľa len v rozsahu s ním dohodnutom v písomnej zmluve.²⁰² Podľa poslednej novely ZOOÚ zákonom č. 84/2014 Z. z. účinnnej od 15. apríla 2014 už nejestvuje kogentné zakotvenie solidárnej zodpovednosti oboch subjektov, čo znamená, že bola zrušená povinnosť sprostredkovateľa nahlasovať Úradu na ochranu osobných údajov Slovenskej republiky porušenia ZOOÚ zo strany prevádzkovateľa (ktorý vystupuje často v praxi v pozícii klienta, resp. zákazníka sprostredkovateľa) a takisto neexistuje jeho solidárna spoluzodpovednosť.²⁰³ Typickými príkladmi využívania sprostredkovateľa v pracovnoprávných vzťahoch je využívanie služieb externých účtovníckych firiem, bezpečnostných služieb alebo obchodných zástupcov v rozsahu upravenom dohodou oboch strán. Pri využívaní marketingových agentúr alebo podnikateľských subjektov zabezpečujúcich pre zamestnávateľa stravovanie zamestnancov častejšie ide o vzťah dvoch prevádzkovateľov osobných údajov.²⁰⁴ Sprostredkovateľ sa však môže stať aj sám prevádzkovateľom, ak si stanoví svoj vlastný účel spracúvania, no v takom prípade musí získať súhlas pôvodného prevádzkovateľa a informovaný súhlas dotknutého subjektu, čo podľa nášho názoru vyplýva z § 9 ods. 2 ZOOÚ.

²⁰¹ § 4 ods. 2 písm. d/ ZOOÚ je sprostredkovateľom „každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve podľa § 8 a v súlade s týmto zákonom“.

²⁰² Porovnaj ÚOOÚ, Metodické usmernenie č. 2/2013 k základným pojmom – osoby pri spracúvaní osobných údajov z 1. júla 2013. (online). Dostupné z: (http://www.dataprotection.gov.sk/uoou/sites/default/files/metodicke_usmernenie_c._2_2013_k_zakladnym_pojmom-osoby_pri_spracuvani_osobnych_udaj_ov_aktualpw.pdf).

²⁰³ Znenie § 8 ods. 8 a 9 ZOOÚ do 14. apríla 2014: (8) „Ak sprostredkovateľ zistí, že prevádzkovateľ sa pri spracúvaní osobných údajov dopustil zjavného porušenia zákona, je povinný ho na to písomne upozorniť a do vykonania nápravy vykonať len také operácie s osobnými údajmi, ktoré neznésu odklad. Prevádzkovateľ je povinný bez zbytočného odkladu vykonať nápravu podľa prvej vety, najneskôr však v lehote jedného mesiaca odo dňa doručenia písomného upozornenia; inak je sprostredkovateľ povinný o tom bez zbytočného odkladu informovať úrad. (9) Ak si sprostredkovateľ nesplní povinnosť podľa odseku 8, zodpovedá za porušenie povinnosti a za škodu spôsobenú porušením tejto povinnosti spoločne a nerozdielne spolu s prevádzkovateľom. Tým nie je dotknutá zodpovednosť sprostredkovateľa podľa tohto zákona alebo osobitného zákona.“

²⁰⁴ MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2. aktuálne a doplnené vyd. Praha: ASPI, Wolters Kluwer, 2008, s. 199.

4.4.3 Prijemca

Do kontaktu s osobnými údajmi popri prevádzkovateľovi a sprostredkovateľovi môže prichádzať aj príjemca. V zmysle § 4 ods. 2 písm. g/ ZOOÚ je ním „každá osoba, ktorej sú osobné údaje poskytnuté alebo sprístupnené.“ Z obsahu ustanovenia je zrejmé, že pojem príjemca osobných údajov úzko súvisí s pojmami „sprístupňovanie“ a „poskytnutie“ osobných údajov. To nás priviedlo k záveru, že príjemcom je osoba, ktorá môže byť aj treťou stranou, ktorej sú osobné údaje poskytnuté s možnosťou ďalšieho spracúvania (ako napr. Sociálna poisťovňa) alebo sprístupnené len jednorazovo (napr. pri nahliadnutí do súdneho spisu). Oprávnenie príjemcu na rozdiel od sprostredkovateľa nie je odvodené od práva prevádzkovateľa sprístupňovať ním zhromaždené informácie.²⁰⁵

V praxi možno za príjemcu považovať napr. personálnu agentúru, ktorá osobné údaje získa a sprístupní potenciálnemu zamestnávateľovi za účelom pozvania uchádzača na pracovný pohovor. Zároveň je agentúra povinná upozorniť uchádzača o zamestnanie už pri získavaní jeho osobných údajov, že tieto údaje môžu byť sprístupnené tretím osobám.²⁰⁶ Prijemcami osobných údajov na druhej strane nie sú úrady a orgány výkonu dozoru, dohľadu, kontroly alebo uplatňovania regulácie, t. j. prevádzkovatelia, ktorí spracúvajú osobné údaje v rámci výkonu verejnej moci pri plnení úloh vymedzených osobitným zákonom. Do tejto skupiny patrí aj Úrad na ochranu osobných údajov Slovenskej republiky.

4.5 Povinnosti zamestnávateľa ako prevádzkovateľa osobných údajov

Základné povinnosti prevádzkovateľa a sprostredkovateľa sú zakotvené v § 6 a § 8 ZOOÚ, pričom ich realizácia musí byť v súlade so základnými pravidlami obsiahnutými v § 5 ZOOÚ. V týchto základných princípoch sa odrážajú ústavné práva, ktoré vymedzujú hranice a limity ich uskutočňovania.²⁰⁷ Podľa § 5 ods. 1 ZOOÚ spracúvaním osobných údajov nesmie dochádzať k porušovaniu základných práv a slobôd dotknutých osôb, najmä k porušovaniu ich ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.

²⁰⁵ KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobných údajů v otázkách a odpovědích*. 1. vyd. Praha: Bova Polygon, 2010, s. 44.

²⁰⁶ KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobných údajů v otázkách a odpovědích*. 1. vyd. Praha: Bova Polygon, 2010, s. 40.

²⁰⁷ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 68.

Vychádzajúc z uvedených obmedzení vyplývajúcich z objektívneho práva s prihliadnutím na potreby zamestnávateľa pri zabezpečovaní nevyhnutnej personálnej a mzdovej agendy môže zamestnávateľ spracúvať nasledujúce osobné údaje uchádzača o zamestnanie: meno, priezvisko, rodné priezvisko alebo predchádzajúce priezvisko a akademický titul, dátum narodenia, bydlisko (trvalé a prechodné), štátnu príslušnosť, iné kontaktné údaje (telefónne číslo a e-mail), údaje o dosiahnutom vzdelaní a kvalifikácii, odbornej praxi, rodné číslo (len ak to ustanoví právny predpis alebo so súhlasom uchádzača), posúdenie zdravotnej spôsobilosti, pracovný posudok z predchádzajúceho zamestnania, fotografie a iné. U mladistvých môže spracúvať aj údaje o rodičoch (kontaktné údaje).

Podmienky spracúvania sa chápu v zmysle materiálnych listinných alebo technických (technologických) prostriedkov a spôsobu výkonu tejto činnosti vrátane vymedzenia zodpovednosti, ktoré musí prevádzkovateľ určiť dostatočne konkrétne, napr. ako sledovanie e-mailovej komunikácie, pretože v opačnom prípade mu hrozia sankcie zo strany ÚOOÚ.²⁰⁸ Najčastejším spôsobom vymedzenia účelu a prostriedkov je ich zakotvenie v internom predpise prevádzkovateľa, ktoré môže s prihliadnutím na úroveň efektivity prispôbovať a meniť v priebehu spracúvania osobných údajov.²⁰⁹

Účel spracúvania osobných údajov je základným pojmom, od ktorého sa odvíjajú zásady a princípy samotného spracúvania osobných údajov (ako napr. primeranosť, nevyhnutnosť, proporcionalita a odôvodnenosť spracúvania osobných údajov). Vychádzajúc z legálnej definície účelu v ustanovení § 4 ods. 3 písm. c/ ZOOÚ sa ním rozumie „*vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť*“. Z tejto legálnej definície možno odvodiť pojmové znaky účelu spracúvania osobných údajov, ktorý musí byť:

- a) stanovený vopred,
- b) určený jednoznačne,
- c) vymedzený prevádzkovateľom alebo ustanovený zákonom,
- d) musí sa vzťahovať na určitú činnosť.²¹⁰

Účel spracúvania osobných údajov je jednoducho povedané zámer spracúvania deklarovaný prevádzkovateľom alebo určený zákonom a konkretizuje činnosť, ku ktorej sa ich spracúvanie viaže. Má tiež dôležitý význam pre vymedzenie hraníc, v ktorých je prevádzkovateľ oprávnený spracúvať osobné údaje a má slúžiť na ochranu práv a právom chránených záujmov jednotlivcov.

²⁰⁸ Porovnaj § 46 ods. 1 písm. g/ ZOOÚ.

²⁰⁹ KUČEROVÁ, A. a kol. *Zákon o ochrane osobných údajů: komentář*. 1. vyd. Praha: C.H. Beck, 2012, s. 108.

²¹⁰ ÚOOÚ, Metodické usmernenie č. 3/2014 k účelu spracúvania osobných údajov z 30. decembra 2014. (online). Dostupné z: (https://dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmernenie_c_3_2014_k_ucelu_spracuvania_osobnych_udajovpw.pdf).

V prípade ak podmienky spracúvania osobných údajov ustanovuje zákon, podmienka legality musí byť splnená automaticky. Pred začiatkom samotného spracúvania osobných údajov musí prevádzkovateľ definovať jeho účel a podmienky, ak nie sú ustanovené osobitným zákonom.²¹¹ V prípadoch, ak zákon neustanovuje účel spracúvania osobných údajov, napr. Zákonník práce v § 75 neustanovuje účel na vedenie osobného spisu zamestnanca, mal by ho určiť sám prevádzkovateľ spôsobom zodpovedajúcim jeho potrebám vo vnútornom predpise. Spracúvanie osobných údajov na základe zákona je typické najmä pre pracovno-právne vzťahy, pretože zamestnávateľ je povinný viesť evidenciu pracovnej doby, mzdy a skutočností, ktoré je povinný oznamovať Sociálnej poisťovni a zdravotným poisťovňam. Ak podmienky spracúvania neustanovuje zákon, môže skupina prevádzkovateľov z oblasti verejného práva stanoviť len taký účel spracovania osobných údajov, ktorý umožňuje zákon²¹² a ostatní prevádzkovatelia z oblasti súkromného práva môžu stanoviť akýkoľvek účel spracovania osobných údajov, ktorý im zákon nezakazuje.²¹³ Nelegálnym spracúvaním údajov sa stáva tiež každý prípad, keď si sám prevádzkovateľ určí účel spracúvania, hoci ho osobitná právna úprava explicitne určuje.

Podľa metodického usmernenia Úradu na ochranu osobných údajov Slovenskej republiky je dôležité, aby prevádzkovateľ vymedzil účel spracúvania osobných údajov vopred, to znamená ešte pred samotným začatím spracúvania v informačnom systéme. Pritom uvádza, že nie je prípustné, aby prevádzkovateľ počas spracúvania osobných údajov v informačnom systéme zmenil účel spracúvania osobných údajov, pretože vtedy by už šlo o vymedzenie nového účelu spracúvania, od ktorého sa odvíjajú povinnosti prevádzkovateľa nezávisle od pôvodného účelu. Prevádzkovateľ tiež musí vymedziť účel, ktorý je logicky spojený s konkrétnou činnosťou, ktorú vykonáva (napr. predaj tovaru).²¹⁴

Zásada legitimacy sa prejavuje tak, že účel spracovania musí byť oprávnený a jasne vyjadrený.²¹⁵ Príkladom legitímneho (oprávneného) spracúvania osobných údajov je v pracovnoprávných vzťahoch prípad, keď zamestnávateľ zisťuje informácie o zdravotnom stave alebo rodinných príslušníkoch kvôli prispôbeniu

²¹¹ Napr. zákon č. 162/1995 Z. z. o katastri nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam (katastrálny zákon) alebo zákon č. 253/1998 Z. z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky.

²¹² Čl. 2 ods. 2 Ústavy SR: „*Štátne orgány môžu konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon.*“

²¹³ Čl. 2 ods. 3 Ústavy SR: „*Každý môže konať, čo nie je zákonom zakázané, a nikoho nemožno nútiť, aby konal niečo, čo zákon neukladá.*“

²¹⁴ ÚOOÚ, Metodické usmernenie č. 3/2014 k účelu spracúvania osobných údajov z 30. decembra 2014. (online). Dostupné z: (https://dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmernenie_c_3_2014_k_ucelu_spracuvania_osobnych_udajovpw.pdf).

²¹⁵ Táto definícia vyplýva aj čl. 6 ods. 1 smernice č. 95/46/ES.

pracovného času alebo pracovného prostredia zamestnanca. Neoprávneným by naopak bolo zisťovanie týchto údajov len na selekciu zamestnancov „najspôsobi-nejších“ na výkon danej práce z hľadiska zdravotných a rodinných pomerov, čo by mohlo diskriminovať zamestnanca. V prípade nejednoznačného vymedzenia účelu spracúvania môže dochádzať k poškodeniu práv dotknutých osôb najmä tým, že im nebude zrejmé, na aký účel poskytujú prevádzkovateľovi svoje osobné údaje.

Povinnosti prevádzkovateľa, resp. každého zamestnávateľa v pozícii prevádzkovateľa, sa rozlišujú vzhľadom na jednotlivé štádiá procesu spracúvania, počas prípravy, pri začatí, v priebehu a po skončení spracúvania osobných údajov.²¹⁶

4.5.1 Oznamovacia povinnosť a osobitná registračná povinnosť

V rámci štádia prípravy na spracúvanie osobných údajov je prevádzkovateľ povinný v zmysle § 6 ods. 2 písm. a/ ZOOÚ jasne a jednoznačne vymedziť účel, resp. cieľ spracúvania, ktorý musí byť v súlade s Ústavou Slovenskej republiky, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná. Ďalej musí stanoviť podmienky spracúvania takým spôsobom, aby neobmedzil práva dotknutých osôb. Stanovenie účelu a podmienok spracúvania sa nevyžaduje, ak je účel stanovený osobitným zákonom alebo podmienky stanovené zákonom či vykonávacím predpisom. Jeho ostatné povinnosti v tomto štádiu súvisia s prijímaním bezpečnostných opatrení (§ 19 a 20 ZOOÚ), povinnosťou mlčanlivosti (§ 22 ZOOÚ) alebo oznamovacou povinnosťou (§ 33 a nasl. ZOOÚ, oznámenie, osobitná registrácia a evidencia informačného systému).

Povinnosť oznámiť ÚOOÚ spracovanie osobných údajov pomocou informačného systému sa viaže k prípravnej fáze, t. j. k momentu vytvárania informačného systému, prostredníctvom ktorého bude prevádzkovateľ spracovávať osobné údaje. Táto povinnosť mu však vzniká aj v prípade, ak nastanú v priebehu spracúvania akékoľvek zmeny oznámených údajov a údajov prihlásených na osobitnú registráciu. Oznamovacia povinnosť prevádzkovateľa osobných údajov má dôležitý význam z hľadiska zaistenia výkonu dozoru a kontroly zo strany ÚOOÚ. Povinným subjektom je len prevádzkovateľ, ako to vyplýva z výslovného znenia § 33 ZOOÚ.

Oznamovacia povinnosť je vymedzená v § 34 jednak z pozitívneho hľadiska (ods. 1) ale aj z hľadiska negatívneho (ods. 2).²¹⁷ Oznámenie musí obsahovať

²¹⁶ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 72 – 75.

²¹⁷ V zmysle § 34 ods. 1 ZOOÚ „*Oznamovacia povinnosť sa vzťahuje na všetky informačné systémy, v ktorých sa spracúvajú osobné údaje úplne alebo čiastočne automatizovanými prostriedkami*“

informácie v rozsahu požadovanom ustanovením § 35 ZOOÚ a podľa platného práva ho možno realizovať aj prostredníctvom elektronického formulára (aj bez zaručeného elektronického podpisu). Splnenie tejto povinnosti potvrdzuje ÚOOÚ osobitným potvrdením, pričom ÚOOÚ je povinný vyhovieť bezplatne komukoľvek, kto požiada o sprístupnenie a zverejnenie oznámení a osobitnej registrácie v predpísanom rozsahu (§ 42 ZOOÚ).

ZOOÚ rozoznáva aj tzv. osobitnú registračnú povinnosť. Tá sa vzťahuje na informačné systémy len v taxatívne uvedených prípadoch (§ 37 ZOOÚ), napr. ak sa spracúvajú osobné údaje v zmysle § 10 ods. 3 písm. g/ ZOOÚ²¹⁸ alebo sa spracúvajú niektoré osobitné kategórie osobných údajov podľa § 13 ods. 1 ZOOÚ a predpokladá sa ich prenos do tretej krajiny, ktorá nezaručuje primeranú úroveň ochrany osobných údajov.

4.5.2 Informačná povinnosť

Pri začatí spracúvania osobných údajov má prevádzkovateľ nasledujúce povinnosti. Ešte pred samotným získavaním údajov, má prevádzkovateľ informačnú povinnosť vo vzťahu k dotknutej osobe (v rozsahu uvedenom v § 15 ZOOÚ). Získavať osobné údaje môže len na vopred ním definovaný alebo zákonom stanovený účel a nesmie ich získavať pod zámkou iného účelu (§ 6 ods. 2 písm. c/ ZOOÚ). Zároveň je jeho povinnosťou vyžiadať si súhlas dotknutej osoby, ak sa na spracúvanie jej osobných údajov nevzťahujú výnimky, ktoré prevádzkovateľa oprávňujú spracovávať osobné údaje dotknutej osoby aj bez jej predchádzajúceho súhlasu.

Každý prevádzkovateľ je povinný informovať dotknuté osoby o tom, že bude spracovávať ich osobné údaje. Jeho informačná povinnosť sa preto spája s fázou začatia spracúvania osobných údajov. Dôvodom existencie informačnej povinnosti prevádzkovateľa je na jednej strane zaistenie efektívneho bránenia práv dotknutej osoby. Z tohto hľadiska je preto prevádzkovateľ povinný informovať dotknutú osobu ešte pred samotným získavaním osobných údajov. Na druhej strane poskytnutie potrebných informácií prevádzkovateľom zabezpečuje väčšiu

spracúvania. “Podľa § 34 ods. 2 ZOOÚ sa povinnosť registrácie podľa ods. 1 nevzťahuje na vybrané informačné systémy (napr. také, ktoré podliehajú osobitnej registrácii podľa § 37 alebo dohľadu zodpovednej osoby alebo obsahujú údaje, ktoré sú spracúvané na základe zákona).

²¹⁸ § 10 ods. 3 písm. g/ ZOOÚ „*Spracúvanie osobných údajov je nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa alebo tretej strany, najmä osobné údaje spracúvané v rámci ochrany majetku, finančných alebo iných záujmov prevádzkovateľa a osobné údaje spracúvané na zabezpečenie bezpečnosti prevádzkovateľa prostredníctvom kamier alebo obdobných systémov; to neplatí, ak pri takomto spracúvaní osobných údajov prevažujú základné práva a slobody dotknutej osoby, ktoré podliehajú ochrane podľa tohto zákona.*“

transparentnosť spracovania osobných údajov, pretože dotknutá osoba vie o tom, kto, kde a akým spôsobom bude spracúvať jej osobné údaje²¹⁹ a akému subjektu môžu byť sprístupnené. Predmetná povinnosť tiež zahŕňa poučenie o tom, či je poskytnutie osobných údajov povinné alebo dobrovoľné, či je daná možnosť slobodne sa rozhodnúť neposkytnúť osobné údaje a či dotknutá osoba vôbec poskytne svoje osobné údaje prevádzkovateľovi alebo inému subjektu. Rozsah informácií, na ktoré má dotknutá osoba nárok, je uvedený v § 15 ods. 1 a 2 ZOOÚ, pričom ods. 3 citovaného paragrafu obsahuje výnimky z informačnej povinnosti prevádzkovateľa. Po splnení informačnej povinnosti spravidla nasleduje fáza, keď sa dotknutá osoba rozhoduje o (ne)udelení súhlasu so spracovaním svojich osobných údajov.

4.5.3 Povinnosť vyžiadať súhlas dotknutej osoby

Základným právnym titulom umožňujúcim spracúvanie osobných údajov je poskytnutie súhlasu dotknutej osoby (zamestnanca). Poskytnutiu súhlasu zodpovedá povinnosť zamestnávateľa ako prevádzkovateľa vyžiadať si tento súhlas. Všeobecne platí, že spracúvanie akýchkoľvek osobných údajov dotknutej osoby je možné len s jej súhlasom, pričom súhlas so spracúvaním osobných údajov sa má poskytnúť vždy až po splnení informačnej povinnosti prevádzkovateľa. Možno mu preto prisúdiť prívlastok „informovaný“.²²⁰ Výnimky z tejto zásady sú ustanovené v ZOOÚ (v § 10) alebo v osobitnom predpise (§ 11 ods. 1 ZOOÚ).

Len dotknutá fyzická osoba môže rozhodovať o tom, komu osobné údaje poskytne, za akých podmienok (na aký účel a akým spôsobom) a na aký dlhý čas, pretože len ona sama môže povoliť oprávnený zásah do jej súkromia. V osobitných prípadoch dáva súhlas so spracúvaním osobných údajov iná než dotknutá osoba. Príkladom sú maloleté deti, za ktoré môžu udeliť súhlas aj zákonní zástupcovia (rodičia dotknutej osoby) alebo splnomocnený zástupca, ktorého fyzická osoba, ktorej údaje sa majú spracovávať, môže splnomocniť na udelenie súhlasu so spracúvaním jej osobných údajov.²²¹ V každom prípade musí byť splnená podmienka, že osoba, ktorá udeľuje súhlas so spracúvaním osobných údajov, má plnú spôsobilosť na právne úkony.

²¹⁹ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 131.

²²⁰ NONNEMANN, F. Náležitosti souhlasu se zpracováním osobních údajů. In: *Právní rozhledy*. ISSN 1210-6410. 2011, roč. 19, č. 14, s. 521.

²²¹ Z rozsudku Nejvyššího správního soudu České republiky z 12. februára 2009 sp. zn. 9 As 34/2008 vyplýva právny názor, že právo disponovať s osobnými údajmi prináleží len fyzickej osobe, ktorej sa tieto údaje týkajú, ale nie tomu, kto ich spracúva.

Ďalším znakom súhlasu ako prejavu vôle, resp. rozhodnutia fyzickej osoby so spracúvaním jej osobných údajov je, že musí mať náležitosti právneho úkonu v zmysle § 34 Občianskeho zákonníka. Z uvedeného vyplýva, že udelený súhlas možno považovať za platný, len ak je slobodný, určitý a zrozumiteľný, jednoznačný, vedomý a výslovný.²²² V opačnom prípade pôjde o neplatný právny úkon (*nullum negotium*). ZOOÚ ponecháva vo väčšine prípadov na prevádzkovateľovi, akú formu súhlasu si zvolí a len v niektorých zákonom stanovených prípadoch sa vyžaduje písomná forma (listinná alebo zaručený elektronický podpis).²²³

Dôležitou podmienkou však je, aby súhlas obsahoval predpísané náležitosti²²⁴ a aby bol preukázateľný (§ 11 ods. 2 a 4 ZOOÚ), čo znamená, že musí byť daný v podobe, ktorá umožňuje jeho kvalitatívne zachytenie a uchovávanie počas celého spracúvania.²²⁵ Podľa nášho názoru aj keď požiadavka výslovnosti súhlasu neznamena, že musí byť súhlas udelený vždy písomne, jeho písomná forma sa odporúča vždy vzhľadom na dôkaznú povinnosť prevádzkovateľa. Taktiež je nevyhnutné, aby bol zo súhlasu zrejмый zoznam alebo rozsah osobných údajov (§ 11 ods. 4 ZOOÚ), na ktorých spracúvanie dotknutá osoba udeľuje súhlas, pretože všeobecná formulácia súhlasu, že osoba súhlasí so spracúvaním svojich osobných údajov, prináša so sebou mnohé výkladové a praktické problémy.²²⁶

Neudelenie súhlasu od dotknutej osoby na konkrétne spracúvanie osobných údajov musí prevádzkovateľ (zamestnávateľ) rešpektovať bez vyvodzovania negatívnych dôsledkov. V praxi sa bežne stáva, že zamestnanec udeľuje súhlas so spracúvaním jeho osobných údajov zo strachu pred stratou zamestnania alebo kvôli strate dôvery u zamestnávateľa. Posúdenie, či ide skutočne o dobrovoľne poskytnutý súhlas, je preto v pracovnoprávných vzťahoch pomerne náročný a zdĺhavý proces.

Pracovná skupina 29 v Stanovisku WP 48 upozornila vo všeobecnosti na niekoľko zásad zameraných na ochranu práv, slobôd a dôstojnosti subjektov údajov

²²² Porovnaj VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 59 – 61.

²²³ Pozri § 12 ods. 1 a 2, § 15 ods. 6 a § 31 ods. 10 ZOOÚ. Odlišná je právna úprava v Českej republike, ktorá v § 4 písm. n/ ZOOÚ ČR pripúšťa aj konkludentný súhlas s výnimkou spracúvania citlivých údajov a netrvá v niektorých prípadoch na udelení súhlasu v písomnej forme.

²²⁴ § 11 ods. 4 ZOOÚ: „Súhlas sa preukazuje zvukovým alebo zvukovo-obrazovým záznamom alebo čestným vyhlásením toho, kto poskytol osobné údaje do informačného systému, alebo iným hodnoverným spôsobom. Písomný súhlas sa preukazuje dokladom, ktorý potvrdzuje poskytnutie súhlasu. Dôkaz o súhlase obsahuje najmä údaj o tom, kto súhlas poskytol, komu sa tento súhlas dáva, na aký účel, zoznam alebo rozsah osobných údajov a čas platnosti súhlasu. Súhlas daný v písomnej podobe je bez vlastnoručného podpisu toho, kto súhlas dáva, neplatný. Za súhlas v písomnej podobe sa považuje aj súhlas podpísaný zaručeným elektronickým podpisom.“

²²⁵ Porovnaj VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 107.

²²⁶ Porovnaj Stanovisko ÚOOÚ ČR č. 2/2008 – Souhlas se zpracováním osobních údajů.

v súvislosti so zamestnávaním. Zaujala pritom taký postoj k výkladu slobodného súhlasu, že „*spracovanie osobných údajov v rámci pracovnoprávných vzťahov na základe súhlasu by sa malo obmedziť zásadne na situácie, kedy má zamestnanec skutočne slobodnú voľbu s postupom zamestnávateľa nesúhlasit' a možnosť následne svoj súhlas odvolať a to bez akýchkoľvek následkov. V situácii, keď je zamestnanec požiadany o poskytnutie súhlasu so spracúvaním osobných údajov, pričom ale existuje riziko akejkoľvek ujmy v prípade jeho odmietnutia, nemožno udelený súhlas považovať za platný právny úkon*“.²²⁷ Dôvodila len teoretickou možnosťou zamestnanca odmietnuť poskytnutie súhlasu, ale s možným následkom straty zamestnania.

V Stanovisku WP 187 Pracovná skupina 29 vyjadrila obdobný názor, že „*súhlas môže byť platný iba vtedy, ak si dotknutá osoba skutočne môže vybrať a neexistuje riziko podvodu, zastrážovania, nátlaku alebo významných negatívnych následkov, ak dotknutá osoba nebude súhlasit'*“.²²⁸ Uviedla tiež príklad, že v prípade, ak zamestnávateľ zriadi intranet, kde sú zverejnené mená a hlavné pracovné úlohy zamestnancov, a rozpošle im žiadosť o zverejnenie fotografie, tak samotné dobrovoľné uloženie fotografie zamestnancom na intranet alebo jeho osobitné výslovné odsúhlasenie, napr. v elektronickom formulári, možno považovať za jeho platný súhlas. V oboch prípadoch sa v plnom rozsahu rešpektuje vôľa zamestnancov.²²⁹

Výnimky zo zásady spracúvania osobných údajov výlučne so súhlasom dotknutej osoby sú upravené v § 10 ZOOÚ. Zamestnávateľia na základe nich nebudú potrebovať súhlas dotknutých osôb najmä, ak:

- „*spracúvanie osobných údajov je nevyhnutné na účely tvorby umeleckých alebo literárnych diel, pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu jeho činnosti; to neplatí, ak spracúvaním osobných údajov na takýto účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti a súkromia alebo takéto spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný zákon alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná*“ (§ 10 ods. 3 písm. a/ ZOOÚ),
- „*spracúvanie je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán alebo v predzmluvných vzťahoch*“ (§ 10 ods. 3 písm. b/ ZOOÚ),
- „*spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby*“ (§ 10 ods. 3 písm. c/ ZOOÚ),

²²⁷ Stanovisko Pracovnej skupiny 29 č. 8/2001 k spracúvaniu osobných údajov v rámci pracovného pomeru z 13. septembra 2001, WP 48.

²²⁸ Stanovisko Pracovnej skupiny 29 č. 15/2011 k definícii súhlasu z 13. júla 2011, WP 187, s. 12.

²²⁹ Stanovisko Pracovnej skupiny 29 č. 15/2011 k definícii súhlasu z 13. júla 2011, WP 187, s. 14.

- „sa spracúvajú osobné údaje, ktoré už boli zverejnené v súlade so zákonom a prevádzkovateľ ich náležite označil ako zverejnené; ten, kto tvrdí, že spracúva zverejnené osobné údaje, na požiadanie preukáže úradu, že spracúvané osobné údaje boli už zákonne zverejnené“ (§ 10 ods. 3 písm. e/ ZOOÚ),
- „spracúvanie osobných údajov je nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa alebo tretej strany, najmä osobné údaje spracúvané v rámci ochrany majetku, finančných alebo iných záujmov prevádzkovateľa a osobné údaje spracúvané na zabezpečenie bezpečnosti prevádzkovateľa prostredníctvom kamier alebo obdobných systémov; to neplatí, ak pri takomto spracúvaní osobných údajov prevažujú základné práva a slobody dotknutej osoby, ktoré podliehajú ochrane podľa tohto zákona“ (znenie § 10 ods. 3 písm. g/ ZOOÚ od prijatia novely účinnej od 15. apríla 2014).

Ďalšou fázou je tzv. **priebeh spracúvania** osobných údajov, kedy je prevádzkovateľ povinný (v zmysle § 6 ods. 2 písm. d/, e/, f/, g/, i/ ZOOÚ) zabezpečiť len spracúvanie osobných údajov zodpovedajúcich účelu ich spracúvania svojím rozsahom a obsahom. Ich spracúvanie je prípustné výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromaždené, a naopak je neprípustné, ak boli údaje získané na osobitne rozdielne účely. Prevádzkovateľ je oprávnený spracúvať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania. Nesprávne a neúplné osobné údaje je povinný blokovat' a bezodkladne opraviť či doplniť. Ak to nie je možné, je povinný ich zreteľne označiť a zlikvidovať. Spracúvanie osobných údajov musí byť uskutočnené v takej forme, ktorá umožní identifikáciu dotknutých osôb len počas obdobia nevyhnutného na dosiahnutie účelu spracúvania. Navyše musí prevádzkovateľ zaistiť spracúvanie osobných údajov v súlade s dobrými mravmi a tak, aby neodporovalo akémukoľvek zákonu.²³⁰

Poslednou fázou je **štádium skončenia spracúvania** osobných údajov, pre ktoré je charakteristické dosiahnutie účelu spracúvania a s tým spojená následná likvidácia osobných údajov, ktorých účel spracúvania zanikol (podľa § 17 ZOOÚ). Je možné pokračovať v spracúvaní osobných údajov aj po tomto štádiu, ale len za podmienok ustanovených zákonom a na účely historického a vedeckého výskumu, prípadne kvôli sledovaniu vývoja alebo vedenia štatistiky.

²³⁰ Porovnaj tiež ÚOOÚ, *Zásady pri spracúvaní osobných údajov*. (online). Dostupné z: (<https://dataprotection.gov.sk/uouu/sk/content/zasady-pri-spracuvani-osobnych-udajov>).

4.5.4 Povinnosť prijať bezpečnostné opatrenia

Všeobecnou povinnosťou prevádzkovateľa, ktorá je platná počas celého obdobia spracúvania osobných údajov, ale aj po jej skončení, je chrániť spracúvané osobné údaje pred ich zničením, sprístupnením, stratou, zmenou a podobne. Preto je povinný prijímať primerané bezpečnostné opatrenia (§ 19 a nasl. ZOOÚ), ktorých rámec je určený prostriedkami a spôsobom spracovania osobných údajov, ich dôvernosti, prípadne posúdením rizík. Za prijateľné a vhodné bezpečnostné opatrenie nemožno považovať prípad, ak personalistka ponechá dokumentáciu s osobnými údajmi zamestnancov v priestore prístupnom verejnosti (napr. v kancelárii v neuzamknutej skrini, ku ktorej majú prístup aj iné nepoverené osoby, zamestnanci upratovacej služby).

Povinnosť chrániť osobné údaje sa môže z obsahového hľadiska zrealizovať vo forme technických, organizačných a personálnych bezpečnostných opatrení, ktoré musia byť v zmysle platného ZOOÚ zdokumentované v dvoch podobách bezpečnostnej dokumentácie. Prvou je základná dokumentácia, druhou je bezpečnostný projekt informačného systému. V prvom prípade ide o opatrenia chrániace osobné údaje spracúvané v informačnom systéme, ktorý nie je prepojený s verejne prístupnou počítačovou sieťou a nejde o spracúvanie osobitnej kategórie osobných údajov (napr. písomné poučenie oprávnenej osoby, písomné poverenie zodpovednej osoby). Bezpečnostný projekt je určený na pokrytie najviac rizikových foriem spracúvania osobných údajov, ak prevádzkovateľ spracúva osobitnú kategóriu osobných údajov v informačnom systéme prepojenom s verejne prístupnou počítačovou sieťou alebo slúžiacom na zabezpečenie verejného záujmu.²³¹

Medzi **technické opatrenia** bezpečnostného projektu patria napr.:

- zabezpečenie objektu, v ktorom sa nachádza informačný systém pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) prípadne pomocou technických zabezpečovacích prostriedkov (poplašný systém),
- umiestnenie informačného systému v priestore chránenom pred prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia,
- bezpečné uloženie fyzických nosičov osobných údajov (listinných dokumentov v uzamykateľných skriniach a trezoroch),
- zariadenia na likvidáciu fyzických nosičov osobných údajov (zariadenia na skartovanie listín), ochrana e-mailového servera prevádzkovateľa softvérovým zabezpečením (antivírusovým a antispamovým programom),

²³¹ Pozri bližšie VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 148 – 151.

- ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. Firewall).

K **personálnym opatreniam** zaraďujeme:

- poučenie oprávnených osôb pred uskutočnením spracúvania osobných údajov,
- písomné poverenie zodpovednej osoby podľa § 23 ZOOÚ,
- vzdelávanie oprávnených osôb (v oblasti práva a informačných technológií),
- zabezpečenie vzájomného zastupovania oprávnených osôb (napr. v prípade práceneschopnosti).

Medzi **organizačné opatrenia** patrí:

- správa hesiel (prideľovanie, zmena, rušenie),
- postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. zrušenie prístupových práv, poučenie o následkoch porušenia povinnosti mlčanlivosti),
- pravidiel spracúvania osobných údajov v chránenom priestore i mimo neho,
- určenie postupov likvidácie osobných údajov z fyzických i dátových nosičov.

V súvislosti s povinnosťou každého zamestnávateľa zabezpečiť primerané opatrenia na ochranu osobných údajov zamestnancov spomenieme rozhodnutie z 12. júla 2011 sp. zn. 1 Sžo 410/2009, v ktorom dospel Najvyšší súd Slovenskej republiky k záveru, že správny orgán (katastrálny úrad ako žalobca) porušil zákonnú povinnosť ustanovenú v § 13 ods. 1 zákona č. 428/2002 Z. z. o ochrane osobných údajov tým, že po splnení účelu spracúvania osobných údajov nezabezpečil riadne a bezodkladne ich likvidáciu. Zo skutkových okolností prípadu vyplýva, že zamestnanci upratovacej firmy, ktorá vykonávala upratovacie služby na pracovisku žalobcu, vyhodila neskartované dokumenty obsahujúce osobné údaje fyzických osôb (aj rodné čísla) na skládku odpadu neďaleko pracoviska. V dôsledku nezodpovedného postupu zamestnancov správneho orgánu pri likvidácii osobných údajov následne Úrad na ochranu osobných údajov Slovenskej republiky uložil žalobcovi pokutu vo výške 2 323,57 € (70 000 Sk) s odôvodnením, že „*osobné údaje boli sprístupnené širokému okruhu osôb, teda boli vystavené možnému riziku ich zneužitia, pričom nie je možné určiť a zistiť, koľko osobných údajov takto uniklo a či sa dostali k neoprávneným osobám*“. Konštatoval pritom, že z nesplnenia tejto povinnosti sa nemôže žalobca vyviníť poukazovaním na skutočnosť, že pre nedostatok finančných prostriedkov nemal k dispozícii skartovací prístroj. Podľa názoru Najvyššieho súdu Slovenskej republiky ako odvolacieho súdu „*bolo v správnom konaní bez akýchkoľvek pochybností preukázané, že žalobca ako právnická osoba sa dopustil správneho deliktu, za ktorý mu bola uložená sankcia v zmysle zákona. Tvrdenie žalobcu, že nemal žiaden úmysel sprístupniť osobné údaje, a teda deliktu sa nedopustil, je irelevantné, pretože u správneho deliktu zavinenie, či už úmyselné alebo nedbanlivostné, teda určitý stav vedomia a vôle subjektu, nie je*

jeho pojmovým znakom. Zodpovedným subjektom je právnická osoba, ktorej zodpovednosť za nedodržanie zákonných povinností je absolútna. Ide teda o zodpovednosť objektívnu a nie subjektívnu. Právnická osoba ako celok zodpovedá za výsledok porušenia, nedodržania zákonnej povinnosti, bez ohľadu na zavinenie. Z tohto dôvodu preto nemožno ani prihliadať na mieru zavinenia upratovacej firmy, pretože bolo povinnosťou žalobcu prijať a zabezpečiť také opatrenia, pri dodržaní ktorých by k porušeniu povinností vyplývajúcich zo zákona č. 428/2002 Z. z. nedošlo“.²³²

4.5.5 Povinnosť likvidácie osobných údajov

Likvidácia údajov súvisí bezprostredne s ukončením spracúvania osobných údajov na daný účel. V okamihu naplnenia účelu spracúvania (a po uplynutí lehoty na uchovávanie osobných údajov) je povinný zamestnávateľ ako prevádzkovateľ osobné údaje bezodkladne zlikvidovať.²³³ Z ustanovenia § 6 ods. 2 písm. h/ ZOOÚ vyplýva, že je povinný „zlikvidovať tie osobné údaje, ktorých účel spracúvania sa skončil; po skončení účelu spracúvania možno osobné údaje ďalej spracúvať len za podmienok ustanovených v odseku 5“.²³⁴ Povinnosť likvidácie osobných údajov zamestnanca vyplýva priamo z platného zákona o štátnej službe alebo zo zákona o účtovníctve.²³⁵

4.6 Práva zamestnanca ako dotknutej osoby

Medzi najdôležitejšie práva dotknutej osoby patrí **právo byť informovaný** o spracúvaní svojich osobných údajov. Poskytuje mu totiž možnosť rozhodnúť sa, či prevádzkovateľovi poskytne informácie o vlastnom súkromí. Tomuto jeho právu zodpovedá oznamovacia povinnosť prevádzkovateľa uvedená v ustanovení § 15 ZOOÚ, ktorý je povinný oznámiť zamestnancovi ako dotknutej osobe ešte

²³² Rozsudok Najvyššieho súdu Slovenskej republiky z 12. júla 2011 sp. zn. 1 Sžo 410/2009.

²³³ ÚOOÚ, Metodické usmernenie č. 3/2014 k účelu spracúvania osobných údajov z 30. decembra 2014. (online). Dostupné z: (https://dataprotection.gov.sk/uouu/sites/default/files/metodicke_usmernenie_c_3_2014_k_ucelu_spracuvania_osobnych_udajovpw.pdf).

²³⁴ V zmysle § 6 ods. 5 ZOOÚ je prípustné zhromaždené osobné údaje spracúvať v nevyhnutnom rozsahu na historický alebo vedecký výskum alebo na účely vedenia štatistiky. Podmienkou však je, že prevádzkovateľ musí také údaje označiť, anonymizovať, ak tým možno dosiahnuť účel spracúvania a zlikvidovať ich hneď, ako sa stanú nepotrebnými.

²³⁵ Podľa § 73 ods. 4 zákona č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov „po skončení štátnozamestnaneckého pomeru je prevádzkovateľ povinný uchovávať osobný spis štátneho zamestnanca 50 rokov“. Po uplynutí tejto lehoty je povinný osobný spis vráťane osobných údajov zlikvidovať.

pred získavaním osobných údajov identifikačné údaje spracovateľa, účel a rozsah spracúvania, prípadne akému predpokladanému okruhu osôb budú tieto údaje sprístupnené. Ďalej je povinný dotknutú osobu poučiť o dobrovoľnosti alebo povinnosti poskytnúť osobné údaje a o jej právach. Podľa nášho názoru jasné znenie ZOOÚ, v zmysle ktorého oznamovacia povinnosť musí byť splnená ešte pred samotným získavaním osobných údajov, aj keď k samotnému spracovaniu nakoniec nedôjde, neposkytuje priestor na diskusné úvahy, či je splnenie oznamovacej povinnosti prípustné aj v priebehu zhromažďovania osobných údajov.

Oznamovacia povinnosť sa nevyžaduje, ak sú súčasne splnené podmienky, keď prevádzkovateľ spracúva osobné údaje na účely vedeckého výskumu alebo štatistiky, alebo ak je to nevyhnutné na účely tvorby umeleckých a literárnych diel alebo informovania verejnosti masovokomunikačnými prostriedkami, ak spracúvanie vykonáva prevádzkovateľ, ktorému to vyplýva z predmetu jeho činnosti alebo ak vie preukázať, že mu údaje už predtým boli poskytnuté. Ak sa však preukáže, že si nespĺnil oznamovaciu povinnosť, prichádza do úvahy popretie platnosti už udeleného súhlasu dotknutej osoby.

Právo dotknutej osoby byť informovaný o podmienkach spracovania je úzko späté s **právom udeliť súhlas so spracúvaním** osobných údajov.²³⁶

Významným právom je aj jeho **právo na prístup k osobným údajom**, ktoré mu umožňuje nárokovať si na základe písomnej žiadosti o opravu, blokáciu či likvidáciu nesprávnych a neaktuálnych údajov, ale aj poskytnutie úplného zoznamu spracúvaných údajov o jeho osobe či informácií o zdroji, z ktorého prevádzkovateľ získal osobné údaje. Ak dotknutá osoba dospeje k názoru, že boli porušené jej práva garantované najmä § 28 ZOOÚ, môže sa domáhať svojich práv buď priamo u prevádzkovateľa, alebo sa môže obrátiť na dozorný orgán – Úrad na ochranu osobných údajov Slovenskej republiky so žiadosťou o odstránenie protiprávneho stavu. V prípade nespokojnosti s jeho postupom zostáva možnosť sa obrátiť na európsku inštitúciu – európskeho dozorného úradníka pre ochranu osobných údajov alebo so žalobou na všeobecný súd.

4.7 Spracúvanie osobných údajov na pracovisku

Ochrane osobných údajov v rámci pracovnoprávnych vzťahov sa nevenuje dostatočná pozornosť v teoretickej ani praktickej rovine. Mnohí zamestnávateľia ju považujú za okrajovú oblasť pracovného práva alebo ich podnikateľských záujmov. Z toho pramenia permanentne výkladové problémy a praktické nejasnosti vo vzťahu k povinnostiam zamestnávateľov, ktoré im vyplývajú z právnych pred-

²³⁶ Bližšie pozri podkapitolu 4.5.3 Povinnosť vyžiadať súhlas dotknutej osoby.

pisov na ochranu súkromia a osobných údajov zamestnancov.

Podstatný význam majú osobné údaje potenciálnych zamestnancov pre budúceho zamestnávateľa. Na základe nich si dokáže adekvátne vybrať najvhodnejšieho uchádzača na obsadzovanú pracovnú pozíciu. Pochopiteľne sa s týmto cieľom snažia zamestnávateľia zabezpečiť pred rozhodnutím čo najširší okruh dostupných informácií, ktoré im majú uľahčiť rozhodovanie. V rámci spracúvania potrebných a nevyhnutných údajov však často dochádza aj k prekračovaniu limitov slúžiacich na ochranu súkromia zamestnancov a porušovaniu zásady proporcionality a zákazu diskriminácie, na ktoré kladie dôraz v judikatúre Európsky súd pre ľudské práva a čoraz častejšie aj vnútroštátne všeobecné súdy.

Spracúvanie osobných údajov môžeme rozdeliť z hľadiska trvania pracovného pomeru na:

- Spracúvanie osobných údajov pred vznikom pracovného pomeru,
- Spracúvanie osobných údajov pri vzniku a počas trvania pracovného pomeru,
- Spracúvanie osobných údajov po skončení pracovného pomeru.

4.7.1 Osobné údaje pred vznikom pracovného pomeru

Predzmluvné vzťahy vznikajúce v štádiu pracovného pohovoru alebo výberového konania medzi zamestnancom a zamestnávateľom sú upravené v ustanovení § 41 Zákonníka práce.²³⁷ Citované ustanovenie obsahuje vymedzenie rozsahu informácií, ktoré je zamestnávateľ oprávnený požadovať od fyzickej osoby v týchto pracovnoprávných vzťahoch, ale aj informácie, ktorých získavanie od uchádzača je výslovne zakázané. Vychádzajúc z ochranej funkcie pracovného práva ako jeho základnej funkcie sa v predzmluvných vzťahoch uplatňuje namiesto princípu subordinácie princíp rovnosti, čím Zákonník práce poskytuje širšiu ochranu slabšej strane pracovnoprávného vzťahu, t. j. fyzickej osobe, ktorá sa uchádza o zamestnanie.

Zamestnávateľ, ktorý plánuje prijať nového zamestnanca, uchádzajúceho sa o voľné pracovné miesto prostredníctvom výberového konania, resp. pracovného pohovoru, zhromažďuje osobné údaje vopred neurčitého počtu uchádzačov, ktorí

²³⁷ Pozri § 41 ods. 5 a 6 Zákonníka práce: „Zamestnávateľ môže od fyzickej osoby, ktorá sa uchádza o prvé zamestnanie, vyžadovať len informácie, ktoré súvisia s prácou, ktorú má vykonávať. Zamestnávateľ môže od fyzickej osoby, ktorá už bola zamestnávaná, požadovať predloženie pracovného posudku a potvrdenia o zamestnaní. Zamestnávateľ nesmie vyžadovať od fyzickej osoby informácie a) o tehotenstve, b) o rodinných pomeroch, c) o bezúhonnosti s výnimkou, ak ide o prácu, pri ktorej sa podľa osobitného predpisu vyžaduje bezúhonnosť, alebo ak požiadavku bezúhonnosti vyžaduje povaha práce, ktorú má fyzická osoba vykonávať, d) o politickej príslušnosti, odborovej príslušnosti a náboženskej príslušnosti.“

prejaví svoj záujem stať sa jeho zamestnancom. V štádiu pred vznikom pracovného pomeru sám uchádzač o zamestnanie poskytuje osobné údaje zamestnávateľovi v rámci životopisu, motivačného listu, dokladov o vzdelaní a podobne. Na také spracúvanie osobných údajov nepotrebuje ich súhlas podľa § 10 ods. 3 písm. b/ ZOOÚ, pretože ide o zákonnú výnimku, kedy sa považuje spracúvanie za nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán alebo v predzmluvných vzťahoch s dotknutou osobou, alebo pri rokovaní o zmene zmluvy uskutočnenej na jej žiadosť.

ÚOOÚ ČR vychádzajúc z ustanovení českého občianskeho práva o kontrakácii²³⁸ vo svojom stanovisku konštatoval, že „*rokovania o uzavretí zmluvy v prípade výberového konania na voľné pracovné miesto sú ukončené v okamihu, keď je uchádzač upovedomený o tom, že nebol na pracovné miesto vybratý, alebo keď je s ním, naopak, v prípade jeho výberu uzavretá pracovná zmluva*“. Vyjadril názor, že zamestnávateľ môže bez súhlasu uchádzača spracovávať jeho osobné údaje len do okamihu, keď mu oznámil, že nebol na pracovné miesto vybratý. Ak by mal záujem spracovávať osobné údaje uchádzača aj naďalej, musí disponovať jeho preukázateľným súhlasom. Neprijatý uchádzač v takom prípade totiž oprávnené predpokladá, že rokovania o uzatvorení pracovnej zmluvy boli ukončené.²³⁹

V rámci predzmluvných vzťahov nie je zamestnávateľ oprávnený požadovať také informácie, ktoré nie sú potrebné a relevantné pre jeho rozhodnutie, či s potenciálnym zamestnancom uzatvorí pracovnú zmluvu, prípadne informácie súvisiace s ochranou jeho dôstojnosti. Právna úprava predzmluvných vzťahov v ustanovení § 41 ods. 6 Zákonníka práce chráni fyzickú osobu pred osobitne vymedzenými otázkami na pracovnom pohovore či výberovom konaní, ktoré sú spôsobilé zasiahnuť do intímnej sféry uchádzača o zamestnanie, resp. do jej súkromia, a tým aj do osobnostných práv. Predmetné ustanovenie zakotvuje ochranu súkromia a ochranu osobných údajov fyzickej osoby uchádzajúcej sa o zamestnanie.²⁴⁰ Do uvedenej skupiny „zakázaných údajov“ patria otázky o rodinných a majetkových pomeroch a zdravotnom stave.²⁴¹ Zákon o službách zamestnanosti obsahuje obdobnú právnu úpravu obsahujúcu navyše osobné údaje o sexuálnej orientácii.²⁴² Slovenská

²³⁸ V slovenskej právnej úprave im zodpovedá § 43b ods. 1 písm. c/ Občianskeho zákonníka.

²³⁹ Z rozhodovacej činnosti ÚOOÚ ČR ke spracováni osobních údajů uchazečů o zaměstnání, č. j. SKO-0629/07.

²⁴⁰ BARANCOVÁ, H. *Zákonník práce. Komentár*. 1. vyd. Praha: C. H. Beck, 2010, s. 203 až 205.

²⁴¹ Na porovnanie ZOOÚ ČR v § 4 písm. b/ zaraďuje medzi také údaje navyše údaje o sexuálnom živote a genetické údaje.

²⁴² § 62 ods. 3 zákona č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov: „*Zamestnávateľ nesmie pri výbere zamestnanca vyžadovať informácie, ktoré sa týkajú národnosti, rasového pôvodu alebo etnického pôvodu, politických postojov, členstva v odborových organizáciách, náboženstva, sexuálnej orientácie, informácie, ktoré odporujú dobrým mravom, a osobné údaje, ktoré nie sú potrebné na plnenie povinností zamestnávateľa ustanovených osobit-*

právna úprava pritom zodpovedá zákazu diskriminácie v práve Európskej únie, konkrétne čl. 14 smernice Európskeho parlamentu a Rady 2006/54/ES z 5. júla 2006 o vykonávaní zásady rovnosti príležitostí a rovnakého zaobchádzania s mužmi a ženami vo veciach zamestnanosti a povolania.²⁴³

S právnou reguláciou povinností zamestnávateľa, týkajúcich sa ochrany osobných údajov zamestnanca v rámci predzmluvných vzťahov, sa stretávame aj v ustanovení § 41 ods. 5 Zákonníka práce, ktoré upravuje na jednej strane situáciu, kedy sa fyzická osoba uchádza o svoje prvé zamestnanie a na strane druhej situáciu, ak sa o zamestnanie uchádza osoba predtým zamestnaná. Podľa niektorých názorov je informačná povinnosť v zmysle ustanovenia § 41 ods. 5 Zákonníka práce formulovaná veľmi všeobecne a relatívne široko.²⁴⁴

Analýzou jeho obsahu sme dospeli k záveru, že :

- **u osoby, ktorá sa uchádza o svoje prvé zamestnanie**, rozsah informácií, ktoré od nej môže zamestnávateľ požadovať, je zúžený na informácie, týkajúce sa výlučne vykonávanej práce,
- **u osoby, ktorá už bola zamestnaná**, je ich rozsah rozšírený o oprávnenie zamestnávateľa vyžadovať aj predloženie pracovného posudku a potvrdenia o zamestnaní. Ide o dokumenty obsahujúce osobné údaje fyzickej osoby, pretože v pracovnom posudku sa môžu uvádzať údaje, ktoré sa týkajú prejavov jej osobnosti a súvisia s predchádzajúcou prácou. Obsahom potvrdenia o zamestnaní je aj údaj o poskytnutej mzde za vykonanú prácu.

V ustanovení § 41 ods. 6 Zákonníka práce sú uvedené údaje, ktoré zamestnávateľ nesmie od fyzickej osoby vyžadovať buď vôbec, alebo len za určitých presne

ným predpisom. Zamestnávateľ je povinný na požiadanie občana preukázať nutnosť vyžadovaného osobného údajá. Kritériá na výber zamestnanca musia zaručovať rovnosť príležitostí pre všetkých občanov.“

²⁴³ Článok 14 ods. 1 smernice č. 2006/54/ES k zákazu diskriminácie: „Nesmie dochádzať k žiadnej priamej alebo nepriamej diskriminácii z dôvodu pohlavia vo verejnom alebo súkromnom sektore vrátane orgánov verejnej správy, pokiaľ ide o:

a) podmienky prístupu k zamestnaniu, samostatne zárobkovej činnosti alebo k povolaniu vrátane výberových kritérií a podmienok náboru bez ohľadu na oblasť činnosti a na všetkých úrovniach profesijnej hierarchie vrátane postupu;

b) prístup k všetkým typom a k všetkým úrovniam odborného vedenia, odbornej prípravy, pokročilej odbornej prípravy a rekvifikácie vrátane praktických pracovných skúseností;

c) zamestnanie a pracovné podmienky vrátane prepustenia, ako aj odmien, ako je stanovené v článku 141 zmluvy;

d) členstvo a účasť v organizácii zamestnancov alebo zamestnávateľov alebo v akejkoľvek organizácii, ktorej členovia vykonávajú určité povolanie, vrátane výhod poskytovaných touto organizáciou.“

²⁴⁴ TROJAN, J. Ochrana základných práv a slobôd osôb pred uzatvorením pracovnej zmluvy pri výkone práce vo verejnom záujme. In: *Teória a prax verejnej správy*. Košice: Univerzita P. J. Šafárika v Košiciach, 2004, s. 421.

stanovených podmienok, pričom uvedený výpočet údajov je taxatívny.²⁴⁵ Považujeme za potrebné zdôrazniť, že ak zákaz spracúvania výslovne uvedených osobných údajov musí platiť pre zamestnávateľa počas trvania pracovného pomeru, argumentačným výkladom *a minori ad maius* (čiže od menšieho k väčšiemu) sa vzťahuje uvedený zákaz na zamestnávateľa aj pred samotným vznikom pracovno-právneho vzťahu.

Na základe normatívnej analýzy znenia ustanovenia § 41 Zákonníka práce podporeného výkladom právnej vedy sme zistili, že sa osobné údaje, ktoré zamestnávateľ nesmie vyžadovať priamo ani prostredníctvom tretích osôb, delia na dve základné skupiny:

- osobné údaje, na ktoré sa vzťahuje **absolútny zákaz** – platí pre informácie **o politickej, odborovej alebo náboženskej príslušnosti, ale aj o sexuálnej orientácii**,²⁴⁶ alebo informácie, ktoré **odporujú dobrým mravom**.²⁴⁷
- osobné údaje, na ktoré sa vzťahuje **relatívny zákaz**, t. j. za splnenia určitých podmienok – platí pre informácie **o bezúhonnosti, tehotenstve a rodinných pomeroch** (počte detí, rodinnom stave). V prípade otázok o bezúhonnosti zákaz neplatí, ak existuje vecný dôvod spočívajúci v povahe práce, ktorá sa má vykonávať (samozrejme, ak je takáto požiadavka primeraná) alebo v prípadoch, keď tak ustanoví zákon.

Údaje o tehotenstve

Hoci to celkom nevyplýva z výslovného znenia ustanovenia § 41 ods. 5 Zákonníka práce, zákaz vyžadovať údaje o tehotenstve uchádzačky o zamestnanie je relatívny, čo znamená, že je možné informácie na zistenie prípadného tehotenstva tolerovať, ak by bola ponúkaná práca fyzicky náročná.²⁴⁸ V porovnaní so slovenskou právnou úpravou § 316 ods. 4 českého Zákonníka práce výslovne pripúšťa otázky o rodinných pomeroch a tehotenstve, ak sú vecne odôvodnené povahou vykonávanej práce, ak je táto požiadavka primeraná, alebo ak to ustanoví osobitný predpis.²⁴⁹

²⁴⁵ Jeho znenie však neobsahuje rozlišovanie medzi fyzickou osobou, ktorá sa prvýkrát uchádza o zamestnanie, a tou, ktorá už bola zamestnaná. Aplikácia tohto ustanovenia je teda možná a nutná na všetkých uchádzačov o pracovnú pozíciu u daného zamestnávateľa.

²⁴⁶ Pozri § 62 ods. 3 zákona č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

²⁴⁷ BARANCOVÁ, H. *Zákonník práce. Komentár*. 1. vyd. Praha: C. H. Beck, 2010, s. 204 a 206.

²⁴⁸ K danému názoru sa prikláňa aj prof. Barancová. Pozri BARANCOVÁ, H. *Zákonník práce. Komentár*. 1. vyd. Praha: C. H. Beck, 2010, s. 204.

²⁴⁹ Pozri bližšie MORÁVEK, J. *Ochrana osobných údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 379 – 381 (Príklad z praxe č. 17).

Z judikatúry Súdneho dvora Európskej únie (predtým označovaného ako Európsky súdny dvor) však vyplýva, že otázky smerujúce k zisteniu prípadného tehotenstva uchádzačky o zamestnanie sú úplne neprípustné, lebo by takéto konanie mohlo byť kvalifikované ako diskriminačné v rámci zabezpečenia rovnakých podmienok v prístupe k zamestnaniu. Za jedno z jeho podstatných rozhodnutí o priamej diskriminácii a vo vzťahu k vyžadovaniu údajov o tehotenstve v predzmluvných vzťahoch sa považuje rozhodnutie z 3. februára 2000 v právnej veci *Silke-Karin Mahlburg v. Land Mecklenburg-Vorpommern*, vec C-207/98. V tomto prípade išlo o pracovníčku nemocnice, ktorá mala zmluvu na dobu určitú, pričom sa počas tehotenstva uchádzala u svojho zamestnávateľa o iné miesto s trvaním na dobu neurčitú. Zamestnávateľ ju odmietol, pretože podľa platných predpisov na tomto mieste tehotné ženy nemohli pracovať kvôli nebezpečenstvu infekčnej nákazy. V odôvodnení rozhodnutia súd dospel k záveru, že odmietnutie zamestnania pre tehotenstvo je priamou diskrimináciou na základe pohlavia, pretože takéto rozhodnutie sa môže týkať len žien. Konštatoval, že aplikácia predpisov na ochranu matiek nesmie znevýhodňovať uchádzačov o zamestnanie v prístupe k zamestnaniu a zamestnávateľ nie je oprávnený odmietnuť uchádzača preto, že počas tehotenstva nesmie pracovať. Z uvedeného teda vyplýva, že ak na pracovisku pracujú muži aj ženy, sú otázky o tehotenstve neprípustné, aj keby išlo o prácu, ktorá je tehotným ženám zakázaná. Táto interpretácia nás privádza k záveru, že ak by v obdobnej veci na pracovisku pracovali len ženy a prípadné tehotenstvo by malo význam z hľadiska vykonávanej práce v tom zmysle, že by išlo o zakázanú prácu pre tehotné ženy, otázky na tehotenstvo uchádzačky by sa mohli tolerovať ako prípustné.

V ďalšom rozhodnutí z 8. novembra 1990 v právnej veci *Dekker v. Stichting Vormingscentrum voor Jong Volwassenen Plus*, vec C-177/88 vyslovil Súdny dvor Európskej únie názor, že zamestnávateľ nie je oprávnený odmietnuť uchádzača ženského pohlavia len preto, že má obavy z možných nepriaznivých dôsledkov (vzhľadom na prísnejšie právne predpisy) v súvislosti so zamestnávaním tehotnej ženy. Dokonca uviedol, že na porušenie zákazu diskriminácie na základe pohlavia nemalo vplyv, že sa o dané miesto uchádzali len ženy, a teda nebolo možné konštatovať, že v konkrétnom prípade bola ženská uchádzačka znevýhodnená vo vzťahu k mužskému uchádzačovi o zamestnanie.

Údaje o zdravotnom stave

Výkon niektorých druhov zamestnaní je podmienený aj zdravotnou alebo psychickou spôsobilosťou. Zamestnanec tak musí v zmysle § 41 ods. 2 Zákonníka práce v prípadoch ustanovených osobitným právnym predpisom absolvovať povinné vstupné lekárske prehliadky a vyšetrenia a na ich základe osvedčiť svoju

zdravotnú spôsobilosť ako nevyhnutnú podmienku, bez splnenia ktorej zamestnávateľ nemôže uzavrieť s uchádzačom pracovnú zmluvu (resp. služobnú zmluvu). Pri prijímaní mladistvého zamestnanca tiež platí, že zamestnávateľ je povinný mať k dispozícii potvrdenie o jeho lekárskej prehliadke ešte pred uzavretím pracovnej zmluvy (§ 41 ods. 3 Zákonníka práce).

Hoci Zákonník práce v § 41 ods. 6 nezahŕňa informácie o zdravotnom stave uchádzača do skupiny informácií, ktoré zamestnávateľ vyslovene nesmie vyžadovať od fyzickej osoby uchádzajúcej sa o prácu, Barancová sa domnieva, že zamestnávateľ nemá dôvod také informácie vyžadovať, ak to nevyžaduje osobitný predpis alebo ak osobitný predpis, stanovujúci zdravotné požiadavky na výkon prác, vôbec neexistuje.²⁵⁰

Vo vzťahu k spracúvaniu zdravotných údajov aj v priebehu trvania pracovného pomeru treba uviesť, že údaje týkajúce sa zdravotného stavu (fyzického aj psychického)²⁵¹ sa považujú za osobitnú kategóriu osobných údajov, ktorých spracúvanie je zakázané so zohľadnením výnimočných situácií, medzi ktoré sa v zmysle dikcie ustanovenia § 13 ods. 1 ZOOÚ zaraďuje aj prípad, ak:

- a) dotknutá osoba písomne alebo iným hodnoverným spôsobom súhlasí s ich spracúvaním (§ 14 písm. a/ ZOOÚ),
- b) právnym základom na spracúvanie zdravotných osobných údajov je osobitný zákon, právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná (§ 14 písm. b/ ZOOÚ),
- c) ich dotknutá osoba sama zverejnila alebo sú nevyhnutné pri uplatňovaní jej právneho nároku (§ 14 písm. e/ ZOOÚ) alebo
- d) sú spracúvané osobami na to určenými s cieľom poskytnúť zdravotnú starostlivosť a kvôli verejnému zdravotnému poisteniu (§ 14 písm. f/ ZOOÚ) a podobne.

Tretím z uvedených prípadov sa zaoberal aj Najvyšší súd Slovenskej republiky v rozhodnutí z 19. decembra 2012 sp. zn. 2 Sžo 12/2012. Preskúmal zákonnosť rozhodnutia žalovaného Úradu na ochranu osobných údajov Slovenskej republiky, potvrdzujúceho opatrenie Úradu na ochranu osobných údajov, ktorým bolo jednému zo slovenských vydavateľstiev ako prevádzkovateľovi (žalobcovi) uložené bezodkladne odstrániť a zlikvidovať osobné údaje týkajúce sa zdravia fyzickej osoby. Podľa názoru žalovaného správneho orgánu totiž predmetné zdravotné údaje boli spracúvané v informačných systémoch prevádzkovateľa bez súhlasu

²⁵⁰ BARANCOVÁ, H. *Zákonník práce. Komentár*. 1. vyd. Praha: C. H. Beck, 2010, s. 201.

²⁵¹ Upozorňujeme pritom, že osobné údaje o psychickej identite fyzickej osoby (správanie, zvyky, zlozvyky, zručnosti) alebo o jej psychickej pracovnej spôsobilosti (schopnosť zastávať určité pracovné miesto) sa nezaraďujú do skupiny zdravotných údajov. Pozri VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 120.

dotknutej osoby. Krajský súd rozhodujúci o žalobe o preskúmanie zákonnosti rozhodnutia uvedeného správneho orgánu v prvom stupni rozhodol výrokom, ktorým zrušil rozhodnutie žalovaného. Poukázal pritom na skutočnosť, že žalovaný sa v odôvodnení svojho rozhodnutia vôbec nevyrovnal s dôvodnosťou tvrdení a námietok žalobcu o skutočnosti, že osobné údaje o zdravotnom stave dotknutej fyzickej osoby, ktoré žalobca spracoval a zverejnil, boli už predtým preukázateľne zverejnené vo viacerých slovenských printových a elektronických médiách (k zverejneniu mala prispieť aj sama dotknutá osoba), preto mu bola povinnosť uložená v rozpore so zákonom o ochrane osobných údajov. Najvyšší súd Slovenskej republiky sa stotožnil so skutkovým a právnym posúdením veci súdom prvého stupňa, námietky žalobcu považoval za dôvodné a po preskúmaní predmetnej veci rozhodnutie krajského súdu potvrdil.

Údaje o zdravotnom či psychickom stave fyzickej osoby sa zaraďujú k osobným údajom, ktoré podliehajú ochrane v pracovnom práve a zamestnávateľ k nim získa prístup spravidla vtedy, keď mu ich poskytne sám zamestnanec (napr. údaje o tehotenstve, pracovnom úraze, chorobe z povolania). Na otázky súvisiace nepriamo so zdravotným stavom zamestnanca kvôli zisteniu informácií o závislostiach od alkoholu alebo omamných látok, súčasná právna úprava nereflektuje, preto ich považujeme za prípustné.

Rešpektovanie dôvernosti zdravotných údajov je dôležitým princípom v právnych systémoch všetkých zmluvných štátov Dohovoru o ochrane ľudských práv a základných slobôd, jednak z hľadiska nevyhnutnosti rešpektovania pocitu súkromia pacienta a jednak kvôli zachovaniu pacientovej dôvery v lekársku profesiu a zdravotnícke služby vôbec. Ak by štát negarantoval dohodnutý štandard ochrany, mohla by sa zvýšiť nedôvera a obavy z odhaľovania informácií o osobnom a intímnom živote u ľudí, ktorí potrebujú lekársku starostlivosť, čo by mohlo vyvolať strach vyhľadať lekársku pomoc.²⁵² Z uvedeného vyplýva, že zamestnávateľ nemôže spracúvať akékoľvek zdravotné údaje zamestnancov. Spravidla je oprávnený bez významných obmedzení spracúvať len údaje, obsahujúce všeobecné konštatovanie o zdravotnej spôsobilosti uchádzača o zamestnanie, resp. zamestnanca. Súvisí to aj s ochranou a obmedzením sprostredkovania tejto osobitnej kategórie osobných údajov zamestnanca jeho zamestnávateľovi ošetrovateľom, ktorý je v zmysle zákona výlučne oprávnený na spracúvanie konkrétnych osobných údajov odhaľujúcich zdravotný stav zamestnanca.

Ak je výkon určitého zamestnania podmienený zdravotnou spôsobilosťou, tak ju musí fyzická osoba, ktorá sa uchádza o pracovnú pozíciu, preukázať spôso-

²⁵² Rozsudok ESEP zo 14. novembra 2002 v právnej veci *Mouisel v. Francúzsko*, sťažnosť č. 67263/01, Pozri ŠTEFKO, M. Ochrana súkromí zamestnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In: *Jurisprudence*, 2012, č. 7/8, s. 20.

bom predpísaným zákonom. Spôsob, akým sa preukazuje zdravotná spôsobilosť, ustanovuje napr. zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti v znení neskorších predpisov. Podľa ustanovenia § 16 citovaného zákona zamestnanec preukazuje zdravotnú spôsobilosť na výkon práce predložením **lekárskeho posudku**, ktorý vydáva poskytovateľ zdravotnej starostlivosti, s ktorým má zamestnanec uzatvorenú dohodu o poskytovaní zdravotnej starostlivosti. Týka sa to tých zamestnaní a povolání, pri ktorých z konkrétnej právnej úpravy vyplýva ako podmienka na ich výkon preukázanie zdravotnej spôsobilosti lekárskeho posudkom.²⁵³

Ďalším spôsobom preukazovania zdravotnej spôsobilosti je predloženie **posudku o zdravotnej spôsobilosti** podľa ustanovenia § 12 zákona č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia v znení neskorších predpisov. Vydáva ho lekár pracovnej zdravotnej služby alebo lekár, s ktorým má zamestnanec uzatvorenú dohodu o poskytovaní zdravotnej starostlivosti. V tomto prípade sú povinní na základe tohto posudku preukázať zdravotnú spôsobilosť zamestnanci vykonávajúci rizikové práce (3. a 4. kategórie) a zamestnanci, ktorým splnenie tejto požiadavky predpisuje príslušná právna úprava, ale neustanovuje presne spôsob, akým to majú urobiť (napr. zamestnanci železničných dráh).²⁵⁴ V posudku je tiež len všeobecný záver, či je osoba zdravotne úplne alebo čiastočne spôsobilá na výkon pracovnej pozície.²⁵⁵

Častým spôsobom preukázania zdravotnej spôsobilosti na výkon práce je čestné vyhlásenie, ktoré tvorí spravidla prílohu žiadosti o prijatie do zamestnania. Ak ho uchádzač o zamestnanie poskytne, možno ho považovať za súhlas s použitím jeho osobných údajov. Využíva sa napr. pri preukazovaní zdravotnej spôsobilosti pri prijímaní zamestnancov do štátnej služby.²⁵⁶

Údaje o bezúhonnosti

Za listinu, ktorá preukazuje bezúhonnosť, právny poriadok Slovenskej republiky považuje výpis z registra trestov a pre niektoré osobitné pracovné kategórie

²⁵³ Napr. zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v § 14 ods. 6 písm. o/ ustanovuje, že služobný úrad spracúva aj osobné údaje o zdravotnej klasifikácii u uchádzača, ktorá vyplýva z lekárskeho posudku o zdravotnej spôsobilosti.

²⁵⁴ § 13 ods. 1 vyhlášky Ministerstva dopravy, pôšt a telekomunikácií Slovenskej republiky č. 245/2010 Z. z. o odbornej spôsobilosti, zdravotnej spôsobilosti a psychickej spôsobilosti osôb pri prevádzkovaní dráhy a dopravy na dráhe.

²⁵⁵ KOVALČÍKOVÁ, M. *Realizácia osobnostných práv pri výkone závislej práce*: dizertačná práca. Košice: Právnická fakulta Univerzity P. J. Šafárika v Košiciach, 2012, s. 141.

²⁵⁶ § 19 ods. 2 písm. a/ zákona č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

aj odpis z registra trestov. Vo väčšine prípadov je osobitnou požiadavkou na výpis určité časové obmedzenie jeho platnosti a použiteľnosti, teda aj jeho relevancia preukázania bezúhonnosti. Väčšinou tento výpis, resp. odpis nesmie byť starší ako tri mesiace.

Zamestnávateľ nemôže v zmysle § 41 ods. 6 písm. c/ Zákonníka práce žiadať od uchádzača o zamestnanie preukázanie jeho bezúhonnosti, iba ak tieto osobné údaje na výkon práce vyžaduje osobitný predpis, alebo ak si to vyžaduje povaha vykonávanej práce. V praxi sa môžeme často stretnúť s tým, že sa preukázanie bezúhonnosti vyžaduje pri prácach, kde sa manipuluje s finančnými prostriedkami, alebo napr. pri výkone práce advokáta²⁵⁷ či pedagogického zamestnanca.²⁵⁸

Pri druhej výnimke Zákonník práce bližšie nešpecifikuje kritériá, podľa ktorých by sme mohli objektívne posúdiť, či je na výkon práce nevyhnutná bezúhonnosť, resp. či si jej preukázanie vyžaduje „povaha vykonávanej práce“. Všeobecný právny pojem „povaha práce“ je široko interpretovateľný a dáva zamestnávateľovi možnosť a určitú voľnosť pri stanovovaní, ktorá práca je podľa jeho uváženia tou, na výkon ktorej musí byť splnená požiadavka bezúhonnosti. Podmienka by mala byť preto považovaná za splnenú, ak požadovaný osobný údaj vecne súvisí s prácou, ktorú má uchádzač pre zamestnávateľa vykonávať, a tiež je nevyhnutná pre rozhodnutie zamestnávateľa zamestnať uchádzača. Preto sa odporúča, aby si bezúhonnosť ako predpoklad na vykonávanie konkrétnej práce vymienil sám zamestnávateľ v pracovnom poriadku a svoje požiadavky primerane odôvodnil.

Na základe tejto analýzy sme dospeli k záveru, že právny poriadok zamestnávateľa neobmedzuje vo výraznej miere, keďže v drvivej väčšine zamestnaní môže požadovať od budúcich zamestnancov preukázanie ich bezúhonnosti. Je nepochybné, že tento údaj, ktorý môže zamestnávateľ požadovať takmer od každého uchádzača o zamestnanie, je vážnym (aj keď legálnym) zásahom do jeho súkromia, keďže informuje o jeho minulosti, ktorá môže ovplyvniť rozhodovanie zamestnávateľa a v konečnom dôsledku jeho neprijatie do pracovného pomeru.

Odlíšná situácia však nastáva, ak sa zamestnávateľ pred alebo v priebehu trvania pracovného pomeru rozhodne spracúvať osobné údaje zamestnanca preukazujúce, že porušil ustanovenia zakladajúce jeho trestnoprávnu a administratívno-právnu zodpovednosť. Spracúvanie tejto osobitnej kategórie osobných údajov v zmysle § 13 ods. 4 ZOOÚ je prípustné len za splnenia zákonom stanovených

²⁵⁷ Pozri § 3 ods. 1 písm. f/ a ods. 3 zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov. Zákon v tomto prípade vyžaduje odpis z registra trestov.

²⁵⁸ Pozri § 6 ods. 1 písm. b/ zákona č. 317/2009 Z. z. o pedagogických zamestnancoch a odborných zamestnancoch a o zmene a doplnení niektorých zákonov.

podmienok (napr. ak zamestnávateľa naň oprávňuje osobitný zákon a získal výslovný alebo inak hodnoverne preukázateľný súhlas dotknutej osoby).²⁵⁹

Pod pojmom „preukazujúce trestnú alebo administratívnoprávnu zodpovednosť“ chápeme „právoplatné odsúdenie“ za trestný alebo správny delikt. Ak z informácií získaných z registra trestov vyplýva, že zamestnanec bol právoplatne odsúdený za úmyselný trestný čin, zamestnávateľ s ním môže okamžite skončiť pracovný pomer ale iba v subjektívnej lehote dvoch mesiacov odo dňa, keď sa o dôvode na okamžité skončenie dozvedel, a v objektívnej lehote jedného roka odo dňa, keď tento dôvod vznikol (§ 68 ods. 1 a 2 Zákonníka práce). Taktiež môže využiť výpovedný dôvod v zmysle § 63 ods. 1 písm. d/ Zákonníka práce, ak prestal spĺňať predpoklady ustanovené právnymi predpismi na výkon dohodnutej práce.

Údaje o výške mzdy, zaradení v platovej triede a o predchádzajúcej odbornej praxi

Údaje, napr. o výške mzdy, zaradení v platovej triede a o predchádzajúcej odbornej praxi, sú tiež informáciami, ktoré za istých okolností možno zaradiť medzi osobné údaje odhaľujúce ekonomickú identitu fyzickej osoby v zmysle § 4 ods. 1 ZOOÚ. Ústavný súd Slovenskej republiky v náleze z 19. januára 2011 sp. zn. PL. ÚS 1/09 vyjadril názor, že „údaj o výške príjmov sa významným spôsobom premieta do súkromnej sféry jednotlivca, vypovedá o jeho sociálnom postavení a jeho zverejnenie môže mať významné (a to aj negatívne) dôsledky na jeho osobné, pracovné či iné spoločenské vzťahy“. Preto by sa v praxi podľa nášho názoru nemalo stávať, že zamestnávateľ uvedie do potvrdenia o zamestnaní aj údaj o mzde alebo plate zamestnanca.

Sporom o porušenie povinností prevádzkovateľa v súvislosti so spracúvaním, konkrétne sprístupnením tejto kategórie osobných údajov sa zaoberal v rámci rozhodovacej činnosti aj Najvyšší súd Slovenskej republiky, ktorý v rozhodnutí z 30. júna 2011 sp. zn. 5 Sži 2/2010 konštatoval, že údaje súvisiace s dĺž-

²⁵⁹ Naša právna úprava je v porovnaní s českou úpravou v rovnakej veci odlišná v tom, že český zákon č. 101/2000 Sb. o ochrane osobných údajů a o zmene některých zákonů rozlišuje medzi výpisom obsahujúcim záznam o právoplatnom odsúdení za spáchaný trestný čin a tým, ktorý takýto záznam neobsahuje. Pričom len výpis so záznamom považuje za „citlivý osobný údaj“. Aj česká odborná verejnosť sa prikláňa k názoru, že doklad o bezúhonnosti konkrétneho zamestnanca, resp. výpis z registra trestov bez záznamu o trestnej činnosti nemožno považovať za osobný údaj patriaci do osobitnej kategórie „citlivých údajov“. Pozri JAKUBKA, J. Ochrana osobných a osobnostných práv zamestnanců, 2. část. In: *Práce a mzda*, ISSN 0032-6208. 2005, roč. 53, č. 13, s. 24, alebo MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 293, alebo KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha: Bova Polygon, 2010, s. 72.

kou predchádzajúcej praxe dovolateľky (žalobkyne) ako štátnej zamestnankyne a s okolnosťami jej vyslania do zahraničia nemožno považovať za jej osobné údaje, pretože postup prevádzkovateľa (Ministerstva vnútra Slovenskej republiky), ktorý sprístupnil tento údaj na žiadosť novinárovi a ten ho zverejnil v tlačovom médiu, nepresiahol rámec poskytnutia údajov o činnosti štátneho orgánu na základe zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Nestotožnil sa pritom ani s názorom žalobkyne, že by žalovaný v rozpore s dikciou zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov sprístupnil zo svojho informačného systému osobný údaj o platovej triede priznanej žalobkyňi, a že by týmto postupom porušil svoju povinnosť mlčanlivosti podľa § 18 alebo ustanovenie § 7 citovaného zákona o ochrane osobných údajov. Dovolací súd dospel k záveru, že údaj o zaradení do platovej triedy nie je osobným údajom, lebo je viazaný na samotnú funkciu bez ohľadu na to, kto túto funkciu momentálne zastáva. Pretože nejde o osobný údaj, považoval v danej veci tiež za irelevantné, či bol tento údaj vopred zverejnený alebo naopak.

4.7.1.1 Získavanie osobných údajov v predzmluvných vzťahoch prostredníctvom sociálnych sietí

Niektorí zamestnávateľia si overujú pravdivosť údajov poskytnutých uchádzačom alebo zamestnancom tak, že o ňom získavajú ďalšie informácie zo sociálnych sietí na internete. Od počiatku 90. rokov 20. storočia, ktoré boli prvopočiatkami internetu a začiatkom 21. storočia, konkrétne od roku 2004, keď bola po prvýkrát spustená web stránka celosvetovej sociálnej siete Facebook,²⁶⁰ došlo k výrazným zmenám v spôsoboch a postupoch, akým zamestnávateľia získavajú informácie o budúcom zamestnancovi. Sociálne siete ako Facebook, Twitter alebo LinkedIn sa stali často využívanými nástrojmi personalistov a headhunterov pri obsadzovaní vhodných uchádzačov o zamestnanie na voľné pracovné pozície.²⁶¹ Začali byť dôležitým zdrojom cenných informácií, na základe ktorých si zamestnávateľia vytvárajú predstavu o osobnom profile a overujú si informácie o perspektívnych

²⁶⁰ Facebook vytvoril v roku 2004 študent Harvardskej univerzity v USA Mark Zuckerberg ako nástroj, ktorý slúžil najskôr na komunikáciu študentov v rámci tejto univerzity, ktorá sa v priebehu nasledujúcich rokov rozrástla na verejne prístupnú celosvetovú sociálnu sieť. Je najpopulárnejšou sociálnou sieťou aj na Slovensku. V súčasnosti má už viac ako 1 miliardu používateľov. Pozri: TVARDZIK, J. Facebook prekonal miliardu užívateľov. In: TECHSme.sk. (online). 2012. (cit. 2014-11-27). Dostupné z: (<http://tech.sme.sk/c/6556489/facebook-prekonal-miliardu-uzivatelov.html>).

²⁶¹ OLEXOVÁ, C. Využitie internetových sociálnych sietí na získavanie a výber zamestnancov. In: *Personálny a mzdový poradca podnikateľa*. ISSN 1335-1508, 2010, č. 15, s. 123.

zamestnancoch ešte pred pracovným pohovorom. Často to robia pod zámienkou zistiť informácie, ktoré nenájdu v tradičných životopisoch ani žiadostiach o zamestnanie. Tieto hodnotiace postupy využívajúce sociálne siete (ďalej nazývané v tejto kapitole ako „skrining osobného profilu“),²⁶² ktoré kvôli bezplatnosti a ľahkej dostupnosti zamestnávateľa využívajú v praxi čím ďalej tým častejšie, platná slovenská právna úprava nepozná.²⁶³ Ide prakticky o nový prostriedok, nový pojem v predzmluvných vzťahoch neregulovaný právnymi normami. To však neznamená, že by mal byť a priori zakázaný. Práve naopak, ak konanie zamestnávateľa neodporuje právnej úprave, je v zásade dovolené. Nesmieme však zabúdať, že vo vzťahu k takýmto praktikám zamestnávateľov je v oveľa väčšej miere potrebné zohľadniť právne a etické hranice ochrany súkromia potenciálnych budúcich zamestnancov.

Je rozdiel v tom, či zamestnávateľ takto získa informácie o žiadateľovi, ktoré sú chránené osobnými nastaveniami súkromia a majú zostať viditeľné len pre samotného žiadateľa alebo úzku skupinu jeho „priateľov“, alebo je jeho profil viditeľný a prístupný pre širší okruh osôb. Ak má žiadateľ nastavenú ochranu súkromia tak, že jeho profil je prístupný „verejne“, predstavuje to obrovské množstvo (dovoliť si tvrdiť, že stovky miliónov) používateľov tejto sociálnej siete, ktorí si môžu profil konkrétnej osoby prehliadať a získať tak neobmedzený prístup k všetkým údajom zverejneným dobrovoľne a vedome samotným používateľom, ale dokonca aj k údajom, ktoré zverejnila o danej osobe tretia osoba bez jeho vedomia a súhlasu. Tieto informácie sú viditeľné nielen pre registrovaných užívateľov sociálnej siete Facebook, ale aj pre akéhokoľvek používateľa internetového prehliadača Google cez verejne dostupnú internetovú sieť, ak nie je ochrana súkromia osobitne nastavená tak, aby k neželaným únikom informácií o osobnosti zo sociálnej siete nedochádzalo.

Aké druhy cenných informácií môže zamestnávateľ získať z osobného profilu uchádzača na sociálnej sieti? Môže ísť o informácie odhaľujúce jeho etnickú alebo rasovú príslušnosť, pohlavie, sexuálnu orientáciu, údaje o rodinnom stave, či tehotenstve, alebo politickej a náboženskej príslušnosti, čo môže porušovať zásady zákazu diskriminácie a zásady rovnakého zaobchádzania, ak ide o prístup k zamestnaniu v zmysle § 41 ods. 8 Zákonníka práce či informácie, ktoré zamestnávateľ z tohto dôvodu nesmie výslovne vyžadovať od fyzickej osoby v procese prijímania do zamestnania podľa § 41 ods. 6 Zákonníka práce.

²⁶² Pojem pochádza z angl. „preemployment background screening“.

²⁶³ Odlišná situácia je v Nemecku a vo Francúzsku, kde sa využívaniu skriningu osobných profilov na sociálnych sieťach venuje pozornosť v odborných kruhoch a vytvárajú sa základy právnej úpravy. Pozri WISSKIRCHEN, G. Background Checks in Europe. In *Labour and Employment*. (online). 2011. (cit. 2014-01-03). Dostupné z (<http://whoswholegal.com/news/features/article/29116/background-checks-europe>).

Zásada rovnakého zaobchádzania môže byť narušená už tým, že sa získajú osobné informácie len o niektorých uchádzačoch o zamestnanie, ktorí sú používateľmi sociálnej siete Facebook, ale nie o všetkých, čo môže spôsobovať nerovnocenné posudzovanie jednotlivých uchádzačov. Potenciálne nebezpečenstvo spočíva aj v riziku dezinterpretácie získaných informácií s nesprávnym a nespravodlivým úsudkom. Prostredníctvom Facebooku sú zamestnávateľia schopní zhromažďovať významné množstvo osobných údajov o budúcich zamestnancoch, ktoré by nemuseli vôbec korešpondovať s reálnymi údajmi získanými v priebehu pohovoru (napr. zamestnanec môže nepravdivo uvádzať informácie o svojej kvalifikácii alebo predchádzajúcich zamestnaniach).

V závislosti od toho, aké informácie zamestnávateľia získavajú a akým spôsobom, môžu konať nelegálne, neeticky, zasahujúc pritom do práva na súkromie svojich zamestnancov. Jedným z etických hľadísk, ktoré treba vziať do úvahy je, že ak sa potenciálny budúci zamestnanec uchádza o zamestnanie u zamestnávateľa, predpokladá sa, že je aj v jeho záujme, aby bol pracovnoprávny vzťah založený na hodnotách otvorenosti, čestnosti a transparentnosti. V prípade, že žiadateľ zistí, že jeho osobný profil na Facebooku bol kedykoľvek podrobený skríningu (inej previerke), takéto konanie zamestnávateľa môže považovať za nedôveryhodné, netransparentné a zasahujúce jeho súkromie.

V závere tejto podkapitoly spomenieme výsledky zahraničného výskumu problematiky skríningu osobného profilu na pracovisku. Štúdia pochádzajúca zo Spojených štátov amerických (ďalej len „USA“) z roku 2010 bola realizovaná so zameraním na výskum, do akej miery zamestnávateľia využívajú Facebook na skríning osobného profilu žiadateľov o zamestnanie a či dochádza pri jeho využívaní k dodržaniu právnych a etických aspektov ochrany súkromia zamestnancov, priniesla výsledky, ktoré sú podľa nášho názoru veľmi aktuálne a majú spoľahlivú výpovednú hodnotu aj v európskom právnom, kultúrnom a sociálnom prostredí.²⁶⁴ Z právneho hľadiska je tiež dôležité uviesť, že ani v USA neexistuje relevantná právna úprava, ktorá by regulovala predmetnú problematiku.

Z výsledkov výskumu na vzorke 718 zamestnávateľov, ktorí sa zúčastnili na tomto výskume uskutočnenom na prelome rokov 2009 a 2010 v USA vyplýva, že:²⁶⁵

²⁶⁴ LORY, B., *Employer Use of Facebook as a Tool in Pre-Employment Screening of Applicants: Benefits and Ethical, Legal, and Privacy Implications*: Master of Arts in Organizational Leadership Theses. St. Paul (Minnesota, USA): St. Catherine University, 2011. s. 63.

²⁶⁵ LORY, B., *Employer Use of Facebook as a Tool in Pre-Employment Screening of Applicants: Benefits and Ethical, Legal, and Privacy Implications*: Master of Arts in Organizational Leadership Theses. St. Paul (Minnesota, USA): St. Catherine University, 2011, s. 62 – 65.

- väčšina (až 61 %) zamestnávateľov nikdy nevyužila skríning osobného profilu ako prostriedok na získanie údajov o uchádzačovi o zamestnanie a zvyšných 39 % ho využila.²⁶⁶ Približne polovica si myslí, že takéto praktiky prinášajú výhody avšak až 70 % vyjadrilo názor, že Facebook by sa nemal na taký skríning využívať,
- len 2,5 % respondentov považovalo informácie na Facebooku za úplne korektné (pravdivé),
- 50 % si nebolo úplne istých, či skríningom môžu získať aj osobné informácie (resp. údaje), ktoré sú chránené zákonom, pričom až 38 % bolo presvedčených, že môžu a 11 %, že nemôžu,
- tí, ktorí využívajú skríning ako hlavné dôvody a výhody, uviedli: získanie prehľadu o charaktere preverovaného jednotlivca (39 %), zistenie, či uchádzač bude dobre reprezentovať zamestnávateľa (jeho firmu či organizáciu) (52%), získanie extra informácií, ktoré nemusia byť uvedené v životopise uchádzača (40 %),
- zo zamestnávateľov, ktorí priznali využívanie skríningu, drvivá väčšina (takmer 92 %) uviedla, že na získanie osobných informácií došlo bez toho, aby predtým požiadali potenciálneho budúceho zamestnanca o prístup k ich profilu a 89 % ich nikdy nepožiadalo o prístup k profilu, ak sa im tento prístup automaticky neumožnil,
- 77 % napriek tomu uviedlo, že sa nerozhodovalo výlučne na základe informácií získaných skríningom profilu na Facebooku, ktoré v konečnom dôsledku smerovalo k neprijatiu na obsadzovanú pracovnú pozíciu,
- medzi tými, ktorí využívajú skríning, väčšina (takmer 64 %) vopred neinformovala žiadateľov, že bol alebo bude vykonaný skríning, ani si nevyžiadala ich písomný súhlas na tento účel,
- zamestnávatelia, ktorí uviedli, že nikdy nevyužili Facebook na skríning profilu uchádzača, medzi hlavné dôvody uviedli: nemali v záujme získať informácie o uchádzačovi, ktoré nesúvisia s ponúkanou prácou (65 %), nechceli podliehať predsudkom v rozhodovaní (59 %) a nemali záujem získať osobné a súkromné informácie o uchádzačovi (61,5 %).

Z realizovaného výskumu je zrejmé, že zamestnávatelia, ktorí sa rozhodli používať Facebook ako nástroj na získanie informácií z osobného profilu žiadateľa o zamestnanie, svoje „previerky“ odôvodnili jednoduchým, rýchlym a legálnym prístupom k osobným údajom o žiadateľovi cez verejnú doménu (public domain). Označili ho za efektívny spôsob, ako sa vyhnúť neuváženým a finančne nákladným nesprávnym rozhodnutiam v procese získavania stálych a spoľahlivých zamestnancov a uviedli, že získané informácie môžu poskytnúť pravdivý obraz

²⁶⁶ Možno predpokladať, že s rapidným rozširovaním Facebooku v posledných rokoch bude toto číslo v súčasnosti oveľa vyššie.

o charaktere, morálke, hodnotách, zvykoch, aktivitách a záujmoch preverovaného jednotlivca.²⁶⁷

Na základe výsledkov uvedeného výskumu (štúdie) autori sformulovali nasledujúce závery a odporúčania. Facebook umožňuje viacero nastavení ochrany súkromia, v rámci ktorých si môže používateľ vybrať, aké údaje a pre koho budú viditeľné, resp. prístupné. Za aktívne vykonanie krokov potrebných na nastavenie požadovanej úrovne ochrany súkromia sú zodpovední samotní používatelia osobných profilov a nemali by tieto ochranné mechanizmy podceňovať. Ak tieto nastavenia nie sú aktívne, neexistujú žiadne iné preventívne mechanizmy, ktoré by bránili zamestnávateľovi v získaní prístupu k verejne dostupnému obsahu profilu potenciálneho zamestnanca. Používatelia by preto mali zvážiť, že ak nechcú, aby niektoré informácie o ich súkromí boli zverejnené a šírené do iných prostredí, je najlepšie vôbec ich nezverejňovať na internete (online). Odhliadnuc od tohto názoru z výsledkov výskumu vyplýva, že aj zamestnávatelia by mali niest' istú zodpovednosť, ak na základe týchto skríningových praktík dochádza k diskriminácii, alebo ak ich prostredníctvom získali informácie nelegálne, t. j. porušením právnych predpisov na ochranu súkromia a osobných údajov zamestnancov.²⁶⁸

4.7.2 Osobné údaje zamestnanca počas trvania pracovného pomeru

Zamestnávatelia sú povinní viesť počas trvania pracovného pomeru rôzne evidencie o svojich zamestnancoch a spracúvať osobné údaje zamestnancov najmä v oblasti sociálneho zabezpečenia. Vedú evidenciu osobných údajov v osobnom spise zamestnanca, v evidencii dochádzky a vyúčtovanej mzdy, v evidencii skutočností oznamovaných zdravotnej poisťovni a na účely sociálneho poistenia a starobného dôchodkového sporenia alebo v mzdových listoch na účely dane z príjmu fyzických osôb zo závislej činnosti. Najčastejšie spracúvané osobné údaje zamestnávateľmi v Slovenskej republike uvádzame v prehľadnej Tabuľke č. 2 Prehľad evidenčných činností zamestnávateľov spracúvajúcich osobné údaje, uvedenej v prílohách tejto práce.²⁶⁹

²⁶⁷ LORY, B., *Employer Use of Facebook as a Tool in Pre-Employment Screening of Applicants: Benefits and Ethical, Legal, and Privacy Implications*: Master of Arts in Organizational Leadership Theses. St. Paul (Minnesota, USA): St. Catherine University, 2011, s. 9 – 10.

²⁶⁸ LORY, B., *Employer Use of Facebook as a Tool in Pre-Employment Screening of Applicants: Benefits and Ethical, Legal, and Privacy Implications*: Master of Arts in Organizational Leadership Theses. St. Paul (Minnesota, USA): St. Catherine University, 2011, s. 119.

²⁶⁹ Pre porovnanie so situáciou v Českej republike pozri MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2. aktual. a dopl. vyd. Praha: ASPI, Wolters Kluwer, 2008, s. 179.

4.7.2.1 Osobný spis zamestnanca

Z ustanovenia § 75 ods. 1 Zákonníka práce nepriamo vyplýva, že zamestnávateľ musí viesť osobný spis zamestnanca, ale priamo mu túto povinnosť neukladá. Tá môže byť stanovená osobitným predpisom. Odporúča sa oprávnenie zamestnanca konkretizovať v pracovnom poriadku.²⁷⁰

Za osobný spis považujú Matoušová a Hejlík „súbor dokumentov, ktoré sú spojené reálne alebo pomyselne jedným obalom so súpisným číslom, ktoré tvorí meno a priezvisko alebo ad hoc identifikačné číslo zamestnanca“.²⁷¹ Ktoré dokumenty by mali byť súčasťou osobného spisu síce nestanovuje žiaden právny predpis, ale z jeho praktickej povahy možno vyvodiť, že v ňom má byť obsiahnutá akákoľvek dokumentácia nevyhnutná na výkon práv a povinností konkrétneho zamestnanca v pracovnoprávnom vzťahu.

V rámci dokumentov súvisiacich s prijatím do pracovného pomeru je v osobnom spise zvyčajne: osobný dotazník,²⁷² životopis, kópie dokladov o dosiahnutom vzdelaní, kvalifikácii a praxi, výpis z registra trestov, potvrdenie o zamestnaní (od bývalého zamestnávateľa), doklad o vstupnej lekárskej prehliadke, údaje o zdravotnom poistení, ale aj pracovná zmluva, mzdový, resp. platový výmer, mzdové listy, opis pracovnej činnosti zamestnanca. Z dokumentov, ktoré vznikajú v priebehu pracovného pomeru, sú v osobnom spise spravidla dodatky k pracovnej zmluve, evidencia pracovného času (dochádzky), doklady o prehlbovaní a zvyšovaní kvalifikácie (§ 140 Zákonníka práce), dohody o neplatenom voľne, hodnotenia, doklady o absolvovaní povinných školení a lekárskech prehliadok. Pri skončení pracovného pomeru sa stávajú súčasťou osobného spisu aj dokumenty, na základe ktorých sa pracovný pomer skončil (výpoveď, dohoda o skončení pracovného pomeru), potvrdenie o zamestnaní, pracovný posudok a evidenčný list dôchodkového zabezpečenia.²⁷³

Ak má zamestnávateľ väčší počet zamestnancov, niektoré dokumenty, ktoré sa týkajú konkrétneho zamestnanca, nemusia byť súčasťou jedného osobného spisu, ale môže ich viesť hromadne pre viacerých zamestnancov podľa predmetu spracú-

²⁷⁰ BARANCOVÁ, H. *Zákonník práce. Komentár*. 1. vyd. Praha: C. H. Beck, 2010, s. 339.

²⁷¹ MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2. aktual. a dopl. vyd. Praha: ASPI, Wolters Kluwer, 2008, s. 117.

²⁷² Na získanie identifikačných a základných osobných údajov zamestnancov zamestnávateľa využijú aj osobné dotazníky, v ktorých sa uvádzajú napr. aj údaje o bezúhonnosti, vykonávaní podnikateľskej alebo inej zárobkovej činnosti, informácie o osobitných oprávneniach a spôsobilostiach (vodičský preukaz). V prípade uchádzačov o zamestnanie je vhodné uviesť, že údaje v osobnom dotazníku sú poskytnuté zamestnávateľovi len na účely konkrétneho výberového konania.

²⁷³ CHLÁDKOVÁ, A. Osobní spis zaměstnanca. In: *Personální a sociálně právní kartotéka*. 2008, roč. 11, č. 6, s. 4 – 7.

vania ich osobných údajov (napr. dokumenty, týkajúce sa bezpečnosti a ochrany zdravia pri práci). Zamestnanec má právo kedykoľvek nahliadať do osobného spisu a robiť si z neho odpisy a kópie na vlastné náklady. Okrem zamestnanca môžu ešte nahliadať do osobného spisu spravidla aj vedúci zamestnanci, jeho priami nadriadení a štátne orgány, ak ich na to splnomocňuje zákon. Zákonník práce neustanovuje dĺžku archivácie osobného spisu, avšak môžu ho stanovovať osobitné právne predpisy.²⁷⁴ Na likvidáciu osobného spisu sa vzťahujú ustanovenia ZOOÚ o likvidácii osobných údajov.

4.7.2.2 Vybrané kategórie osobných údajov spracúvaných počas trvania pracovného pomeru

Zamestnávateľ je oprávnený spracúvať **rodné číslo**, resp. všeobecne použiteľný identifikátor, len v prípadoch, ak je to nevyhnutné na dosiahnutie účelu daného spracúvania. Z rodného čísla možno určiť pohlavie osoby a predovšetkým z čísla uvedeného za lomkou možno identifikovať konkrétnu osobu v informačných systémoch. Práve preto je rodné číslo, tzv. „citlivým údajom“,²⁷⁵ patriacim do osobitnej kategórie osobných údajov a pri ich spracúvaní sa na prevádzkovateľov kladú vyššie nároky na zaistenie bezpečnosti.²⁷⁶ Komentár k § 13 ZOOÚ dopĺňa, že jeho spracúvanie je odôvodnené, ak by bez jeho použitia existovalo ohrozenie alebo porušenie práv dotknutých osôb v dôsledku ich zámery alebo by mohlo dôjsť k značným problémom pri spracúvaní osobných údajov. Spracúvanie rodných čísel zamestnancov je teda odôvodnené v rámci výkonu mzdovej a personálnej agendy. Pre spracúvanie rodných čísel platí tiež zákaz ich zverejňovania nepripúšťajúci žiadnu výnimku.²⁷⁷

Údaje o trvalom a prechodnom bydlisku majú pre zamestnávateľa význam pri doručovaní písomností súvisiacich s pracovnoprávnym vzťahom (§ 38 Zákonníka práce) a tiež pri určovaní jeho práv a povinností, pokiaľ ide o priznanie cestovných náhrad alebo možnosti vysielania na pracovné cesty.

Údaje o štátnej príslušnosti majú pre zamestnávateľa význam vo vzťahu k jeho povinnosti sledovať, či nenastal zákonný dôvod skončenia pracovného pomeru

²⁷⁴ Napr. zákon č. 595/2003 Z. z. o dani z príjmov ustanovuje v § 39 ods. 8 uchovávanie vybraných dokumentov po dobu ustanovenú zákonom č. 431/2002 Z. z. o účtovníctve, zákon č. 580/2004 Z. z. o zdravotnom poistení ustanovuje v § 24 písm. d/ a e/ desaťročnú lehotu na uchovávanie dokladov potrebných na správne určenie vymeriavacieho základu, výšky poistného a jeho platenia a evidenciu o zamestnancoch.

²⁷⁵ K pojmu „citlivý údaj“ pozri kapitolu 4.2 Osobitné kategórie osobných údajov.

²⁷⁶ Pozri rozhodnutie Najvyššieho súdu Slovenskej republiky z 12. júla 2011 sp. zn. 1 Sžo 410/2009.

²⁷⁷ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 120.

s cudzincom alebo osobou bez štátnej príslušnosti uvedený v § 59 ods. 3 Zákonníka práce (napr. právoplatnosťou rozsudku, ukladajúcemu zamestnancovi trest vyhostenia z územia Slovenskej republiky).

Bežným osobným údajom, ktorý zamestnávateľa vyžadujú pri nástupe do zamestnania je predloženie **fotografie** pre vyhotovenie preukazu (identifikačnej karty) zamestnanca. Aj na osobné údaje zachytené na tejto obrazovej snímke sa vzťahujú ustanovenia ZOOÚ a Občianskeho zákonníka. Aby takéto údaje mohol spracúvať zamestnávateľ bez súhlasu dotknutej osoby, musí byť splnená niektorá z podmienok uvedených v § 10 ZOOÚ. Konkrétne výnimka zakotvená v § 10 ods. 2 ZOOÚ sa uplatňuje v rámci vyhotovovania služobných preukazov, pretože je priamo osobitným zákonom ustanovená povinnosť vyhotoviť služobný preukaz s fotografiou fyzickej osoby. To znamená, že v tomto prípade sa nevyžaduje súhlas zamestnanca so spracúvaním osobných údajov. Akýkoľvek ďalší spôsob použitia fotografie (napr. jej zverejnenie na internetovej stránke zamestnávateľa) je už podmienený udelením súhlasu zamestnanca a tiež splnením oznamovacej povinnosti Úradu na ochranu osobných údajov Slovenskej republiky (ďalej aj „Úrad“).²⁷⁸ Osobné údaje, ktoré fotografia zachytáva, sa môžu považovať za „citlivé“, resp. údaje osobitnej kategórie, ak odhaľujú rasový alebo etnický pôvod zamestnanca. Vtedy na ich spracúvanie bude potrebný výslovný súhlas dotknutej osoby alebo splnenie predpokladov pre inú zákonnú výnimku uvedenú v § 14 ZOOÚ. V prípade, ak účelom spracúvania osobných údajov zachytených na fotografii je napríklad len rozlíšenie jednotlivých zamestnancov, prípadne zvýšenie bezpečnosti na pracovisku, tieto osobné údaje nebudú patriť pod pojem osobitnej kategórie osobných údajov.²⁷⁹ Podľa názoru Úradu, vyjadrenom v stanovisku ku konkrétnemu prípadu vyhotovovania fotografií zamestnancov kvôli evidencii ich vstupu na pracovisko (bez ich súhlasu), spracúvanie osobných údajov vo forme fotografie zamestnanca získavanej pri každom vstupe na pracovisko a pri jeho opustení nebolo nevyhnutné na dosiahnutie účelu kontroly príchodov a odchodov zamestnancov v zmysle platného § 6 ods. 2 písm. d) zákona o ochrane osobných údajov.²⁸⁰ Prikláňame sa k tomuto názoru Úradu a domnievame sa, že za daných skutkových okolností šlo o neprimeraný zásah do súkromia, pretože nebol v súlade so zásadou proporcionality.

Z hľadiska pracovného práva majú svoj osobitný význam **osobné údaje**

²⁷⁸ BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. 2. vyd. Praha: Linde, 2010, s. 167.

²⁷⁹ ÚOOÚ ČR k problémům z praxe č. 3/2010 – K použití fotografie, obrazového a zvukového záznamu fyzické osoby.

²⁸⁰ ÚOOÚ, Správa o stave ochrany osobných údajov za roky 2011 a 2012. (online). 2013. (cit. 2015-01-30). Dostupné z: (https://dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_roky_2011_a_2012.pdf).

o členstve v odborových organizáciách. Odhaľujú totiž vnútorné názory a vzťahy človeka, ktoré môžu viesť k nerovnakému zaobchádzaniu zo strany zamestnávateľa, ale aj kolegov. Dokonca možno pod týmto spojením chápať členstvo alebo podporovanie akéhokolvek združenia (aj bez právnej subjektivity), ktorého cieľom je ochrana a uplatňovanie práv zamestnancov v pracovnoprávných vzťahoch.²⁸¹ Zamestnávateľ práve preto, že ide o „citlivý údaj“, nesmie zisťovať, ktorí zamestnanci sú členmi odborovej organizácie. Keďže sa v niektorých ustanoveniach Zákonníka práce predpokladá vedomosť zamestnávateľa o členstve konkrétnych zamestnancov v odborovej organizácii,²⁸² má zamestnávateľ právo byť informovaný o týchto skutočnostiach. Podľa nášho názoru, by túto vedomosť mal získať priamo od zamestnanca a následne podľa toho postupovať.

Medzi najcitlivejšie osobné údaje patria **biometrické údaje**, lebo na ich základe je možné fyzickú osobu jednoznačne identifikovať. Biometrickým údajom je v zmysle § 4 ods. 3 písm. f) ZOOÚ „osobný údaj fyzickej osoby označujúci jej biologickú alebo fyziologickú vlastnosť alebo charakteristiku, na základe ktorej je jednoznačne a nezameniteľne určiteľná; biometrickým údajom je najmä odtlačok prsta, odtlačok dlane, analýza deoxyribonukleovej kyseliny“.

Tento pojem zahŕňa biologické vlastnosti, fyziologické znaky, črty alebo opakovateľné činnosti, v prípade, ktorých sú tieto vlastnosti alebo činnosti špecifické pre uvedeného jednotlivca a zároveň merateľné, aj keď spôsoby používané v praxi na ich technické meranie zahŕňajú určitý stupeň pravdepodobnosti.²⁸³ Definícia tohto pojmu obsahuje len demonštratívny (príkladný) výpočet biometrických údajov. Medzi ďalšie typické príklady patrí aj sietnica, tvar tváre, hlas, ale aj geometria ruky, štruktúra žíl alebo dokonca určitá hlboko zakorenená schopnosť alebo iná vlastnosť týkajúca sa správania (napr. vlastnoručný podpis, údery na klávesnici, osobitný spôsob chôdze alebo reči). ZOOÚ navyše predpokladá, že charakteristickým znakom každého biometrického údaju je, že umožňuje jednoznačnú a nezameniteľnú identifikáciu fyzickej osoby, od ktorej tento údaj pochádza.²⁸⁴

Vzhľadom na technologický pokrok v každej sfére spoločenských vzťahov sa stretávame aj na pracoviskách s využívaním biometrických technológií, ktoré zamestnávateľia využívajú na zabezpečenie kontrolovaného vstupu do určených

²⁸¹ BARTÍK, V., JANEČKOVÁ, E. *Zákon o ochrane osobných údajů s komentářem*. 1. vyd. Olomouc: ANAG, 2010, s. 38.

²⁸² Napr. § 74 Zákonníka práce o účasti zástupcov zamestnancov pri skončení pracovného pomeru a § 87a Zákonníka práce o konte pracovného času.

²⁸³ Vymedzenie tohto pojmu korešponduje so Stanoviskom Pracovnej skupiny 29 č. 3/2012 k vývoju v oblasti biometrických technológií z 27. apríla 2012, WP 193 a pracovným dokumentom z roku 2003 o biometrii pod číslom WP 80.

²⁸⁴ VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 62.

priestorov či dochádzky. V praxi prestáva byť niečím výnimočným využívanie zariadenia na snímanie odtlačkov prstov na evidenciu dochádzky do zamestnania. V nasledujúcich odsekoch sme preto analyzovali, či a za akých podmienok je možné pristúpiť k spracúvaniu biometrických údajov podľa zákona.

Podľa § 13 ods. 5 ZOOÚ je zamestnávateľ (prevádzkovateľ) oprávnený spracúvať biometrické údaje len vtedy, ak je to

- primerané účelu spracúvania (zásada primeranosti),
- nevyhnutné na jeho dosiahnutie (zásada nevyhnutnosti),
- a ak také spracúvanie má zodpovedajúci právny základ.²⁸⁵ To znamená, že spracúvanie osobných údajov je možné
 - len na základe právnej úpravy explicitne vyjadrenej v osobitnom právnom predpise (resp. zákone),
 - zamestnanec (ako dotknutá osoba) dal na spracúvanie písomný alebo inak hodnoverne preukázateľný súhlas,
 - alebo ak je to nevyhnutné na plnenie zmluvy (§ 10 ods. 3 písm. b/ ZOOÚ),
 - alebo ak je to nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa (§ 10 ods. 3 písm. g/ ZOOÚ).

Podľa § 13 ods. 6 ZOOÚ primeranosť, nevyhnutnosť a právny základ spracúvania biometrických údajov posudzuje Úrad na ochranu osobných údajov Slovenskej republiky v osobitnom konaní (§ 37 až 39 ZOOÚ). Pritom je veľmi dôležité dbať pri spracúvaní aj na bezpečnosť údajov v zmysle § 19 a § 20 ZOOÚ.

K prípadu zamestnávateľa, ktorý využíval zariadenie na snímanie odtlačkov prstov na evidenciu a kontrolu dochádzky zamestnancov, vyjadril Úrad stanovisko, z ktorého vyplýva, že zariadenia na snímanie odtlačkov prstov sú podľa ZOOÚ prostriedkami spracúvania biometrických údajov (obdobne aj snímače geometrie ruky) a ich využitie na tento účel je prípustné iba pre dôležité, osobitne chránené objekty a vyhradené priestory. Zamestnávateľ (prevádzkovateľ) pritom musí požiadať Úrad o osobitnú registráciu informačného systému, ktorý bude biometrické údaje dotknutých osôb spracúvať. Dôležitou súčasťou žiadosti je jej odôvodnenie, na základe ktorého Úrad posúdi a schváli osobitnú registráciu až pri splnení všetkých podmienok uvedených v § 37 a nasl. ZOOÚ. Na rozhodovanie Úradu nemá z právneho hľadiska vplyv ani skutočnosť, že zamestnávateľ disponuje súhlasom dotknutých osôb. Tvrdí, že súhlas dotknutých osôb so spracúvaním biometrických údajov nie je schopný prelomiť kogentnosť súvisiacich ustanovení, a preto je z právneho hľadiska irelevantný.²⁸⁶ Prikláňame sa k názoru

²⁸⁵ Porovnaj VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 121.

²⁸⁶ ÚOOÚ, Vyjadrenie k žiadosti z 24. júna 2009. (online). Dostupné z: (<http://www.biometric.sk/prospekt/Vyjadrenie-k-biometrickej-dochadzke.pdf>).

autorov komentára k ZOOÚ, že spracúvanie biometrických údajov v rámci dochádzkového systému na pracovisku nepredstavuje zákonnú výnimku z hľadiska primeranosti a nevyhnutnosti na dosiahnutie účelu, pretože právo fyzickej osoby na ochranu súkromia prevyšuje nad záujmom zamestnávateľa kontrolovať dochádzku práve týmto spôsobom.²⁸⁷

4.7.3 Osobné údaje zamestnanca po skončení pracovného pomeru

Po spracúvaní, napr. pri skončení pracovného pomeru, má zamestnávateľ povinnosť zlikvidovať všetky osobné údaje, ktorých účel spracúvania sa skončil (§ 17 ZOOÚ). Tak ako sme už skôr uviedli, pokračovať v spracúvaní osobných údajov aj po tomto štádiu je oprávnený len za podmienok ustanovených zákonom a na účely historického alebo vedeckého výskumu alebo v rámci sledovania vývoja alebo kvôli vedeniu štatistiky.

Zamestnávateľa sa často stretávajú s problémom definovania najdlhšej prípustnej dĺžky na uchovávanie osobných údajov svojich bývalých zamestnancov. Nepovažujeme za správne konanie zamestnávateľa, ktorý zlikviduje všetky osobné údaje zamestnanca, pretože sa obáva porušenia zákona, ale svoje opodstatnenie nemá ani uchovávanie jeho údajov niekoľko rokov po skončení pracovného pomeru. Súhlasíme s názorom, že primeraný čas závisí od účelu uchovávania (napr. na daňové účely) stanoveného osobitným predpisom aj so všeobecnou trojročnou premlčacou lehotou podľa Občianskeho zákonníka ako odporúčanou dobou na uchovávanie osobných údajov, v rámci ktorej môže zamestnanec alebo zamestnávateľ uplatniť svoje nároky z pracovnoprávneho vzťahu.²⁸⁸

4.8 Prostriedky ochrany osobných údajov zamestnanca v Slovenskej republike

Podľa občianskeho práva ako subjekty všeobecných osobnostných vzťahov oprávnených domáhať sa ochrany proti neoprávneným zásahom môžu iba občania v zmysle fyzických osôb. Pod pojmom „fyzická osoba“ sa rozumie človek ako ľudská bytosť bez ohľadu na štátnu príslušnosť, pričom subjektom občianskeho práva môžu byť aj cudzí štátni občania, resp. bezdomovci za podmienky, že sa na-

²⁸⁷ Porovnaj VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 121.

²⁸⁸ MORÁVEK, J. *Ochrana osobných údajů v pracovněprávní agendě*. Praha: BMSS Start, 2010, s. 52.

chádzajú na území Slovenskej republiky.²⁸⁹ O neoprávnený zásah nepôjde vtedy, keď fyzická osoba so zásahom do svojej osobnosti súhlasila, alebo keď to výslovne umožňuje zákon (napr. „zákonné licencie“ podľa § 12 ods. 2 a 3 Občianskeho zákonníka).

V slovenskom právnom poriadku poznáme všeobecné a špeciálne (osobitné) prostriedky občianskoprávnej ochrany osobnosti fyzických osôb.²⁹⁰

Medzi **všeobecné prostriedky občianskoprávnej ochrany** osobnosti fyzických osôb (podľa Občianskeho zákonníka) zaraďujeme:

- *ochranu dohodou*

Fyzické a právnické osoby, štátne orgány a orgány miestnej samosprávy dbajú na to, aby nedochádzalo k ohrozovaniu a porušovaniu práv z občianskoprávných vzťahov a aby sa prípadné rozpory medzi účastníkmi odstránili predovšetkým ich dohodou (§ 3 ods. 2 Občianskeho zákonníka).

- *vlastnú ochranu (svojpomoc)*

Ak hrozí neoprávnený zásah do práva bezprostredne, môže ten, kto je takto ohrozený, primeraným spôsobom zásah sám odvrátiť (§ 6 Občianskeho zákonníka). Rovnako sem zaraďujeme aj osobitné inštitúty svojpomoci, a to krajnú núdzu a nutnú obranu (§ 418 ods. 1 a 2 Občianskeho zákonníka).

- *ochranu, ktorú poskytuje orgán verejnej správy*

Ak došlo k zrejmemu zásahu do pokojného stavu, možno sa domáhať ochrany na príslušnom orgáne štátnej správy, ktorý môže predbežne zásah zakázať alebo uložiť, aby bol obnovený predošlý stav (§ 5 Občianskeho zákonníka).

- *súdnu ochranu*

Do tejto skupiny všeobecných prostriedkov patrí činnosť súdu pred začatím konania, predbežné opatrenia, určovacie žaloby a žaloby o náhradu škody.

Medzi špeciálne (osobitné) prostriedky občianskoprávnej ochrany osobnosti fyzických osôb v zmysle § 13 Občianskeho zákonníka patrí najmä *súdna ochrana* prostredníctvom:

- *odstraňovacej žaloby*

Fyzická osoba má právo najmä sa domáhať, aby sa upustilo od neoprávnených zásahov do práva na ochranu jej osobnosti a aby sa v nich nepokračovalo, prípadne aby sa odstránili následky týchto zásahov, najmä obnovením pôvodného stavu (napr. vydaním neoprávnene získaných prejavov osobnej povahy).

- *satisfakčnej žaloby*

Pri závažných zásahoch do práva na ochranu osobnosti, má právo sa obrátiť každá fyzická osoba aj zamestnanec priamo na všeobecný súd so žalobou a do-

²⁸⁹ VOJČÍK, P. a kol. *Občiansky zákonník. Stručný komentár*. Bratislava: Iura Edition, 2008, s. 44.

²⁹⁰ KIRSTOVÁ, K. Ochrana osobnosti fyzickej osoby. In: LAZAR, J. a kol. *Občianske právo hmotné*. I. diel. Bratislava: Iura Edition, 2010, s. 189.

máhať sa aj náhrady nemajetkovej ujmy v peniazoch. Fyzická osoba má v takom prípade právo, aby sa jej dostalo primerané zadostučinenie. V rámci toho rozlišujeme morálnu a peňažnú satisfakciu. Ak morálne zadostučinenie nepostačuje so zreteľom na zníženú dôstojnosť alebo vážnosť fyzickej osoby v spoločnosti, a to v značnej miere, má taká osoba právo na peňažnú satisfakciu. Toto právo na náhradu nemajetkovej ujmy v peniazoch má fyzická osoba aj vtedy, keď morálna satisfakcia už nie je aktuálna. Výšku náhrady určí v zmysle § 13 ods. 3 Občianskeho zákonníka súd s prihliadnutím na závažnosť vzniknutej ujmy a na okolnosti, za ktorých k porušeniu práva došlo.

Prípustné sú aj ďalšie prostriedky ochrany v zákone taxatívne neuvedené. Tieto prostriedky občianskoprávnej ochrany možno použiť buď samostatne, alebo kumulovane, pričom nie je vylúčené, že závažný zásah do osobnostných práv osoby môže presahovať rámec súkromnoprávnej zodpovednosti (napr. v prípade zneužitia spracovaných údajov a podobne).

Na tomto mieste treba zdôrazniť, aká je povaha občianskoprávnej zodpovednosti v prípade zásahu do osobnostných práv, teda či ide o objektívnu alebo subjektívnu zodpovednosť. V prípade, ak neoprávneným zásahom do osobnostných práv fyzickej osoby vzniká primárne nemajetková ujma, ktorej nápravu je možné dosiahnuť prostredníctvom špeciálnych prostriedkov na ochranu osobnosti v zmysle § 13 Občianskeho zákonníka, prichádza použitie týchto prostriedkov do úvahy bez ohľadu na zavinenie pôvodcu neoprávneného zásahu. Ide teda o objektívnu zodpovednosť. Ak však vznikne neoprávneným zásahom do osobnostných práv majetková škoda (ujma), všeobecným prostriedkom na ochranu osobnosti je žaloba na náhradu škody, na ktorú nepriamo odkazuje § 16 Občianskeho zákonníka. Zodpovednosť pôvodcu zásahu je v druhom uvedenom prípade subjektívna, čo znamená, že vyžaduje skúmanie existencie zavinenia a posudzuje sa podľa ustanovenia § 420 Občianskeho zákonníka o všeobecnej zodpovednosti za škodu spôsobenú porušením právnej povinnosti.

Občiansky zákonník poskytuje normatívnu platformu právnych prostriedkov ochrany osobnostných práv jednotlivcov, ktoré je možné využiť aj v ďalších druhoch súkromnoprávnych vzťahov vrátane pracovnoprávnych vzťahov. Vzhľadom na to má spomenuté všeobecné a špeciálne prostriedky ochrany osobnosti k dispozícii každý zamestnanec, ak dôjde k zásahu do niektorého z jeho osobnostných práv zo strany zamestnávateľa, iného zamestnanca alebo tretej osoby. Potrebné je však pamätať aj na špecifické ustanovenia Zákonníka práce, ktoré modifikujú niektoré prostriedky ochrany osobnostných práv zamestnanca, ako napríklad prevenčná, zakročovacia a oznamovacia povinnosť zamestnanca (§ 178 ods. 1 a 2 Zákonníka práce), ktoré za istých podmienok vylučujú použitie inštitútu svojpomoci alebo konanie v krajnej núdzi.

Medzi ďalšie „*mimosúdne*“ prostriedky ochrany osobnosti fyzických osôb **pod-**

la osobitných predpisov patria napr. mediácia a rôzne návrhy, žiadosti, podnety a sťažnosti, ktoré riešia vybrané správne orgány. Niektoré z nich môžu ukladať aj pokuty ako správne sankcie.

Ak by monitorovanie (sledovanie) kamerovým systémom prekračovalo zákonné medze a zasahovalo by do súkromia zamestnanca (napr. kamery na toaletách), má stále možnosť sa obrátiť **osobne na zamestnávateľa** so žiadosťou, aby upustil od tohto konania. Medzi prostriedky ochrany práva zamestnanca ako dotknutej osoby patrí aj právo vyžadovať od zamestnávateľa (prevádzkovateľa) informácie o spracovávaných údajoch, žiadať ich blokovanie a likvidáciu v zmysle § 28 ods. 1 ZOOÚ.

Orgánmi, na ktoré sa zamestnanci môžu obrátiť svojím *podnetom*²⁹¹ alebo *sťažnosťou*,²⁹² ak majú podozrenie, že dochádza k ohrozovaniu či porušovaniu ich práva na súkromie, sú **inšpektoráty práce**, ktoré podľa § 150 Zákonníka práce a osobitného zákona č. 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov (ďalej len „zákon o inšpekcii práce“) u zamestnávateľov dozerajú nad dodržiavaním pracovnoprávných predpisov, predpisov o bezpečnosti a ochrane zdravia pri práci, dodržiavaním predpisov z oblasti sociálnej legislatívy v doprave a dodržiavaním zákazu nelegálneho zamestnávania a nelegálnej práce. Príslušný inšpektorát práce je z titulu svojej pôsobnosti oprávnený vykonať kontrolnú činnosť a prešetriť aj dôvodnosť sťažnosti podanej na základe zákona č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov. V kompetencii orgánov inšpekcie práce je podľa nášho názoru aj základné posúdenie, či inštalovaný kamerový systém určený na monitorovanie zamestnancov spĺňa podmienky legálneho monitorovania. Pokiaľ orgán inšpekcie dospeje k tomu, že inštalovaný monitorovací systém nezodpovedá zákonným podmienkam, môže

²⁹¹ Podnetom podľa vnútorných smerníc vydaných Národným inšpektorátom práce sa rozumie podanie fyzickej alebo právnickej osoby, ktorá poukazuje na porušovanie povinností vyplývajúcich z ustanovenia § 2 ods. 1 písm. a/ zákona o inšpekcii práce. Zamestnanec môže podať podnet písomnou formou prostredníctvom pošty, mailu, osobne na podateľni, prípadne telefonicky do záznamu.

²⁹² Podľa ustanovenia § 3 zákona č. 9/2010 Z. z. o sťažnostiach je „*sťažnosť podanie fyzickej osoby alebo právnickej osoby, ktorým sa domáha ochrany svojich práv alebo právom chránených záujmov, o ktorých sa domnieva, že boli porušené činnosťou alebo nečinnosťou orgánu verejnej správy, poukazuje na konkrétne nedostatky, najmä na porušenie právnych predpisov, ktorých odstránenie je v pôsobnosti orgánu verejnej správy*“. Podľa ustanovenia § 4 citovaného zákona „*sťažnosťou nie je podanie, ktoré má charakter dopytu, vyjadrenia, názoru, žiadosti, podnetu alebo návrhu a nie je v ňom jednoznačne vyjadrené, ochrany akého svojho práva alebo právom chráneného záujmu sa osoba domáha, poukazuje na konkrétne nedostatky v činnosti orgánu verejnej správy, ktorých odstránenie alebo vybavenie je upravené iným právnym predpisom, je sťažnosťou podľa osobitného predpisu, smeruje proti rozhodnutiu orgánu verejnej správy vydanému v konaní podľa iného právneho predpisu*“.

ukladať *pokuty* ako správno-právne sankcie. Problematickou otázkou však zostáva nízka úroveň efektivity a vymožiteľnosti opatrení uložených orgánom inšpekcie práce.

Možnosť obrátiť sa s *návrhom* či *podnetom* priamo na Úrad na ochranu osobných údajov Slovenskej republiky zakotvuje § 46 ods. 1 písm. c/ ZOOÚ, ak má osoba podozrenie z porušovania povinností ustanovených ZOOÚ pri spracúvaní osobných údajov. Podnet môže podať osobne alebo klasickou písomnou (poštou) či elektronickou formou. Kontrola dodržiavania zákonných povinností v oblasti ochrany osobných údajov patrí totiž do kompetencie Úradu ako dozorného orgánu, ktorý je oprávnený vstupovať do informačných systémov kontrolovaných subjektov. Za porušenie ZOOÚ hrozia prevádzkovateľom informačných systémov sankcie, a to podľa závažnosti porušenia povinností a dôsledkov. Úrad môže v tomto prípade (aj ex offo) predvolať prevádzkovateľa alebo sprostredkovateľa na podanie vysvetlenia alebo vydať účinnejšie rozhodnutie, ktorým uloží subjektu porušujúcemu povinnosti zo ZOOÚ, aby niečo konal alebo niečoho sa zdržal alebo mu uloží pokutu. V zmysle § 65 ods. 1 ZOOÚ je Úrad oprávnený v rozhodnutí uložiť, aby prevádzkovateľ alebo sprostredkovateľ v určenej lehote vykonali opatrenia na odstránenie zistených nedostatkov a príčin ich vzniku s následkom zastavenia konania o ochrane osobných údajov, ak k náprave nedôjde. Má možnosť tiež uložiť ďalšie opatrenia uvedené v § 65 ods. 2 ZOOÚ, napr. zakázať spracúvanie konkrétnych osobných údajov, nariadiť ich odstránenie alebo likvidáciu, uložiť povinnosť prijať technické, organizačné a personálne opatrenia alebo vypracovať bezpečnostný projekt či zmeniť sprostredkovateľa. Z hľadiska sankcií má oprávnenie ukladať ako donucujúce opatrenia pokuty a poriadkové pokuty v zmysle § 68 a nasl. ZOOÚ. V Slovenskej republike je strop finančnej sankcie za porušenie stanovený na 200 000 €. ²⁹³

4.9 Ochrana osobných údajov v Európskej únii z hľadiska empirického výskumu

Od roku 1995 v európskom priestore platí smernica Európskeho parlamentu a Rady 95/46/EHS o ochrane fyzických osôb pri spracúvaní osobných údajov

²⁹³ Hoci Európska komisia navrhuje, aby sa výška maximálnej pokuty za porušenie ochrany osobných údajov stanovila na 1 milión € alebo dve percentná z globálneho ročného obratu spoločnosti, v Slovenskej republike sa tento trend akoby ignoruje a poslednou novelou ZOOÚ zákonodarcu pristúpil dokonca k zníženiu maximálnych sadzieb pokút. K zníženiu horných hraníc pokút, ktoré je oprávnený Úrad ukladať za porušenie povinností podľa § 68 ods. 1 až 7 ZOOÚ došlo novelou zákona č. 84/2014 Z. z. s účinnosťou od 15. apríla 2014.

a voľnom pohybe týchto údajov. Už dlhodobo sa diskutuje o potrebe jej reformy a prijatí nového právneho rámca, ktorý by zavádzal adekvátne komplexné pravidlá ochrany osobných údajov obyvateľov Európskej únie. Novým nariadením by mala byť nahradená spomínaná smernica č. 95/46/EHS a všeobecnou smernicou o ochrane osobných údajov aj Rámcové rozhodnutie o ochrane osobných údajov z roku 2008.²⁹⁴

V tejto súvislosti v roku 2012 bol vykonaný komparatívny výskum multidisciplinárnej výskumnej siete – Agentúry Európskej únie pre základné práva vystupujúcej pod označením FRA²⁹⁵ (ďalej len „agentúra FRA“). Do výskumu bolo zapojených 16 členských štátov vrátane štyroch susedných krajín Slovenskej republiky (Maďarska, Poľska, Českej republiky, Rakúska). Plasticky zobrazuje realitu uplatňovania vnútroštátnych právnych úprav ochrany osobných údajov vybraných členských štátov, čo považujeme za podstatný prínos do rozoberanej problematiky a s ňou súvisiacej odbornej diskusie. Získané dáta pritom nie sú jednostranne zamerané a poskytujú údaje tak zo strany tých, ktorých údaje majú byť chránené, ako aj tých, ktorí s týmito údajmi pracujú a pri svojej činnosti ich spôsobom stanoveným právnym predpisom využívajú.

Výskum mal charakter kvalitatívneho prieskumu, v ktorom sa jednotlivcom zo 6 cieľových skupín (1. sťažovatelia, 2. osoby, ktoré sa nestážovali, 3. sudcovia, prokurátori, 4. pracovníci inštitúcií na ochranu osobných údajov, 5. sprostredkovatelia a 6. právnici z praxe) položilo viacero otázok týkajúcich sa ochrany osobných údajov, čím boli zapojení buď do rozhovorov, alebo sa zúčastnili na diskusii v špecializovaných skupinách. Cieľom výskumu bolo zozbierať dáta, ktoré by preukazovali jednotlivé typy porušenia ochrany osobných údajov. Výsledný efekt preto nemal mať štatistický charakter, ale naopak mal tvoriť reprezentatívnu vzorku dát. Výpovedná hodnota získanej vzorky preto spočívala v jej schopnosti zastúpiť dáta, s ktorými sa nepracovalo.

Z hľadiska ochrany osobných údajov v pracovnom práve sa najčastejšie stretávame s porušením ochrany súkromia zamestnancov práve pri využívaní bezpečnostných kamier na pracovisku. Agentúra FRA uvádza, že základné typy porušenia ochrany osobných údajov sa spájajú s používaním internetu, priamym marketingom a sledovaním prostredníctvom utajených bezpečnostných kamier CCTV (t. j. mimo televízneho okruhu). V rámci výskumu sa viacero respondentov z rôznych krajín vyjadrilo, že zamestnávatelia porušujú ochranu osobných údajov najmä tým, že získavajú osobné údaje zamestnancov uložené v technic-

²⁹⁴ Správa FRA. *Prístup k prostriedkom nápravy v oblasti ochrany údajov v členských štátoch EÚ – zhrnutie*. (online). Viedeň: FRA, 2013, (cit. 2015-01-18). Dostupné z: (http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_sk.pdf). s. 3.

²⁹⁵ Z anglického názvu European Union Agency for fundamental rights.

kých komunikačných zariadeniach (počítačoch, telefónoch), využívajú kartové prístupové systémy a systémy GPS. Zamestnanci však uvádzajú, že okrem uvedených porušení ochrany osobných údajov zamestnancov, zamestnávateľa s diskriminačnými dôsledkami spracúvajú aj „citlivé“ osobné údaje zozbierané prostredníctvom prieskumov alebo auditov a často prístupujú k ich neoprávnenému zverejňovaniu.²⁹⁶

Zaujímavosťou je, že v rozhovoroch a diskusiách opýtaní uviedli, že najčastejším následkom vyplývajúcim z porušenia ochrany ich osobných údajov bol vznik škody, ktorú opisovali ako psychickú alebo sociálnu ujmu v podobe emocionálneho stresu alebo v poškodení ich dobrého mena a povesti. Pri skúmaní následkov porušenia právnych predpisov upravujúcich ochranu osobných údajov na pracovisku sme sa stretli s nezvyčajným javom. Z výskumu totiž vyplýva, že obeť porušenia ochrany osobných údajov (resp. medzi nimi aj dotknutí zamestnanci) sa primárne sústreďujú na potenciálne hroziacu, ale aj reálnu nemajetkovú ujmu, ktorá im porušením vznikla, pričom takmer vo všetkých prípadoch si až sekundárne uvedomujú vznik možnej majetkovej ujmy a vážnosť jej dôsledkov. Medzi najčastejšie majetkové škody vzniknuté porušením ochrany osobných údajov opýtaní zahrnuli neschopnosť získať pôžičku, stratu nároku na zdravotnú starostlivosť, disciplinárne opatrenia, poškodenia ich profesionálnej alebo osobnej povesti alebo až stratu zamestnania či obmedzenie pracovných príležitostí. So skutočnosťou, že za závažnejší následok porušenia ochrany osobných údajov dotknuté osoby považovali vznik nemajetkovej ujmy súvisí aj motivácia jednotlivcov, ktorí sa domáhali nápravy. Najčastejšie sa totiž dotknuté osoby nedožadovali finančnej kompenzácie, ale chceli hlavne zabrániť porušeniu ich práv v budúcnosti, zvýšiť povedomie o ochrane osobných údajov, zastaviť protiprávnu činnosť a získať uznanie kompetentného orgánu, že boli porušené ich práva, ale v neposlednom rade aj potrestanie osoby, ktorá ochranu súkromia nejakým spôsobom narušila.²⁹⁷

Komplexným zhodnotením situácie úrovne ochrany osobných údajov vo vybraných členských štátoch na základe vykonaného empirického výskumu dospievame k obrazu „bezzubého papierového tigra“.²⁹⁸ Zo získaných údajov a výsled-

²⁹⁶ Správa FRA. *Prístup k prostriedkom nápravy v oblasti ochrany údajov v členských štátoch EÚ – zhrnutie*. (online). Viedeň: FRA, 2013. (cit. 2015-01-18). Dostupné z: (http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_sk.pdf), s. 3 až 4.

²⁹⁷ Správa FRA. *Prístup k prostriedkom nápravy v oblasti ochrany údajov v členských štátoch EÚ – zhrnutie*. (online). Viedeň: FRA, 2013. (cit. 2015-01-18). Dostupné z: (http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_sk.pdf), s. 4.

²⁹⁸ Vyjadrenie zamestnanca Úradu na ochranu osobných údajov v Nemecku, In: Správa FRA. *Prístup k prostriedkom nápravy v oblasti ochrany údajov v členských štátoch EÚ – zhrnutie*. (online). Viedeň: FRA, 2013. (cit. 2015-01-18). Dostupné z: (http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_sk.pdf), s. 6.

kov možno dospieť k záveru, že vnútroštátne orgány zodpovedné za kontrolu dodržiavania ochrany osobných údajov nevyužívajú všetky dostupné prostriedky, aby na jednej strane zabránili porušovaniu vnútroštátnych i európskych právnych noriem na ochranu osobných údajov, ale na druhej strane urobili nápravu a odradili od ďalšieho porušovania. Výsledná kritika vyplývajúca z predmetného výskumu sa preto sústreďuje hlavne na nedostatočné fungovanie uvedených orgánov vo vybraných členských štátoch Európskej únie, ktoré buď nemajú dostatočné právomoci, alebo výška udeľovaných pokút neodrádza od porušovania ochrany osobných údajov.

Podľa nášho názoru závery a výsledky predmetného empirického výskumu z roku 2012 reprezentujú súčasnú úroveň ochrany osobných údajov zamestnancov v celej Európskej únii. A hoci závery výskumu nie sú odvodené z dát získaných aj od cieľových skupín zúčastnených subjektov v Slovenskej republike, tvrdíme, že majú výpovednú hodnotu aj v rámci slovenského právneho poriadku a priestoru. Dôvodom, prečo sme dospeli k uvedenému záveru je skutočnosť, že výsledkom tohto výskumu nie je len opis stavu, v ktorom sa nachádza ochrana osobných údajov v rámci jednotlivých členských štátov, ale hlavne vytvorenie jednotlivých charakteristických črt, čiže typologicky rovnakých problémov, ktoré sú spoločné pre všetky členské krajiny Európskej únie. Na základe uvedených dôvodov sme dospeli k záveru, že ak by sa do výskumu zapojila aj reprezentatívna vzorka opýtaných zo Slovenskej republiky, výsledky by boli veľmi podobné alebo by úplne zodpovedali výsledkom v okolitých štátoch Európskej únie a boli by v súlade s celkovými závermi výskumu.

ZÁVER

Zamestnávateľa bežne v praxi využívajú elektronické monitorovacie zariadenia, ktorými kontrolujú, či sú zamestnanci na pracovisku, či si plnia svoje pracovné povinnosti vyplývajúce z pracovnej zmluvy a príslušných predpisov, a akým spôsobom využívajú im zverené prostriedky na výkon práce (napr. prístroje, zariadenia, počítače, telefóny alebo služobné motorové vozidlá). S používaním strojových zariadení, informačných a telekomunikačných technológií zamestnancami počas pracovnej doby sa popri mnohých pozitívnych aspektoch vynárajú i určité ťažkosti či sporné otázky spojené s ochranou súkromia zamestnancov. Tie sa objavujú v prípadoch, keď zamestnávateľa monitorujú spôsob využívania rôznych zariadení a technológií zamestnancami. Ak chce zamestnávateľ sledovať zamestnanca, musí okrem príslušných ustanovení Zákonníka práce a požiadaviek judikatúry Európskeho súdu pre ľudské práva dodržiavať aj všetky povinnosti, ktoré mu vyplývajú zo zákona o ochrane osobných údajov.

Vo všeobecnosti je súkromie zamestnanca chránené nielen voči neoprávneným zásahom orgánov verejnej moci, ale z medzinárodných dohovorov o ochrane ľudských práv a základných slobôd vyplýva štátu pozitívny záväzok chrániť jednotlivca pred zásahmi do jeho súkromia aj zo strany zamestnávateľa ako subjektu súkromného práva. V zmysle konštantnej judikatúry Európskeho súdu pre ľudské práva sa pod pozitívnym záväzkom štátu rozumie jeho aktívne pôsobenie na súkromnoprávne vzťahy medzi jednotlivcami. Jednou zo základných povinností štátu je teda aktívne vstupovať do vzťahov medzi súkromnými subjektmi a prijímať aj také opatrenia, ktoré sú spôsobilé zabezpečiť rešpektovanie vzájomných práv a povinností medzi zamestnávateľom a zamestnancom. Prejavom tohto pôsobenia je snaha o dosiahnutie rovnovážneho stavu, rešpektujúceho tak oprávnené záujmy zamestnávateľa, ako aj zamestnanca. Hľadanie rovnovážneho stavu vnímame ako kooperatívnu hru, ktorej výsledok má byť pre všetkých zúčastnených čo najpriateľnejší. Nezastupiteľnú úlohu pritom zohráva štát, ktorý prostredníctvom svojich orgánov prispieva k stabilizácii spoločenských vzťahov.

Základy fungujúceho a efektívneho systému ochrany súkromia a osobných údajov na pracovisku, ktorý vedie k zvyšovaniu úrovne právnej istoty a z ktorého budú mať prospech všetci zúčastnení, sú postavené na nasledujúcich nosných pilieroch. Zaraďujeme medzi ne jasné pravidlá stanovené právnym poriadkom, ako aj jednotnú aplikačnú prax súdov a orgánov slúžiacich na ochranu osobných

údajov. Jednu z najdôležitejších úloh pri dosahovaní uvedeného cieľa plní Ústavný súd Slovenskej republiky, ktorý pristupuje podľa vzoru Európskeho súdu pre ľudské práva k ochrane súkromia a osobných údajov zamestnanca tak, že v rámci rozhodovacej činnosti aplikuje najmä tzv. test proporcionality. Prihliada pritom na skutočnosť, či je zásah do súkromia zamestnanca zo strany zamestnávateľa legálny (t. j. v súlade s právnym poriadkom) a legitímny (t. j. odôvodnený z hľadiska záujmu štátu, spoločnosti alebo jednotlivcov). Až následne skúma, či je proporcionálny, a teda či je vhodný, potrebný a zodpovedajúci závažnosti obmedzenia v kolízii stojacich základných práv a slobôd.

Čiastkovými cieľmi predloženej monografie bolo priblížiť osobitosti využívania moderných monitorovacích zariadení na pracovisku, komplexne posúdiť ich prínosy a riziká a definovať hranice medzi právami a povinnosťami zamestnávateľa a zamestnanca v oblasti ochrany súkromia a osobných údajov aj prostredníctvom dôsledného uplatňovania zásady proporcionality. Obsahovú náplň práce preto tvoria úvahy vo vzťahu ku skúmaným problémom a odpovede na nasledujúce otázky. Je pojem súkromie otvoreným alebo uzavretým pojmom? Môže vôbec zamestnávateľ sledovať pohyb zamestnanca na pracovisku, jeho pracovnú elektronickú komunikáciu vrátane používania internetu alebo telefonické hovory? Aké sú hranice, za ktoré zamestnávateľ pri jednotlivých spôsoboch monitorovania na pracovisku nemôže zájsť? Aké sú povinnosti každého zamestnávateľa vyplývajúce z platného zákona o ochrane osobných údajov? Zameranie sa na hľadanie odpovedí na tieto a podobné otázky nás priviedlo postupne až k úvahám o aktuálnej úrovni ochrany práva zamestnanca na súkromie vrátane jeho osobných údajov a návrhom na skvalitnenie pracovnoprávnej úpravy a úpravy v príslušných osobitných právnych predpisoch v Slovenskej republike.

V monografii sme dospeli k záveru, že samotný pojem súkromie je pojem obsiahly, o čom svedčí aj judikatúra Európskeho súdu pre ľudské práva. Pojem „súkromie“ súčasná právna teória explicitne nedefinuje a chápe ho ako významovo otvorený. Jednou z príčin, prečo súkromie nemá svoju jasnú definíciu, je nepochybne skutočnosť, ktorá súvisí s rýchlym rozvojom nových technológií monitorovania zamestnancov. Právo na súkromie zamestnanca sa tak dostáva do ešte výraznejšej kolízie s vlastníckym právom zamestnávateľa, ktorý pracovisko považuje za svoj súkromný priestor, v ktorom majú „platiť výhradne jeho pravidlá“. V súčasnosti sa v právnej vede živo diskutuje a hľadajú sa mechanizmy, ktorých cieľom je vytvoriť podmienky na dosiahnutie vyváženého stavu medzi oprávnenými záujmami zamestnávateľa a zamestnanca. Považujeme preto za potrebné nanovo vyvažovať práva a povinnosti zamestnanca a zamestnávateľa tak, aby nedochádzalo k neprimeraným zásahom do vlastníckeho práva zamestnávateľa na jednej strane a práva na súkromie zamestnanca na druhej strane.

V predloženej práci sme sa venovali analýze platnej právnej úpravy ochrany

súkromia a osobných údajov fyzických osôb v oblasti pracovnoprávných vzťahov v Slovenskej republike a snažili sme sa zistiť, či zodpovedá prijatým štandardom medzinárodného a komunitárneho práva. Dospeli sme k záveru, že právna úprava ochrany súkromia zamestnanca v slovenskom Zákonníku práce a súvisiacich právnych predpisoch je v súlade s medzinárodnými zmluvami a dokumentmi na ochranu ľudských práv a zároveň reflektuje aj základné normy sekundárneho práva, čiže nariadenia a smernice Európskej únie, ktorými sme sa podrobnejšie zaoberali v druhej kapitole tejto monografie. Najmä na európskej úrovni však v súčasnosti prebieha rozsiahla diskusia medzi rôznymi organizáciami a inštitúciami o nevyhnutnosti zdokonalenia a prispôsobenia doteraz prijatých štandardov týkajúcich sa ochrany súkromia a ochrany osobných údajov novým podmienkam. Dôvodom je skutočnosť, že súčasné štandardy na medzinárodnej, ale aj európskej úrovni nedokážu poskytnúť dostatočnú ochranu proti neoprávneným zásahom do súkromia zamestnanca práve kvôli dynamickému rozvoju informačných technológií a novým možnostiam ich využitia.

Obdobnú diskusiu môžeme pozorovať aj v podmienkach slovenskej právnej úpravy. Jej analýzou sme dospeli k názoru, že je nedostatočná a vágna, pretože na jednej strane síce poskytuje minimálnu „európsku“ úroveň ochrany zamestnanca ako slabšej zmluvnej strany pracovnoprávneho vzťahu, ale poskytuje zamestnávateľom pomerne široký priestor na zásahy do súkromia zamestnancov v rámci kontroly výkonu práce a plnenia ďalších pracovných povinností. V ustanovení § 13 ods. 4 Zákonníka práce totiž chýba presnejšie vymedzenie „vážneho dôvodu spočívajúceho v osobitnej povahe činnosti zamestnávateľa“, ktorý umožňuje zamestnávateľovi v takom prípade narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch tým, že ho monitoruje, vykonáva záznam telefonických hovorov, prípadne kontroluje elektronickú poštu odoslanú alebo doručenú na pracovnú elektronickú adresu aj bez jeho predchádzajúceho súhlasu. Zamestnávatelia sa uvedené ustanovenie snažia interpretovať čo najširšie bez ohľadu na to, či svojím konaním zasiahnu do základných práv zamestnanca alebo nie. Je totiž pochopiteľné, že pre zamestnávateľa je vážnym dôvodom všetko, čo ohrozuje jeho podnikateľské zámery. Podľa nášho názoru je navyše aj zákon o ochrane osobných údajov pomerne zložitý a podlieha pod tlakom meniacej sa európskej právnej úpravy častým novelizáciám.

Z uvedených dôvodov zamestnávateľa zastávajú z nášho hľadiska výhodnejšiu pozíciu, pretože sú lepšie oboznámení s právnou úpravou a v rámci orientácie v nej sú flexibilnejší a vedia ju preto efektívnejšie využívať vo svoj prospech. Náš záver nepochybne súvisí aj so skutočnosťou, že zamestnávatelia disponujú vyššími finančnými prostriedkami na zabezpečenie a prevádzkovanie monitorovacích zariadení a vedia sa lepšie orientovať v právnej úprave vďaka právnym oddeleniam a profesionálnym právnym zástupcom. Aktuálny stav ochrany súkromia

a osobných údajov zamestnancov v Slovenskej republike zároveň reflektuje to, že znalosti a orientácia zamestnancov v danej problematike nie je na príliš vysokej úrovni a menej výhodné postavenie ich často privádza až k rezignácii na uplatňovanie ich základných práv. Pracovná sféra je pritom dôležitou súčasťou života každého jednotlivca a zásahy do súkromia na pracovisku môžu mať výrazný vplyv na ďalšie oblasti súkromného a rodinného života, ktoré treba vnímať veľmi citlivo. Je preto dôležité, aby mali zamestnanci dostatočný prehľad o svojich právach a povinnostiach v oblasti ochrany súkromia a osobných údajov a poznali limity neoprávnených zásahov zo strany zamestnávateľa.

Zlepšenie úrovne právneho povedomia verejnosti v oblasti ochrany súkromia a osobných údajov by malo zabezpečiť posilnenie postavenia organizácií občianskej spoločnosti, ktoré fungujú v zahraničí na rovnakom princípe ako združenia na ochranu spotrebiteľov alebo centrá právnej pomoci. Tie by mohli napríklad na žiadosť dotknutých osôb, resp. zamestnancov poskytovať právne poradenstvo, prípadne právne zastúpenie v oblasti sporov týkajúcich sa ochrany ich súkromia a osobných údajov. Vychádzali sme pritom z výskumu Agentúry FRA, ktorá uvádza, že vo väčšine členských krajín Európskej únie je veľmi náročné nájsť zástupcov z radov organizácií, ktoré sa špecializujú na problematiku ochrany osobných údajov, poskytujú podporu obetiam porušenia ochrany alebo majú rozsiahle skúsenosti v tejto oblasti.²⁹⁹ Nedostatočné zastúpenie občianskej spoločnosti na ochrane osobných údajov považujeme za jednu z príčin nízkej úrovne informovanosti obetí porušenia ochrany osobných údajov. Hlavnou úlohou občianskej spoločnosti by pritom malo byť poskytnutie pomoci jednotlivcom so sťažnosťami prípadne žalobami, ktorými by sa domáhali nápravy. Medzi ďalšie aktivity by mali patriť vzdelávanie, výskum, školenia, ako aj mediálne kampane, články a publikácie, ktorých hlavným cieľom by bolo zvýšiť povedomie verejnosti o právoch na ochranu súkromia a osobných údajov. Tým by sa priamo zvýšila aktivita a záujem ľudí o domáhanie sa ochrany ich základných práv v tejto oblasti. Zároveň by sa tým tiež zvýšil celospoločenský tlak na prijímanie kvalitnejšej právnej úpravy a jej rešpektovanie v praxi.

Dôležitú úlohu majú, samozrejme, aj súdy, ktoré sa vzniknutú nerovnováhu medzi právami a povinnosťami zamestnanca a zamestnávateľa snažia potláčať v rámci svojej aplikáčnej praxe. V prípade sporu totiž ad hoc posudzujú, či zamestnávateľ bol naozaj oprávnený zasiahnuť do súkromia zamestnanca a či ním uvedený vážny dôvod vyhovuje testu proporcionality (z hľadiska vhodnosti, potrebnosti a závažnosti obmedzenia v kolízii stojacich práv zamestnanca a za-

²⁹⁹ Správa FRA. *Prístup k prostriedkom nápravy v oblasti ochrany údajov v členských štátoch EÚ – zhrnutie*. (online). Viedeň: FRA, 2013. (cit. 2015-01-18). Dostupné z: (http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_sk.pdf), s. 8.

mestnávateľa). Súčasný stav rozhodovacej činnosti súdov v Slovenskej republike v oblasti ochrany súkromia a ochrany osobných údajov však nehodnotíme ako vyhovujúci. Stále sa stretávame s problémom neexistencie dostatočného množstva judikatúry slovenských súdov, ktorá by bola z hľadiska výkladu prínosom a významnou pomocou pre komplexnú a lepšiu orientáciu v tejto problematike. V odbornej literatúre sa objavujú výrazne odlišné názory odborníkov na túto tému, preto najmä chýbajúca judikatúra by podľa nášho názoru mohla a mala prispieť k zjednoteniu rôznych názorových smerov.

Súhlasíme so záverom agentúry FRA, že najdôležitejším krokom na zlepšenie situácie v oblasti ochrany osobných údajov je zabezpečenie čo najširšej nezávislosti orgánov, do ktorých pôsobnosti patrí kontrola dodržiavania právnych predpisov na ochranu osobných údajov.³⁰⁰ Lepšie výsledky pri hľadaní rovnovážneho stavu je teda možné dosiahnuť aj prostredníctvom posilňovania kompetencií Úradu na ochranu osobných údajov Slovenskej republiky, ktorý by mal zastávať úlohu stabilného nezávislého orgánu, schopného promptne zakročiť, ak dôjde zo strany zamestnávateľov k ohrozovaniu či porušovaniu ochrany súkromia a osobných údajov ich zamestnancov. Je však nevyhnutné, aby rozšírené právomoci tento orgán kontroly využíval tak, aby neposkytoval ochranu len osobám, ktorých sa ochrana týka, ale aj tým, ktorí údaje získavajú a následne ich v rámci svojej činnosti zákonom stanoveným spôsobom spracúvajú.

Úrad ako orgán zodpovedný za kontrolu dodržiavania predpisov na ochranu osobných údajov disponuje síce právomocou zakročiť proti ich porušovaniu viacerými opatreniami, väčšinou sa však v praxi stretávame s tým, že preferuje skôr minimálne finančné sankcie (pokuty a poriadkové pokuty), čím zákon o ochrane osobných údajov stráca svoj preventívny charakter, pretože neodrádza osoby, ktoré sa dopustili porušenia od ďalšieho takéhoto konania. V Slovenskej republike je strop finančnej sankcie zákonom o ochrane osobných údajov stanovený na 200 000 €. Európska komisia pritom dlhodobo navrhuje, aby sa výška maximálnej pokuty za porušenie ochrany osobných údajov skôr zvyšovala a stanovila až na 1 milión € alebo dve percentá z globálneho ročného obratu spoločnosti. V rámci vývoja maximálnej finančnej sankcie dokonca došlo k zníženiu najvyšších sadzieb pokút, ktoré je oprávnený Úrad ukladať za porušenie zákonných povinností, a to prijatím zákona č. 84/2014 Z. z. s účinnosťou od 15. apríla 2014, ktorý zmenil ustanovenia § 68 ods. 1 až 7 zákona o ochrane osobných údajov. Uvedená situácia podľa nášho názoru oslabuje postavenie a kompetencie Úradu

³⁰⁰ Stanovisko FRA č. 2/2012. *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*. (online). Viedeň: FRA, 2012. (cit. 2015-01-18). Dostupné z: (<http://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf>), s. 29 až 33.

a vnímame ju ako nesystémové riešenie. Prikláňame sa skôr k návrhu, aby sa okrem maximálneho stropu finančnej sankcie zvýšila aj minimálna sadzba pokuty. Dostatočne vysoké finančné pokuty majú totiž svoje opodstatnenie, keďže pôsobia preventívne a podporujú potlačanie recidívy, teda opakované porušovanie ochrany osobných údajov a zásahy do súkromia dotknutých osôb. Podľa nášho názoru efektívne právomoci Úradu sú základom na získanie a zachovanie dôveryhodnosti a autority u všetkých fyzických a právnických osôb. Posilnenie jeho pozície (prostredníctvom osobitného správneho konania a ukladania sankcií) bez zbytočnej a často likvidačnej byrokratickej záťaže pre zamestnávateľov by malo v konečnom dôsledku viesť k tomu, že by sa v našich podmienkach Úrad stal preferovaným orgánom, ktorý by obeť porušenia vyhľadávali a prostredníctvom neho by sa domáhali nápravy.

V predloženej práci sme uviedli niektoré základné princípy, ktoré by sa mali stať piliermi pri tvorbe novej, resp. reformnej právnej úpravy ochrany súkromia a osobných údajov v pracovnoprávných vzťahoch. Právna úprava, ako aj aplikačná prax v oblasti ochrany súkromia a osobných údajov by mala byť vyvážená, pretože sa tu stretávajú protichodné práva a záujmy zamestnancov na súkromie a vlastnícke práva zamestnávateľov. Na základe komplexného skúmania tejto problematiky sme dospeli k záveru, že dosiahnutie celkom rovnovážneho stavu medzi právami a povinnosťami zamestnancov a zamestnávateľov v oblasti ochrany súkromia a osobných údajov je utópiou, čo však neznamená, že by snaha o čo najväčšie priblíženie sa k tomuto ideálnemu stavu strácala svoj význam. Kľúčovým riešením je podľa nášho názoru okrem skvalitňovania právnej úpravy aj zvyšovanie všeobecného právneho povedomia o ochrane súkromia a osobných údajov na pracovisku, posilňovanie právomocí orgánov zabezpečujúcich kontrolu dodržiavania právnych predpisov v tejto oblasti a väčšie množstvo kvalitnej a jednotnej judikatúry, ktorá by mala byť prirodzeným dôsledkom argumentácie právne uvedomelých účastníkov najmä občianskoprávných a v rámci nich aj pracovnoprávných sporov.

ZOZNAM POUŽITEJ LITERATÚRY

Monografie

- BARANCOVÁ, H. a kol. *Monitorovanie zamestnancov a právo na súkromný život*. Bratislava: Sprint dva, 2010. 192 s. ISBN 978-80-89393-43-5.
- BARANCOVÁ, H. a kol. *Základné práva a slobody v pracovnom práve*. Plzeň: Aleš Čeněk, 2012. 377 s. ISBN 978-80-7380-422-0.
- BARANCOVÁ, H. *Zákonník práce. Komentár*. 1. vyd. Praha: C. H. Beck, 2010. 673 s. ISBN 978-80-7400-172-7.
- BARANCOVÁ, H., SCHRONK, R. *Pracovné právo*. Bratislava: SPRINT, 2007. 814 s. ISBN 978-80-89085-95-8.
- BARTÍK, V., JANEČKOVÁ, E. *Zákon o ochraně osobních údajů s komentářem*. 1. vyd. Olomouc: ANAG, 2010. 383 s. ISBN 80-72636-13-8.
- BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. 2. vyd. Praha: Linde, 2010. 264 s. ISBN 978-80-7201-817-8.
- ČAPEK, J. *Evropská úmluva o ochraně lidských práv a základních svobod. I. část – Úmluva*. Praha: Linde, 2010. 887 s. ISBN 978-80-7201-789-4.
- ELIÁŠ, K. a kol. *Občanský zákoník – Velký akademický komentář. 1. sv.* Praha: Linde, 2008. 1391 s. ISBN 978-80-7201-687-7.
- FRIDRICH, B., MIHÁLIKOVÁ, S., MOKRÁ, L., SIMAN, M. *Ochrana lidských práv v Evropské unii*. Bratislava: Univerzita Komenského, 2008. 245 s. ISBN 978-80-223-2522-6.
- HABERMAS, J. *Budoucnost lidské přirozenosti. Na cestě k liberální eugenice?* 1. české vyd. Praha: FILOSOFIA, 2003. 132 s. ISBN 80-7007-174-5.
- JANEČKOVÁ, E., BARTÍK, V. *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde Praha, a.s., 2011. 240 s. ISBN 978-80-7201-850-5.
- KLÍMA, K. a kol. *Komentář k Ústavě a Listině. 2. díl. 2. vyd.* Plzeň: Aleš Čeněk, 2009. 1441 s. ISBN 978-80-7380-140-3.
- KNAP, K., ŠVESTKA, J., JEHLIČKA, O., PAVLÍK, P., PLECITÝ, V. *Ochrana osobnosti podle občanského práva*. 4. podstatně přepracované a doplněné vyd. Praha: Linde, 2004. 435 s. ISBN 80-7201-484-6.
- KNAPP, V. *Vědecká propedeutika pro právníky*. Praha: Eurolex Bohemia, 2003. 233 s. ISBN 80-86432-54-8.
- KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha: Bova Polygon, 2010. 150 s. ISBN 978-80-7273-163-3.
- KUČEROVÁ, A. a kol. *Zákon o ochraně osobních údajů: komentář*. 1. vyd. Praha: C.H. Beck, 2012. 516 s. ISBN 978-807-1792-260.
- KUNER, CH. *European data privacy law and online business*. Oxford: University Press, 2003. 72 s. ISBN 978-0-19-928385-9.

- LAZAR, J. a kol. *Občianske právo hmotné*. I. diel. Bratislava: Iura Edition, 2010. 715 s. ISBN 978-808078-346-4.
- MATEJKA, J. *Internet jako objekt práva: Hledání rovnováhy autonomie a soukromí*. 1. vyd. Praha: CZ.NIC, 2013. 256 s. ISBN 978-80-904248-7-6.
- MATES, P. *Ochrana osobních údajů*. 1. vyd. Praha: Karolinum, 2002. 73 s. ISBN 80-246-0469-8.
- MATES, P. *Ochrana soukromí ve správním právu*. 2. vyd. Praha: Linde, 2006. 320 s. ISBN 80-720-1589-3.
- MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2. aktual. a dopl. vyd. Praha: ASPI, Wolters Kluwer, 2008. 468 s. ISBN 978-80-7357-322-5.
- MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013. 436 s. ISBN 978-80-7478-139-1.
- MORÁVEK, J. *Ochrana osobních údajů v pracovněprávní agendě*. Praha: BMSS Start, 2010, 143 s. ISBN 978-80-86140-64-3.
- MOSNÝ, P. a kol. *Právněhistorická realita sociálnej doktríny 20. storočia*. Kraków: Spolek Slovákov v Poľsku-Towarzystwo Słowaków w Polsce, 2014. 336 s. ISBN 978-83-7490-742-2.
- ONDŘEJEK, P. *Princip proporcionality a jeho role při interpretaci základních práv a svobod*. Praha: Leges, 2012. 224 s. ISBN 978-80-87576-31-1.
- PAVLÍČEK, V. a kol. *Ústava a ústavní řád České republiky: komentář*. 2. vyd. Praha: Linde, 1999. 975 s. ISBN 80-720-1170-7.
- PROST, A., VINCENT, G. *History of Private Life Volume V: Riddles of Identity in Modern Times*. Cambridge: Harvard University Press, 1991, s. 31-36.
- SVÁK, J. *Ochrana ľudských práv. Z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práv*. 2. rozšírené vydanie. Bratislava: Eurokódex, 2006. 1116 s. ISBN 80-88931-51-7.
- ŠTURMA, P. *Mezinárodní a evropské kontrolní mechanismy v oblasti lidských práv*, 3. vydanie, Praha: C. H. Beck, 2011. 184 s. ISBN 978-80-7400-318-9.
- VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J. *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013. 351 s. ISBN 978-80-971476-4-8.
- VETERNÍKOVÁ, M. *Právna ochrana osobnosti*. Bratislava: Procom, 2003. 160 s. ISBN 80-85717-12-3.
- VOJČÍK, P. a kol. *Občiansky zákonník. Stručný komentár*. Bratislava: Iura Edition, 2008. 1218 s. ISBN 978-80-8078-183-5.

Články v časopisoch a zborníkoch

- BARANCOVÁ, H. Monitorovanie zamestnancov a ochrana súkromného života v judikatúre európskych súdov. In BARANCOVÁ, H. a kol. *Monitorovanie zamestnancov a právo na súkromný život*. Bratislava: Sprint dva, 2010. 192 s. ISBN 978-80-89393-43-5, s. 11 – 37.
- BARTÍK, V., JANEČKOVÁ, E. Kamery se záznamovým zařízením na pracovišti. In: *Práce a mzda*, ISSN 0032-6208. 2010, roč. 58, č. 3, s. 29 – 33
- DWORKIN, R. Law as Interpretation. In *Texas Law Review*, vol. 60, 1981 – 1982, p. 527 – 550.
- FOLDOVÁ, V., NONNEMANN, F. Zverejňovanie platů zamestnanců veřejné sféry ve světle

- aktuálneho rozsudku Nejvyššího správního soudu. In: *Právní rozhledy*, 2015, č. 2, s. 63 – 70.
- FORD, M. Two conceptions of Worker Privacy. In: *Industrial Law Journal*, 2002, vol. 31, no. 2, p. 135 – 155.
- CHLÁDKOVÁ, A. Osobní spis zaměstnance. In: *Personální a sociálně právní kartotéka*. 2008, roč. 11, č. 6, s. 4 – 7.
- JAKUBKA, J. Ochrana osobních a osobnostních práv zaměstnanců, 1. část. In: *Práce a mzda*, 2005, roč. 53, č. 12, s. XX.
- JAKUBKA, J. Ochrana osobních a osobnostních práv zaměstnanců, 2. část. In: *Práce a mzda*, ISSN 0032-6208. 2005, roč. 53, č. 13, s. XX.
- KOVALČÍKOVÁ, M. Ochrana osobných údajov v súvislosti s monitorovaním zamestnancov. In: BARANCOVÁ, H. a kol. *Monitorovanie zamestnancov a právo na súkromný život*, Bratislava: Sprint dva, 2010. 192 s. ISBN 978-80-89393-43-5. s. 96-98.
- MORÁVEK, J. Možnosti monitorování zaměstnanců na pracovišti v právním řádu České republiky. In: BARANCOVÁ, H. a kol. *Monitorovanie zamestnancov a právo na súkromný život*, Bratislava: Sprint dva, 2010. 192 s. ISBN 978-80-89393-43-5. s. 38-68.
- MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. In: *Právní rozhledy*. ISSN 1210-6410. 2012, roč. 20, č. 5, s. 175 – 181.
- NONNEMANN, F. Náležitosti souhlasu se zpracováním osobních údajů. In: *Právní rozhledy*. ISSN 1210-6410. 2011, roč. 19, č. 14, s. 520 – 522.
- OLEXOVÁ, C. Využitie internetových sociálnych sietí na získavanie a výber zamestnancov. In: *Personálny a mzdový poradca podnikateľa*. ISSN 1335-1508, 2010, č. 15.
- ŠTEFKO, M. Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochrane lidských práv a základních svobod. In: *Jurisprudence*, 2012, č. 7/8, s. 17 – 21.
- TELEC, I. Chráněné statky osobnostní. In: *Právní rozhledy*. ISSN 1210-6410, 2007, roč. 15, č. 8, s. 271 – 281.
- TROJAN, J. Ochrana základných práv a slobôd osôb pred uzatvorením pracovnej zmluvy pri výkone práce vo verejnom záujme. In: *Teória a prax verejnej správy*. Košice: Univerzita P. J. Šafárika v Košiciach, 2004. ISBN 80-7097-595-4 , 421 s.

Vedecko-kvalifikačné práce

- KOVALČÍKOVÁ, M. *Realizácia osobnostných práv pri výkone závislej práce: dizertačná práca*. Košice: Právnická fakulta Univerzity P. J. Šafárika v Košiciach, 2012. 228 s.
- LORY, B., *Employer Use of Facebook as a Tool in Pre-Employment Screening of Applicants: Benefits and Ethical, Legal, and Privacy Implications: Master of Arts in Organizational Leadership Theses*. St. Paul (Minnesota, USA): St. Catherine University, 2011. 157 s.

Elektronické dokumenty

- BERECZ, A. *Boj so zdegenerovanou komunikáciou: Firma ľuďom zatrhla e-maily*. (online). 2014. (cit. 2014-12-02). Dostupné z: (<http://podnikanie.etrend.sk/podnikanie-riadenie/boj-so-zdegenerovanou-komunikaciou-firma-ludom-zatrhla-e-maily.html>).
- COHEN, C. F., COHEN, M. E. On-duty and Off-duty: Employee Right to Privacy and Employer's Right to Control the Private Sector. In *Employee Responsibilities and Rights*

- Journal*, 11/2007, p. 235-246. (online). 2007. (cit. 2015-01-26). Dostupné z: (http://www.researchgate.net/publication/225629872_On-duty_and_Off-duty_Employee_Right_to_Privacy_and_Employers_Right_to_Control_in_the_Private_Sector).
- EDPS, *European data protection supervisor video-surveillance guidelines*. (online). 2010, (cit. 2015-01-10). Dostupné z: (https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf).
- Európska komisia. Tlačová správa: *Komisia navrhuje komplexnú reformu pravidiel ochrany údajov na posilnenie kontroly používateľov nad ich údajmi a na zníženie nákladov pre podniky*. (online). 2012. (cit. 2015-03-18). Dostupné z: (http://europa.eu/rapid/press-release_IP-12-46_sk.htm).
- HRADILOVÁ, J. *Ochrana osobných údajů v Evropské unii*. Ikaros (online). 2008, roč. 12, č. 2. (cit. 2014-12-18). Dostupné z: (<http://www.ikaros.cz/ochrana-osobnich-udaju-v-evropske-unii>).
- HVOZDOVIČOVÁ, J. *Sledovanie v práci je na dennom poriadku*. Sme (online). 2011. (cit. 2015-02-10). Dostupné z: (<http://ekonomika.sme.sk/c/6129902/sledovanie-v-praci-je-na-dennom-poriadku.html#ixzz1dEZACiRX>).
- OLŠOVSKÁ, A. *Skončenie pracovného pomeru z dôvodu porušenia pracovnej disciplíny*. e-pravo (online). 2014. (cit. 2015-03-09). Dostupné z: (<http://www.epravo.sk/top/clanky/skoncenie-pracovneho-pomeru-z-dvodu-porusenia-pracovnej-discipliny-1796.html>).
- Opinion of the European Data Protection Supervisor on the data protection reform package*. (online). Brusel: EDPS. 2012. (cit. 2014-12-07). Dostupné z: (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf).
- Pracovný dokument útvarov Komisie. Zhrnutie posúdenia vplyvu*. (online). Brusel: Európska komisia. 2012. (cit. 2014-12-07). Dostupné z: (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2012:0073:FIN:SK:PDF>).
- REICHERTS, M. *The right to be forgotten and the EU data protection reform: Why we must see through a distorted debate and adopt strong new rules soon*. (online). 2014. (cit. 2014-12-07). Dostupné z: (http://europa.eu/rapid/press-release_SPEECH-14-568_en.htm).
- SLUK, M. *Ochrana osobnosti. Judikatúra Najvyššieho súdu Slovenskej republiky*. (online). JA SR. 2014. (cit. 15.9.2014). Dostupné z: (http://www.ja-sr.sk/files/Ochrana_osobnosti_judikatúra_NS_SR.pdf).
- Správa FRA. *Prístup k prostriedkom nápravy v oblasti ochrany údajov v členských štátoch EÚ – zhrnutie*. (online). Viedeň: FRA, 2013, 11 s. (cit. 2015-01-18). Dostupné z: (http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_sk.pdf).
- Stanovisko FRA č. 2/2012. *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*. (online). Viedeň: FRA, 2012. 34 s. (cit. 2015-01-18). Dostupné z: (<http://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf>).
- Stanovisko Spolkovej rady SRN*. (online). 2014. (cit. 2014-12-07). Dostupné z: (http://www.europarl.europa.eu/RegData/commissions/juri/communication/2012/487796/JURI_CM%282012%29487796_CS.pdf).
- Tlačová správa. *Giovanni Buttarelli named new data protection watchdog*. (online). 2014. (cit.

- 2015-01-01). Dostupné z (<http://www.europarl.europa.eu/news/en/news-room/content/20141127IPR81016/html/Giovanni-Buttarelli-named-new-data-protection-watch-dog>).
- TOWNS, D. M., COBB, L. M. Notes on: GPS technology; Employee monitoring enters a new area. In *Labor Law Journal*, vol. 63, issue 3, p. 203-208. (online). 2012. (cit. 2015-01-30). Dostupné z: (<http://connection.ebscohost.com/c/articles/80170931/notes-on-gps-technology-employee-monitoring-enters-new-era>).
- TVARDZIK, J. *Facebook prekonal miliardu užívateľov*. In: TECHSme.sk. (online). 2012. (cit. 2014-11-27). Dostupné z: (<http://tech.sme.sk/c/6556489/facebook-prekonal-miliardu-uzivatelov.html>).
- ÚOOÚ, Správa o stave ochrany osobných údajov za roky 2011 a 2012. (online). 2013. (cit. 2015-01-30). Dostupné z: (https://dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_roky_2011_a_2012.pdf).
- ÚOOÚ, Zásady pri spracúvaní osobných údajov. (online). Dostupné z: (<https://dataprotection.gov.sk/uouu/sk/content/zasady-pri-spracuvani-osobnych-udajov>).
- ÚOOÚ, Vyjadrenie k žiadosti z 24. júna 2009. (online). Dostupné z: (<http://www.biometric.sk/prospekt/Vyjadrenie-k-biometrickej-dochadzke.pdf>).
- VOBOŘIL, J. *Jaké budou dopady zrušení směrnice o data retention?* (online). 2014. (cit. 2014-12-17). Dostupné z: (<http://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html>).
- WARREN, D. S., BRANDEIS, L. D. The Right to Privacy. In *Harvard Law Review*, 1890, vol. 4, no. 5. (online). (cit. 2014-12-13). Dostupné z: (<http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>).
- WISSKIRCHEN, G. Background Checks in Europe. In *Labour and Employment*. (online). 2011. (cit. 2014-01-03). Dostupné z (<http://whoswholegal.com/news/features/article/29116/background-checks-europe>).

Dokumenty Úradu na ochranu osobných údajov Slovenskej republiky a Úradu na ochranu osobných údajů České republiky a Pracovnej skupiny 29

- ÚOOÚ, Metodické usmernenie č. 1/2013 k pojmu osobné údaje z 1. júla 2013.
- ÚOOÚ, Metodické usmernenie č. 2/2013 k základným pojmom – osoby pri spracúvaní osobných údajov z 1. júla 2013.
- ÚOOÚ, Metodické usmernenie č. 3/2014 k účelu spracúvania osobných údajov z 30. decembra 2014.
- Stanovisko ÚOOÚ ČR č. 2/2008 – Souhlas se zpracováním osobních údajů.
- Stanovisko ÚOOÚ ČR, č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.
- ÚOOÚ ČR k problémům z praxe č. 3/2010 – K použití fotografie, obrazového a zvukového záznamu fyzické osoby.
- Z rozhodovacej činnosti ÚOOÚ ČR ke spracovaniu osobných údajů uchazečů o zaměstnání, č. j. SKO-0629/07.
- Stanovisko Pracovnej skupiny 29 č. 8/2001 k spracúvaniu osobných údajov v rámci pracovného pomeru z 13. septembra 2001, WP 48.
- Stanovisko Pracovnej skupiny 29 č. 2/2006, ktoré sa zaoberá problematikou ochrany súkro-

mia v kontexte poskytovania služieb spočívajúcich v skríningu elektronickej pošty z 21. februára 2006, WP 118.

Stanovisko Pracovnej skupiny 29 č. 15/2011 k definícii súhlasu z 13. júla 2011, WP 187.

Stanovisko Pracovnej skupiny 29 č. 13/2011 ku geolokačným službám inteligentných mobilných zariadení zo 16. mája 2011, WP 185.

Stanovisko Pracovnej skupiny 29 č. 3/2012 k vývoju v oblasti biometrických technológií z 27. apríla 2012, WP 193.

Rozhodnutia Európskeho súdu pre ľudské práva

Rozsudok ESELP zo 16. februára 2000 v právnej veci Amann v. Švajčiarsko, sťažnosť č. 27798/95

Rozsudok ESELP z 3. apríla 2007 v právnej veci Copland v. Spojené kráľovstvo, sťažnosť č. 62617/00

Rozhodnutie ESELP z 11. júla 2002 v právnej veci Goodwin v. Spojené kráľovstvo, sťažnosť č. 28957/95

Rozsudok ESELP z 25. júna 1997 v právnej veci Halford v. Spojené kráľovstvo, sťažnosť č. 20605/92

Rozsudok ESELP zo 6. septembra 1978 v právnej veci Klass a ostatní v. Spolková republika Nemecko, sťažnosť č. 5029/71, § 55

Rozsudok ESELP z 24. apríla 1990 v právnej veci Krusslin v. Francúzsko, sťažnosť č. 11801/85

Rozsudok ESELP z 26. marca 1987 v právnej veci Leander v. Švédsko, sťažnosť č. 9248/81

Rozsudok ESELP z 2. augusta 1984 v právnej veci Malone v. Spojené kráľovstvo, sťažnosť č. 8691/79, § 68

Rozsudok ESELP zo 14. novembra 2002 v právnej veci Mouisel v. Francúzsko, sťažnosť č. 67263/01

Rozsudok ESELP zo 16. decembra 1992 v právnej veci Niemietz v. Nemecko, sťažnosť č. 13710/88

Rozsudok ESELP z 26. júla 2007 v právnej veci Peev v. Bulharsko, sťažnosť č. 64209/01

Rozsudok ESELP zo 17. júla 2003 v právnej veci Perry v. Spojené kráľovstvo, sťažnosť č. 63737/00

Rozsudok ESELP zo 4. mája 2000 v právnej veci Rotaru v. Rumunsko, sťažnosť č. 28341/95

Rozsudok ESELP zo 6. apríla 2000 v právnej veci Thlimmenos v. Grécko, sťažnosť č. 34369/97, § 41

Rozsudok ESELP z 2. septembra 2010 v právnej veci Uzun v. Nemecko, sťažnosť č. 35623/05

Rozsudok ESELP z 25. októbra 2007 v právnej veci Van Vondel v. Holandsko, sťažnosť č. 38258/03

Rozsudok ESELP z 26. marca 1985 v právnej veci X. a Y. v. Holandsko, sťažnosť č. 8978/80

Rozhodnutia Súdneho dvora Európskej únie

Rozhodnutie SD EÚ zo 6. novembra 2003 v právnej veci Bodil Lindqvist, vec C-101/01

Rozhodnutie SD EÚ z 8. apríla 2014 v spojených právnych veciach Digital Rights Ireland Ltd. a Kärntner Landesregierung, veci C-293/12 a C-594/12

Rozhodnutie SD EÚ z 8. novembra 1990 v právnej veci Dekker v. Stichting Vormingscen-

- trum voor Jong Volwassennen Plus, vec C-177/88
Rozhodnutie SD EÚ z 11. decembra 2014 v právnej veci František Ryněš v. Úřad pro ochranu osobních údajů České republiky, vec C-212/13
Rozhodnutie SD EÚ z 20. mája 2003 v spojených právnych veciach Österreichischer Rundfunk, veci C-465/00, C-38/01 a C-139/01
Rozhodnutie SD EÚ z 3. februára 2000 v právnej veci Silke-Karin Mahlburg v. Land Mecklenburg-Vorpommern, vec C-207/98
Rozhodnutie SD EÚ z 9. novembra 2010 v spojených právnych veciach Volker und Markus Schecke GbR a Hartmut Eifert v. Hessensko, veci C-92/09, C-93/09

Rozhodnutia všeobecných a ústavných súdov v Slovenskej republike a Českej republike

- Rozhodnutie Najvyššieho súdu Slovenskej republiky z 25. novembra 2009 sp. zn. 6 Sžo 250/2008
Rozhodnutie Najvyššieho súdu Slovenskej republiky z 30. júna 2011 sp. zn. 5 Sži 2/2010
Rozhodnutie Najvyššieho súdu Slovenskej republiky z 12. júla 2011 sp. zn. 1 Sžo 410/2009
Rozhodnutie Najvyššieho súdu Slovenskej republiky z 19. decembra 2012 sp. zn. 2 Sžo 12/2012
Rozhodnutie Najvyššieho súdu Slovenskej republiky z 19. mája 2010 sp. zn. 5 Cdo 108/2009
Rozhodnutie Najvyššieho súdu Slovenskej republiky z 26. septembra 2013 sp. zn. 3 Cdo 228/2012
Rozhodnutie Najvyššieho súdu Slovenskej republiky z 24. septembra 2014 sp. zn. 5 Cdo 248/2013
Rozhodnutie Krajského súdu v Bratislave z 15. februára 2006 sp. zn. 2S 94/05
Rozhodnutie Krajského súdu v Bratislave zo 16. januára 2013 sp. zn. 4 CoPr 1/2012, 4 CoPr 2/2012
Nález Ústavného súdu Slovenskej republiky z 29. novembra 1995 sp. zn. I. ÚS 33/95
Nález Ústavného súdu Slovenskej republiky z 27. februára 1997 sp. zn. PL. ÚS 7/96
Nález Ústavného súdu Slovenskej republiky zo 14. júna 2006 sp. zn. I. ÚS 274/05
Nález Ústavného súdu Slovenskej republiky zo 4. februára 2009 sp. zn. I. ÚS 117/07
Nález Ústavného súdu Slovenskej republiky z 19. januára 2011 sp. zn. PL. ÚS 1/09
Uznesenie Ústavného súdu Slovenskej republiky z 10. septembra 2009 sp. zn. II. ÚS 280/09-16
Rozhodnutie Nejvyššího soudu České republiky zo 16. augusta 2012 sp. zn. č. 21 Cdo 1771/2011
Rozhodnutie Nejvyššího správního soudu České republiky z 12. februára 2009 sp. zn. 9 As 34/2008
Rozhodnutie Ústavního soudu České republiky z 8. februára 2000 sp. zn. I. ÚS. 452/09
Rozhodnutie Ústavního soudu České republiky zo 7. novembra 2012 sp. zn. I. ÚS. 3933/12

PRÍLOHY

Tabuľka č. 1. Vzťah základných právnych predpisov k ochrane súkromia a osobných údajov

Porovnávané právne predpisy	LEX GENERALIS	LEX SPECIALIS
OZ a ZP	OZ	ZP
OZ a ZOOÚ	OZ	ZOOÚ
ZP a ZOOÚ	ZOOÚ	ZP

Tabuľka č. 2. Prehľad vybraných evidenčných činností zamestnávateľov spracúvajúcich osobné údaje

Názov evidencie	Zákon	Ustanovenie
Osobný spis	z. č. 311/2001 Z. z. Zákonník práce	§ 75 ods. 1
Evidencia dochádzky (prac. čas, práca nadčas, nočná práca, prac. pohotovosť)	z. č. 311/2001 Z. z. Zákonník práce	§ 99
Evidencia vyúčtovanej mzdy	z. č. 311/2001 Z. z. Zákonník práce	§ 130 ods. 5
Mzdové listy na účely dane z príjmu fyzických osôb zo závislej činnosti	z. č. 595/2003 Z. z. o dani z príjmov	§ 39 ods. 1
Evidencia skutočností oznamovaných zdravotnej poisťovni	z. č. 580/2004 Z. z. o zdravotnom poistení	§ 24 písm. e/
Evidencia skutočností na účely sociálneho poistenia a starobného dôchodkového sporenia	z. č. 461/2003 Z. z. o sociálnom poistení	§ 232 ods. 1
Evidenčný list dôchodkového zabezpečenia	z. č. 461/2003 Z. z. o sociálnom poistení	§ 290 ods. 1
Evidencia pracovných úrazov („kniha úrazov“)	z. č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci	§ 17 ods. 8
Evidencia zamestnancov, ohrozených/ s priznanou chorobou z povolania	z. č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci	§ 17 ods. 8
Evidencia zamestnancov v súvislosti s bezpečnosťou a ochranou zdravia pri práci	z. č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci	§ 6 ods. 1 písm. n/
Evidencia zamestnancov vykonávajúcich rizikové práce	z. č. 126/2006 Z. z. o verejnom zdravotníctve a o zmene a doplnení niektorých zákonov	§ 20 ods. 8
Evidencia osôb oprávnených oboznamovať sa s utajovanými skutočnosťami	z. č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov	§ 42

O AUTORKE

JUDr. Katarína Siskovičová PhD. vyštudovala právo na Právnickej fakulte Trnavskej Univerzity v Trnave. V roku 2011 obhájila svoju diplomovú prácu na tému *Domáce väzenie – trestnoprávne a kriminologické aspekty* a v roku 2013 svoju rigoróznou prácu na tému *Exekučné tituly na území Slovenska v období prvej ČSR a v súčasnosti..* V roku 2015 ukončila doktorandské štúdium na Právnickej fakulte Trnavskej univerzity v Trnave v študijnom odbore pracovné právo obhajobou dizertačnej práce na tému *Ochrana súkromia a osobných údajov zamestnanca*. Autorka v súčasnosti pôsobí ako asistent sudcu na Najvyššom súde Slovenskej republiky.

JUDr. KATARÍNA SISKOVIČOVÁ, PhD.

**OCHRANA SÚKROMIA
A OSOBNÝCH ÚDAJOV
ZAMESTNANCA**

Zodpovedný redaktor Jozef Molitor
Grafická úprava a zalomenie Jana Janíková
Obálka Marek Petržalka

Vydalo vydavateľstvo TYPUS UNIVERSITATIS TYRNAVENSIS,
spoločné pracovisko Trnavskej univerzity v Trnave
a VEDY, vydavateľstva Slovenskej akadémie vied, v roku 2015
ako 181. publikáciu.
Vytlačila VEDA, vydavateľstvo SAV.

ISBN 978-80-8082-932-2