

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH
STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE**

BAKALÁŘSKÁ PRÁCE

2011

LIBOR ŠINDLER

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH
STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE**

BAKALÁŘSKÁ PRÁCE

**ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ PŘI JEJICH
ZPRACOVÁNÍ POLICIÍ ČESKÉ REPUBLIKY**

Autor práce: Libor Šindler

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: kombinovaná

Vedoucí práce: Mgr. Jan Vágner

Katedra: Katedra právních oborů a bezpečnostních studií

2011

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Poděkování

Děkuji vedoucímu bakalářské práce Mgr. Janu Vágnerovi za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

ŠINDLER, L. *Zabezpečení osobních údajů při jejich zpracování Policií České republiky : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2011. 71 s. Vedoucí bakalářské práce : Mgr. Jan Vágner.

Klíčová slova: osobní údaj, citlivý údaj, zpracování osobních údajů, souhlas se zpracováním, výjimky pro zpracování osobních údajů bez souhlasu subjektu údajů, správce a zpracovatel osobních údajů, povinnosti správce a zpracovatele osobních údajů, ochrana osobních údajů, bezpečnostní opatření přijímaná správcem a zpracovatelem osobních údajů, bezpečnostní opatření při automatizovaném zpracování.

Práce pojednává o problematice zpracování osobních údajů v rámci Policie České republiky při plnění úkolů policie v souvislosti s celou řadou policejních činností, např. při zjišťování totožnosti osob, vedení policejních evidencí, zpracování spisů, výměně informací a osobních údajů s jinými orgány, zveřejňování osobních údajů, pátrání po hledaných a pohřešovaných osobách nebo při monitorování prostranství. Se zaměřením na praxeologické využití se zabývá zabezpečením osobních údajů, riziky, která musí správce a zpracovatel v rámci přijetí opatření k ochraně osobních údajů posuzovat. Specifikuje povinnosti správce a zpracovatele při zabezpečení osobních údajů v oblasti automatizovaného zpracování osobních údajů. Shrnuje opatření na úseku personální bezpečnosti, objektové bezpečnosti, bezpečnosti informačních a komunikačních technologií a bezpečnosti dat. Analyzuje zjištěná pochybení příslušníků Policie ČR v souvislosti se zpracováním osobních údajů. V závěru práce řeší kamerové systémy provozované Policií České republiky z pohledu ochrany osobních údajů a jejich přínosu pro plnění úkolů policie.

ABSTRACT

ŠINDLER, L. *Securing personal data while being processed by the Czech Police* : *bachelors dissertation*. České Budějovice : Vysoká škola evropských a regionálních studií, o.p.s. (College of European and Regional Studies), 2011. 71 p. Supervisor : Mgr. Jan Vágner.

Key words: personal data, sensitive data, personal data processing, agreement with the processing, exceptions to personal data processing without the data subjects' agreement, personal data administrator and processor, obligations of the personal data administrator and processor, personal data protection, security measures adopted by the personal data administrator and processor, security measures in automated processing.

The paper deals with the issue of personal data processing within the framework of Czech Police while carrying out police tasks in connection with a number of police activities, such as finding out the identities of persons, keeping police evidence, processing the files, exchanging information and personal data with other authorities, publishing personal data, searching for wanted and missing persons, and monitoring the area. With a focus on practical usage, it deals with personal data protection, risks that the administrator and processor must evaluate while adopting the measures to protect personal data. It specifies the obligations of the administrator and processor while securing personal data in the field of automated personal data processing. It sums up measures in the field of personal security, object security, security of information and communication technologies, and data security. It analyses recognized offences of the Czech Police members in connection with personal data processing. In the end, the paper deals with camera systems run by the Czech Police from the point of view of personal data protection and their benefits for fulfilling the police task.

OBSAH

ÚVOD	8
1 CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE	10
2 DEFINICE ZÁKLADNÍCH POJMŮ	11
2.1 Pojem osobní údaj.	11
2.2 Pojem citlivý údaj.	12
2.3 Pojem zpracování osobních údajů.	13
2.4 Pojem subjekt údajů.	14
2.5 Pojem správce údajů.	14
2.6 Pojem zpracovatel údajů.	15
3 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ POLICIÍ ČESKÉ REPUBLIKY	17
3.1 Obecná ustanovení o zpracování informací policií.	17
3.2 Podání vysvětlení.	18
3.3 Pořizování záznamů.	20
3.4 Prokázání totožnosti.	21
3.5 Získávání osobních údajů pro účely budoucí identifikace.	23
3.6 Získávání informací z evidencí (předávání osobních údajů Policii ČR).	25
3.7 Získávání informací v souvislosti s odhalováním a šetřením přestupků	27
3.8 Pátrání po osobách a věcech.	29
3.9 Získávání poznatků o trestné činnosti.	31
3.10 Předávání informací.	32
3.11 Zvláštní ustanovení o zpracování osobních údajů policií.	32
3.12 Předávání nebo zpřístupňování osobních údajů.	33
3.13 Zveřejňování osobních údajů.	36
3.14 Prověřování potřebnosti dalšího zpracování osobních údajů.	36
3.15 Informování o osobních údajích a oprava nepravdivých nebo nepřesných osobních údajů.....	37
3.15.1 Postup při přijetí žádosti týkající se informace o zpracování osobních údajů Policií České republiky	39
3.16 Zpracování údajů v Schengenském informačním systému.	40
3.16.1 Právní podklad existence SIS.....	42

3.16.2 Schengenský informační systém	42
3.16.3 Obsah Schengenského informačního systému	43
3.16.4 Zdrojové informační systémy – N. SIS České republiky	44
3.17 Zpracování osobních údajů při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů a zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti.	45
4 RIZIKA POSUZOVANÁ SPRÁVCEM A ZPRACOVATELEM V RÁMCI PŘIJETÍ OPATŘENÍ K OCHRANĚ OSOBNÍCH ÚDAJŮ	48
5 OPATŘENÍ PŘI ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V SCHENGENSKÉM INFORMAČNÍM SYSTÉMU	50
6 POVINNOSTI SPRÁVCE A ZPRACOVATELE PŘI ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V OBLASTI AUTOMATIZOVANÉHO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	52
7 POCHYBENÍ PŘÍSLUŠNÍKŮ POLICIE ČR V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ	54
7.1 Profesní pochybení příslušníků Policie ČR v souvislosti se zpracováním osobních údajů zjištěná ÚVK Policejního prezidia ČR.....	54
7.2 Profesní pochybení příslušníků Policie ČR v souvislosti se zpracováním osobních údajů: zdroje informací mimo resort MV.....	56
8 MĚSTSKÉ KAMEROVÉ SYSTÉMY.....	58
8.1 Obecný úvod do problematiky používání kamerových systémů v Policii ČR z pohledu ochrany osobních údajů	58
8.2 Základní principy provozu městského kamerového dohlížecího systému.....	59
8.3 Využívání městských kamerových dohlížecích systémů Policií České republiky...60	
8.4 Městský kamerový systém hlavního města Prahy využívaný policisty Krajského ředitelství policie hl. m. Prahy	62
8.5 Konkrétní příklady přínosu MKS při plnění úkolů policie útvaru Integrované operační středisko KŘP hl. m. Prahy OŘ Praha II.....	63
ZÁVĚR	66
SEZNAM POUŽITÝCH ZDROJŮ	68
PŘÍLOHY	72

ÚVOD

Osobní údaje jsou fenoménem, který občany civilizované společnosti provází od okamžiku narození až do smrti. Nejprve je naše existence stvrzena zápisem do matriky, přidělením rodného čísla, přihlášením do evidence pobytu. V průběhu let přibývají údaje např. o vzdělání, o zdravotním stavu, o pracovních aktivitách, o uzavření manželství, o narození dětí... V praktickém životě občan zpravidla velmi pečlivě zvažuje, co by jiní lidé o něm měli znát a co by jim naopak mělo být utajeno. Ostatní osoby, jimiž jsme obklopeni, rozlišujeme také podle toho, jaké informace o nás bychom jim byli ochotni poskytnout a jaké jejich otázky by již tuto hranici překročily. Současně si však určité informace o lidech kolem nás uchováváme. Obdobně, avšak ve formě sofistikovanější a ucelenější, toto provádějí různé instituce, s nimiž spojujeme svůj život (např. peněžní nebo pojišťovací ústavy), zaměstnavatelé a v míře největší pak stát.

V rámci každé společnosti jsou skupiny osob, které těžce nesou, pokud je jejich dosavadní volnost jednání omezoována právním předpisem, avšak nutno konstatovat, že s rozvojem civilizace právem nedotčených oblastí neustále ubývá. Hromadné nasazování výpočetní techniky a elektronických komunikací velmi dramaticky zvýšilo rizika zpracování osobních údajů vůči soukromým sféram jedinců. Hromadný sběr dat je v dnešní době oblíbený a často používaný způsob, jak zjistit velmi cenné informace. Extrémní zvýšení zájmu o implementaci bezpečnostních technologií a monitorování občanů v globálním měřítku je spojeno s datem 11. září 2001.¹ Pod záštitou bezpečnosti lidstva se začaly ve velkém měřítku vytvářet integrované databáze údajů, schvalovaly se výjimky ze zákonů o ochraně osobních údajů a vznikaly nové kompetence zpravodajských služeb. Právě z rozvoje moderních technologií vyplývají největší problémy spojené s ochranou osobních údajů a soukromí.

V rámci Evropské unie jsou v současné době vedeny diskuze nejen o reformě zpracování osobních údajů v tzv. III. pilíři (v souvislosti s bezpečnostní agendou), ale i o novelizaci základního dokumentu, kterým je Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a jejich volným pohybem. Z uvedeného základního dokumentu vychází i český zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který je třeba vždy citovat s přídomkem „ve znění pozdějších předpisů“. Citovaný zákon byl totiž za svoji z historického hlediska krátkou dobu existence již více než

¹ Uvedeného dne došlo k teroristickému útoku na věžové domy World Trade Centra v New Yorku (USA), čímž byl spuštěn boj proti terorismu v globálním měřítku.

desetkrát dílčím způsobem novelizován a jeho další novelizace možno tušit již za blízkým horizontem.² V této souvislosti je třeba uvést, že ke změnám v legislativě týkající se ochrany osobních údajů bude docházet i nadále, a to v důsledku společenského vývoje a pokroku technologií.

Technologickému pokroku v podobě zavádění výpočetní techniky do každodenní praxe se nemohla vyhnout ani instituce, kterou je Policie České republiky. Dnes si již plnění úkolů policie bez možnosti využívání informačních technologií, různých evidencí, databází a elektronické komunikace ani nedokážeme představit. Policie České republiky je subjektem, který je při plnění svých zákonných úkolů oprávněn nakládat s osobními údaji, včetně údajů citlivých. Otázce shromažďování a zpracovávání osobních údajů by měla být věnována patřičná pozornost, jelikož nezákonným nakládáním s těmito údaji může dojít k citelnému zásahu do soukromého života jednotlivce, do jeho ústavně zaručených práv. V minulosti docházelo k porušování právních předpisů z oblasti ochrany osobních údajů příslušníky Policie ČR. Uvedené potvrzuje řada správních řízení, která Úřad pro ochranu osobních údajů vedl či zahájil s Českou republikou, zastoupenou Ministerstvem vnitra (ve věcech týkajících se Policie ČR jedná jménem České republiky Ministerstvo vnitra). Z rozhodnutí, které úřad vydal, vyplývá, že Policie ČR nejčastěji porušuje povinnosti vyplývající z § 13 odst. 1 zákona č. 101/2000 Sb. Dle tohoto ustanovení „správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů³“. Aktuálnost tématu potvrzuje důrazná apelace Odboru bezpečnostní politiky Ministerstva vnitra ČR na všechny zainteresované subjekty, aby oblasti ochrany osobních údajů věnovaly zvýšenou pozornost, aby byly důsledně plněny všechny povinnosti vyplývající z právních předpisů tak, aby Úřad pro ochranu osobních údajů neměl jakýkoliv důvod zahájit s Ministerstvem vnitra správní řízení pro podezření ze spáchání správního deliktu v souvislosti s nakládáním s osobními údaji.⁴

² MAŠTALKA, J. *Osobní údaje, právo a my*. 1. vyd. C. H. Beck Praha, 2008, s. VI.

³ Ustanovení § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

⁴ Stanovisko OBP MV ČR k ochraně osobních údajů OU/2006. Dostupný z Intranetu MV WWW: <<http://ppportal.pcr.cz/kancelar/skou/skou.asp>>

1 CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE

Hlavním cílem bakalářské práce bude pomocí metody abstrakce, která umožňuje proniknout do jevu a vyčlenit jeho podstatné vlastnosti popsat a objasnit specifiku ochrany osobních údajů při jejich zpracování Policií České republiky a konkrétní způsoby zabezpečení osobních údajů při jejich zpracování. Vedlejším cílem bude metodou generalizace (zobecnění) umožnit praxeologického využití práce. Autor této práce má prokázat schopnost samostatně využívat teoretické poznatky získané během studia na vysoké škole a aplikovat je při řešení konkrétního úkolu v oboru své specializace. To znamená, systematicky pracovat s prameny a databázemi, znát dostupnou odbornou literaturu a badatelsky ji využívat, získat přehled v problematice ochrany osobních údajů při jejich zpracování Policií České republiky. Práce by měla kriticky posoudit danou problematiku a vyhodnotit ji, vystihnout klíčové momenty problematiky a aktuální potřeby praxe. Kvantitativní vymezení rozsahu práce má přímou návaznost na samotný název práce, tedy řeší problematiku ochrany osobních údajů při jejich zpracování příslušníky a zaměstnanci Policie České republiky. Práce má vztahy mezi jevy objasňovat, vysvětlovat je i na základě různých teorií, systemizovat je a komentovat na základě svých zkušeností a znalostí, propojit teorii s praxí.

Výsledkem by měl být ucelený a obsahově vyvážený odborný text s jasnou strukturou práce, který předkládá přehledně a výstižně důležité prvky problematiky, a to text slohově vytříbený, s náležitou jazykovou úrovní a adekvátní grafickou úpravou práce.

2 DEFINICE ZÁKLADNÍCH POJMŮ

2.1 Pojem osobní údaj

V rámci respektování systematiky zákona o ochraně osobních údajů je potřebné nejprve vysvětlit pojem osobní údaj. Pro účely zákona o ochraně osobních údajů se rozumí „osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“⁵

Co je to určenost, popřípadě určitelnost? Určení konkrétní osoby lze definovat jako odlišení příslušné osoby od jiných, avšak tato odlučitelnost musí mít určitou konkrétní kvalitu. K naplnění konkrétní identifikovanosti je třeba, aby osoba byla jednoznačně odlišená od všech dalších do té míry, že je vyhledatelná. Základní identifikátory lze rozdělit na:

- ty, které nám byly přiděleny pro obecnou identifikaci (jméno a příjmení),
- ty, které nám byly vrozeny (otisk prstu, obličej, DNA),
- ty, které nám byly přiděleny pro určitý účel (PIN, platební karty, adresa označující bydliště).

Některé základní identifikátory jsme nuceni svému okolí odkrývat v rámci běžného sociálního kontaktu (např. obličej si na veřejnosti nezakrýváme). Chránění plné základní identity je součástí našeho práva na soukromí. Občanský průkaz, který obsahuje soubor údajů umožňujících plnou základní identifikaci nikomu bezdůvodně neukazujeme. Ostatně ani Policie ČR nemá právo kdykoli žádat prokázání totožnosti, ale policista je oprávněn vyzvat k prokázání totožnosti osobu jen z důvodů taxativně vyjmenovaných v ustanovení § 63 odst. 2 zákona č. 273/2008 Sb., o Policii České republiky.

Rodné číslo je podle naší právní úpravy jedinečný soubor číselných údajů individuálně přidělených fyzické osobě, avšak bez přístupu do evidencí nejsme schopni takovou osobu jen na základě rodného čísla identifikovat (získáme tím pouze znalosti ohledně data narození a pohlaví osoby). Identifikace osoby podle rodného čísla se nám podaří, pokud disponujeme přístupem do nějaké evidence disponujícími rodnými čísly

⁵ Ustanovení § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

všech občanů a dalšími údaji o nich (např. přístupem do evidence obyvatel nebo do registru řidičů). V tomto případě můžeme považovat rodné číslo za osobní údaj, v opačném případě jím pravděpodobně nebude.⁶ Rodné číslo slouží v zásadě jako doplňkový nástroj pro potřeby dosažení plné základní identifikace vůči státu, původně vůči orgánům sociálního zabezpečení. Postupné uzavírání celostátních evidencí založených na rodném čísle, je důsledkem snah o rozšiřování jeho působnosti do soukromého sektoru. Vzhledem k tomuto trendu proto právní řád České republiky užívání rodného čísla omezil.⁷

Osobní údaj vytváří souhrn datových položek:

a) které především poskytují základní identifikaci osoby nebo umožňují dosažení takové identifikace a

b) na které se pak váží anebo mohou být navázány další informace týkající se příslušné osoby.

2.2 Pojem citlivý údaj

Pro účely zákona o ochraně osobních údajů se rozumí „citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“⁸

V praxi je třeba odlišit údaje o národnostním původu od údajů o státním občanství, které jsou mylně spojovány. Údaj o členství v politické straně je třeba považovat za údaj o politických postojích. S členstvím v odborových organizacích je spojeno placení příspěvků, členský příspěvek placený prostřednictvím zaměstnavatele, pokud je označený jako odborářský příspěvek, je citlivým údajem. Za citlivé údaje se považují údaje o odsouzení za trestný čin, nikoli o jednání, které by mohlo být kvalifikováno jako přestupek. Takovým údajem nemůže být ani negativní výpis z rejstříku trestů. Za údaje o zdravotním stavu je třeba považovat nejen všechny údaje,

⁶ Uvádí MAŠTALKA, J. *Osobní údaje, právo a my*. Praha. 2008, str. 18.

⁷ Ustanovení § 13c zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů.

⁸ Ustanovení § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

keré zdravotní stav kvalifikují, ale i ty, které umožňují zdravotní stav bezprostředně kvalifikovat. Údaj o sexuálním životě zahrnuje i údaje o sexuální orientaci osoby, takovýmto údajem evidentně není pouhý údaj o uzavření manželství. Biometrické údaje (DNA, otisky papilárních linií prstů) se nyní začínají častěji používat i při automatizovaných postupech autentizace (verifikace). Z hlediska poslední novelizace zákona o ochraně osobních údajů se biometrický údaj považuje za senzitivní pouze v případě, kdy umožňuje přímou identifikaci nebo autentizaci subjektu údajů.⁹

Pro používání rodného čísla, které není citlivým údajem, nýbrž údajem osobním, platí pravidla uvedená v zákoně o evidenci obyvatel.¹⁰ Pravidla lze nejstručněji vyjádřit tak, že rodné číslo mohou bez ohledu na postoj subjektu údajů – nositele rodného čísla, využívat správní úřady a orgány a další subjekty v případech výslovně stanovených zákonem. Pro všechny ostatní případy je nutný souhlas nositele rodného čísla nebo jeho zákonného zástupce.¹¹

2.3 Pojem zpracování osobních údajů

Za zpracování se zpravidla považují jakékoli operace nebo soustava operací, které se provádějí s osobními údaji. Pro účely zákona o ochraně osobních údajů se rozumí „zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace“.¹² Shromažďováním můžeme nazvat především operace, kterými informace získáváme do svého držení. Uchovávání počíná začleněním informací do jisté struktury (kartotéka, databáze), která umožňuje jejich další zpřístupňování. Zpřístupňováním osobních údajů rozumíme jejich postoupení k využití, příjemce údajů však musí být k převzetí a užití těchto osobních

⁹ Ustanovení § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

¹⁰ Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů.

¹¹ MATOUŠOVÁ, M. A KOL., *Ochrana osobních údajů v otázkách a odpovědích*. Praha, 2004, s. 17.

¹² Ustanovení § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

údajů oprávněn. Blokování je vytvoření stavu, kdy jsou informace na určitou dobu vyloučeny z dalších operací (např. z důvodu prověřování jejich přesnosti). Likvidací rozumíme trvalé vyloučení informace z dalších zpracování formou likvidace nosiče nebo fyzického vymazání (naformátováním diskety, začerněním na papírovém nosiči).

2.4 Pojem subjekt údajů

Takto se označuje fyzická osoba, k níž se osobní údaje vztahují¹³. Pojem „fyzická osoba“ zákon o ochraně osobních údajů nedefinuje¹⁴. V případě úmrtí, respektive v případě, že se počaté dítě nenarodí živé, informace, které se k těmto subjektům váží, přestávají být osobními údaji a zákon o ochraně osobních údajů se stává neaplikovatelný. Pak připadá v úvahu ochrana údajů jinými mechanismy (ochrana osobnosti podle občanského zákoníku).

V praxi často dochází k situaci, kdy jsou zpracovávány osobní údaje jednotlivce, ale tyto osobní údaje mohou mít vztah i k další fyzické osobě, tj. k jinému subjektu údajů. Tímto může dojít k tomu, že shromáždí-li se určitá skupina údajů, které lze označit jako osobní údaje, může mít takto vytvořený soubor vztah nejen k jedinci, ale i k celé skupině jedinců. Osobní údaj (ve smyslu ust. § 4 písm. a) zákona o ochraně osobních údajů) by se měl vždy vztahovat k jedinému subjektu údajů, a to zejména proto, že přesná určenost nebo určitelnost subjektu údajů prostřednictvím zpracovávaných osobních údajů je jedním ze základních znaků definice osobní údaj.¹⁵

2.5 Pojem správce údajů

Jako správce je definován každý subjekt, který určuje účel a prostředky zpracovávání osobních údajů, provádí zpracování a odpovídá za proces zpracování. Není rozhodné, zda jde o fyzickou nebo právnickou osobu. Správcem je kdokoliv, kdo v rámci své podnikatelské činnosti, profese, živnosti apod. zpracovává osobní údaje, to znamená, že systematicky spravuje databázi svých obchodních partnerů, klientů,

¹³ Ustanovení § 4 písm. d) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

¹⁴ Ustanovení § 7 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů. Podle něho „způsobilost fyzické osoby mít práva a povinnosti vzniká narozením“ a „smrtí tato způsobilost zanikne“.

¹⁵ Uvádí KUČEROVÁ, A. A KOL. *Zákon o ochraně osobních údajů: komentář*. Praha, 2003, s. 53.

pacientů, zákazníků atd. Kromě lékařů lze za správce označit také advokáty, notáře, soudní znalce a další osoby, které vykonávají nezávislé povolání. Při zpracování osobních údajů v oblasti státní správy a samosprávy účel obvykle vyplývá přímo ze zvláštního zákona, na základě kterého ke zpracování osobních údajů bude docházet. Správci jsou jak ústřední správní úřady, tak ostatní správní úřady, jiné organizační složky státu a orgány obcí, popřípadě profesní komory. Významnými správci jsou soudy. Mezi správce osobních údajů patří také např. zaměstnavatel, který zpracovává osobní údaje svých zaměstnanců a jejich rodinných příslušníků. Pokud jde o prostředky zpracování, máme na mysli zpravidla skutečnost, jaký bude podíl manuálního a jaký automatizovaného zpracování osobních údajů. Automatizované zpracování se provádí s využitím výpočetní techniky, manuální zpracování jsou např. systematicky uspořádané kartotéky.

Z ustanovení zákona¹⁶ vyplývá skutečnost, že správce provádí zpracování osobních údajů a odpovídá za něj. Existuje však i možnost, že zvláštní zákon stanoví nebo že správce uzavře dohodu o zpracování s dalším subjektem, který se v tomto případě považuje za zpracovatele osobních údajů, aby některé operace nebo i veškeré operace prováděného zpracování osobních údajů prováděl za správce. Za případnou škodu způsobenou subjektu údajů v souvislosti se zpracováním osobních údajů odpovídají správce a zpracovatel společně a nerozdílně.¹⁷

2.6 Pojem zpracovatel údajů

Pro účely zákona o ochraně osobních údajů se rozumí „zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona“.¹⁸ Pozice zpracovatele je odvozena od pozice správce, rovněž zpracovatel musí být subjektem práva. Zákon na ochranu osobních údajů pak výslovně povoluje, aby zpracovatel za správce plnil i povinnosti správce vůči subjektu údajů (např. poskytování informací podle § 11 a § 12 zákona o ochraně osobních údajů). Zpracovatel se tak nachází v pozici jisté podřízenosti vůči správci, za zpracování ale v plném rozsahu odpovídá správce.

¹⁶ Ustanovení § 4 písm. j) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

¹⁷ KUČEROVÁ, A. A KOL. *Zákon o ochraně osobních údajů: komentář*. Praha, 2003, s. 60.

¹⁸ Ustanovení § 4 písm. k) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

Zmocnění ke zpracování osobních údajů¹⁹ prostřednictvím zpracovatele může vyplývat přímo ze zvláštního právního předpisu, příslušný vztah se pak řídí speciální právní úpravou. Na druhé straně zpracování osobních údajů prostřednictvím zpracovatele může být zvláštním zákonem vyloučeno, a to výslovně, anebo to může vyplynout z vlastní povahy zpracování osobních údajů. Například jedním z oprávnění a úkolů Policie ČR je „zpracovávat osobní údaje včetně citlivých údajů bez souhlasu osoby, jíž se tyto údaje týkají (dále jen „subjekt údajů“), pokud je to nezbytné pro plnění jejích úkolů.“²⁰ Tedy tyto informace shromažďuje prostřednictvím uplatnění svých pravomocí. Je logické, že tak, jako jsou nepřenositelné tyto pravomoci (provádění výsledků, daktyloskopování, odebírání biologických vzorků umožňujících získání informací o genetickém vybavení apod.), nebylo by ani přípustné shromažďování osobních údajů prostřednictvím zpracovatele.

Správce ani zpracovatel nemají ze zákona o ochraně osobních údajů povinnost informovat subjekt údajů o možnosti odvolání souhlasu či vyslovení nesouhlasu se zpracováním jeho osobních údajů, které získal v souvislosti se svojí činností.²¹

¹⁹ Ustanovení § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů: „Pokud zmocnění nevyplyvá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.“

²⁰ Ustanovení § 79 odst. 1 zákona č. 273/2008 Sb., o Policii České republiky, ve znění změn provedených zákonem č. 41/2009 Sb.

²¹ KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v otázkách a odpovědích*. Praha, 2010. s. 26.

3 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ POLICIÍ ČESKÉ REPUBLIKY

3.1 Obecná ustanovení o zpracování informací policií

Velmi specifická, a vůči zákonu o ochraně osobních údajů i speciální jsou pravidla pro zpracování osobních údajů Policií ČR, upravená zákonem č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů. Jako jednu ze zásadních změn v rámci citovaného zákona oproti předešlému zákonu o policii (zákon č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů) lze uvést v tomto zákoně podrobně upravené nakládání s informacemi a osobními údaji a jeho efektivní kontrola. Pokud se jedná o pravidla pro zpracování osobních údajů v souvislosti s trestním řízením, tyto musí vycházet ze standardu představovaného Úmluvou 108 a zejména Doporučením Rady Evropy č. R(87)15 o úpravě používání osobních dat v policejním sektoru. Především je nutné zdůraznit, že Policie ČR může osobní údaje získávat jen způsobem, který dovoluje zákon. Pokud by totiž jejich zdroj byl nezákonný, musely by být ze zpracování vyloučeny. Vzhledem k úkolům policie²² netřeba dále zdůrazňovat, že za základní právní titul pro získávání a zpracování osobních údajů nelze stanovit souhlas subjektu údajů.

Dalšími obecně závaznými právními předpisy vztahujícími se k problematice jsou zákon č. 274/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o Policii České republiky a již zmiňovaný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

„1) Policie zpracovává v souladu s tímto zákonem a jiným právním předpisem informace včetně osobních údajů v rozsahu nezbytném pro plnění svých úkolů.

2) Zpracovávané informace musí policie zabezpečit před neoprávněným přístupem, změnou, zničením, ztrátou nebo odcizením, zneužitím nebo jiným neoprávněným zpracováním. Tímto nejsou dotčeny povinnosti podle jiného právního předpisu.“²³

²² Ustanovení § 2 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů: „Policie slouží veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku a veřejný pořádek, předcházet trestné činnosti, plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, přímo použitelnými předpisy Evropských společenství nebo mezinárodními smlouvami, které jsou součástí právního řádu (dále jen „mezinárodní smlouva“)“.

²³ Ustanovení § 60 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

Zákonným předpokladem pro zpracovávání informací je podmínka jejich nezbytnosti pro plnění úkolů policie. Zpracovávané informace lze rozdělit podle toho, zda obsahují nebo neobsahují osobní údaje. Zpracovávání se řídí zákonem o policii a v případě osobních údajů také zákonem o ochraně osobních údajů. Úpravou zpracování informací není dotčena právní úprava ochrany utajovaných informací. Ustanovení § 60 odst. 2 zákona o policii České republiky stanoví obecná pravidla pro zpracování informací policií. Jiným právním předpisem je v případě osobních údajů zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů. V rámci činnosti policie přichází v úvahu zejména osobní údaje, které zákon o ochraně osobních údajů označuje jako citlivé. Je nutné si uvědomit, že ustanovení zákona o ochraně osobních údajů se na zpracování osobních údajů policií nevztahuje absolutně. V souladu s požadavky policejní činnosti jsou v zákoně o policii stanoveny nezbytné výjimky z obecné právní regulace. Z pohledu zákona o ochraně osobních údajů se tedy jedná o zpracování, které je upravené zvláštním zákonem.

Dalším právním předpisem, který se vztahuje k práci s informacemi v rámci Policie České republiky je zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.²⁴

3.2 Podání vysvětlení

Důvody oprávnění požadovat vysvětlení, jeho podmínky a následky nevyhovění výzvy upravuje ustanovení § 61 odst.1 až 6 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

Činnost policie vychází mj. ze získávání odpovídajících informací, které jsou důležité z hlediska policí plněných úkolů. Osoba požádaná o poskytnutí vysvětlení se nemůže sama rozhodnout, zda žádosti vyhoví nebo ne, může pouze využít právní překážku stanovenou v odst. 3. Formální požadavky pro podání vysvětlení nejsou stanoveny. Je třeba si uvědomit, že podání vysvětlení podle zákona o policii není součástí ani trestního, ani správního řádu. Osoba podávající vysvětlení nemůže být policií krácena na právu na právní pomoc, to však neznamená, že by policie byla povinna takovou pomoc vlastní péčí zajišťovat. Informace získaná podle § 61 odst. 1 písm. a) není důkazem, ale pouze „indikátorem“ trestného činu nebo přestupku. Podání

²⁴ ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 196-197.

vysvětlení podle zákona o policii nelze využít k objasňování skutečností důležitých pro odhalení jiného správního deliktu a jeho pachatele. V tomto případě se uplatní postup podle správního řádu.

Hledanou osobou se rozumí (pro účely zák. o policii) fyzická osoba, bez ohledu na její stát. příslušnost, u které je dán některý ze zákonných důvodů pro omezení její osobní svobody, místo jejího pobytu není známo a policií po ní bylo vyhlášeno pátrání. Pohřešovanou osobou se rozumí (pro účely zák. o policii) fyzická osoba bez ohledu na její stát. příslušnost, o níž se lze důvodně domnívat, že je ohrožen její život nebo zdraví, místo jejího pobytu není známo a policií po ní bylo vyhlášeno pátrání.

Podle § 61 odst. 1 písm. c) může policie požadovat vysvětlení rovněž v souvislosti s přípravou a realizací opatření k zajištění bezpečnosti a ochrany určených osob a osob, jimž je poskytována krátkodobá ochrana osoby. Dále ustanovení zakládá možnost žádat o podání vysvětlení při poskytování ochrany podle jiného právního předpisu, kterým je zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

Před podáním vysvětlení musí být osoba podávající vysvětlení poučena nejen o možnosti zániku nároku na náhrady, ale i o možnosti odepřít podání vysvětlení ze zákonem stanovených důvodů. Tomu nasvědčuje i obecná poučovací povinnost podle § 13; poučení po provedení úkonu v případě podání vysvětlení nepřichází v úvahu.

Sdělí-li osoba, od níž je požadováno podání vysvětlení, že tomuto brání povinnost mlčenlivosti, jde o překážku, kterou lze odstranit pouze zproštěním této mlčenlivosti. Povinnost mlčenlivosti je běžnou součástí právních předpisů, např. samotný zákon o policii zavazuje touto povinností policistu, zaměstnance policie, inspektora a zaměstnance Inspekce policie, ale i každého, koho útvar policie (ust. § 6 zákona o policii), policista nebo inspektor požádá o poskytnutí pomoci.²⁵ Státem uznanou mlčenlivostí se rozumí např. zpovědní tajemství.

Osobou blízkou se podle občanského zákoníku rozumí příbuzný v pokolení přímém, sourozenec a manžel, partner podle zákona o registrovaném partnerství²⁶; jiné osoby v poměru rodinném nebo obdobném se pokládají za osoby sobě navzájem blízké, jestliže by újmu, kterou utrpěla jedna z nich, druhá důvodně pocítovala jako újmu vlastní.

²⁵ Ustanovení § 115 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

²⁶ Zákon č. 115/2006 Sb., o registrovaném partnerství a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

Právním následkem neuposlechnutí výzvy k podání vysvětlení je předvedení. Samotné předvedení není spojeno s formálními požadavky, vždy je však třeba o předvedení sepsat úřední záznam s uvedením času a důvodu předvedení, průběhu předvedení a dalších významných okolností. Tento úřední záznam musí být uložen po dobu nejméně pěti let.

3.3 Pořizování záznamů

„1) Policie může, je-li to nezbytné pro plnění jejích úkolů, pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných a zvukové, obrazové nebo jiné záznamy o průběhu úkonu.

2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatizované systémy, policie informace o zřízení takových systémů vhodným způsobem zveřejní.“²⁷

Na získané informace z pořízených záznamů se vztahuje jak úprava ze zákona o policii, tak úprava podle zákona o ochraně osobních údajů. Podmínkou pro pořizování záznamů je nezbytnost získaných informací pro plnění úkolů policie (např. prevence kriminality, ochrana bezpečnosti osob a majetku). Toto zákonné zmocnění představuje tzv. „úřední licenci“, kterou při zásahu do osobnostních práv vyžaduje občanský zákoník, zároveň se tímto ustanovením dociluje souladu se zákonem na ochranu osobních údajů, který vylučuje podmínku souhlasu subjektů v případě zpracování osobních údajů za účelem dodržení právní povinnosti.

Monitorování může být prováděno jak z míst veřejně přístupných, tak i z míst neveřejných (např. z okna bytu). Uvedeným způsobem získává policie informace plošně, bez výběrové selekce a tak jsou v rámci získaných informací na záznamech obsaženy i údaje o osobách, u nichž nejsou symptomy porušení právního předpisu. Proto je nezbytné separaci těchto policejně nevyužitelných informací provést bez zbytečného odkladu s jejich následnou likvidací.

Za veřejně přístupné místo se považuje prostor určený pro široký okruh lidí, kdy limitem může být účel přístupu (např. nemoc, ubytování, přeprava vlakem) nebo vymezení doby přístupu (např. provozní doba) a veřejné prostranství.

²⁷ Ustanovení § 62 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

Veřejným prostranstvím jsou náměstí, ulice, chodníky, tržiště, parky, veřejná zeleň a další prostory přístupné každému bez omezení, pokud slouží veřejnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru.

Právní úprava rovněž umožňuje pořizovat zvukové, obrazové nebo jiné záznamy o průběhu úkonu. V této souvislosti je třeba poukázat na ustanovení § 59 zákona o policii, které ukládá, že rozhodnutí velitele zakročující jednotky a jeho nadřízeného o použití donucovacího prostředku a zbraně bude zaznamenáno obligatorně. V tomto případě zákon nedává žádný prostor úvahám, zda záznam pořizovat nebo nikoli.

Zákon o policii nespécifikuje, co se rozumí vhodným způsobem uveřejnění (ve smyslu ustanovení § 62 odst. 2). Vhodným způsobem bude uveřejnění například pomocí internetu nebo informačních tabulí na začátcích obce.²⁸

3.4 Prokázání totožnosti

Institut prokázání totožnosti můžeme zařadit mezi zásadní oprávnění, která zákon o policii upravuje. Cílem zjišťování totožnosti je identifikace konkrétní osoby, touto osobou se rozumí konkrétní fyzická osoba. Prokazování totožnosti je běžnou součástí právních předpisů,²⁹ tyto předpisy však blíže nespécifikují, jak se totožnost prokazuje. Zákon o policii, který prokázání totožnosti upravuje v ustanovení § 63 odst. 1 až 6 je konstruován jinak, v ustanovení odst. 2 písm. a) až l) totiž vymezuje rozsah údajů, které lze na základě tohoto oprávnění zjišťovat. Platí zásada, že totožnost policista zjišťuje u osoby jemu neznámé, osoby fyzické, kterou může být občan České republiky nebo cizinec. Zákon o policii stanoví jako podmínku, že účel zjišťování totožnosti je kritériem ovlivňujícím rozsah a způsob zjišťování požadovaných údajů.

Zákon o policii nespécifikuje, čím může osoba totožnost prokázat. V prvé řadě přichází v úvahu doklady totožnosti (občanský průkaz, cestovní doklad). Kromě uvedených dokladů mohou za některých okolností sloužit k prokázání totožnosti i doklady vydávané zaměstnancům nebo i jiné hodnověrné doklady. Záleží vždy na

²⁸ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 203.

²⁹ Např. zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů, zakládá oprávnění právnických osob požadovat od toho, kdo předložil podezřelé bankovky nebo mince, aby prokázal svou totožnost.

konkrétní situaci, jaké podklady mohou být k prokázání totožnosti uznány, někdy vzhledem k účelu prokázání totožnosti postačí prohlášení, které učiní jiná osoba.³⁰

Důvodným podezřením ve smyslu ust. § 63 odst. 2 písm. g) zákona o policii lze rozumět podezření, které se opírá o objektivní skutečnosti. Zbraní se pro účely tohoto oprávnění rozumí cokoli, čím je možno učinit útok proti tělu důraznějším.

Pro účely ust. § 63 odst. 2 písm. h) zákona o policii je při posouzení, zda se osoba zdržuje v blízkosti místa např. trestného činu, nutno postupovat v souladu se zásadou přiměřenosti. Pod pojmem správní delikt je nutno rozumět jak přestupek, tak i jiný správní delikt. Za mimořádnou událost se považuje škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací.

Podmínkou ke zjišťování totožnosti podle ustanovení písm. k) je, že jiná osoba má na zjištění totožnosti osoby právní zájem (např. revizor DP, který zjistil, že přepravovaná osoba nedodržela přepravní podmínky nebo číšník, kterému host po konzumaci nemůže nebo nechce uhradit účet). Žádající osoba musí současně prokázat i svou vlastní totožnost. Jsou-li uvedené požadavky naplněny, může policista zjištěné osobní údaje předat osobě, která o prokázání totožnosti požádala s poukazem na právní zájem. Podmínka právního zájmu u tohoto ustanovení brání nedůvodným požadavkům. Právní zájem lze vymezit jako předpoklad pro dovolávání se ochrany u orgánu zákonem k tomu určenému.³¹

Ustanovení § 63 odst. 2 písm. l) zákona o policii je tzv. „zbytkovým ustanovením“, které policii umožňuje nad rámec předchozích ustanovení získávat údaje o totožnosti osoby, pokud je to nutné při plnění úkolu v zájmu ochrany bezpečnosti osob a majetku, veřejného pořádku nebo v zájmu předcházení trestné činnosti.

Prvotním úkonem po předvedení osoby podle ustanovení § 63 odst. 3 zákona o policii je provedení evidenčního šetření. Nepodaří-li se ani tímto způsobem zjistit totožnost osoby, následují možnosti spojené se zásahem do tělesné integrity osoby podle odst. 4. Je však třeba dbát, aby úkony spojené např. se zjišťováním tělesných znaků prováděla osoba stejného pohlaví nebo lékař. Předchozí poučení osoby o možnosti vynutit si provedení úkonu podle odst. 4 je podmínkou pro přijetí opatření

³⁰ ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 205-206.

³¹ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 209.

k překonání odporu osoby ve smyslu odst. 5. Intenzita překonávání odporu osoby nesmí být v rozporu se zásadou přiměřenosti.³²

Z ustanovení § 63 odst. 6 zákona o policii vyplývá, že pokud byla prokázáním totožnosti zjištěna osoba pohřešovaná, vyrozumí policista se souhlasem této osoby toho, kdo pohřešování osoby oznámil. Bez souhlasu pohřešované osoby policie oznamovateli sdělí, že pátrání po pohřešované osobě bylo ukončeno. Pokud je pohřešovaná osoba zbavena způsobilosti k právním úkonům, vyrozumí policista o ztotožnění pohřešované osoby toho, kdo pohřešování osoby oznámil a jejího zákonného zástupce. Z uvedeného vyplývá, že v případě osob mladších 15 let je nutno přihlídnout k zákonem uložené rodičovské odpovědnosti. Osoba mladší 15 let tedy souhlas ve smyslu tohoto ustanovení udělit nemůže.³³

Podle ustanovení § 64 zákona o policii je limitem pro předvedení osoby za účelem zjištění totožnosti podle § 63 trvání důvodu provádění úkonů zjišťování totožnosti. Pokud pomine důvod podle citovaného ustanovení (totožnost osoby byla zjištěna), je policista osobu povinen propustit. Druhým limitem je lhůta 24 hodin od počátku předvedení, tuto lhůtu nelze prodloužit. O provedených úkonech a opatřeních je policista povinen bez zbytečného odkladu sepsat úřední záznam (včetně časových údajů a důvodu zjišťování). V případě pozdějšího zjištění důvodu pro zadržení osoby podle trestního řádu, dochází k zápočtu doby, po kterou byla osoba omezena na svobodě podle zákona o policii.³⁴

3.5 Získávání osobních údajů pro účely budoucí identifikace³⁵

Oproti dřívějšímu zákonu (zákon č. 283/1991 Sb.) došlo ke změně v rámci získávání osobních údajů pro budoucí identifikaci osob (účelem není ztotožnit osobu). Změna nastala především ve stanovení okruhu subjektů tím, že došlo k zpřesnění dosavadního okruhu subjektů a v odklonu od subsidiárního pojetí získávání osobních údajů pro budoucí identifikaci (není stanoven limit). Ustanovení § 65 zákona o policii představuje na jedné straně zpřesnění, ovšem z druhé strany nelze opomenout absenci subsidiárního postupu získávání osobních údajů. Vzhledem k tomu je nutné zdůraznit,

³² Ustanovení § 11 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

³³ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 210.

³⁴ Zdroj: Judikatura: Nález Ústavního soudu, spisová značka IV. ÚS 305/97 pod názvem „Zahrnutí bezprávného omezení osobní svobody do doby zadržení“.

³⁵ Upravuje ustanovení § 65 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

že i v tomto případě platí obecné zásady policejní činnosti a na uvedenou oblast se vztahuje i zákon o ochraně osobních údajů.³⁶ Ustanovení § 65 odst. 1 zákona o policii definuje okruh osob, které mají povinnost nechat si odebrat osobní údaje z důvodu budoucí identifikace. Limitem je plnění úkolů policie podle ustanovení § 2 zákona o policii.

Jedná se o následující kategorie osob:

- a) **osoba obviněná ze spáchání úmyslného trestného činu** – osoba v procesním postavení podle trest. řádu, proti níž bylo zahájeno trestní stíhání podle § 160 trest. řádu pro úmyslný trestný čin, (když pachatel naplnil subjektivní stránku skutkové podstaty tr. činu ve formě úmyslu podle § 15 trestního zákoníku);³⁷
- b) **osoba, které bylo sděleno podezření pro spáchání takového trestného činu** (osobě bylo sděleno podezření pro spáchání úmyslného trest. činu ve smyslu § 179b odst. 3 trest. řádu, tj. v rámci zkráceného přípravného řízení. Osoba, které bylo ve zkráceném přípravném řízení sděleno podezření má obdobné procesní postavení jako osoba obviněná;³⁸
- c) **osoba ve výkonu trestu odnětí svobody za spáchání úmyslného trestného činu** (osoba byla uznána vinou ze spáchání úmyslného trest. činu, byla pravomocně odsouzena za tento trestný čin a nastoupila výkon trestu odnětí svobody);³⁹
- d) **osoba, již bylo uloženo ochranné léčení soudem** podle § 99 trest. zákoníku nebo **zabezpečovací detence** podle § 100 trest. zákoníku;
- e) **osoba nalezená, po níž bylo vyhlášeno pátrání**⁴⁰ a která **nemá způsobilost k právním úkonům v plném rozsahu.**

U osob, které naplňují některou z výše uvedených kategorií lze snímat daktyloskopické otisky, zjišťovat tělesné znaky, provádět měření těla, pořizovat obrazové, zvukové a obdobné záznamy (např. fonoskopické záznamy hlasu) a odebírat biologické vzorky umožňující získání informací o genetickém vybavení (tzv. odběr šroubovice DNA).

³⁶ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 213-214.

³⁷ Zákon č. 40/2009 Sb., trestní zákoník.

³⁸ Ustanovení § 179b odst. 2 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů.

³⁹ Zákon č. 169/1999 Sb., výkonu trestu odnětí svobody a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

⁴⁰ Upravuje ustanovení § 68 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

Ustanovení § 65 odst. 2 umožňuje, aby mohla policie získat osobní údaje pro účely budoucí identifikace po předchozí marné výzvě i za předpokladu překonání odporu osoby. Osoby uvedené v odst. 1 mají povinnost strpět provedení tohoto úkonu, mají postavení toliko pasivního subjektu. Policista musí nejprve vyzvat osobu k provedení úkonů, až poté může přiměřeným způsobem překonat její odpor. Odpor nelze překonat, je-li úkon (sledující cíl získat příslušné osobní údaje) spojen se zásahem do tělesné integrity osoby (ustanovení uvádí jmenovitě příklad – odběr krve). Na základě uvedeného lze vyvodit, že zásahem do tělesné integrity lze rozumět zásah do tělesné tkáně osoby. Proto tzv. bukální stěr, který je využíván policií pro získávání osobních údajů pro účely budoucí identifikace, nelze s ohledem na způsob provádění stěru považovat za zásah do tělesné integrity.

Většinou není možné provést takové získání osobních údajů na místě. Proto ustanovením § 65 odst. 3 zákon zakládá možnost předvést dotčenou osobu na vhodné místo. Tímto místem nemusí být vždy jen služebna policejního útvaru, ale je nutné mít na zřeteli především hledisko taktické a etické. Po provedení úkonu policista osobu propustí. Ve smyslu ust. § 65 odst. 4 policista sepiše o provedených úkonech úřední záznam.⁴¹

Ustanovení § 65 odst. 5 zákona o policii lze považovat za jednu z řady výjimek z obecné úpravy ochrany osobních údajů, které Policie ČR jako specifický bezpečnostní subjekt má. Proto zákon nestanovuje pro takto získané osobní údaje žádný přesný časový limit, ovšem vymezuje dobu nakládání s těmito osobními údaji jejich věcnou potřebou pro plnění úkolů policie.⁴²

3.6 Získávání informací z evidencí⁴³ (předávání osobních údajů Policii České republiky)

Podmínky, za nichž je možné nebo nutné poskytnout osobní údaje z určité evidence Policii České republiky (dále jen "Policie"), potřebují znát zejména personalisté, kteří zpracovávají osobní údaje zaměstnanců, dále Úřady práce,

⁴¹ Upravuje ustanovení § 109 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů (Dokumentace).

⁴² Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 215.

⁴³ Ustanovení § 66 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

zpracovávající osobní údaje uchazečů o zaměstnání, i správci nebo zpracovatelé řady dalších evidencí obsahujících osobní údaje osob.

Z hlediska zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, se v takovémto případě jedná o zpracování osobních údajů bez souhlasu subjektu údajů, které je podle § 5 odst. 2, písm. a) tohoto zákona možné, jestliže se jedná o zpracování stanovené zvláštním zákonem nebo nutné pro plnění povinností stanovených zvláštním zákonem. Zvláštním zákonem je v tomto případě zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů. Při odpovědi na danou otázku je třeba vycházet z ustanovení § 18 a § 66 tohoto zákona. Podle citovaného ustanovení § 18 je policista v rozsahu potřebném pro splnění konkrétního úkolu Policie oprávněn požadovat od ozbrojených sil, bezpečnostních sborů a dalších orgánů veřejné správy, jakož i od právnických a fyzických osob věcnou a osobní pomoc, zejména potřebné podklady a informace včetně osobních údajů. Podle následujícího citovaného ustanovení § 66 odst. 1 zákona o Policii ČR může Policie žádat od správce evidence nebo zpracovatele poskytnutí informací z evidence provozované na základě jiného právního předpisu, a to bezplatně, nestanoví-li jiný právní předpis jinak. Správce evidence nebo zpracovatel jsou povinni bez zbytečného odkladu žádosti vyhovět, nestanoví-li zvláštní právní předpis pro poskytnutí informací Policii České republiky jiný režim.

Citovaný paragraf stanoví, že rozsah požadovaných údajů musí odpovídat potřebám plnění konkrétního úkolu Policie. Podle odst. 4 ustanovení § 66 způsob předávání údajů musí umožňovat uchovávání identifikačních údajů o útvaru Policie nebo o policistovi, který o poskytnutí informací žádal, a o účelu, k němuž bylo o poskytnutí informací žádáno, a to nejméně po dobu pěti let.

V odstavcích 2 a 3 ustanovení § 66 jsou taxativně vymezeny evidence, u nichž je Policie České republiky oprávněna žádat poskytnutí informací způsobem umožňujícím dálkový a nepřetržitý přístup. Je to například oprávnění Policie požadovat informace od správce databáze účastníků veřejně dostupné telefonní služby s odkazem na příslušná ustanovení zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. V citovaném ustanovení § 66 odst. 3 takto stanovená povinnost vyhovět této žádosti bez zbytečného odkladu a ve vyžádané formě však neznamená, že by se tak mohlo stát způsobem, který by byl neověřený a neumožňoval by (ve smyslu ustanovení odst. 4 citovaného paragrafu) uchování výše zmíněných identifikačních údajů o útvaru Policie ČR nebo policistovi, který o předání údajů požádal.

„Z uvedených ustanovení vyplývá, že žádosti o předávání osobních údajů Policii České republiky by v žádném případě neměly být vyřizovány na základě neověřeného telefonického dotazu. Vždy by měly být policii podávány pouze v písemné formě a měly by být správcem nebo zpracovatelem uchovávané včetně odpovědi příslušného správce nebo zpracovatele osobních údajů. V případě osobního jednání s policistou je třeba, aby správce nebo zpracovatel obdržel kopii úředního protokolu. Jen při splnění těchto podmínek může správce či zpracovatel dostat zákonnému požadavku, jehož obsahem je prokázat, kdy, komu a za jakým účelem předal osobní údaje zpracovávané v příslušné evidenci.“⁴⁴

Policie nebo ministerstvo může od správce nebo zpracovatele evidence vedené na základě jiných právních předpisů požadovat, aby policii oznamovali každý výdej osobních údajů, za účelem zajištění ochrany osoby, o níž lze důvodně předpokládat, že by mohl být ohrožen její život nebo zdraví, nebo pro účely pátrání po hledané anebo pohřešované osobě.⁴⁵ Podle § 66 odst. 5 je tedy správce nebo zpracovatel evidence vedené na základě právního předpisu povinen oznamovat jakýkoli výdej osobních údajů (i údajů, které nemají vazbu na osobu chráněnou, nebo osobu hledanou či pohřešovanou). Avšak oproti dřívější právní úpravě došlo doplněním osob hledaných či pohřešovaných k problematizaci tohoto řešení, jehož cílem má být globálním poskytováním údajů zajistit nevyzrazení osoby, které je policií poskytována ochrana, avšak již nikoli nevyzrazení hledané či pohřešované osoby.

3.7 Získávání informací v souvislosti s odhalováním a šetřením přestupků

Ustanovení § 67 zákona o policii vytváří předpoklad pro plnění úkolů, které orgánům policie ukládá přestupkový zákon.⁴⁶ Podle uvedeného právního předpisu mj. orgány policie oznamují příslušným správním orgánům přestupky, o nichž se dozví, jedná-li se o přestupek, k jehož projednávání nejsou příslušné.

„Policie je v souvislosti s odhalováním a šetřením přestupku oprávněna vyžadovat

⁴⁴ Názory Úřadu pro ochranu osobních údajů/K problémům z praxe/č. 3/2001-aktualizace 06/2009. Dostupný z WWW: < <http://www.uoou.cz/uoou.aspx?menu=14>>.

⁴⁵ Ustanovení § 66 odst. 5 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁴⁶ Zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů.

- a) výpis z evidence Rejstříku trestů v případech, ve kterých by předchozí trestní postih mohl vést k posouzení skutku jako trestného činu,
- b) provedení orientačního vyšetření při podezření na ovlivnění alkoholem nebo jinou návykovou látkou pomocí dechové zkoušky nebo odběrem slin anebo potu,
- c) odborné lékařské vyšetření ke zjištění alkoholu nebo jiné návykové látky včetně odběru krve, moči, slin nebo potu, a to i v případě, že osobu nelze předem pro její zdravotní stav ke strpění příslušných úkonů vyzvat, nebo
- d) jiné odborné vyšetření.⁴⁷

Ve výpisu rejstříku trestů jsou uvedena všechna dosud nezahmlazená odsouzení včetně údajů o průběhu výkonu uložených trestů a ochranných opatření, pokud se podle zákona na pachatele nehledí, jako by nebyl odsouzen. Předchozím trestním postihem se rozumí i postih za správní delikt.

Orientačním vyšetřením se rozumí dechová zkouška, odběr slin, stěr kůže nebo sliznic nebo jiný obdobně účinný způsob.⁴⁸ Alkoholem se rozumí organická sloučenina vzniklá z uhlovodíků náhradou jednoho nebo více atomů vodíku hydroxylovou skupinou „OH“. Jedná se o návykovou chemickou látku, která ovlivňuje činnost nervového systému člověka. Jinými návykovými látkami jsou omamné látky a psychotropní látky.

Odborným lékařským vyšetřením se rozumí cílené vyšetření lékařem a podle jeho ordinace provedení dechové zkoušky, odběru vzorku biologického materiálu nebo jiného obdobně účinného vyšetření. Odborné lékařské vyšetření provádí na žádost policisty zdravotnické zařízení k tomu odborně a provozně způsobilé. Oprávnění vyžadovat odborné lékařské vyšetření není vázáno na zdravotní stav osoby, lze je tedy provést i v případě, kdy osobu nelze vzhledem k jejímu zdravotnímu stavu vyzvat, aby takový úkon strpěla (např. u zraněného účastníka dopravní nehody převezeného do zdravotnického zařízení).

Jiné odborné vyšetření musí být zaměřeno na zjištění skutečností důležitých pro přestupkové řízení, kdy je nutné pro další postup v řešení konkrétního problému tento podrobit odbornému posouzení. Může se jednat například o posouzení z pohledu medicínského nebo technického. Forma odborného vyjádření není v zákoně o policii

⁴⁷ Ustanovení § 67 odst. 1 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁴⁸ Podle zákona č. 379/2005 Sb., o opatřeních k ochraně před škodami způsobenými tabákovými výrobky, alkoholem a jinými návykovými látkami a o změně souvisejících zákonů, ve znění pozdějších předpisů.

vyjádřena, musí se však jednat o kvalifikovaný závěr, využitelný v přestupkovém řízení (nejde o znalecký posudek).⁴⁹

Ohledáním místa přestupku a ohledáním věci mající vztah ke spáchanému přestupku (podle § 67 odst. 2 zákona o policii) se rozumí zejména odpovídající dokumentace místa přestupku, vyhledávání a zajištění stop. Policista provádí ohledání zpravidla vlastním pozorováním místa přestupku nebo věci, která má vztah ke spáchanému přestupku.

Zda je úkon nebezpečný pro zdraví osoby (ve smyslu ust. § 67 odst. 3), nemůže posuzovat policista, osobou kvalifikovanou pro takové posouzení je pouze lékař. Tímto není dotčena možnost, kterou má podezřelý z přestupku, odmítnout provedení úkonu se všemi právními důsledky. Například přestupku se dopustí ten, kdo v provozu na pozemních komunikacích se přes výzvu podle zákona o provozu na pozemních komunikacích odmítne podrobit vyšetření, zda při řízení vozidla nebo jízdě na zvířeti nebyl ovlivněn alkoholem nebo jinou návykovou látkou, ačkoliv takové vyšetření není spojeno s nebezpečím pro jeho zdraví.⁵⁰

Požadavek osoby podezřelé z přestupku na vyšetření podle § 67 odst. 4 nesmí policista odmítnout, dále je povinností policisty provedení odběru krve zajistit. „Smyslem citovaného ustanovení je umožnit osobě, která je podezřelá z trestného činu nebo z přestupku spáchaného pod vlivem alkoholu, dosáhnout provedení objektivního důkazu o tom, zda tu ovlivnění alkoholem skutečně je a jaká je jeho míra.“⁵¹

3.8 Pátrání po osobách a věcech

Problematika pátrání po osobách a věcech je uceleně upravena ust. § 68 odst. 1) až 5) zákona o policii. Pátrání se zaměřuje nejen na zjištění místa výskytu osoby nebo věci, ale i na zjištění totožnosti osoby, ať již živé nebo mrtvé. Z hlediska zákona o policii není rozhodující, zda se pátrá po státním občanovi ČR nebo cizinci. Osobní údaje vypátrané hledané nebo pohřešované osoby policie bez zbytečného odkladu zlikviduje, toto nemusí učinit za podmínky, že osoba byla pohřešována nebo hledána opakovaně, a lze důvodně předpokládat, že bude opětovně pohřešována nebo hledána, anebo její osobní údaje jsou zpracovávány v souvislosti s trestnou činností. Pátrání po

⁴⁹ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 227.

⁵⁰ Ustanovení § 22 odst. 1 písm. d) zákona č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů.

⁵¹ Judikát: Usnesení Nejvyššího soudu České republiky spis. zn. 7 Tdo 1124/2003, ze dne 15. 10. 2003.

osobách a věcech zákon o policii koncipuje jako součást jednotlivých úkolů plněných policií. Pátrání, s výjimkou pátrání po hledané nebo pohřešované osobě, kde zákon o policii ukládá takové pátrání vyhlásit, není podmíněno formálními požadavky.⁵² S pátráním je spojena řada oprávnění policisty, např. oprávnění zastavit dopravní prostředek a provést jeho prohlídku podle ustanovení § 42 odst. 1) až 3) zákona o policii.

Lokalizační údaje osoby poskytnuté právnickou nebo fyzickou osobou zajišťující provoz veřejné komunikační sítě nebo poskytující veřejně dostupnou službu elektronických komunikací (podle ust. § 68 odst. 2 zákona o policii) nemohou být využity jinak, než za účelem v tomto odstavci uvedeném. Cílem získání těchto dat je prostřednictvím telekomunikačních prostředků například nalézt pohřešovanou osobu.

Údaje podle odst. 3 písm. a) a b) citovaného ustanovení lze žádat jen pro účely již zahájeného pátrání po konkrétní hledané nebo pohřešované osobě. V rámci České republiky je nejrozšířenějším elektronickým platebním prostředkem platební karta, která je současně i bezhotovostním platebním prostředkem, přitom použití platební karty nemusí být vázáno pouze na výběr hotovosti, ale i na provedení platebního příkazu nebo jiné operace. Banka ale tyto konkrétní údaje neposkytne, k žádosti podle ust. § 68 odst. 3 písm. a) zákona o policii sdělí pouze, kdy a kde byl tento platební prostředek použit.⁵³ Obdobně tak podle písmene b) citovaného ustanovení jsou zdravotní pojišťovnou nebo zdravotnickým zařízením sděleny toliko údaje o době a místě poskytnutí zdravotní péče.

Ustanovení § 68 odst. 4 zákona o policii stanoví, že „informace získané podle odstavců 2 a 3 lze použít pouze pro účely zjištění doby místa pobytu osoby“. Tímto se stanovuje pojistka, která potvrzuje, co lze dovodit z předchozích odstavců.

Specifické oprávnění podle ustanovení odst. 5 citovaného paragrafu, umožňující policii poskytnutí údajů ze zdravotnické dokumentace za účelem zjištění totožnosti neznámé mrtvoly, se uplatní zejména při činnostech specializovaného celorepublikového útvaru policie – Kriminalistického ústavu Praha.

⁵² Hledanou osobou se podle zákona o policii rozumí fyzická osoba, u které je dán některý ze zákonných důvodů omezení její osobní svobody a místo jejího pobytu není známo. Pohřešovanou osobou se podle zákona o policii rozumí fyzická osoba, o níž se lze důvodně domnívat, že je ohrožen její život nebo zdraví a místo jejího pobytu není známo.

⁵³ Bližší podrobnosti lze nalézt v zákonu č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku), ve znění pozdějších předpisů.

3.9 Získávání poznatků o trestné činnosti

Podle ustanovení § 69 odst. 1 zákona o policii „policista před zahájením úkonů trestního řízení z vlastní iniciativy nebo na základě podnětu jiné osoby anebo orgánu za účelem získání poznatků o trestné činnosti vyhledává, odhaluje, a je-li to třeba i dokumentuje skutečnosti nasvědčující tomu, že byl spáchán trestný čin. V rámci činnosti podle věty první, je povinen předcházet trestné činnosti.“⁵⁴

Povinnosti policejního orgánu před zahájením trestního řízení stanoví § 158 odst. 1 trestního řádu. Takto má policie činit před zahájením trestního řízení, což znamená postupem podle zákona o policii. Zákon o policii totiž uplatňuje obecný princip, že zásahy do práv uplatněné v něm sledují bezpečnostní, nikoliv důkazní účel, avšak postupy upravené v trestním řádu mají za cíl opatření důkazu, tedy mají procesní účel. Uvedené upravuje odst. 2 citovaného ustanovení: „Policista při výkonu činností podle odstavce 1 postupuje podle tohoto zákona, za využití oprávnění a prostředků v něm uvedených.“

Zvýšený výskyt trestné činnosti můžeme předpokládat v *zájmovém prostředí*, což je nový právní pojem. V rámci úpravy zájmového prostředí vymezuje postup policisty před zahájením úkonů trestního řízení ustanovení § 70 odst. 1 zákona o policii.

„1) Zájmovým prostředím se pro účely tohoto zákona rozumí prostředí, v němž lze důvodně předpokládat získání poznatků důležitých pro zamezování, odhalování a dokumentování trestných činů, ke zjišťování jejich pachatelů a k předcházení těmto trestným činům.“

Získávání poznatků ze zájmového prostředí je činností, která předchází trestnímu řízení. V rámci této činnosti může policista využívat informátora, krycí prostředky, zabezpečovací techniku a zvláštní finanční prostředky. Může využívat i další oprávnění upravené zákonem o policii, avšak za dodržení obecných limitů policejní činnosti (např. přiměřenost postupu dle § 11 zákona o policii).

⁵⁴ Trestným činem se pro účely zákona o policii rozumí i jednání vykazující znaky trestného činu spáchané osobou, která není trestně odpovědná (ust. § 111 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů). Zahájení úkonů trestního řízení upravuje ust. § 158 odst. 3 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

3.10 Předávání informací⁵⁵

Policie předává informace včetně informací zpracovávaných v policejních evidencích, které získala při plnění svých úkolů, je-li to nezbytné pro plnění úkolů v rámci jejich působnosti:

- zpravodajským službám České republiky
- Vojenské policii
- ministerstvu
- Vězeňské službě České republiky
- Celní správě České republiky
- dalším orgánům veřejné správy

Policie informace nepředá, pokud by to ohrozilo plnění úkolů policie. Nezbytnost těchto informací pro plnění úkolů adresáta a současně neohrožení plnění úkolů policie v souvislosti s tímto předáním je podmínkou předání údajů.

3.11 Zvláštní ustanovení o zpracovávání osobních údajů policií

Zákon č. 273/2008 Sb., o Policii České republiky v rámci ustanovení o práci s informacemi důkladněji oproti předešlému zákonu o policii propracovává část o zpracovávání osobních údajů. Důraz je kladen na jedné straně o zřetelnější provázanost na obecnou úpravu v zákoně o ochraně osobních údajů a současně na straně druhé, aby tato část úpravy odpovídala potřebám moderní praxe policie v informační společnosti.

V souladu se zákonem na ochranu osobních údajů (jako obecnou právní úpravou), se vymezuje základní rozdělení režimů zpracování na

- režim zpracování osobních údajů podle obecné úpravy zákona o ochraně osobních údajů;
- zpracování podle obecné úpravy s výjimkami v případě zpracování pro bezpečnostní účely. Tyto účely jsou terminologicky uvedeny do souladu s ust. § 3 odst. 6 zákona o ochraně osobních údajů tak, aby bylo zcela jednoznačně stanoveno, za jakých podmínek má policie možnost využívat výjimky z obecné úpravy zpracování osobních údajů.

⁵⁵ Ustanovení § 78 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

Policie podléhá dozoru Úřadu na ochranu osobních údajů podle zákona o ochraně osobních údajů. Na případy vedení informačních systémů podle zákona o policii se vztahuje ust. § 13 zákona o ochraně osobních údajů, kromě výjimek daných zákonem o policii.⁵⁶

„1) Policie může zpracovávat osobní údaje včetně citlivých údajů bez souhlasu osoby, již se tyto údaje týkají (dále jen „subjekt údajů“), pokud je to nezbytné pro plnění jejích úkolů.

2) Shromažďovat údaje o rasovém původu, náboženském nebo politickém přesvědčení, o příslušnosti k zákonem nezakázanému sdružení nebo sexuálním chování lze pouze tehdy, je-li to nezbytné pro účely konkrétního trestního řízení.“⁵⁷

Nezbytnost plnění úkolů je dána úkoly policie podle ustanovení § 2 zákona o policii. Je nutné v konkrétním případě specifikovat nezbytnost vedení osobních nebo citlivých údajů.

Shromažďováním údajů se rozumí systematické postupy podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

3.12 Předávání nebo zpřístupňování osobních údajů

„1) Policie předává nebo zpřístupňuje osobní údaje,

- a) stanoví-li tak tento zákon nebo jiný právní předpis, mezinárodní smlouva nebo přímo použitelný předpis Evropských společenství,
- b) je-li předání nebo zpřístupnění osobních údajů nezbytné k odstranění závažného ohrožení bezpečnosti osob nebo veřejného pořádku, nebo
- c) je-li to ve prospěch osoby, k níž se osobní údaje vztahují a tato osoba dala k předání nebo zpřístupnění souhlas nebo lze její souhlas na základě okolností důvodně předpokládat.

2) V případě podle odstavce 1 písm. a) lze osobní údaje předat příjemci bez žádosti, nestanoví-li právní předpis, mezinárodní smlouva nebo přímo použitelný předpis Evropských společenství jinak. V případě podle odstavce 1 písm. b) lze předat osobní údaje příjemci i bez žádosti. V případě podle odstavce 1 písm. c) lze předat osobní údaje

⁵⁶ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 244.

⁵⁷ Ustanovení § 79 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

příjemci pouze na základě písemné žádosti, která musí obsahovat účel, pro který mají být osobní údaje předány.

3) Je-li to možné, připojí se k předávaným osobním údajům informace o pravomocných rozhodnutích orgánů činných v trestním řízení, pokud k těmto údajům mají vztah.

4) Nepravdivé nebo nepřesné osobní údaje nelze předávat; neověřené osobní údaje se při předávání označí a uvede se míra jejich spolehlivosti. Dojde-li k předání nepravdivých nebo nepřesných osobních údajů, policie o tom bez zbytečného odkladu informuje příjemce těchto údajů.

5) Příjemce osobních údajů je oprávněn zpracovávat osobní údaje k jinému účelu, než ke kterému byly předány nebo zpřístupněny, za podmínky, že policie s tímto zpracováním souhlasí.

6) Policie může i bez žádosti předat nebo zpřístupnit osobní údaje do zahraničí

a) při využívání informačního systému vytvořeného státy, které jsou vázány mezinárodními smlouvami o odstraňování kontrol na společných hranicích a s nimi souvisejícími předpisy Evropské unie⁵⁸ (dále jen „Schengenský informační systém“), v rozsahu a za účelem stanoveným těmito mezinárodními smlouvami a předpisy Evropské unie, nebo

b) při předcházení trestné činnosti, prověřování skutečností nasvědčujících tomu, že byl spáchán trestný čin, odhalování a vyšetřování trestných činů nebo při zajišťování veřejného pořádku a bezpečnosti

1. mezinárodní organizaci Interpol,

2. Evropskému policejnímu úřadu,

3. zahraničnímu bezpečnostnímu sboru, nebo

4. příslušnému orgánu nebo instituci členského státu Evropské unie v rozsahu a za účelem stanoveným mezinárodní smlouvou nebo předpisy Evropské unie o policejní spolupráci.⁵⁹

Citované ustanovení § 80 zákona o policii upravuje podmínky za kterých lze osobní údaje předávat nebo zpřístupňovat. Současně tato právní úprava vytváří i předpoklad pro předávání osobních údajů do zahraničí ve významném zahraničněpolitickém nebo bezpečnostním zájmu. Předáním osobních údajů podle

⁵⁸ Úmluva podepsaná dne 19. června 1990 v Schengenu mezi Belgickým královstvím, Spolkovou republikou Německo, Francouzskou republikou, Lucemburským velkovévodstvím a Nizozemským královstvím k provedení dohody podepsané dne 14. června 1985 o postupném odstraňování kontrol na společných hranicích. Rozhodnutí Rady 2005/211/SVV ze dne 24. února 2005 o zavedení některých nových funkcí v Schengenském informačním systému, včetně boje proti terorismu. Nařízení Rady (ES) č. 871/2004 ze dne 29. dubna 2004 o zavedení některých nových funkcí Schengenského informačního systému, také se zřetelem k boji proti terorismu.

⁵⁹ Ustanovení § 80 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

zákonu o ochraně osobních údajů (Hlava III) se rozumí jejich předávání do jiných zemí. V zákonu o policii tento postup vymezen není, avšak z povahy zákona o policii vyplývá, že je předáním myšleno předání osobního údaje jinému subjektu. Závažné ohrožení bezpečnosti osob a veřejného pořádku (§ 80 odst. 1 písm. b) zák. o policii) se vztahuje k plnění úkolů policie podle ust. § 2 zákona o policii. Podle Ústavního zákona o bezpečnosti spočívá bezpečnost v zajištění svrchovanosti a územní celistvosti, ochraně jejích demokratických základů a rovněž tak v ochraně životů, zdraví a majetkových hodnot občanů.

Ve smyslu odst. 3 se pravomocným rozhodnutím orgánu činného v trestním řízení (soud, státní zástupce a policejní orgán) rozumí pravomocný rozsudek či usnesení.

Odst. 4 je ve vztahu k zákonu o ochraně osobních údajů, který stanoví, že zpracovávat lze pouze přesné a pravdivé osobní údaje, které jsou získány v souladu s právním řádem (zákon o ochraně osobních údajů pojem „neověřené údaje“ nezná). Uvedený odstavec upravuje výjimku danou zákonem o ochraně osobních údajů (ust. § 3 odst. 6 k ust. § 5 odst. 1 zák. č. 101/2000 Sb.). „Pokud je to nezbytné, musí policie osobní údaje aktualizovat, aby naplnila zákonnou povinnost. Zjistí-li policie, že jí zpracovávané osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje doplní, jinak osobní údaje zlikviduje.“⁶⁰

Nepřesné osobní údaje⁶¹ musí policie označit a může s nimi nakládat pouze v mezích zákona o ochraně osobních údajů. Správce je povinen předat bez zbytečného odkladu všem příjemcům informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů.

Neověřené osobní údaje⁶² – nový pojem, který uvádí zákon o policii, tento pojem nedefinuje a specifikuje možnost jejich použití tím, že budou označeny a bude uvedena míra jejich spolehlivosti.

⁶⁰Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 249.

⁶¹ „Nepřesné osobní údaje“ definuje zákon o ochraně osobních údajů jako údaje, které jsou pravdivé, ovšem z pohledu komplexnosti údajů nemají ucelenou hodnotu, např. nejsou úplné, a lze je zpracovávat pouze v mezích povolených výjimek v rámci plnění povinností správce stanovených zvláštními zákony.

⁶² „Neověřeným osobním údajem je údaj, který vzhledem ke své formě zjištění (neoficiální pramen či databáze) a svému zpětnému oficiálnímu neověření nemá věrohodnou vypovídací hodnotu.“ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 249.

3.13 Zveřejňování osobních údajů

Ustanovení § 81 zákona o policii upravuje možnost zveřejňovat osobní údaje policií za stanovených podmínek, takto stanovené podmínky souvisejí s úkoly policie.

„Policie může zveřejňovat osobní údaje

a) v rozsahu nezbytném k plnění úkolů policie v souvislosti

1. se zajišťováním bezpečnosti České republiky,
2. s pátráním po osobách, nebo
3. s předcházením a vyhledáváním trestné činnosti, nebo

b) pro účely předcházení a zamezování závažných ohrožení veřejného pořádku a bezpečnosti.“⁶³

Pojmem „bezpečnost České republiky“ se podle Ústavního zákona o bezpečnosti rozumí zajištění svrchovanosti a územní celistvosti, ochrana jejích demokratických základů a rovněž ochrana životů, zdraví a majetkových hodnot občanů.

Pátráním po osobách se rozumí postup podle ustanovení § 68 zákona o policii.

Definovat trestnou činnost lze na základě trestního zákona, kde jsou popsány skutkové podstaty trestných činů, tedy jednání, která jsou postihována trestněprávními sankcemi. Předcházet trestné činnosti lze také prostřednictvím opatření prevence kriminality, tj. cíleným, plánovitým, koordinovaným a komplexním působením na příčiny a podmínky, které trestnou činnost vyvolávají či umožňují, s cílem takovému jednání předcházet.⁶⁴

Ve smyslu ust. § 23 zákona o policii má policie možnost na základě žádosti nechat uveřejnit informace v hromadných sdělovacích prostředcích, a to i údaje vztahující se k § 81 zákona o policii.

3.14 Prověřování potřebnosti dalšího zpracování osobních údajů

„1) Policie nejméně jednou za 3 roky prověří, jsou-li osobní údaje zpracováváné pro účely podle § 85 nadále potřebné pro plnění jejích úkolů v této oblasti.

2) Orgány činné v trestním řízení, Ministerstvo spravedlnosti, Ústavní soud a Kancelář prezidenta republiky policii v mezích své působnosti průběžně informují pro účely

⁶³ Ustanovení § 81 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁶⁴ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 251.

prověřování podle odstavce 1 o svých pravomocných rozhodnutích, promlčení trestního stíhání, výkonu trestu nebo o rozhodnutích prezidenta republiky týkajících se trestního řízení, trestů nebo udělené amnestie anebo milosti.⁶⁵

Úprava vychází z výjimek, které má policie podle zákona o ochraně osobních údajů. Konkrétně jde o výjimky z ustanovení § 5 odst. 1 a § 11 a § 12 zákona o ochraně osobních údajů. Institute uvedené v odstavci 2 mají povinnost v rámci své působnosti policii průběžně informovat o jednotlivých rozhodnutích podle zákonných postupů. Limitem je, že se musí jednat o věci spadající do působnosti policie a z povahy věci se jedná o pravomocné rozhodnutí v trestněprávní rovině.

3.15 Informování o osobních údajích a oprava nepravdivých nebo nepřesných osobních údajů

Problematiku upravuje ustanovení § 83 odst. 1 až 6 zákona o policii. Toto ustanovení stanoví závazná pravidla, kterými je při nakládání s osobními údaji policie vázána.

„1) Policejní prezidium na písemnou žádost sdělí žadateli bezplatně osobní údaje vztahující se k jeho osobě, a to do 60 dnů od jejího doručení.

2) Policejní prezidium na písemnou žádost osoby provede neprodleně po jejím doručení bezplatně

a) opravu, likvidaci, blokování nebo doplnění nepravdivých nebo nepřesných osobních údajů vztahujících se k osobě žadatele nebo žadateli poskytne vysvětlení. Pokud by opravou, likvidací, blokováním nebo doplněním osobních údajů bylo ohroženo plnění úkolů podle § 85, může policie místo těchto operací připojit k souboru opravné prohlášení,

b) označení údajů vztahujících se k osobě žadatele, jestliže žadatel popírá jejich přesnost a nelze zjistit, zda jsou přesné nebo nikoli. Toto označení se odstraní pouze se souhlasem žadatele nebo na základě rozhodnutí příslušného soudu anebo Úřadu pro ochranu osobních údajů (dále jen „úřad“).

3) Novou žádost v téže věci lze podat nejdříve po uplynutí 6 měsíců od podání žádosti předchozí.

⁶⁵ Ustanovení § 82 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

4) Policie žádostem podle odstavců 1 a 2 nevyhoví, popřípadě vyhoví pouze částečně, pokud by sdělením došlo k ohrožení

- a) plnění úkolu podle § 85,
- b) utajovaných informací, nebo
- c) oprávněných zájmů třetí osoby.

5) O vyřízení žádosti policie žadatele písemně informuje. Informace o vyřízení žádosti obsahuje odůvodnění, s výjimkou případů, kdy se žadateli vyhovuje v plném rozsahu. Pokud by vyhověním žádosti nebo sdělením o nevyhovění žádosti došlo k ohrožení plnění úkolu podle § 85, policie žadatele písemně vyrozumí o tom, že nezpracovává žádné osobní údaje vztahující se k jeho osobě. Informace o vyřízení žádosti musí obsahovat poučení o tom, že žadatel má právo obrátit se na úřad.

6) Na postup při vyřizování žádosti se vztahuje část čtvrtá správního řádu.⁶⁶

Policejní prezidium je útvarem policie podle ustanovení § 6 zákona o policii.

Žadatel je osoba žádající o sdělení osobních údajů, které vede policie. Obsah písemné žádosti není stanoven. Datem doručení se rozumí doručení Policejnímu prezidiu. Způsob doručování není stanoven, je možné doručování podle subsidiarity správního řádu, osobně, prostřednictvím provozovatele poštovní licence nebo elektronickou formou.

Ve smyslu odst. 2 může žadatel, tj. osoba, která zjistí některou z podmínek uvedených v písm. a) nebo b), požádat o určitý uvedený úkon. Policejní prezidium musí tento úkon neprodleně provést. Výjimkou jsou úkony zpracování podle § 85 citovaného zákona, který umožňuje policii specifické zpracovávání osobních údajů při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů a zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti. V žádosti je třeba konkrétně uvést, kterého osobního údaje se žádost týká, (který údaj považuje žadatel za nepravdivý či nepřesný).

K odst. 4 písm. b): Utajovanou informací se rozumí informace v jakémkoliv podobě, zaznamenaná na jakémkoliv nosiči a označená v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací.⁶⁷

⁶⁶ Ustanovení § 83 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁶⁷ Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 255.

K ustanovení odstavce 6: Část čtvrtá správního řádu upravuje vyjádření, osvědčení a sdělení.⁶⁸ Touto právní úpravou se vylučuje použití části druhé a třetí správního řádu, upravující správní řízení. Úkony prováděné podle ustanovení § 83 zákona o policii nejsou jak z hlediska obsahu, tak z hlediska účinků rozhodnutím ve smyslu ustanovení § 9 správního řádu.

3.15.1 Postup při přijetí žádosti týkající se informace o zpracování osobních údajů Policíí České republiky⁶⁹

Podle § 83 odst. 1 zákona č. 273/2008 Sb., o Policii České republiky, má kdokoliv právo obrátit se na Policii České republiky s písemnou žádostí o sdělení informací o zpracování jeho osobních údajů Policií České republiky. V poslední době žadatelé nejčastěji požadují sdělení osobních údajů zpracovávaných v Schengenském informačním systému, popř. žádají sdělení všech údajů, které k nim Policie České republiky má.

O předmětných žádostech rozhoduje a tyto žádosti vyřizuje Policejní prezidium České republiky (k vyřízení žádosti je věcně příslušná skupina správy a kontroly osobních údajů). Žadatel ovšem ne vždy adresuje své podání na Policejní prezidium České republiky, ale mnohdy je přinese osobně na některou služebnu Policii České republiky. V takovém případě je Policie České republiky povinna (na kterémkoliv místě, které zajišťuje výkon spisové služby) podání přijmout. Zvolí-li žadatel místo, jehož úřední hodiny jsou zveřejněny (např. podatelna Policejního prezidia České republiky - www.policie.cz - povinně zveřejňované informace), je příjem podání omezen na úřední hodiny.

Podaná žádost je vyřizována v zákonné lhůtě 60-ti dnů v českém jazyce zasláním sdělení/rozhodnutí do vlastních rukou žadatele. Nezbytné identifikační údaje žadatele tvoří: jméno a příjmení, datum narození, adresa trvalého bydliště (popř. doručovací adresa pro zaslání odpovědi).

Bližší informace k žádostem týkajícím se zpracování osobních údajů Policií České republiky poskytne skupina správy a kontroly osobních údajů kanceláře

⁶⁸ Ustanovení § 154 až § 158 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

⁶⁹ Zdroj: Sběrka stanovisek, upozornění a metodických pokynů v oblasti osobních údajů, Policejní prezidium ČR, Kancelář policejního prezidia, Skupina správy a kontroly osobních údajů, č.j. PPR-6025-3/ČJ-2008-99KU, aktualizováno v souvislosti s nabytím účinnosti z. č. 273/2008 Sb.

policejního prezidenta – tel. 974 835 775 nebo 974 835 759. Další informace jsou k dispozici na <http://www.policie.cz> (povinně zveřejňované informace).

Postup při přijetí žádosti podle § 83 zákona č. 273/2008 Sb.:

Pokud se osoba dostaví na Policii České republiky v úředních hodinách podatelny a sdělí, že jde podat žádost týkající se osobních údajů, pak podatelna písemnou žádost přijme. Pokud se osoba dostaví na Policii České republiky mimo úřední hodiny podatelny a sdělí, že jde podat žádost týkající se osobních údajů, ochranná služba/recepční informuje osobu o úředních hodinách podatelny a o možnosti zaslat žádost poštou na adresu Policejního prezidia České republiky, Strojnická 27, 170 89 Praha 7; příp. doporučí osobě opětovně se dostavit s žádostí v úředních hodinách.

Pokud se osoba dostaví na Policii České republiky a sdělí, že jde projednat/uplatnit své právo týkající se osobních údajů a nemá s sebou písemnou žádost, poučí ochranná služba/recepční osobu podle § 83 odst. 1 až 3 zákona č. 273/2008 Sb., o Policii České republiky – „Policie na písemnou žádost sdělí žadateli bezplatně osobní údaje vztahující se k osobě žadatele, a to do 60 dnů od jejího doručení.“ (Nezbytné identifikační údaje žadatele potřebné k vyřízení žádosti jsou: jméno a příjmení, datum narození, adresa trvalého bydliště (popř. doručovací adresa pro zaslání odpovědi).

3.16 Zpracování údajů v Schengenském informačním systému

Právní úprava zpracování osobních údajů v Schengenském informačním systému vychází z předešlého zákona o policii (zákon č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů), kam byla vložena jako legislativní důsledek vstupu České republiky do schengenského systému.

„1) Policie v souladu se závazky České republiky vyplývajícími z mezinárodních smluv o odstraňování kontrol na společných hranicích a s nimi souvisejících předpisů Evropské unie⁷⁰ provádí zpracování informací včetně osobních údajů v Schengenském informačním systému.

⁷⁰ Úmluva podepsaná dne 19. června 1990 v Schengenu mezi Belgickým královstvím, Spolkovou republikou Německo, Francouzskou republikou, Lucemburským velkovévodstvím a Nizozemským královstvím k provedení dohody podepsané dne 14. června 1985 o postupném odstraňování kontrol na společných hranicích. Rozhodnutí Rady 2005/211/SVV ze dne 24. února 2005 o zavedení některých nových funkcí v Schengenském informačním systému, včetně boje proti terorismu. Nařízení Rady (ES) č. 871/2004 ze dne 29. dubna 2004 o zavedení některých nových funkcí Schengenského informačního systému, také se zřetelem k boji proti terorismu.

2) Policejní prezidium provozuje národní součást Schengenského informačního systému a plní úkoly orgánu centrálně odpovědného za národní součást Schengenského informačního systému a úkoly orgánu zajišťujícího výměnu doplňujících informací k záznamům v Schengenském informačním systému.

3) Policejní prezidium provede na základě žádosti soudu, státního zástupce, celního orgánu nebo zpravodajské služby podané v souladu se závazky České republiky vzniklými na základě mezinárodních smluv o odstraňování kontrol na společných hranicích a s nimi souvisejícími předpisy Evropské unie operaci v Schengenském informačním systému. Operaci učiní bez zbytečného odkladu a v rozsahu vyplývajícím z této žádosti. V odůvodněném případě tak učiní po předchozím projednání s orgánem navrhujeícím příslušnou operaci.⁷¹

Soudy se rozumí podle zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích), ve znění pozdějších předpisů, státní orgán

- projednávající a rozhodující spory a jiné věci patřící do jejich pravomoci podle zákonů o občanském soudním řízení;
- projednávající a rozhodující trestní věci patřící do jejich pravomoci podle zákonů o trestním řízení;
- rozhodující v dalších případech stanovených zákonem nebo mezinárodní smlouvou, s níž vyslovil souhlas Parlament ČR, již je Česká republika vázána a která byla vyhlášena.

Státním zástupcem se rozumí jmenovaná osoba, jejímž prostřednictvím státní zastupitelství vykonává svou činnost.

Zpravodajskou službou se rozumí podle zákona o zpravodajských službách instituce působící v České republice, kterými jsou

- Bezpečnostní informační služba, jejíž příjmy a výdaje tvoří samostatnou kapitolu státního rozpočtu,
- Úřad pro zahraniční styky a informace, jehož rozpočet je součástí rozpočtové kapitoly ministerstva vnitra,
- Vojenské zpravodajství jako součást ministerstva obrany.

⁷¹ Ustanovení § 84 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

3.16.1 Právní podklad existence SIS

Schengenská prováděcí úmluva (SPÚ) ze dne 19. června 1990 (k Schengenské dohodě ze dne 14. 6. 1985, o postupném rušení kontrol na společných hranicích). SPÚ je rozsáhlý dokument, který má 142 článků a obsahuje ustanovení o fungování SIS (články 92 – 119), včetně otázky ochrany osobních údajů (články 126 – 130). Česká republika se k SIS připojila 1. 9. 2007 a ke dni 21. 12. 2007 je deklarován vstup ČR do Schengenského prostoru.⁷²

3.16.2 Schengenský informační systém⁷³

Je chráněný počítačový informační a dotazovací systém, který je určen k pátrání po osobách a věcech uvnitř smluvních států Schengenských dohod. Je nezbytný k tomu, aby schengenská spolupráce naplnila své cíle. Přístup k uloženým datům v SIS je vyhrazen výlučně orgánům státu příslušným k provádění kontrol na hranicích nebo k provádění jiných policejních a celních kontrol ve vnitrozemí a k jejich koordinaci.

Každá osoba má právo obdržet informaci o údajích evidovaných k její osobě v SIS. Poskytnutí této informace je zamítnuto, jestliže je to nezbytné k provedení (legálního) úkolu v souvislosti se záznamem, nebo k ochraně práv a svobod třetích osob. Je zamítnuto vždy, pokud u záznamu trvá účel utajeného sledování.

SIS umožňuje příslušníkům bezpečnostních složek na vnějších hranicích členských států i ve vnitrozemí monitorovat údaje o osobách a předmětech, které byly do databáze zaneseny v jakékoli jiné členské zemi a v určitých případech adekvátně reagovat – například zabránit ve vstupu na území schengenského prostoru osobě, které byl udělen zákaz vstupu v jiné členské zemi, nebo naopak zadržet osobu hodlající opustit území schengenského prostoru, která je hledána policií v jiném členském státě.

SIS tvoří:

- centrální systém C.SIS umístěný ve Štrasburku (Francie),
- národní systémy N.SIS (jeden v *každém* smluvním státě).

⁷² Uvádí HAVLÍČKOVÁ, J., LIŠKOVÁ, J. *Administrativa a informační technologie*. VPŠ a SPŠ MV v Praze, 2010, s. 23-25. Dostupný z datové sítě Intranet MV „HERMES“ z WWW: <www.spshr.mv.cz>.

⁷³ Definice informačních systémů – Příloha I. bakalářské práce (Zdroj: SMEJKAL, V. *Informační systémy veřejné správy ČR*. VŠE v Praze, 2003, s. 25-27).

N.SIS - zřizuje a vede každý smluvní stát. Platí, že datový soubor každé jednotlivé N.SIS je obsahově totožný s datovými soubory všech ostatních národních součástí členských států, jedná se vlastně o kopii centrální databáze C.SIS. Každý stát si pro provoz své národní součásti SIS musí ustanovit organizaci, která bude za činnost N.SIS zodpovědná. Touto organizací je národní kancelář SIRENE. Jejím hlavním úkolem je být komunikačním bodem k pátracím záznamům v SIS, udržovat on-line přístup do centrálního počítače C-SIS, realizovat rychlou výměnu kriminálně relevantních informací mezi bezpečnostními a justičními složkami členských států, spolupracovat s ostatními národními kanceláři SIRENE a s kanceláři VISION (VISION je orgán, který provádí konzultace žádostí o víza s ústředními orgány smluvních států).

Veškerá *dožádání od národní centrály SIRENE* vyřizují dožádané útvary policie podle stupně pilnosti, a to ve lhůtách velmi pilné do 24 hodin, pilné do 10 dnů, běžné do 30 dnů.

3.16.3 Obsah Schengenského informačního systému

Do systému SIS jsou zaváděny údaje podle článků SPÚ (čl. 95 – 100) a jsou dostupné koncovým uživatelům ze základního a komplexního dotazu v programu Dotazy do IS. V tomto programu se automaticky při zadání dotazu do informačních systémů PATROS, PATRMV, P-Zbraně a C-ENO označí v nabídce dostupných IS také požadavek na provedení dotazu do národní součásti Schengenského informačního systému.

Postup po zásahu (vypátrání) osoby/věci je uveden přímo v odpovědi na zadaný dotaz. Platí vždy, že po kladné odezvě ze systému je třeba vyplnit formuláře, které jsou k dispozici na stránkách ÚSKPV – SIRENE (<http://mail-inter.pcr.cz/interpol/sirene/formulare.htm>), a zaslat je v elektronické podobě na adresu kanceláře SIRENE.

3.16.4 Zdrojové informační systémy - N. SIS České republiky

Mezi informační systémy, ze kterých jsou prostřednictvím národní součásti (N.SIS) předávány do centrální součásti požadavky na vytvoření (změnu nebo výmaz) českých záznamů v Schengenském informačním systému, patří:

- **PATROS** - pátrání po osobách (osoby hledané, pohřešované, pátrání po pobytu),
- **PATRMV** - pátrání po vozidlech (vozidla odcizená, neoprávněně užívaná, pohřešovaná),
- **CIS** - úloha C-ENO - evidence nežádoucích osob (odepření vstupu cizincům na základě příslušných rozhodnutí správních orgánů a soudů) + úloha ZZD (ztracené a zcizené doklady cizinců),
- **P-ZBRANĚ** - evidence zbraní (odcizené, neoprávněně užívané, pohřešované zbraně),
- **KSU** – kriminalisticky sledované události (část věci),
- **OPATŘENÍ** - skryté sledování a cílené kontroly,
- **AFIS 2000** - pro vložení otisků prstů jako dalších údajů umístěných v centrální součásti,
- **CEO, CRV, CRŘ** a dále údaje z evidence občanských průkazů (**EOP**), z evidence cestovních dokladů (**ECD**), z evidence diplomatických a služebních pasů (**EDP**).

Lze konstatovat, že prověření a vyškolení uživatelé N.SIS (v podstatě se jedná o naprostou většinu výkonných příslušníků PČR) mohou v souladu s ustanovením čl. 102 SPÚ vytěžovat a využívat údaje v systému SIS především v průběhu policejních, celních a dalších kontrol konaných v souladu s národním právem na vlastním území a při prověřování žádostí o víza a vydávání povolení k pobytu.

3.17 Zpracování osobních údajů při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů a zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti

Tuto problematiku policejní činnosti upravují ustanovení § 85 až § 88 zákona o policii. V podstatě se jedná o výjimku z úpravy zákona o policii v části o práci s informacemi, která je v souladu se zákonem o ochraně osobních údajů dána policii pro účely tohoto věcně omezeného zpracování. Jedná se o skupinu osobních údajů, pro kterou platí zvláštní podmínky uchování a likvidace.

„1) Policie může při plnění svých úkolů

- a) zpracovávat nepřesné nebo neověřené osobní údaje; pokud je to možné, policie osobní údaje takto označí,
- b) zpracovávat osobní údaje i k jinému účelu, než ke kterému byly shromážděny,
- c) shromažďovat osobní údaje otevřeně i utajeným způsobem nebo pod záminkou jiného účelu anebo jiné činnosti,
- d) sdružovat osobní údaje, které byly získány k rozdílným účelům, za účelem předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů, zajištění vnitřního pořádku a bezpečnosti včetně pátrání po osobách a věcech a zajištění bezpečnosti České republiky.

2) Policie zpracovává osobní údaje podle odstavce 1 odděleně od osobních údajů zpracovávaných při plnění jiných úkolů policie.“⁷⁴

Většina pojmů citovaného ustanovení již byla vysvětlena v předcházejících podkapitolách.

Označení údajů znamená určité odlišení osobních údajů pro přesnou specifikaci v případě nepřesných nebo neověřených údajů (taková možnost je i v rámci elektronického systému). Je nutné vždy hodnotit možnosti (vhodnost v daném případě) této specifikace.

Utajený způsob shromažďování osobních údajů znamená možnost systematického postupu nebo souboru postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější

⁷⁴ Ustanovení § 85 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

zpracování, které jsou dostupné pouze pro daný okruh subjektů (např. pouze prostřednictvím stanoveného zabezpečení vstupu).⁷⁵

Policii je umožněno sdružovat osobní údaje, které byly získány k rozdílným účelům, což je výjimka z ustanovení § 5 odst. 1 písm. h) zákona o ochraně osobních údajů. Avšak i v tomto případě platí omezení, že musí být stanoven účel, k němuž mají být osobní údaje zpracovávány, a údaje lze zpracovávat jen v rozsahu nezbytném pro plnění úkolů policie.

„Při zpracování osobních údajů podle § 85 policie

- a) stanoví účel, k němuž mají být osobní údaje zpracovávány,
- b) neprodleně ohlásí úřadu zřízení každé evidence obsahující tyto osobní údaje; součástí tohoto hlášení je název útvaru odpovědného za zpracování osobních údajů, účel evidence, kategorie subjektu údajů a osobních údajů, které se těchto subjektů týkají, a popis opatření k zajištění požadované ochrany osobních údajů.“⁷⁶

Vedení samostatné evidence, které vychází z ustanovení § 85 odst. 2 zákona o policii, kdy policie musí shromážděné, zpracované či sdružené osobní údaje podle § 85 odst. 1 písm. a) až d) zákona o policii zpracovávat odděleně od osobních údajů zpracovávaných při plnění jiných úkolů, podléhá ohlášení Úřadu pro ochranu osobních údajů. Ohlášení ve smyslu ustanovení § 86 písm. b) zákona o policii je povinné a musí nastat neprodleně po zpracování, shromáždění či sdružení následně oddělené evidence osobních údajů a musí v něm být uvedeny všechny požadované náležitosti.⁷⁷

„1) Policie uchovává osobní údaje pro účely podle § 85 po dobu, která je nezbytná k účelu jejich zpracování. Pomine-li tento účel, osobní údaje zlikviduje.

2) Policie osobní údaje nezlikviduje,

- a) jsou-li dále využívány při plnění úkolu podle tohoto zákona nebo se jedná o osobní údaje, které jsou součástí spisového materiálu, bez ohledu na to, zda jsou zpracovány v listinné nebo automatizované podobě, nebo
- b) jde-li o zpracování osobních údajů pohřešované nebo hledané osoby, za podmínky, že
 1. osoba byla pohřešována nebo hledána opakovaně,
 2. lze důvodně předpokládat, že bude opět pohřešována nebo hledána, nebo

⁷⁵Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 259.

⁷⁶Ustanovení § 86 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁷⁷Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 260.

3. její osobní údaje jsou zpracovávány při plnění úkolů policie v souvislosti s trestnou činností.⁷⁸

Uchováním osobních údajů se rozumí udržování údajů v takové podobě, která je umožňuje dále zpracovávat, neboli jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky.

Co je trestnou činností je specifikováno v trestním zákoníku⁷⁹, kde jsou mj. popsány skutkové podstaty jednotlivých trestných činů, tedy jednání, která jsou postihována trestněprávní sankcí. Procesní postupy policie v jednotlivých stádiích trestního řízení upravuje trestní řád.⁸⁰

„Při zpracování osobních údajů pro účely podle § 85 bez vědomí subjektu údajů sdělí policie tomuto subjektu v okamžiku, kdy není ohroženo plnění úkolů policie v souvislosti s těmito účely, že pro své potřeby zpracovává jeho osobní údaje. Sdělení učinit nemusí,

- a) jsou-li tyto údaje zlikvidovány bez zbytečného odkladu po zániku uvedeného ohrožení, nebo
- b) pokud by sdělení těchto údajů bylo spojeno s neúměrným úsilím.⁸¹

Citované ustanovení se vztahuje k ustanovení § 85 zákona o policii a zakládá povinnost policie jako zpracovatele osobních údajů při zpracování údajů podle ustanovení § 85 odst. 1 písm. a) až d) bez vědomí subjektu, o kterém se tyto údaje vedou, sdělit tomuto subjektu informaci o zpracovávání těchto údajů pro potřeby policie. Doporučuje se písemná forma sdělení z důvodu zadokumentování. Předpokladem je, že účel uchovávání těchto údajů pominul. Úprava dále stanovuje výjimky, kdy takto policie činit nemusí.⁸²

⁷⁸ Ustanovení § 87 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁷⁹ Zákon č. 40/2009 Sb., trestní zákoník.

⁸⁰ Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

⁸¹ Ustanovení § 88 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁸² Uvádí ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň, 2009, s. 262.

4 RIZIKA POSUZOVANÁ SPRÁVCEM A ZPRACOVATELEM V RÁMCI PŘIJETÍ OPATŘENÍ K OCHRANĚ OSOBNÍCH ÚDAJŮ

Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

Správce nebo zpracovatel je povinen zpracovat, ale také dokumentovat přijatá a provedená technická a organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

V rámci přijímaných opatření správce nebo zpracovatel posuzuje rizika týkající se:⁸³

- plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
- zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
- zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahující osobní údaje,
- opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

Konkrétní podoba ochrany osobních údajů byla ponechána zákonodárcem na správci a zpracovateli. Bylo stanoveno, před čím vším je třeba osobní údaje při zpracování ochraňovat. V dnešní době pokročilých vědomostí o ochraně informačních systémů by se mohlo zdát, že k naplnění povinností stanovených k zabezpečení (ochraně) osobních údajů se vystačí se zjednodušenými přístupy. Všeobecně je známo, že informační systémy je možné chránit hesly, šifrováním apod. Avšak již méně pozornosti je věnováno organizačním opatřením, personální bezpečnosti a také fyzické ochraně informačních systémů nebo jejich technologiím.⁸⁴ Rovněž musí být vnímána nezbytnost zabezpečení prostor a objektů (místností a budov), ve kterých se uskutečňuje zpracování, shromažďování a uchovávání osobních údajů. Technické zabezpečení prostor, v nichž ke zpracování osobních údajů dochází, by mělo být chráněno alespoň

⁸³ Ustanovení § 13 odst. 1 až 3 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

⁸⁴ KUČEROVÁ, A. A KOL. *Zákon o ochraně osobních údajů: komentář*. C. H. Beck Praha, 2003, s. 136-137.

pomocí zámků, instalací mříží, bezpečnostními fóliemi na oknech a skleněných výplních dveří, případně nepojením objektů a místností na pulty centralizované ochrany. K ochraně a ostraze objektů a prostor, ve kterých jsou osobní údaje zpracovávány a uchovávány, lze využít i soukromých bezpečnostních služeb.

Jaká konkrétní opatření má správce či zpracovatel učinit, bude záviset na tom, o jaké osobní údaje se bude jednat, jaký bude rozsah zpracovávaných osobních údajů, jaké technické prostředky budou použity apod. Správce je tedy povinen sám vyhodnotit, rizika a stanovit prostředky a způsob ochrany, a to jak ochrany před jednáním osob, tak i před následky přírodních událostí. V důvodové zprávě k návrhu zákona o ochraně osobních údajů se uvádí, že subsidiárně lze ke stanovení a aplikaci bezpečnostních opatření využít vyhlášek Národního bezpečnostního úřadu č. 12/1999 Sb., o zajištění technické bezpečnosti utajovaných skutečností a certifikaci technických prostředků, dále vyhlášky č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátů. Jako pomůcka a inspirace může správci a zpracovateli posloužit také vyhláška NBÚ č. 339/1999 Sb., o objektové bezpečnosti.⁸⁵

Z hlediska technického je nutné odlišovat, zda se jedná o **manuální zpracování** osobních údajů či **automatizované zpracování** (zpracování osobních údajů prostřednictvím výpočetní techniky).

Osobní údaje zpracovávané v různých manuálních kartotékách nebo pořadačích mohou být ukládány do odpovídajících uzamykatelných kovových skříní nebo trezorů, stejně tak i zálohy počítačově zpracovávaných osobních údajů (na disketách, CD a DVD discích, flasch discích nebo externích pevných discích). Počítače, na kterých jsou zpracovávány osobní údaje, by měly být chráněny alespoň vstupním heslem uživatele, případně dalšími přístupovými právy v režimu jejich periodické obměny, které mají znát jen osoby, které mají u správců a zpracovatelů oprávnění s příslušnými osobními údaji pracovat.

⁸⁵ KUČEROVÁ, A. A KOL. *Zákon o ochraně osobních údajů: komentář*. C. H. Beck Praha, 2003, s. 138.

5 OPATŘENÍ PŘI ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V SCHENGENSKÉM INFORMAČNÍM SYSTÉMU

Ochrana osobních údajů v Schengenském informačním systému (SIS) je popsána v Schengenské prováděcí úmluvě (SPÚ) v článcích 126 – 130, délky uschovacích lhůt pro záznamy a osobní údaje jsou stanovené v článcích 112 a 113.

Pokud jde o automatizované zpracování osobních údajů, které jsou předávány v rámci SIS na základě Schengenské prováděcí úmluvy, musí přijmout každá smluvní strana nezbytné vnitrostátní právní předpisy pro zajištění ochrany osobních údajů. Česká republika díky své legislativě této úrovni ochrany osobních údajů dosahuje a je schopna ji v SIS zajišťovat. Zpracování informací včetně osobních údajů v Schengenském informačním systému řeší § 84 zákona č. 273/2008 o Policii ČR.

Ochrana osobních údajů v SIS – SIS může obsahovat pouze taxativně uvedené informace. Každá osoba má právo obdržet informaci o údajích, které jsou k ní evidovány v SIS. Poskytnutí takové informace může být zamítnuto, jestliže je to nezbytné k provedení úkonu v souvislosti se záznamem nebo k ochraně práv a svobod třetích osob. Poskytnutí informace je zamítnuto vždy, pokud u záznamu trvá účel utajeného sledování. Pokud dojde k neoprávněnému vložení osobních údajů do SIS nebo k neoprávněnému nakládání s nimi, může se postižená osoba bránit stanoveným postupem u kontrolního úřadu členského státu. V případě zjištění pochybení musí být údaje neprodleně opraveny nebo vymazány.

Zásady ochrany dat v SIS

- Data v SIS jsou ve vlastnictví jednotlivých členských států a nesmí být poskytnuta mimo orgány činné v trestním řízení nebo použita pro jiný účel.
- Záznamy vkládané do SIS musí být aktuální a právně podložené. Trvá-li potřeba pátrání v SIS, je třeba po určité době (osoby – 3 roky, věci – 10 let, skrytá kontrola – 1 rok/5 let) záznamy prodloužit.
- Dotazy do SIS jsou registrovány (stejně jako u národních databází), vždy je třeba uvést odpovídající důvod dotazu.
- Musí být zabráněno neoprávněnému přístupu k záznamům v SIS (přístup do IS Dotazy na heslo, stanovení přístupových práv, obrazovka /monitor/ otočená tak, aby na ni neviděla neoprávněná osoba, musí být zajištěna integrita databáze, zálohování, evidence přístupů apod.).

- Data z SIS mohou být kopírována pouze v případě řešení zásahu na příslušný záznam.
- Oprávněné osoby mohou mít při užívání databáze SIS přístup pouze k údajům, které spadají do jejich působnosti.
- Neoprávněné použití dat z SIS znamená trestní odpovědnost a mezinárodní skandál!

Pro předávání doplňujících informací o osobách a věcech evidovaných v Schengenském informačním systému je příslušná kancelář SIRENE. Plní všechny úkoly v oblasti získávání informací, jejich toku a koordinace, které souvisejí s pátráním a je kontaktním místem pro všechny ostatní národní kanceláře SIRENE. SIRENE (Supplementary Information Request at the National Entry) je strukturou národních kanceláří v rámci EU (Schengenu), která poskytuje dodatky k informacím vyžadovaným při práci s informacemi v národním SIS. Každý z členských států má svoji národní kancelář SIRENE, které mezi sebou komunikují přímo. Praktická činnost je pak pro státy Schengenské dohody upravena v příručce SIRENE.

Právní úprava

- Příručka SIRENE. SCH/Com-ex (99)5 z 28. dubna 1999.
- Rozhodnutí Rady č. 2003/19/ES z 14. října 2002, kterým se odtajňují některé části Příručky SIRENE.

Právní úprava používání SIS

- Schengenská prováděcí úmluva
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů
- Závazný pokyn policejního prezidenta č. 71/2007 o SIS
- Závazný pokyn policejního prezidenta č. 76/2007 o NC SIRENE
- Interní akty řízení Policejního prezidia ČR k jednotlivým zdrojovým IS

6 POVINNOSTI SPRÁVCE A ZPRACOVATELE PŘI ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V OBLASTI AUTOMATIZOVANÉHO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

„V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci přijímaných opatření povinen také

- a) zajistit, aby systémy pro automatizované zpracování osobních údajů používaly pouze oprávněné osoby,
- b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
- c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány,
- d) zabránit neoprávněnému přístupu k datovým nosičům.⁸⁶

Pokud se jedná o automatizované zpracování osobních údajů, mají přijímaná opatření

- zamezit neoprávněným osobám přístupu k zařízením, která se používají k zpracování osobních údajů, tj. kontrola přístupu k zařízením, tedy především popis zabezpečení prostor a objektů, kde se provádí zpracování osobních údajů (zámky, mříže, čidla a napojení na pult centralizované ochrany apod.),
- zabránit neoprávněnému čtení, kopírování, úpravě nebo mazání nosičů osobních údajů, tedy zejména popis zabezpečení výpočetní techniky, na které jsou zpracovávány osobní údaje (vstupní hesla, přístupová práva, režim obměny hesel atd.),
- zabránit neoprávněnému vkládání osobních údajů a neoprávněnému čtení, kopírování, úpravě nebo vymazání uložených osobních údajů (kontrola ukládání),

⁸⁶ Ustanovení § 13 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

- zabránit užití automatizovaných systémů zpracování osobních údajů neoprávněnými osobami, které jsou uživateli zařízení pro přenos osobních údajů (kontrola uživatele),
- zajistit, aby oprávněné osoby používat automatizovaný systém zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob (kontrola přístupu k údajům), a to na základě zvláštních přístupových práv zřízených výlučně pro tyto osoby,
- zajistit, aby bylo možné prostřednictvím uložených elektronických záznamů určit a ověřit, kdy, kým a z jakého důvodu a kterým subjektům byly nebo mohly být osobní údaje zpřístupněny za použití zařízení pro sdělování osobních údajů (kontrola sdělování),
- zajistit, aby bylo možné pomocí uložených elektronických záznamů určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje vloženy do automatizovaných systémů zpracování osobních údajů nebo jinak zpracovávány (kontrola vkládání a úpravy),
- zabránit neoprávněnému čtení, kopírování, úpravě nebo výmazu osobních údajů v průběhu přenosů osobních údajů nebo v průběhu přepravy nosičů údajů (kontrola přenosů a přepravy),
- zajistit, aby nainstalované systémy mohly být v případě výpadku systému okamžitě obnoveny (obnova systému),
- zajistit, aby systém fungoval bezchybně, výskyt chyb ve funkcích byl okamžitě hlášen (spolehlivost) a aby uložené osobní údaje nebylo možné poškodit špatným fungováním systému (integrita systému).

Pokud jednu počítačovou sestavu používá více pracovníků, kteří zpracovávají spisy nebo dokumenty obsahující osobní údaje, s kterými nejsou ostatní uživatelé této počítačové sestavy oprávněni se seznámit (příčemž je nutné zohlednit konkrétní okolnosti zpracování osobních údajů a působnost organizačního celku), musí mít každý jednotlivý pracovník pro práci na počítačové sestavě vytvořeno své uživatelské konto pro přístup k počítačové sestavě. Pokud to používaný operační systém nedovoluje, musí být zajištěno, aby pracovník mohl spisy či dokumenty obsahující osobní údaje ukládat pouze na přenosné paměťové médium (disketa, flash disk, CD, DVD apod.), a toto médium následně zajistit proti zneužití.⁸⁷

⁸⁷ Závazný pokyn policejního prezidenta č. 215/2008, kterým se stanoví některé bližší podmínky a postupy pro zpracování osobních údajů (o ochraně osobních údajů) ze dne 31. 12. 2008, čl. 75.

7 POCHYBENÍ PŘÍSLUŠNÍKŮ POLICIE ČR V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

7.1 Profesní pochybení příslušníků Policie ČR v souvislosti se zpracováním osobních údajů zjištěná ÚVK PP ČR⁸⁸

- 1) Příslušník operačního střediska OŘ PČR lustroval osoby na základě požadavku hlídek v terénu, které mu byly předány pomocí radiostanice. Při lustracích nezaznamenal účel dotazu do informačních systémů ani ve služební pomůcce.
- 2) Příslušník místního oddělení PČR, dozorčí služba, provedl lustraci osoby, tuto lustraci nebyl schopen doložit záznamem v účelu dotazu v IS ani ve služební pomůcce. Na pracovní stanici, ze které byl dotaz učiněn, se v době lustrace střídalo několik pracovníků. Dle vyjádření příslušníka mohla být lustrace provedena neoprávněně někým jiným na jeho „login“, protože při odchodu od počítače neprovedl odhlášení z informačního systému.
- 3) Příslušník Pohotovostní motorizované jednotky hl. m. Prahy Policie ČR lustroval osobu pro soukromé účely.
- 4) Příslušník místního oddělení Policie České republiky provedl lustraci osob a do účelu dotazu uvedl „č.j.“. Lustrované osoby však ve spise neprocházejí, důvodnost lustrace nebyl příslušník schopen doložit.
- 5) Příslušník obvodního oddělení Policie ČR při prošetřování neobjasněného přestupku tipoval možného pachatele lustrací v informačním systému pomocí dotazu na osoby bydlící na adrese. Při zadání dotazu omylem zaměnil dvě čísla popisná na stejné adrese a lustroval tak osoby na jiné adrese, než jak je uvedeno ve spisovém materiálu.
- 6) Příslušník obvodního oddělení Policie ČR se při lustraci osoby dle jména, příjmení a rozsahu data narození dotkl evidenčně chráněné osoby. Při lustraci do účelu dotazu uvedl "WW", lustraci nezapsal do služební pomůcky a nebyl schopen zpětně doložit účel dotazu.
- 7) Příslušník obvodního oddělení PČR provedl lustraci osoby ve snaze pomoci svému kolegovi upamatovat si a vybavit si osobu, kterou měl v minulosti

⁸⁸ Úřad vnitřní kontroly Policejního prezidia ČR je součástí organizační struktury Policejního prezidia ČR, přičemž vedoucí tohoto úřadu je podřízen přímo policejnímu prezidentovi. Zdroj: datová síť Intranet Ministerstva vnitra „HERMES“/Policejní prezidium/ÚVK/důležitá stanoviska/profesní pochybení. Dostupné z WWW: <http://ppportal.pcr.cz/oks/Profesni_pochybeni_osobni_udaje/Profesni_poch_osob>.

lustrovat. Lustraci provedl na základě ústní žádosti kolegy, který mu potřebu lustrace odůvodnil tím, že není volný jiný počítač, ze kterého by mohl lustraci provést sám.

- 8) Příslušník služby kriminální policie a vyšetřování obvodního ředitelství PČR opětovně lustroval evidenčně chráněnou osobu, což odůvodnil tím, že kontrolním orgánům musel zdůvodňovat její předchozí lustraci a chtěl si rozpomenout, proč tuto osobu v minulosti lustroval.
- 9) Příslušník obvodního oddělení PČR při lustraci rodinných příslušníků evidenčně chráněné osoby do účelu dotazu uvedl „dot“ a zpětně nebyl schopen provedenou lustraci odůvodnit.
- 10) Příslušník obvodního oddělení PČR lustroval svoji osobu podle jména a příjmení, což odůvodnil potřebou zjistit číslo svého cestovního pasu. Vzhledem k tomu, že při dotazu použil interval datumu narození, dotkl se neúmyslně evidenčně chráněné osoby stejného jména.
- 11) Občanský zaměstnanec obvodního ředitelství PČR neodůvodněně (neoprávněně) lustroval svého dřívějšího známého.
- 12) Příslušník obvodního oddělení PČR nebyl schopen doložit účel a oprávněnost dotazu do IS na osobu s odvoláním na velké množství zákroků v dané době, kdy pravděpodobně ověřoval totožnost osoby kontrolované při zákroku. Do účelu dotazu v IS uvedl pouze "šetření", nevyplnil kontrolní lístek pro vložení do IS KONTROLA, ani lustraci nezapsal do služební pomůcky.
- 13) Příslušník odboru služby cizinecké policie provedl lustraci osoby při dotazu na obyvatele domu dle adresy a čísla popisného. Do služební pomůcky nezapsal účel dotazu, a lustraci odůvodnil tím, že zkoušel možnosti aplikace „Dotaz do IS“, protože s tímto programem již delší dobu nepracoval a chtěl si ověřit svoji znalost práce s tímto programem.
- 14) Kontrolní pracovník odboru vnitřní kontroly obvodního ředitelství Policie České republiky v době pracovní neschopnosti telefonicky požádal bývalého kolegu zařazeného u ředitelství služby cizinecké policie, aby v informačním systému C-LOOK ověřil registrační značku vozidla. Tento požadavek vznesl nad rámec svých pracovních povinností pro soukromou potřebu. Oslovený příslušník žádosti vyhověl, přičemž výsledek lustrace sdělil v té době nepovolané osobě i přes to, že kontrolní pracovník neuvedl řádný důvod lustrace.

7.2 Profesní pochybení příslušníků Policie ČR v souvislosti se zpracováním osobních údajů: zdroje informací mimo resort MV⁸⁹

Příslušník Inspekce MV stane před soudem (Lidové noviny, 1. 3. 2004)

Neoprávněného nakládání s citlivými osobními daty se měl dopouštět vysoký funkcionář Inspekce ministra vnitra. Případ se týkal útvaru, který byl podřízen přímo ministru vnitra Grossovi. Na lavici obžalovaných měl dosednout v dohledné době jeden z nejnvýše postavených funkcionářů Inspekce ministra vnitra, citlivého útvaru, který se zabývá odhalováním policejních zločinů. Speciální tým státního zástupce Michala Zachystala z OSZ Praha 1 uzavíral případ důstojníka M. K., který podle obvinění ze září 2003 neoprávněně nakládal s citlivými osobními daty z nejrůznějších chráněných evidencí, do kterých měl hladký přístup právě díky svým úředním pravomocím a své funkci. „Případ je v podstatě uzavřen, zbývá mi dovyslechnout pár svědků, s nimiž byly nějaké problémy, ale hned poté navrhnu podání obžaloby,“ sdělil LN státní zástupce Michal Zachystal, podle nějž byla důkazní situace taková, že kauzu rozhodně nebude zastavovat nebo odkládat. Případ byl skandální nejen tím, že aféra se týkala útvaru, který byl kvůli svým úkolům a citlivosti podřízen přímo ministru vnitra Stanislavu Grossovi, ale i tím, že důstojník M. K. byl dokonce jedním z šéfů odboru, který v rámci Inspekce MV patřil mezi klíčové, totiž velel sekci zabývající se vyšetřováním kriminality policistů v hlavním městě, kde sídlí nejen množství obvodních a dvě krajské policejní správy, ale také specializované složky Policie ČR s celostátní působností a Policejní prezidium ČR.⁹⁰

Policista donášel podsvětí (MF Dnes, 3. 10. 2003)

Policista za úplatu vynášel obchodníkovi s drogami informace z policejních spisů. Za zneužití pravomoci veřejného činitele mu byl uložen podmíněný trest, navíc zákaz činnosti, kdy nesmí po dobu pěti let vykonávat službu v bezpečnostním sboru. Bývalému policistovi Miroslavu Tolarovi, který sloužil na policejním oddělení v Plzni, soud prokázal, že poskytl informace známému Albánci Dželalu Muričimu o vyšetřování převozu 1 kg heroinu do Německa. Vzhledem k úniku uvedených informací musel útvar pro odhalování organizovaného zločinu vyměnit některé detektivy pracující na případu

⁸⁹ LANGER, I. *Černá kniha policejních hříchů II*. Praha, říjen 2003 – říjen 2004. ODS, stínový ministr vnitra, Praha : Pdf, 2004. Dostupné z WWW: <http://www.ods.cz/docs/dokumenty/kniha_policejnich_hrichu_II.pdf>.

⁹⁰ LANGER, I. *Černá kniha policejních hříchů II*. Praha, říjen 2003 – říjen 2004. ODS Praha, 2004, s. 55. Dostupné z WWW: <http://www.ods.cz/docs/dokumenty/kniha_policejnich_hrichu_II.pdf>.

nebo stáhnout vyzrazená vozidla, z nichž specializovaný policejní útvar sledoval pašeráky heroinu.⁹¹

Policisté prodávali data zadržených (TV Prima, 17. 10. 2003)

Jeden z největších policejních skandálů za posledních pět let řešila Inspekce ministra vnitra. Dva vysocí pražští policejní důstojníci byli obviněni, že obchodovali s osobními údaji. Osobní údaje zadržených měli dokonce prodávat jednomu významnému českému médiu. Obvinění policejní důstojníci patřili k takzvané elitě policejního sboru. Podle informací TV Prima měli být totiž obviněni šéf pražského odboru pro boj s organizovaným zločinem a jeho zástupce, tedy policisté, kteří vyšetřují ty nejzávažnější trestné činy.⁹²

Policista varoval podezřelého, dostal podmínku (MF Dnes, 9. 1. 2004)

Bývalý chrudimský policejní důstojník Jiří Kasl mařil práci svých kolegů tím, že mužům podezřelým z rozsáhlé trestné činnosti vyhradil, že je odposlouchává policie, navíc jim pomáhal radami, jak se mají chovat, aby nebyli dopadeni. Krajský soud v Hradci Králové vyměřil bývalému policistovi podmíněný trest v trvání tří let.⁹³

Policejní podplukovník obviněn z vynášení informací mafiánům (Právo, 26. 8. 2004)

Podplukovník z policejního prezidia Jiří Pavlík byl obviněn ze zneužití pravomoci veřejného činitele. Inspekce ministra vnitra ho podezřívá, že vyzrazoval tajné informace lidem, kteří se mohou podílet na organizovaném zločinu. „Policistu jsem obvinil z trestného činu zneužití pravomoci veřejného činitele. Bližší informace sdělit nemohu, protože případ navazuje na vyšetřování velice závažné trestné činnosti jiných osob,“ řekl státní zástupce Jan Hudzieczek z Ústí nad Labem, který vyšetřuje trestné činy policistů. Bývalý okresní policejní ředitel Jiří Pavlík, později služebně zařazen ve funkci vedoucího skupiny krajské expozitury útvaru pro boj s organizovaným zločinem v Plzni, měl poskytovat choulostivé údaje z tzv. „živých vyšetřovacích spisů“ závažných trestních kauz. Inspekce MV následně prověřovala, zda za poskytnuté informace nebral peníze.⁹⁴

⁹¹ LANGER, I. *Černá kniha policejních hříchů II*. Praha, říjen 2003 – říjen 2004. ODS Praha, 2004, s. 59. Dostupné z WWW: <http://www.ods.cz/docs/dokumenty/kniha_policejnich_hrichu_II.pdf>.

⁹² LANGER, I. *Černá kniha policejních hříchů II*. Praha, říjen 2003 – říjen 2004. ODS Praha, 2004, s. 59. Dostupné z WWW: <http://www.ods.cz/docs/dokumenty/kniha_policejnich_hrichu_II.pdf>.

⁹³ LANGER, I. *Černá kniha policejních hříchů II*. Praha, říjen 2003 – říjen 2004. ODS Praha, 2004, s. 59. Dostupné z WWW: <http://www.ods.cz/docs/dokumenty/kniha_policejnich_hrichu_II.pdf>.

⁹⁴ LANGER, I. *Černá kniha policejních hříchů II*. Praha, říjen 2003 – říjen 2004. ODS Praha, 2004, s. 60-61. Dostupné z WWW: <http://www.ods.cz/docs/dokumenty/kniha_policejnich_hrichu_II.pdf>.

8 MĚSTSKÉ KAMEROVÉ SYSTÉMY

8.1 Obecný úvod do problematiky používání kamerových systémů v Policii ČR z pohledu ochrany osobních údajů

Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je vedle kamerového sledování prováděn současně záznam pořizovaných záběrů, anebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.⁹⁵

Městské kamerové dohlížecí systémy (dále jen „MKDS“) jsou určitým specifickým druhem využití kamerových systémů k odhalování protiprávní činnosti v nejzatíženějších městech a obcích České republiky, na které jsou uvolňovány státní finanční prostředky. V posledních několika letech se velmi rozšířily žádosti obcí, které chtěly provozovat kamerové systémy na veřejných prostranstvích, tzn. monitorovat obecní náměstí, ulice, parky apod. Žádosti byly odůvodňovány nutností chránit obecní majetek a veřejný pořádek, potřebou odhalovat a dokumentovat trestnou činnost, zabránit narůstajícímu vandalismu. Tyto uváděné účely jsou veřejnoprávní, a proto je musí plnit pouze stát prostřednictvím svých orgánů k tomu zřízených, anebo v přenesené působnosti, v případech zákonem taxativně vymezených, je plní i orgány obcí. Úřad pro ochranu osobních údajů k této problematice vydal stanovisko, jehož závěrem je, že obec, která by chtěla nainstalovat kamerové systémy na veřejných prostranstvích, porušuje právní předpisy České republiky, protože kamerový systém je v obcích možné provozovat jedině prostřednictvím Policie České republiky nebo obecní policie.⁹⁶

Pozoruhodný záměr byl například zaznamenán v Chomutově, kde tamní radní chtěli využívat kamerový systém k monitorování návštěvníků veřejných domů. Cílem bylo vytlačit prostituci z ulic města, ale vzhledem k hrozbě nadměrného narušování soukromí museli zástupci chomutovského magistrátu od tohoto záměru ustoupit.

⁹⁵ Samotné kamerové sledování fyzických osob není zpracováním osobních údajů ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů, protože postrádá úroveň podmínek pro zpracování údajů ve smyslu § 4 písm. e) citovaného zákona, což však nevylučuje aplikaci jiných právních předpisů, zejména ustanovení občanského zákoníku upravujícího podmínky ochrany osobnosti.

⁹⁶ Stanovisko Úřadu pro ochranu osobních údajů č. 2/2008 uveřejněné ve Věstníku ÚOOÚ č. 49/2008. Dostupné z WWW: <<http://www.uoou.cz>>.

8.2 Základní principy provozu městského kamerového dohlížecího systému⁹⁷

- a) Základní charakteristikou provozování a využívání MKDS je jejich preventivní funkce, tj. vytváření bezpečných zón v exponovaných lokalitách.
- b) MKDS jsou zejména instalovány v místech, kde se nejčastěji pohybují obyvatelé a návštěvníci měst, kde jsou koncentrovány kulturní, komerční a společenské instituce a kde jsou dopravní uzly měst (např. pěší a obchodní zóny měst, náměstí, autobusové nebo vlakové nádraží, sídliště, parkoviště apod.)
- c) MKDS slouží k dohledu nad dodržováním obecně závazných právních předpisů o ochraně veřejného pořádku, přispívají k bezpečnosti osob a majetku.
- d) MKDS slouží také k záznamu protiprávního jednání pachatelů trestných činů, pachatelů přestupků a napomáhají při jejich odhalování.
- e) Provozování MKDS musí být v souladu se zákonem č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, zákonem ČNR č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů, avšak také v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.
- f) MKDS musí monitorovat pouze veřejné prostranství.⁹⁸
- g) Riziková místa měst a obcí vhodná k nasazení MKDS stanovuje na základě podrobných analýz Policie České republiky.
- h) MKDS přinášejí obvykle okamžitý výsledek, tj. snížení kriminality ve vytipovaném místě, avšak musí být součástí celkové strategie prevence kriminality v určité lokalitě.
- i) MKDS jsou využitelné pro aktuální koordinaci činnosti složek Integrovaného záchranného systému při závažnějším ohrožení bezpečnosti občanů (technologické havárie v průmyslu, živelní pohromy, havárie v dopravě apod.).
- j) MKDS se musí stát součástí celkové strategie prevence kriminality v konkrétní lokalitě.

⁹⁷ KONÍČEK, T. Ochrana osobních údajů v oblasti využívání kamerových systémů. *Měsíčník POLICISTA* : vydává MV ČR, odbor prevence kriminality, červenec 2008, č. 7/2008, příloha s. 7.

⁹⁸ Veřejným prostranstvím se rozumí podle ust. § 34 zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů, všechna náměstí, ulice, tržiště, chodníky, veřejná zeleň, parky, a další prostory sloužící každému bez omezení, tedy sloužící obecnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru.

- k) Obrazové záznamy MKDS nejsou určeny pro veřejnost, ale pro vymezený okruh uživatelů – pouze pro Policii České republiky a obecní policii, a pro přesně vymezený účel.
- l) Režim dispečerského pracoviště MKDS musí být zajištěn tak, aby manipulaci s příslušnou technikou prováděla kompetentní a vyškolená obsluha a aby byl k němu zabráněn přístup nepovolaným osobám.
- m) O skutečnosti, že je veřejné prostranství monitorováno, musí být občané města a jeho návštěvníci dostatečně a srozumitelně informováni, například pomocí informačních tabulí s textem „Tento prostor je pod nepřetržitým dohledem kamer městské policie“ nebo se informace zveřejní na internetu.

8.3 Využívání městských kamerových dohlížecích systémů Policií České republiky

Policie České republiky (dále jen „policie“) může využívat kamerové systémy v rámci plnění úkolů uložených zákonem, příslušné oprávnění je zakotveno v ustanovení § 62 zákona č. 273/2008 Sb., o policii České republiky. Do této kategorie spadají stálé i přechodně instalované kamerové systémy instalované zejména pro předcházení páchaní přestupků a trestných činů a pro předcházení narušování veřejného pořádku, ale i pro další úkoly policie. Dále může policie využívat kamerové systémy v případě, že je to nezbytné pro ochranu jejich práv a právem chráněných zájmů.⁹⁹ Jedná se např. o provozování kamerových systémů k ochraně objektů a majetku v právu hospodaření a užívání policie¹⁰⁰ a kamerové systémy provozované k ochraně utajovaných informací.¹⁰¹

Kamerové sledování nesmí *nadměrně zasahovat do soukromí*, pokud to není pro plnění úkolů policie nutné a kamerový systém lze využívat pouze v mezích vymezených účelem (plnění úkolů policie – ust. § 2 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů).

⁹⁹ Ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

¹⁰⁰ Ustanovení § 14 zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, ve znění pozdějších předpisů.

¹⁰¹ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Doba uchování záznamů je omezena pouze účelem, k němuž byly záznamy pořízeny, avšak je nutno upozornit na zákonné omezení, že je povinností policie prověřovat potřebnost uchování osobních údajů nejméně jednou za tři roky, pokud jsou osobní údaje zpracovávány za účelem předcházení, vyhledávání a odhalování trestné činnosti a stíhání trestných činů, zajištění vnitřního pořádku a bezpečnosti včetně pátrání po osobách a věcech a zajištění bezpečnosti České republiky.¹⁰²

Ve většině záznamů kamerových sledování by se zejména s ohledem na technické důvody a praktickou využitelnost měla doba uchování údajů blížit době uchovávání u „klasických“ kamerových systémů, tedy v řádu dnů, případně využít tzv. „samo-přemazávací smyčky“.¹⁰³

Povinnost **zabezpečit ochranu osobních údajů** (snímacích zařízení, přenosových cest a nosičů dat, na nichž jsou záznamy uloženy) je stanovena v ust. § 13 zákona o ochraně osobních údajů – v praxi jde o zamezení neoprávněného nebo nahodilého přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Povinnost **informovat osoby o tom, že v místě je používán kamerový systém**¹⁰⁴ - většina stálých kamerových systémů sloužících k plnění úkolů policie má preventivně sledovací účel, tedy zveřejnění informace o tom, že je v místě užit, prakticky podpoří preventivní funkci systému. Samozřejmě existují výjimky, kdy je nutné užit kamerový systém pro plnění úkolů policie tak, aby zaznamenávaná osoba neměla tušení, že je nahrávána. V takovém případě nutnost osobu o zpracování jejích osobních údajů informovat odpadá.

Přístup subjektu údajů k údajům se v případě kamerových systémů určených pro plnění úkolů policie bude řídit ustanovením § 83 zákona o policii. Prakticky to ovšem zcela možné nebude, pokud osoba na záznamu nebude zcela identifikována, resp. nebudou v souvislosti se záznamem zpracovávány její další osobní údaje.

¹⁰² Ustanovení § 82 odst. 1 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

¹⁰³ Kamerové systémy v Policii České republiky z pohledu ochrany osobních údajů. *Policejní prezidium České republiky-Kancelář policejního prezidenta-Oddělení správy a kontroly osobních údajů*. Sbíрка stanovisek, upozornění a metodických pokynů v oblasti zpracování osobních údajů. Ročník 2008, Praha, 28. červenec 2008, číslo 3, s. 4.

¹⁰⁴ Ustanovení § 62 odst. 2 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů (příčemž forma informování není zákonem stanovena).

Provozování kamerových systémů určených pro plnění úkolů policie není potřeba oznamovat ani ohlašovat Úřadu pro ochranu osobních údajů.¹⁰⁵

Předpisy, které se z pohledu ochrany osobních údajů vztahují na kamerové systémy určené k plnění úkolů policie: 1) zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů, 2) zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, 3) Závazný pokyn policejního prezidenta č. 215/2008, kterým se stanoví některé bližší podmínky a postupy pro zpracování osobních údajů (o ochraně osobních údajů) ze dne 31. 12. 2008.

8.4 Městský kamerový systém hlavního města Prahy využívaný policisty Krajského ředitelství policie hl. m. Prahy

Městský kamerový systém hl. m. Prahy vznikl od roku 1997 a jeho budování vychází vstříc přání drtivé většiny obyvatel hlavního města žít v bezpečné Praze. Koncepce rozvoje Městského kamerového systému hl. m. Prahy (dále jen „MKS HMP“) byla před deseti lety schválena Zastupitelstvem hl. m. Prahy. Kvůli větší efektivitě vynaložených finančních prostředků se radní rozhodli instalovat technicky otevřený metropolitní kamerový systém s přístupem více uživatelů tak, aby byl schopen využívat také kamery ze systému Dopravního podniku hl. m. Prahy (dále jen „DPP“) a kamery Technické správy komunikací hl. m. Prahy (dále jen „TSK“). Tento systém poskytuje služby policejním složkám jak na úrovni krajského ředitelství, tak na úrovni policejních ředitelství obvodních částí I. až IV., vedle toho slouží i ostatním složkám Integrovaného záchranného systému. Systém je v nepřetržitém provozu, k 1. lednu 2010 bylo jeho uživatelům k dispozici celkem 560 kamer MKS HMP, 914 kamer DPP a 99 kamer TSK. Obraz ze 72 kamer je zpřístupněn veřejnosti na webové stránce hl. m. Prahy na adrese <<http://kamery.praha-mesto.eu>>, uživatelům internetu umožňuje sledovat aktuální situaci na exponovaných místech pražské dopravy. Moderní programové vybavení umožňuje např. automatickou ochranu kulturních památek proti vandalismu. V současnosti je tímto systémem střeženo třicet významných městských kulturních památek, kdy narušení zóny ochrany (tzv. elektronický plot) je automaticky hlášeno na pracoviště Policie ČR a současně na nejbližší služebnu městské policie. Pro

¹⁰⁵ Ustanovení § 18 odst. 1 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

snadnější odhalování průjezdů kradených vozidel jsou v MKS HMP instalovány programy schopné zajistit automatické vyhledávání odcizených vozidel porovnáním registračních značek s databází odcizených vozidel. Systém automaticky nahlásí výskyt odcizeného vozidla na příslušné operační středisko Policie ČR včetně fotografie odcizeného vozidla a jeho řidiče. MKS hl. m. Prahy se stal v průběhu let jedním z důležitých nástrojů k zajištění bezpečnosti občanů metropole a jejich návštěvníků. MKS HMP poskytují údaje k dopadení pachatelů a napomáhají k zvládnutí následků trestné činnosti, havárií, dopravních nehod nebo živelních neštěstí. To se týká také ochrany před teroristickými útoky jako relativně novým druhem ohrožení. Nutno dodat, že MKS hl. m. Prahy má i své odpůrce, třebaže i ti volají po větším bezpečí v metropoli, vyjadřují své obavy, že Městský kamerový systém hl. m. Prahy narušuje jejich soukromí.¹⁰⁶

Základní schéma MKS hl. m. Prahy a graf zobrazující výsledky využívání MKS HMP Krajským ředitelstvím policie ČR hl. m. Prahy jsou uvedeny v příloze II.

8.5 Konkrétní příklady přínosu MKS při plnění úkolů policie útvarem Integrované operační středisko KŘP hl. m. Prahy OŘ Praha II

V roce 2004 došlo v rámci reorganizace organizační struktury Správy hlavního města Prahy Policie České republiky mimo jiné ke sloučení obvodních ředitelství Prahy 2 a Prahy 5, čímž vzniklo Obvodní ředitelství Policie České republiky Praha II. Tím došlo i ke sloučení pracovišť operátorů kamerových systémů a umístění tohoto centra na operační středisko OŘ Policie ČR Praha II v Sokolské ulici. V červenci roku 2004 proběhla celková rekonstrukce operačního střediska včetně vytvoření moderního pracoviště operátorů MKS, kdy v nepřetržitém směnném provozu (12-ti hodinové denní a noční směny) zajišťuje obsluhu kamerových systémů v obvodu OŘ PČR Praha II dvojice operátorů. Postupně dochází k navyšování počtu kamer, také starší kamery jsou na vytipovaných místech měněny za nové s podstatně lepšími technickými parametry. V současné době lze v obvodu OŘ PČR Praha II využívat 86 kamer, přičemž jejich počet a umístění se průběžně aktualizuje na intranetových stránkách OŘ Praha II IOS MKS. Na těchto intranetových stránkách můžou policisté zařazení na základních

¹⁰⁶ Internetový portál Praha.eu/Popis městského kamerového systému. Dostupný z WWW: <http://www.praha.eu/jnp/cz/home/život_v_praze/bezpecnost/kamerovy_system/detailni_popis_mestskeh_o_kameroveho_systemu.html>.

útvarech OŘ PČR Praha II, příslušníci služby kriminální policie a vyšetřování, ale také např. příslušníci oddělení dopravních nehod, kteří prošetřují nápad trestné činnosti nebo přestupků dle územní a věcné příslušnosti, zjišťovat přesnou lokalizaci kamer MKS a prostranství, které jsou tyto kamery schopny monitorovat. Podle místa události pak dožadující policista vznáší požadavek operátorům MKS na vyhledání a uložení záznamu události z MKS. Znázornění možností některých kamer je v příloze III.

K dalšímu zvýšení efektivity činnosti operátorů MKS došlo, když jim byla zpřístupněna aplikace integrovaného komunikačního a řídicího systému „Dispečer-Maják 158“. Operátoři MKS tak mohou okamžitě reagovat na oznámenou událost a nejbližší kamerou nebo kamerami v dosahu monitorovat tuto událost, čímž pomáhají policistům operačního střediska získat další informace o předmětné události, tito policisté následně mohou rychle učinit potřebná opatření a efektivně řídit nasazení policejních sil a prostředků.

Na rychlost a úspěšnost opatření na místě události při předávání poznatků získaných z kamerového sledování hlídce nebo hlídkám v terénu mají vliv tyto faktory:

- schopnosti operátora MKS (znalost městského kamerového systému, zejména přesného umístění jednotlivých kamer MKS a jejich monitorovacích možností, místní znalost, dovednosti v ovládnutí MKS, iniciativa)
- schopnosti policistů operačního střediska (jejich místní znalost, přehled o silách a prostředcích, schopnost srozumitelně a rychle předat vizuální informace z MKS verbálně pomocí radiostanice hlídkám v terénu, zkušenosti, iniciativa)
- schopnosti policejních hlídek v terénu (místní znalost, výcvik, zkušenosti, iniciativa)
- technické možnosti (např. možnosti komunikace prostřednictvím digitální radiové sítě Pegas-Matra).

Operátoři MKS také vytěží denně podle hlášení událostí za posledních 24 hodin v informačním systému „UDÁLOST“ záznamy kamer v monitorovacím dosahu jednotlivých míst činů těchto událostí. V případě zjištění poznatků k události uloží příslušný kamerový záznam a vyrozumí o tom příslušné místní oddělení policie nebo službu kriminální policie a vyšetřování. Nejčastěji jsou zaznamenávány krádeže vloupáním do motorových vozidel, výtržnosti, rvačky, kapesní krádeže, loupežná přepadení, dopravní nehody apod. Operátoři MKS dále dohledávají záznamy událostí dle dožadání místních oddělení policie, služby kriminální policie a vyšetřování

a oddělení dopravních nehod. Předané záznamy událostí se stávají součástí spisových dokumentací a přispívají tak při dalším šetření jednotlivých skutků.

Zásluhou provozování MKS a kvalitní práce operátorů došlo k významnému snížení kriminality v oblastech monitorovaných kamerami. Některé konkrétní příklady využití MKS HMP policisty OŘ PČR Praha II jsou uvedeny v příloze IV.

ZÁVĚR

V závěrečném shrnutí lze konstatovat, že práce splnila své cíle. Tvůrčí část rozebírá problematiku práce s informacemi a řeší problematiku ochrany osobních údajů při jejich zpracování příslušníky a zaměstnanci Policie České republiky. Policie se v současnosti principiálně mění, část reformy již proběhla, ale mnoho zásadních kroků je před námi. Hlavním cílem reformy policie je policie otevřená a vstřícná, policie, kterou občané budou vnímat jako tu, která pomáhá a chrání. Zásadní význam pro reformu policie měl legislativní proces přípravy návrhu nového zákona o policii a s ním souvisejícího změnového zákona. Oba návrhy zákonů byly schváleny Senátem dne 17. července 2008 a podepsány prezidentem republiky dne 29. července 2008. K nabytí účinnosti zákona č. 273/2008 Sb., o Policii České republiky a zákona č. 274/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o Policii České republiky došlo dnem 1. ledna 2009. Jako zásadní změny v rámci zákona o policii lze uvést zejména: 1) postupné zvyšování počtu krajských správ z původních 8 až na celkový počet dnešních 14 krajských ředitelství, odpovídajících počtu a hranicím vyšších územních samosprávných celků a změnu jejich právního statusu na organizační složku státu; 2) zachování jednotnosti a hierarchického řízení bezpečnostního sboru; 3) plnění úkolů policie celou policií, tedy i zaměstnanci policie v pracovním poměru; 4) **podrobně upravené nakládání s informacemi a osobními údaji a jeho efektivní kontrola**; 5) nově nastavené podmínky kontroly policie Inspekcí policie. Bakalářská práce podrobně analyzuje problematiku práce s informacemi v Policii České republiky (Hlava X, § 60 až § 88 zákona o policii), uvádí souvislosti s ostatními zákony, interními předpisy a stanovisky Úřadu pro ochranu osobních údajů nebo interními stanovisky Oddělení správy a kontroly osobních údajů Policejního prezidia ČR k dílčím otázkám ochrany osobních údajů při jejich zpracování Policií České republiky. Ukazuje se, že vedle znalostí předpisů z oblasti zpracování a ochrany osobních údajů má ve vztahu k profesním pochybením příslušníků a zaměstnanců Policie ČR zásadní vliv účinná kontrola v oblasti nakládání s osobními údaji a jejich ochranou. S tím souvisí interní předpisy o vnitřní kontrole, ale zejména je nutno poukázat na základní povinnosti příslušníka podle ustanovení § 45 odst. 1 písm. a) až i) zákona č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů, a na povinnosti vedoucích příslušníků podle § 45 odst. 2 citovaného zákona, podle kterého je vedoucí příslušník mimo jiného též povinen „hodnotit výkon služby

podřízených policistů, zabezpečovat, aby příslušníci byli pro výkon služby náležitě vyškoleni a vycvičeni, oceňovat příkladné plnění služebních povinností, vyvozovat důsledky z porušení služebních povinností a přijímat podněty k odstranění závad a nedostatků, které ohrožují nebo ztěžují výkon služby“.

V části, která se zabývá městskými kamerovými systémy, práce podrobně analyzuje problematiku a zásady využívání kamerových systémů Policií České republiky. Provozování kamerových systémů je jednou z legitimních možností jak přispívat k ochraně životů, zdraví a majetku, ochraně veřejného pořádku a zabezpečení ostatních zákonem chráněných zájmů. Na druhou stranu musí být splněny veškeré zákonem stanovené podmínky o ochraně osobních údajů včetně principu přiměřenosti zásahu do osobnostních práv subjektů údajů. Je třeba si uvědomit, že při kamerovém sledování dochází většinou k neselektivnímu zaznamenávání jednání osob, z nichž se jen velmi malé procento dopouští protiprávního jednání. Záznamy kamerových sledování z městských kamerových systémů nesmí být v žádném případě použity z jiných důvodů, než je plnění úkolů policie. Příklad Městského kamerového systému hl. města Prahy potvrzuje, že jeho existence má příznivce i odpůrce, třebaže i ti volají po větším bezpečí v každodenním životě metropole. Lze konstatovat, že jednoznačně převažuje přínos využívání městského kamerového systému, který se stal v průběhu let jedním z důležitých nástrojů k zajištění bezpečnosti občanů hl. města Prahy a jeho návštěvníků. Na základě záznamů kamerového systému bylo dopadeno mnoho pachatelů trestných činů a přestupků, podařilo se najít mnoho odcizených vozidel, kamery napomáhají při opatřeních vedoucích k zvládnutí následků dopravních nehod, havárií nebo živelních pohrom. Díky dobré práci operátorů Městského kamerového systému hl. m. Prahy došlo v mnohých lokalitách pokrytých kamerami k výraznému snížení kriminality.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. 1. vyd. Praha : Linde Praha, a. s., 2009. 277 s. ISBN 978-80-7201-740-9.
2. FILKA, J. *Metodika tvorby diplomové práce*. 1. vyd. Brno : KNIHAŘ Brno, 2002. 224 s. ISBN 80-86292-05-3.
3. JANKOVÁ, L., DOLEŽAL, T., SVÁROVSKÁ, K. *Bezpečnostní sbory: texty zákonů s názvy paragrafů a věcným rejstříkem*. 1. vyd. Praha : C. H. Beck Praha, 2009. 334 s. ISBN 97880-7400-133-8.
4. KUČEROVÁ, A. A KOL. *Zákon o ochraně osobních údajů: komentář*. 1. vyd. Praha : C. H. Beck Praha, 2003. 388 s. ISBN 80-7179-762-6.
5. KUČEROVÁ, A., NONNEMANN, F. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha : BOVA POLYGON PRAHA, 2010. 152 S. ISBN 978-80-7273-163-3.
6. MAŠTALKA, J. *Osobní údaje, právo a my*. 1. vyd. Praha : C. H. Beck Praha, 2008. 212 s. ISBN 978-80-7400-033-1.
7. MATES, P. *Ochrana soukromí ve správním právu*. 2. aktualizované a přepracované vyd. Praha : Linde Praha, a. s., 2006. 313 s.
8. MATOUŠOVÁ, M. A KOL. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha : ASPI Publishing, s. r. o., 2004. 159 s. ISBN 80-7357-037-8.
9. MORÁVEK, J. *Průvodce ochranou osobních údajů v pracovněprávní agendě*. 1. vyd. Praha : Linde Praha, a. s., 2010. 144 s. ISBN 978-80-86140-64-3.
10. POLČÁK, R. *Právo na internetu*. 1. vyd. Brno : Computer Press, a. s., 2007. 154 s. ISBN 97880-251-1777-4.
11. SMEJKAL, V. *Informační systémy veřejné správy ČR*. 1. vyd. Praha : Vysoká škola ekonomická v Praze, 2003. 121 s. ISBN 80-245-0533-9.
12. SPOUSTA, V. *Vádemékum autora odborné a vědecké práce humanitního a sociálního zaměření*. 1. vyd. Brno : AKADEMICKÉ NAKLADATELSTVÍ CERM, s. r. o., Brno, 2009. 230 s. ISBN 978-80-7204-617-1.
13. ŠKODA, J., VAVERA, F., ŠMERDA, R. *Zákon o policii s komentářem*. Plzeň : Aleš Čeněk, s. r. o, 2009. 397 s. ISBN 978-80-7380-160-1.

Ostatní zdroje

1. KONÍČEK, T. Ochrana osobních údajů v oblasti využívání kamerových systémů. *Měsíčník POLICISTA : vydává MV ČR, odbor prevence kriminality*, červenec 2008, č. 7/2008, příloha s. 6-8.
2. Česko. Kamerové systémy v Policii České republiky z pohledu ochrany osobních údajů. *Policejní prezidium České republiky-Kancelář policejního prezidenta-Oddělení správy a kontroly osobních údajů*. Sbíрка stanovisek, upozornění a metodických pokynů v oblasti zpracování osobních údajů. Ročník 2008, Praha, 28. červenec 2008, číslo 3.
3. Česko. Upozornění gestora problematiky zpracování osobních údajů v Policii České republiky : Kamerové systémy se záznamovým zařízením. *Policejní prezidium České republiky-Kancelář policejního prezidenta-Oddělení správy a kontroly osobních údajů*. Sbíрка stanovisek, upozornění a metodických pokynů v oblasti zpracování osobních údajů. Ročník 2009, Praha, 19. červen 2009, číslo 2.

Legislativní dokumenty

1. Česko. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In *Sbíрка zákonů, Československá socialistická republika*. 1961, částka 66, s. 513-571. Dostupný z WWW: <[http://aplikace.mvcr.cz/sbirka-zakonu/sb66-61\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/sb66-61[1].pdf)>.
2. Česko. Zákon č. 200/1990 Sb., o přestupcích. In *Sbíрка zákonů, Česká republika*. 1990, částka 35, s. 810-826. Dostupný z WWW: <[http://aplikace.mvcr.cz/sbirka-zakonu/sb035-90\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/sb035-90[1].pdf)>.
3. Česko. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In *Sbíрка zákonů, Česká republika*. 2000, částka 32, s. 1521-1532. Dostupný z WWW: <[http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb032-00\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb032-00[1].pdf)>.
4. Česko. Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). In *Sbíрка zákonů, Česká republika*. 2000, částka 39, s. 1865-1871. Dostupný z WWW: <[http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb039-001\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb039-001[1].pdf)>.

5. Česko. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. In *Sbírka zákonů, Česká republika*. 2000, částka 99, s. 4666-4671. Dostupný z WWW:
< [http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb099-001\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb099-001[1].pdf)>.
6. Česko. Zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů. In *Sbírka zákonů, Česká republika*. 2003, částka 121, s. 5850-5910. Dostupný z WWW:
< [http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb121-03\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2000/sb121-03[1].pdf)>.
7. Česko. Zákon č. 379/2005 Sb., o opatřeních k ochraně před škodami způsobenými tabákovými výrobky, alkoholem a jinými návykovými látkami a o změně souvisejících zákonů. In *Sbírka zákonů, Česká republika*. 2005, částka 133, s. 7093-7101. Dostupný z WWW:
< [http://aplikace.mvcr.cz/sbirka-zakonu/2005/sb133-05\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2005/sb133-05[1].pdf)>.
8. Česko. Zákon č. 273/2008 Sb., o Policii České republiky. In *Sbírka zákonů, Česká republika*. 2008, částka 91, s. 4086-4116. Dostupný z WWW:
< [http://aplikace.mvcr.cz/sbirka-zakonu/2008/sb0091-2008\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2008/sb0091-2008[1].pdf)>.
9. Česko. Zákon č. 274/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o Policii České republiky. In *Sbírka zákonů, Česká republika*. 2008, částka 91, s. 4117-4154. Dostupný z WWW:
< [http://aplikace.mvcr.cz/sbirka-zakonu/2008/sb0091-2008\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2008/sb0091-2008[1].pdf)>.
10. Česko. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 354-462. Dostupný z WWW:
< [http://aplikace.mvcr.cz/sbirka-zakonu/2008/sb0011-2009\[1\].pdf](http://aplikace.mvcr.cz/sbirka-zakonu/2008/sb0011-2009[1].pdf)>.

Elektronické zdroje

1. HAVLÍČKOVÁ, J., LIŠKOVÁ, J. *Administrativa a informační technologie*. VPŠ MV v Praze, březen 2011. Datová síť Intranet Ministerstva vnitra „HERMES“. Dostupný z WWW: < <http://www.spsshr.mv.cz> >.
2. LANGER, I. *Černá kniha policejních hříchů II*. ODS Praha, 2004. Dostupný z WWW:
< http://www.ods.cz/docs/dokumenty/kniha_policejnich_hrichu_II.pdf>.

3. Hlavní město Praha, Městský kamerový systém hl. m. Prahy – *Detailní popis městského kamerového systému* [online]. Praha 2010. Dostupný z WWW: <http://www.praha.eu/jnp/cz/home/život_v_praze/bezpecnost/kamerovy_system/detailni_popis_mestskeho_kameroveho_systemu.html>.
4. Policejní prezidium ČR/Kancelář policejního prezidenta/Oddělení správy a kontroly osobních údajů/*Sbírka stanovisek a doporučení v oblasti ochrany osobních údajů*. Praha 2011 [online]. Datová síť Intranet Ministerstva vnitra „HERMES“. Dostupný z WWW: <<http://ppportal.pcr.cz/kancelar/skou/skou.asp>>.
5. Policejní prezidium ČR/Úřad vnitřní kontroly/*Pochybení policistů při nakládání s osobními údaji*. Praha 2010 [online]. Datová síť Intranet Ministerstva vnitra „HERMES“. Dostupný z WWW: <http://ppportal.pcr.cz/oks/Profesni_poch_osobni_udaje/prof_poch_osob.htm>.
6. Policie České republiky/Krajské ředitelství policie hl. m. Prahy/Obvodní ředitelství Praha II/*MKS Praha II*. Praha 2011 [online]. Datová síť Intranet Ministerstva vnitra „HERMES“. Dostupný z WWW: <<http://p12.pcr.cz/mks/home.html>>.
7. Ministerstvo vnitra ČR. *Stanovisko OBP MV ČR k ochraně osobních údajů OU/2006*. 2010 [online]. Datová síť Intranet Ministerstva vnitra „HERMES“. Dostupný z Intranetu MV WWW: <<http://ppportal.pcr.cz/kancelar/skou/skou.asp>>.
8. Úřad pro ochranu osobních údajů. *Názory Úřadu pro ochranu osobních údajů/K problémům z praxe/č. 3/2001-aktualizace 06/2009* [online]. Dostupný z WWW: <<http://www.uoou.cz/uoou.aspx?menu=14>>.
9. Policejní prezidium České republiky. *Závazný pokyn policejního prezidenta č. 215 ze dne 31. prosince 2008, kterým se stanoví některé bližší podmínky a postupy pro zpracování osobních údajů (o ochraně osobních údajů)* [online]. Datová síť Intranet Ministerstva vnitra „HERMES“. Dostupný z WWW: <http://ppportal.pcr.cz/centralni_portal/interni_akty_rizeni_ppcr.asp>.

PŘÍLOHY

Seznam příloh

I.	Přehled definic informačních systémů podle různých zdrojů.....	73
II.	Základní schéma MKS hl. m. Prahy a graf zobrazující výsledky využívání MKS HMP Krajským ředitelstvím Policie ČR hl. m. Prahy.....	76
III.	Ukázky mapového vyobrazení ze seznamu kamer Městského kamerového systému hl. m. Prahy, Obvodního ředitelství Policie ČR Praha II.....	78
IV.	Některé konkrétní příklady využití MKS HMP policisty OŘ Policie České republiky Praha II.....	83
V.	Sankce za delikty spáchané v souvislosti se zpracováním osobních údajů.....	88

PŘÍLOHA I.

Pro získání komplexnějšího pohledu na pojem informační systém je uváděno více používaných definicí:¹⁰⁷

1. definice:

Identifikovatelný funkční celek, zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací uložených na hmotném nosiči v údajových základnách a reprodukovatelných technickými prostředky. Informační systém integruje (zahrnuje) informační základnu (data), technické a programové prostředky, technologie, finanční prostředky a procedury a pracovníky.

Zdroj: Standardy státního informačního systému ČR, ÚSIS, Praha, prosinec 1996, s. 63.

2. definice:

Funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Každý informační systém zahrnuje informační základnu, technické a programové prostředky, technologie a procedury a pracovníky.

Zdroj: § 4 zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech (zrušený zákonem č. 101/2000 Sb.)

3. definice:

Systém zpracování informací spolu s návaznými organizačními prostředky, např. personálem, technickými a finančními prostředky; takový systém získává a distribuuje informace.

Zdroj: Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník. Část 1: Základní termíny. Český normalizační institut, Praha 1997, s. 11.

4. definice:

Informační systém zahrnuje informační dokumenty, informační pracovníky a informační procesy. Informační dokumenty jsou nosiče informací, na nichž jsou zaznamenávány tématické obsahy těchto informací. Informační procesy jsou všechny

¹⁰⁷ SMEJKAL, V. *Informační systémy veřejné správy ČR*. 1. vyd. Praha : Vysoká škola ekonomická v Praze, 2003, s. 25-27.

činnosti, jimiž se manipuluje s informacemi a vztahy mezi nimi. Informační systém v širším pojetí zahrnuje vlastní informační systém, ale i jeho okolí, tj. tvůrce a uživatele informací.

Zdroj: SMEJKAL, V., SOKOL, T., VLČEK, M. *Počítačové právo*. 1. Vydání, C. H. Beck Praha 1995, s. 198.

5. definice:

Systém pro sběr, zpracování, ukládání, vyhledávání a šíření informací.

Zdroj: KNAPP, V. *Právo na informace*. Academia Praha 1988, s. 31.

6. definice:

Systém, v němž vazby mezi prvky se chápou jako informace (data), resp. směry jejich toků a jednotlivé prvky jako místa vzniku, sběru, předzpracování, přenosu, uchování, zpracování, distribuce či zániku informací (dat); jeho účelem je tvorba a prezentace informací.

Zdroj: VESELÝ, J. *Systémové nástroje řízení*. IŘ Praha 1982, s. 302.

7. definice:

Dynamický systém, jehož vazby systému tvoří informace a prvky systému jsou místa transformací těchto informací.

Zdroj: Oborová encyklopedie Výpočetní a řídicí technika. SNTL Praha 1982, s. 279.

8. definice:

Informační systém je systém jehož prvky jsou informační a komunikační technologie, data a lidé. Cílem informačního systému je efektivní podpora informačních a rozhodovacích procesů na všech úrovních řízení organizace (podniku). Při návrhu a implementaci nové verze informačního systému organizace je třeba brát v úvahu řadu aspektů (dimenzí) a jejich vazeb:

- *hardware* – z jakých technických komponent bude vytvořena technologická infrastruktura informačního systému,
- *software* – jaké softwarové komponenty bude informační systém obsahovat a jaká bude funkcionalita a vzájemné vztahy těchto komponent,
- *data* – jaká data budou v informačním systému uložena, jaká data budou z okolí (např. od dodavatelů, od zákazníků) do IS vstupovat, jaká data budou naopak z IS do okolí poskytována,

- *procesy*- na podporu kterých podnikových procesů a činností bude IS sloužit a jakým způsobem,
- *informační služby* – služby, které bude IS poskytovat svým uživatelům; Služba je vymezena zejména dodavatelem služby, uživatelem služby, funkcionalitou, objemem (počet uživatelů, objem zpracovávaných dat), kvalitou (dostupnost, doba odezvy a zabezpečení jednotlivých aplikací) a cenou,
- *lidé* – kdo bude uživatelem jednotlivých aplikací/služeb a jejich funkcionality a jaké budou jejich kvalifikační předpoklady pro efektivní využití aplikací/služeb,
- *organizace* – jaké organizační změny a změny předpisů si implementace nové verze IS vyžádá,
- *legislativa* – jaké zákony a normy se k provozování jednotlivých aplikací vztahují,
- *ekonomika* – jaké náklady a jaké přínosy jsou s provozem IS spojeny.

Příklady vazeb mezi dimenzemi jsou: jaká data a jaké softwarové komponenty jsou uloženy na daném počítači, na funkcionalitu kterých softwarových komponent má vliv daný zákon apod.

Zdroj: HINDS, R., HOLMAN, R., HRONOVÁ, S. A KOL. *Ekonomický slovník*. C. H. Beck Praha 2003.

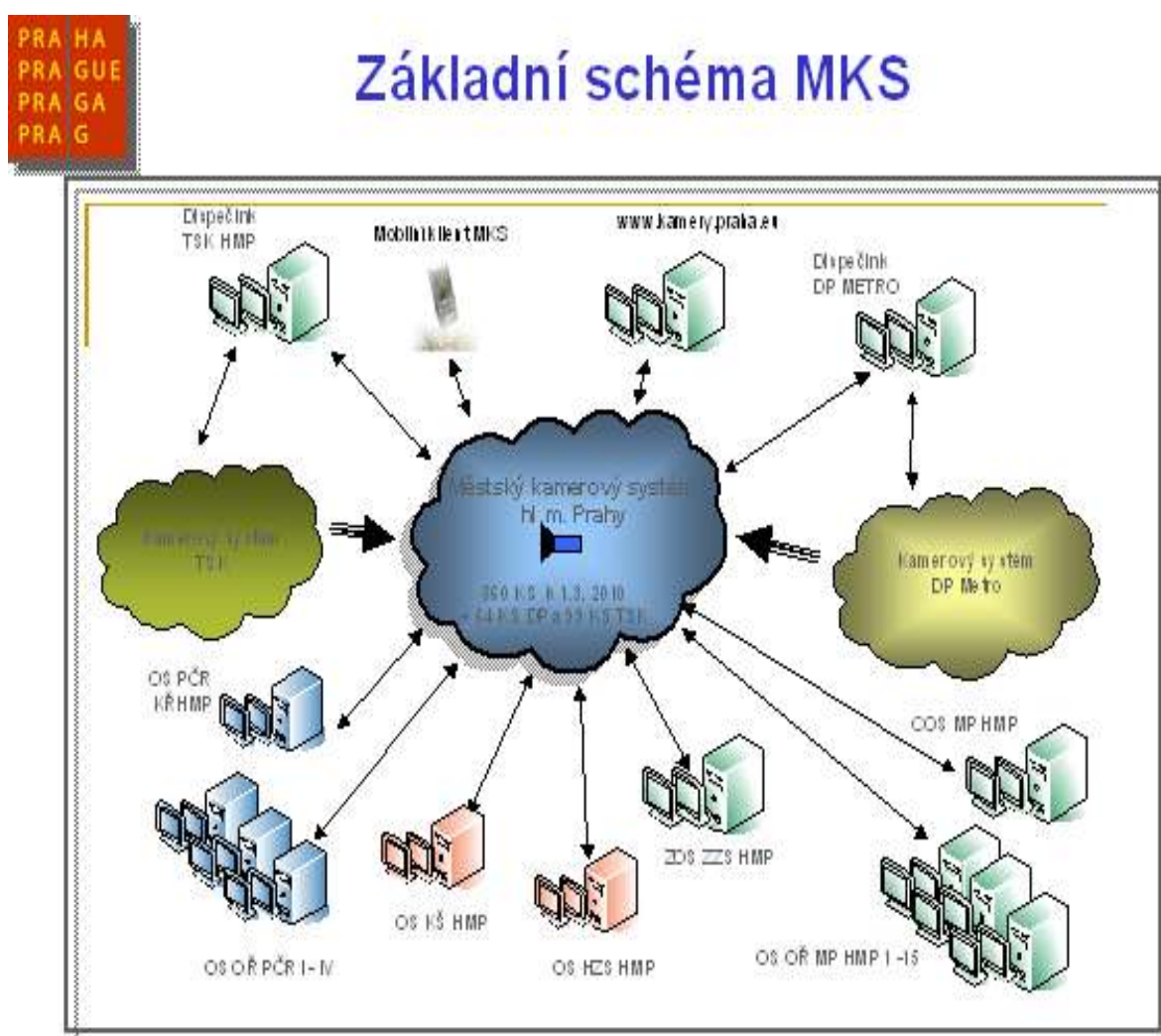
9. definice:

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

Zdroj: § 2 písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

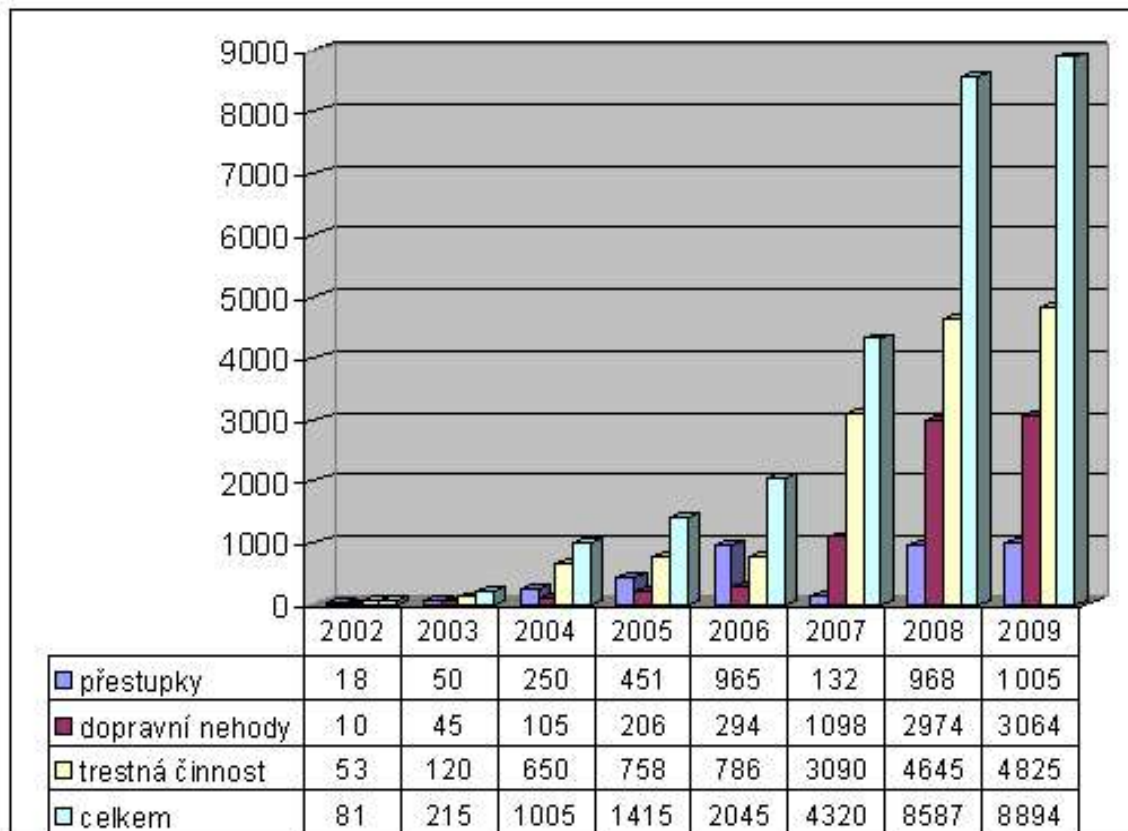
PŘÍLOHA II.

Základní schéma MKS hl. m. Prahy a graf zobrazující výsledky využívání MKS HMP Krajským ředitelstvím Policie ČR hl. m. Prahy



Obrázek č. 1 - Základní schéma městského kamerového systému hlavního města Prahy¹⁰⁸

¹⁰⁸ Zdroj: Internet - Hlavní město Praha, Městský kamerový systém hl. m. Prahy – Detailní popis městského kamerového systému [online]. Praha 2010. Dostupný z WWW: <http://www.praha-mesto.cz/detailni_popis_mestskeho_kameroveho_systemu_pdf>.



Graf č. 1 – Výsledky využívání Městského kamerového systému hl. m. Prahy Krajským ředitelstvím Policie České republiky hl. m. Prahy¹⁰⁹

¹⁰⁹ Zdroj: Internet - Hlavní město Praha, Městský kamerový systém hl. m. Prahy – Detailní popis městského kamerového systému [online]. Praha 2010. Dostupný z WWW: <http://www.praha-mesto.cz/detailni_popis_mestskeho_kameroveho_systemu_pdf>.

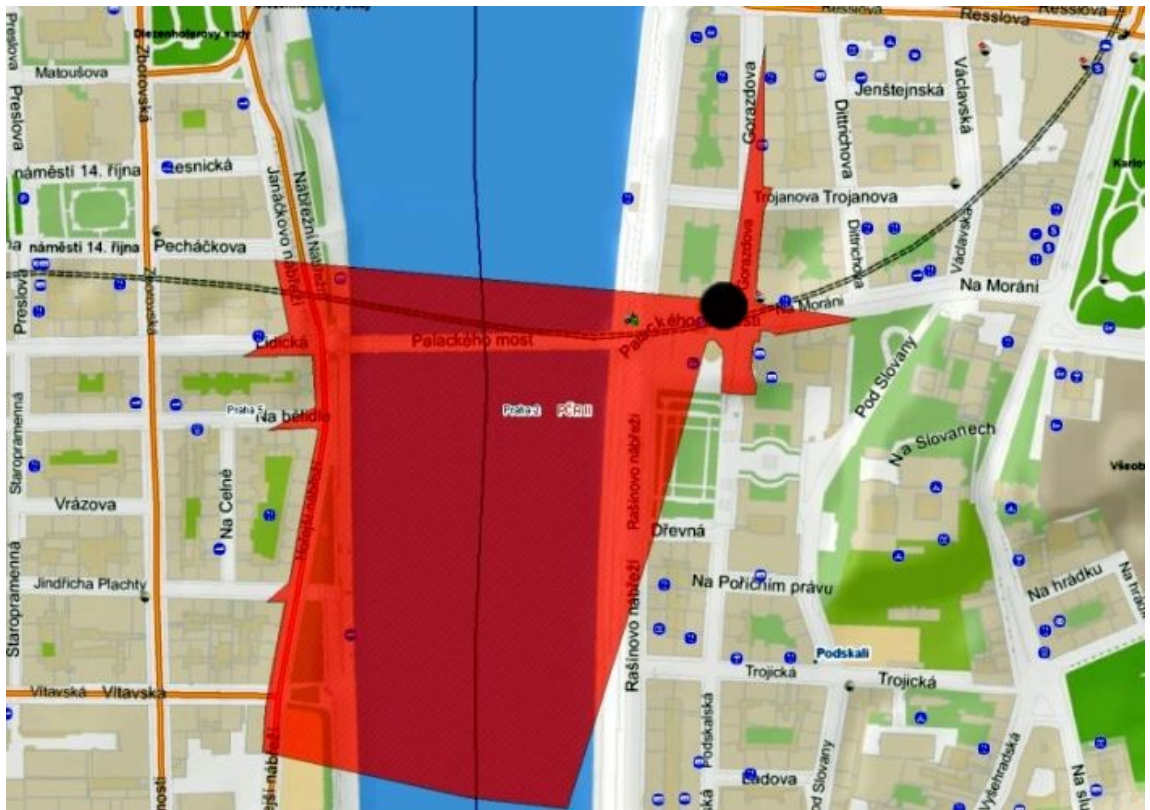
PŘÍLOHA III.

Ukázky mapového vyobrazení ze seznamu kamer Městského kamerového systému hl. m. Prahy, Obvodního ředitelství Policie ČR Praha II.

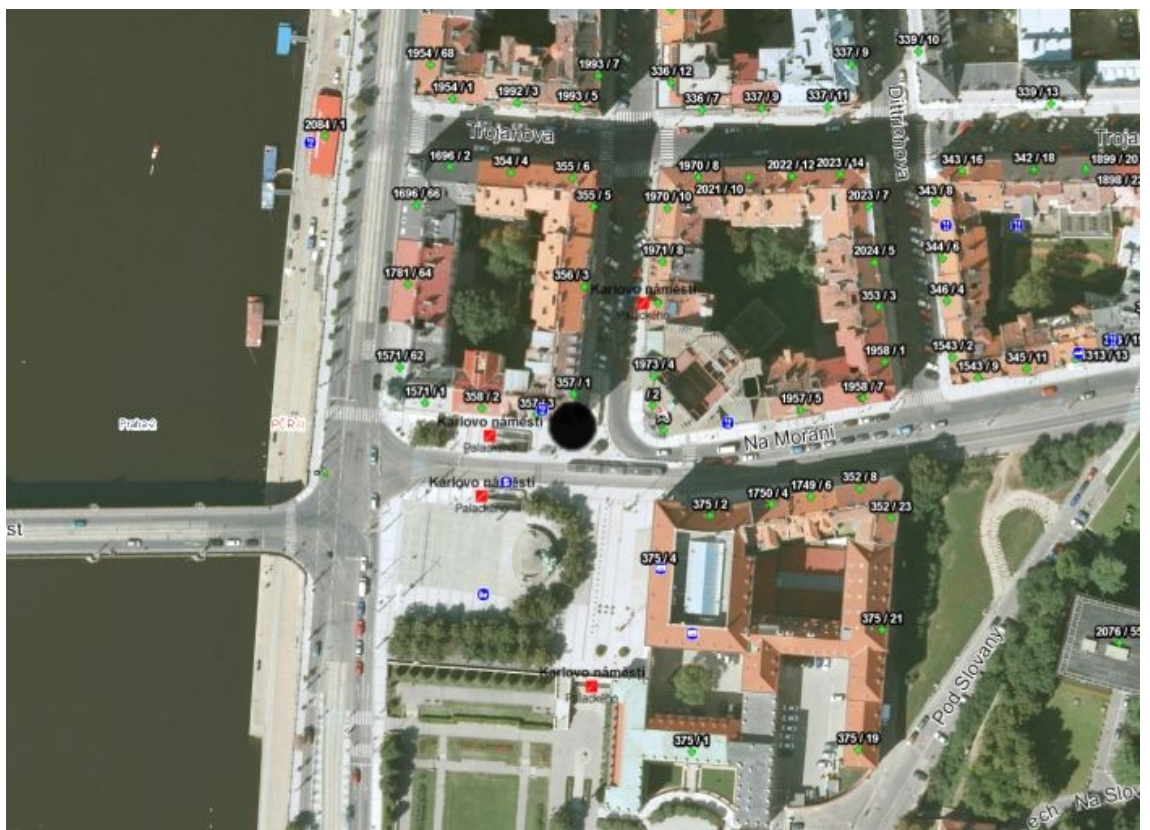
Na intranetových stránkách Policie ČR Obvodní ředitelství Policie ČR Praha II – MKS jsou ke každé kameře MKS vyobrazeny dva výřezy z mapy. Na prvním výřezu (A) je na mapovém podkladu červenou barvou zvýrazněn teoretický polygon dohledu kamery. Jedná se o tzv. možný záběr kamery v ideálních podmínkách, v praktických podmínkách často viditelnosti brání větve stromů, sloupy, keře, reklamní tabule, dopravní značky apod.

Na druhém výřezu (B) je snímek letecké mapy lokality, kde je kamera umístěna. Zde jsou již vidět např. i stromy, které omezují monitorovací možnosti konkrétní kamery. Policista místního oddělení Policie ČR nebo služby kriminální policie a vyšetřování či oddělení dopravních nehod si tak může ještě před tím, než vznesе požadavek na operátora MKS o zajištění kamerového záznamu ke konkrétní události ověřit, zda místo události je nebo není v monitorovacím dosahu kamery MKS.¹¹⁰

¹¹⁰ Zdroje obrázků č. 2 až 9: Policie České republiky/Krajské ředitelství policie hl. m. Prahy/Obvodní ředitelství Praha II/MKS Praha II. Praha 2011 [online]. Datová síť Intranet Ministerstva vnitra „HERMES“. Dostupný z WWW: <<http://p12.pcr.cz/mks/home.html>>.



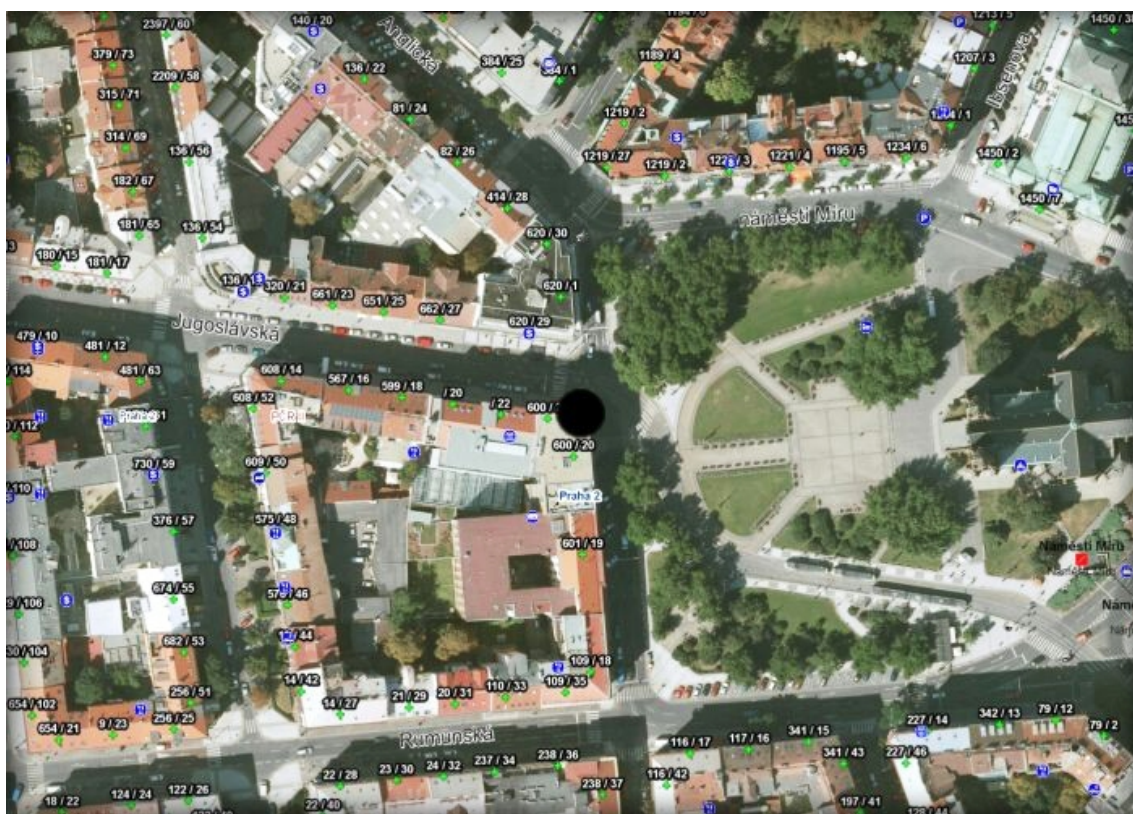
Obrázek č. 2 – Kamera Gorazdova 1; výřez na mapovém podkladu (A)



Obrázek č. 3 – Kamera Gorazdova 1; snímek letecké mapy (B)



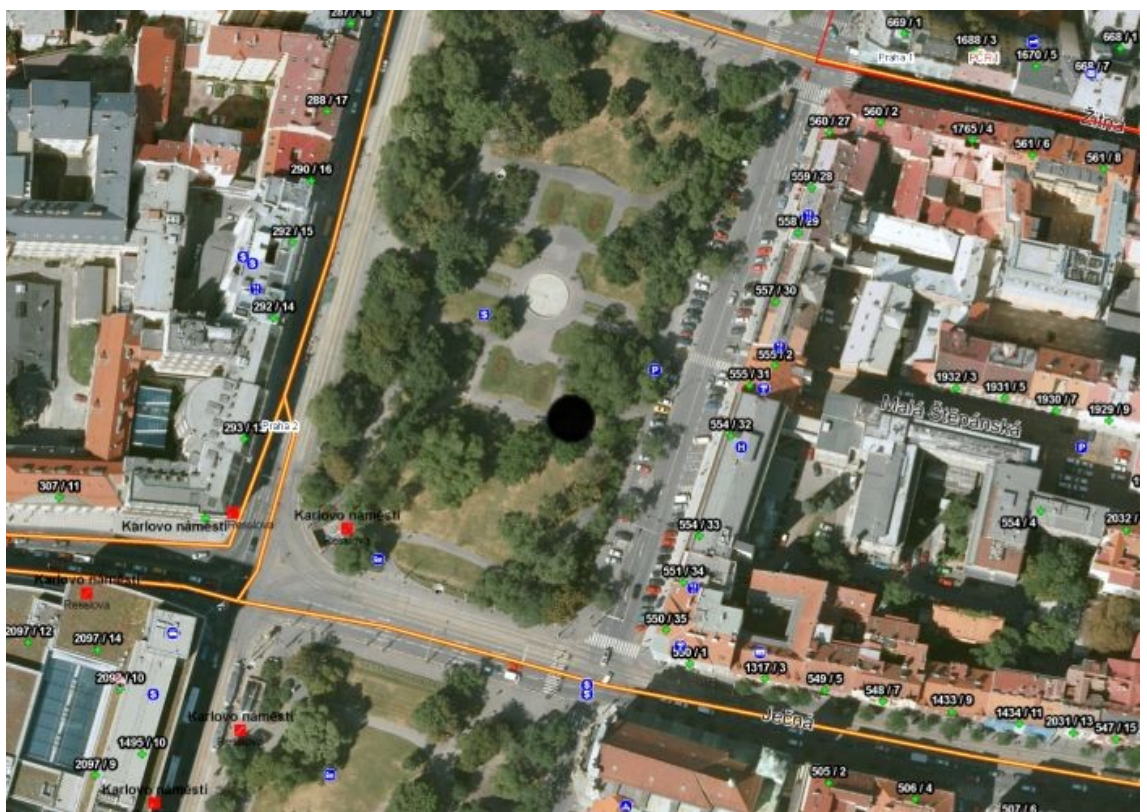
Obrázek č. 4 – Kamera na budově MěÚ Praha 2, nám. Míru; výřez na mapovém podkladu (A)



Obrázek č. 5 – Kamera na budově MěÚ Praha 2, nám. Míru; snímek letecké mapy (B)



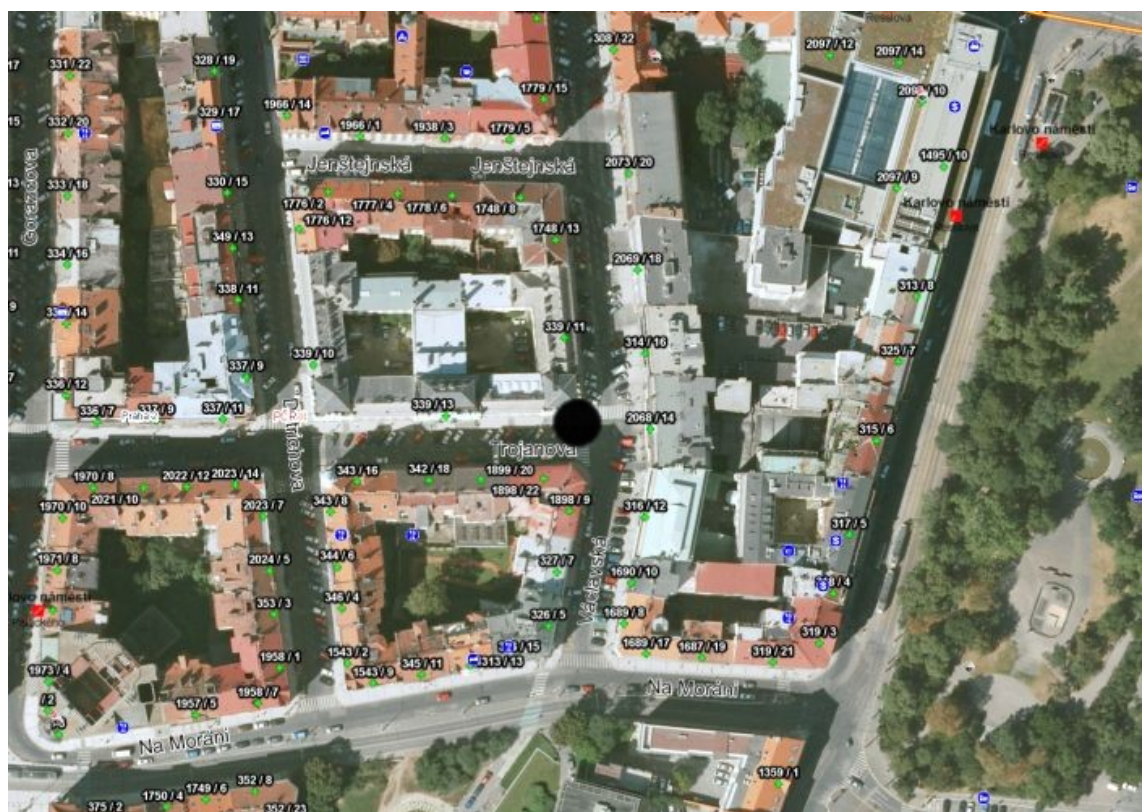
Obrázek č. 6 – Kamera na sloupu VO park Karlovo nám. II; výřez na mapovém podkladu (A)



Obrázek č. 7 – Kamera na sloupu VO park Karlovo nám. II; snímek letecké mapy (B)



Obrázek č. 8 – Kamera ul. Václavská X ul. Trojanova; výřez na mapovém podkladu (A)



Obrázek č. 9 – Kamera ul. Václavská X ul. Trojanova; snímek letecké mapy (B)

PŘÍLOHA IV.

Některé konkrétní příklady využití MKS HMP policisty OŘ Policie ČR Praha II.



Obrázek č. 10 – Operátor MKS monitoruje jednání pachatele vloupání do vozidla



Obrázek č. 11 – Zadržení podezřelého hlídkou Policie ČR



Obrázek č. 12 – Operátor MKS monitoruje jednání pachatele vloupání do vozidla německého turisty



Obrázek č. 13 – Zadržení podezřelého hlídkou Policie ČR



Obrázek č. 14 – Operátor MKS monitoruje fyzické napadení na ulici, jeden podezřelý kope opakovaně do hlavy muže, který leží na ulici



Obrázek č. 15 – Zadržení podezřelého hlídkou Policie ČR



Obrázek č. 16 – Operátor MKS monitoruje jednání kapsářů na nám. I. P. Pavlova



Obrázek č. 17 – Zadržení podezřelých osob hlídkou Policie ČR



Obrázek č. 18 – Operátor MKS monitoruje rvačku před klubem na Šostakovičově nám.



Obrázek č. 19 – Zadržení podezřelých osob příslušníky Policie ČR

PŘÍLOHA V.

Sankce za delikty spáchané v souvislosti se zpracováním osobních údajů

Správní trestání, svěřené do působnosti Úřadu pro ochranu osobních údajů, upravuje zákon o ochraně osobních údajů v ustanoveních § 44 až § 46. Činnost správního trestání navazuje logicky na fáze zjišťování a hodnocení, které jsou obsahem kontroly samé. Nenastupuje však ve všech případech, ale pouze tehdy, pokud je možno doložit nesoulad mezi skutečným stavem a právními normami požadovaným chováním kontrolovaného. Výnos z pokut je příjmem státního rozpočtu, to znamená, že pokuta nemá satisfakční povahu vůči poškozené osobě (především vůči subjektu údajů).

I tato část zákona o ochraně osobních údajů prošla v nedávné době některými změnami, jejichž důvodem bylo přizpůsobit právní úpravu nové legislativní koncepci. Cílem této koncepce bylo sjednotit velmi roztržitěnou úpravu tzv. správního trestání v českém právním řádu. Byly zpřesněny jednotlivé skutkové podstaty deliktů, k nim byly vytvořeny některé kvalifikované skutkové podstaty. Dále byla rozčleněna odpovědnost za jednotlivé druhy deliktů ve smyslu, že fyzické osoby jsou odpovědny za tzv. přestupek, s výjimkou fyzických osob podnikajících, které stejně tak jako právnické osoby mohou svým jednáním naplnit skutkovou podstatu tzv. jiného správního deliktu.¹¹¹

Zákon o ochraně osobních údajů rozlišuje několik typů správních deliktů:

- **PŘESTUPKY**; fyzickou osobu nepodnikající, která není v postavení správce nebo zpracovatele, lze potrestat pouze za přestupek, který spočívá v porušení povinnosti mlčenlivosti, a to pokutou do výše 100 000,- Kč, fyzickou osobu nepodnikající, která je v postavení správce nebo zpracovatele, lze trestat za podstatně větší škálu zaviněného jednání, a to až pokutou do výše 5 000 000,- Kč,
- **JINÉ SPRÁVNÍ DELIKTY**; ty může spáchat právnická osoba jako správce či zpracovatel, nebo fyzická osoba podnikající jako správce či zpracovatel, lze je potrestat uložením pokuty až do výše 10 000 000,- Kč.

¹¹¹ MAŠTALKA, J. *Osobní údaje, právo a my*. C. H. Beck Praha 2008, s. 185-187.

Dále, v souvislosti se zmiňovanou novou legislativní koncepcí, přibýlo liberační ustanovení, podle kterého právnická osoba neodpovídá za správní delikt v případě, že prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.¹¹²

Přestupky a jiné správní delikty projednává Úřad z úřední povinnosti (uplatňuje se zásada oficiality), která v tomto případě znamená, že jakmile nastanou, a Úřadu budou známy, skutečnosti odůvodňující zahájení řízení, je povinen řízení zahájit. Procesním předpisem pro oba druhy řízení je zákon č. 500/2004 Sb., správní řád, v případě řízení o přestupcích je speciálním právním předpisem zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů.

Výše zmiňované sankční řízení by nepochybně mohlo být konzumováno případným trestním řízením, tedy pokud by závadové jednání dosáhlo intenzity trestného činu. Pak je další postup spojen s aplikací trestního práva a úkony trestního řízení konají orgány činné v trestním řízení (procesní stránka řízení je upravena zákonem č. 141/1961 Sb., trestní řád, v účinném znění). O vině a trestu pak rozhoduje soud.

Především je nutno zmínit trestný čin neoprávněné nakládání s osobními údaji podle § 180 odst. 1 až 4 trest. zákoníku.¹¹³ Skutková podstata tohoto trestného činu jednak postihuje osobu, která i z nedbalosti neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném člověku v souvislosti s výkonem veřejné moci a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, již se osobní údaje týkají. Dále postihuje osobu, která osobní údaje o jiném, a to i z nedbalosti, neoprávněně zveřejní, sdělí nebo zpřístupní a tím poruší státem uloženou nebo uznanou povinnost mlčenlivosti, přičemž osobě, již se údaje týkají způsobí vážnou újmu na právech nebo oprávněných zájmech. Skutková podstata však není spojena se zpracováním osobních údajů, avšak s jakýmkoli nakládáním s osobními údaji a tedy překračuje rámeček zákona o ochraně osobních údajů. Jednání uvedené v odst. 1 a 2 se postihuje trestem odnětí svobody až na tři léta nebo zákazem činnosti, jednání uvedené v odst. 3 se postihuje odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti. Kvalifikovaná skutková podstata podle odst. 4 se postihuje trestem odnětí svobody na tři léta až osm let.

¹¹² Ustanovení § 46 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů.

¹¹³ Zákon č. 40/2009 Sb., trestní zákoník.

Závadné zpracování osobních údajů může mít za následek také spáchání trestného činu pomluvy podle § 184 trest. zákoníku. Skutková podstata tohoto trestného činu spočívá ve sdělení nepravdivého údaje o jiném, a tento nepravdivý údaj je způsobilý značnou měrou ohrozit vážnost jiné osoby u spoluobčanů, zejména poškodit její v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu. Jednání podle odst. 1 se trestá odnětím svobody až na jeden rok, jednání podle odst. 2 se trestá odnětím svobody až na dvě léta nebo zákazem činnosti.

V této souvislosti lze zmínit i trestný čin poškození cizích práv podle § 181 trest. zákoníku, kdy se postihuje způsobení vážné újmy na právech tím, že je někdo uveden v omyl nebo něčího omylu využije.