

**Univerzita Karlova v Praze
Filozofická fakulta
Ústav informačních studií a knihovnictví**

Diplomová práce

2006

Bc. Lenka Bucharová

Univerzita Karlova v Praze
Filozofická fakulta
Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví
Studijní obor: informační studia a knihovnictví

Bc. Lenka Bucharová

Informační zdroje v oblasti bezpečnosti státu a občana

Diplomová práce

Praha 2006

Vedoucí diplomové práce: PhDr. Richard Papík, Ph.D.

Oponent diplomové práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a že jsem uvedla všechny použité informační zdroje.

V Praze, 10. prosince 2006

.....
podpis diplomanta

Poděkování:

Ráda bych poděkovala vedoucímu své diplomové práce PhDr. Richardu PAPÍKOVI, Ph.D. za vstřícný přístup při jejím zpracování a také za podnětné náměty. Zároveň bych ráda poděkovala pplk. Jaroslavu Kochovi (absolvent, VVŠ, 40 let služby v armádě ČR) za cenné rady a konzultace. Za poskytnutí aktuálních informací o Vězeňském informačním systému děkuji zaměstnanci valdické věznice Janu Sirovátkovi.

Identifikační záznam

BUCHAROVÁ, Lenka. *Informační zdroje v oblasti bezpečnosti státu a občana [Information sources in the field of state and citizen's security]*. Praha, 2006. 103 s., 5 s. příl. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2006. Vedoucí diplomové práce PhDr. Richard Papík, Ph.D.

Abstrakt

Tématem diplomové práce je problematika informačních zdrojů v činnosti bezpečnostních složek státu. Práce se zabývá především informačními zdroji využitelnými Policií České republiky a zpravodajskými službami. Uvádí však i příklady informačních zdrojů využitelných ostatními bezpečnostními složkami. Zmiňuje se například o informačních zdrojích z oblasti vojenství, které mohou využívat ozbrojené síly České republiky. Avšak stěžejním předmětem zájmu diplomové práce, jak již bylo naznačeno, zůstávají dva vybrané subjekty – zpravodajské služby a Policie České republiky. Práce je tak rozdělena na část zabývající se informačními zdroji zpravodajských služeb a na část týkající se informačních zdrojů Policie České republiky. V rámci těchto částí pojednává práce nejprve o významu samotných informací pro tyto bezpečnostní složky, a poté podává příklady konkrétních informačních zdrojů (včetně zahraničních) s jejich stručnou charakteristikou. Diplomová práce popisuje nejen veřejně přístupné informační zdroje, ale i některé speciální zdroje informací, mezi něž se řadí například policejní informační systémy. V neposlední řadě se práce věnuje také právním aspektům využívání informačních zdrojů v rámci vybraných bezpečnostních složek. Cílem práce bylo podat základní vhled do problematiky bezpečnosti státu a občana ve vztahu k informačním zdrojům se zaměřením na zpravodajskou a policejní oblast. Informační zdroje jsou zde prezentovány jako jeden z prostředků, který umožňuje chránit zájmy státu a jeho občanů.

Klíčová slova

bezpečnost státu, policejní informační systémy, policie, zpravodajské služby, neutajované informace, utajované informace, informační zdroje, databáze, informační

systemy, zpravodajství, otevřené zdroje, vojenství, internet, zpravodajský cyklus, osobní údaje, kriminalita, zpravodajské informace, trestné činy, CIA, citlivé údaje, biometrické informace, civilně správní evidence

PŘEDMLUVA.....	12
1. ÚVOD	14
2. BEZPEČNOST STÁTU A OBČANA	17
2.1. Pojem bezpečnost obecně	17
2.2. Bezpečnost státu – výklad pojmu, typologie.....	18
2.3. Bezpečnostní terminologie v rámci České republiky.....	19
2.4. Subjekty zajišťující bezpečnost České republiky	23
3. INFORMAČNÍ ZDROJE V OBLASTI BEZPEČNOSTI STÁTU.....	25
3.1. Využitelnost informačních zdrojů.....	25
3.2. Informační zdroje z oblasti vojenství.....	26
3.3. Vězeňský informační systém (VIS)	31
4. INFORMAČNÍ ZDROJE ZPRAVODAJSKÝCH SLUŽEB.....	32
4.1. Vybrané termíny z oblasti zpravodajských služeb	32
4.1.1. Pojem zpravodajská služba.....	32
4.1.2. Typologie zpravodajských služeb	32
4.1.3. Zpravodajské služby České republiky	33
4.1.4. Pojem zpravodajská informace	34
4.2. Zpravodajský cyklus a jeho podobnost s cyklem informačním	35
4.3. Využití zpravodajského cyklu v rámci Competitive Intelligence.....	37
5. METODY SBĚRU ZPRAVODAJSKÝCH INFORMACÍ	39
5.1. Významy zpravodajského termínu intelligence	39
5.2. Stručná charakteristika jednotlivých metod sběru	39
5.2.1. Možnosti vzniku nových metod sběru informací	44
5.2.2. Blog jako zdroj informací pro zpravodajství	44
6. OTEVŘENÉ ZDROJE U ZPRAVODAJSKÝCH SLUŽEB.....	46
6.1. Úvod do problematiky otevřených zdrojů.....	46
6.2. Charakteristika otevřených zdrojů ve zpravodajství.....	49
6.2.1. Možné definice otevřených zdrojů a jejich informací pro oblast zpravodajství	50
6.2.2. Typologie otevřených zdrojů.....	52
6.2.3. Výhody a nevýhody otevřených zdrojů.....	53
6.2.4. Zřízení specializovaných oddělení zaměřených na otevřené zdroje.....	54
6.3. Otevřené zdroje z hlediska obsažených informací.....	54

6.3.1.	Utajované versus neutajované informace	55
6.3.2.	Klasifikace utajovaných informací.....	55
6.3.3.	Rozdíly mezi utajovanými a neutajovanými informacemi	56
7.	INTERNET VERSUS ZPRAVODAJSKÉ SLUŽBY	58
7.1.	Prostřednictvím internetu lze odhalit agenty CIA.....	58
7.2.	Katastr nemovitostí jako nástroj k získání informací.....	62
8.	VÝZNAM INFORMACÍ PRO POLICII	63
8.1.	Informace při odhalování, objasňování a vyšetřování trestných činů.....	63
8.2.	Informace jako prostředek kriminalistické prevence a policejní statistiky	64
8.3.	Pojem informace v trestním zákoně.....	65
8.3.1.	Trestněprávní ochrana osobních údajů	65
8.3.2.	Další kategorie informací výslovně zmiňované trestním zákonem.....	66
8.4.	Role rodného čísla při individuální identifikaci osob, příklady jeho využití	67
9.	INFORMAČNÍ ZDROJE V POLICEJNÍ PRAXI.....	69
9.1.	Civilně-správní informační systémy.....	69
9.2.	Policejní informační systémy	70
9.2.1.	Historie a současnost policejních informačních systémů.....	70
9.2.2.	Předpočítačová éra policejních databází	70
9.2.3.	Moderní počítačové informační systémy	71
9.3.	Kriminalistické sbírky	72
9.4.	Informační zdroje obsahující citlivé údaje.....	74
9.4.1.	Biologické, biometrické a genetické informace	74
9.4.2.	Možnosti oboru biometrie v souvislosti s identifikací osob	74
9.4.3.	Projekt US-Visit	75
9.4.4.	Archivy DNA	76
9.4.5.	Daktyloskopické systémy.....	77
9.5.	Právní aspekty vedení policejních informačních systémů	79
9.6.	Přístup do policejních informačních systémů	80
9.7.	Informační činnosti v rámci informačních systémů policie.....	80
9.8.	Stručná charakteristika vybraných policejních informačních systémů	81
9.9.	Příklady zahraničních informačních zdrojů pro policii.....	86
9.9.1.	Americký projekt National Sex Offender Public Registry	86
9.9.2.	NCJRS Abstracts Database	88
9.9.3.	FORENSICnetBASE a InfoSECURITYnetBASE	89
9.9.4.	Criminal Justice Abstract	89
9.9.5.	CRIMINAL JUSTICE PERIODICAL INDEX	90
10.	NEJROZŠÍŘENĚJŠÍ CIVILNĚ SPRÁVNÍ EVIDENCE.....	91

10.1.Registry spravované Ministerstvem vnitra	91
10.1.1. Registr občanů.....	91
10.1.2. Registr vozidel.....	91
10.2.Registr řidičů spravovaný Ministerstvem dopravy	91
11. ZÁVĚR.....	92
SEZNAM POUŽITÉ LITERATURY	94
PŘÍLOHY	98
EVIDENCE VÝPŮJČEK	103

PŘEDMLUVA

Tématem mé diplomové práce je problematika informačních zdrojů využitelných bezpečnostními složkami státu. Toto téma jsem si zvolila zejména z toho důvodu, že mi je tato oblast bezpečnosti profesně blízká. Vyústěním pro zvolení tohoto tématu bylo i moje předchozí bakalářské studium na Policejní akademii České republiky (dále jen PA ČR), kde jsem měla možnost seznámit se s obory vztahujícími se k policejní činnosti jako např. s kriminalistikou nebo trestním právem. V rámci výuky jsme se mimo jiné zabývali také problematikou informačních zdrojů využitelných v bezpečnostní praxi. V této diplomové práci jsem tak využila možnosti navázat na předešlé znalosti získané v bakalářském studiu na PA ČR. Zároveň jsem se pokusila rozšířit tyto vědomosti, v rámci studia na PA ČR nahlížené zejména ve vztahu k odhalování trestných činů, o informační hledisko, které v rámci předešlého studia nebylo do hloubky rozebíráno. Informace jako pojem jsou v rámci zpracované diplomové práce pojímány jako základní prostředek umožňující činnost všech složek zajišťujících bezpečnost České republiky. Informace zásadním způsobem ovlivňují schopnost státu ubránit se nepříteli a zajistit bezpečnost pro své občany. Cílem diplomové práce je blíže specifikovat význam informací pro bezpečnostní složky státu, konkrétně pro zpravodajské služby a policii. Jsou v ní uvedeny i konkrétní zdroje informací využitelné v rámci jejich činností. Zpravodajské služby a policii lze považovat za primární subjekty zajišťující bezpečnost České republiky. Tou třetí je armáda, které se však diplomová práce věnuje pouze ve stručné podobě. Problematika informačních zdrojů z oblasti vojenství by si vzhledem k významu ozbrojených sil v rámci bezpečnostního systému České republiky a od toho se odvíjející rozsáhlosti problematiky obrany zasluhovala samostatné zpracování.

Diplomovou práci lze pomyslně rozdělit na dvě základní části. První z nich se zabývá významem informací a využitelnými zdroji informací v rámci zpravodajských služeb, druhá pak stejnou problematikou v rámci policie. Informačních zdrojů přímo určených nebo alespoň částečně využitelných v oblasti národní bezpečnosti existuje ve světě celá řada (některé z nich zmiňuje i tato diplomová práce). V souvislosti s vývojem bezpečnostní situace ve světě, zejména za existence mezinárodního terorismu, existence hrozeb použití chemických a

biologických zbraní teroristy, použití zbraní hromadného ničení totalitními režimy proti svým „nepřátelům“, v souvislosti s neustálým nárůstem celosvětové i národní kriminality lze předpokládat, že bude stoupat potřeba využívání informačních zdrojů jako jednoho z prostředků, které se na zajišťování bezpečnosti státu a občana podílejí.

Při psaní diplomové práce jsem informace čerpala pouze z otevřených zdrojů, zejména odborných knih, periodik, televize, rozhlasu a internetu. V textu jsou citovány také vybrané pojmy z problematikových slovníků. V neposlední řadě jsou do textu zahrnuty i pasáže právních předpisů. Podkladů, ze kterých bylo možné čerpat podnětné informace k jednotlivým částem diplomové práce bylo dostatek.

Použitá literatura je citována v souladu s normami ISO 690 a ISO 690-2.

1. ÚVOD

Diplomová práce je rozdělena do dvou pomyslných hlavních částí. První se zabývá problematikou informačních zdrojů v rámci zpravodajských služeb, druhá zdroji policie. V rámci těchto dvou aspektů se zabývá nejprve významem informací pro tyto dva představitele bezpečnostních složek státu, a poté charakteristikou vybraných informačních zdrojů. Práce je členěna do deseti základních kapitol, jejichž obsah stručně vystihují následující odstavce.

V kapitole nazvané *Bezpečnost státu a občana* jsou definovány základní termíny z oblasti bezpečnosti státu a občana, které je vhodné předem vymezit. Pro správné pochopení problematiky informačních zdrojů využitelných v oblasti bezpečnosti státu a občana je nutné nejprve porozumět základním pojmům bezpečnostní terminologie platným pro Českou republiku. Definován je samotný pojem bezpečnost státu, ale i další pojmy jako bezpečnostní politika státu, bezpečnostní situace nebo bezpečnostní systém státu. V této kapitole je podán i výčet subjektů, které bezpečnost České republiky zajišťují.

Po vymezení základních pojmů z oblasti bezpečnosti státu následuje kapitola *Informační zdroje v oblasti bezpečnosti státu*. Zabývá se významem a využitelností těchto zdrojů. V této části diplomové práce je věnována pozornost také informačním zdrojům z oblasti vojenství, jsou zde uvedeny i konkrétní případy zdrojů. V krátkosti je zmíněn i Vězeňský informační systém jako stěžejní zdroj informací pro oblast českého vězeňství.

Čtvrtá kapitola již směřuje do oblasti *informačních zdrojů zpravodajských služeb*. Také tato kapitola podává vymezení základních pojmů, tentokrát ze zpravodajské terminologie. Kapitola mimo jiné uvádí typologii zpravodajských služeb. V kapitole jsou zmiňovány i zpravodajské služby působící v České republice. S ohledem na téma této diplomové práce jsou blíže specifikovány pojmy zpravodajská informace a zpravodajský cyklus.

Pátá kapitola s názvem *Metody sběru zpravodajských informací* podává základní charakteristiku vybraných disciplín sběru zpravodajských informací. V samotném úvodu se kapitola zabývá významy zpravodajského termínu intelligence. Okrajově se zajímá i o roli fámy ve zpravodajství. Zajímavým tématem je

využitelnost blogů ve zpravodajství (podkladem pro zpracování tohoto tématu do práce byly především zahraniční internetové zdroje).

Šestá kapitola nese název *Otevřené zdroje u zpravodajských služeb*. Kapitola provádí srovnání otevřených zdrojů s utajovanými, a následně provádí charakteristiku otevřených zdrojů. Dále kapitola zmiňuje i jednotlivé definice otevřených zdrojů (zejména z hlediska šíře jejich pojetí). V rámci kapitoly je provedena typologie otevřených zdrojů a jsou konkretizovány výhody a nevýhody tohoto zdroje informací. Na závěr se kapitola v krátkosti věnuje zřizování informačních pracovišť pro oblast otevřených zdrojů v rámci zpravodajských služeb. Důležitou částí kapitoly je i pojednání o otevřených zdrojích z hlediska obsažených informací.

V sedmé kapitola se diplomová práce v souvislosti se zpravodajskými službami zabývá *internetem*, mimo jiné z hlediska *množství informací*. Zmiňuje se i o případu z USA, kdy byly pomocí internetu získány informace, prostřednictvím nichž bylo možné se dopátrat totožnosti agentů americké zpravodajské služby CIA. V souvislosti s tímto případem je probírán i případ podobného rázu, který se stal v České republice. Prostřednictvím katastru nemovitostí byly shromážděny takové informace, na základě nichž by bylo možné se dopátrat i totožnosti příslušníků české zpravodajské služby.

Osmá kapitola se již zabývá významem informací pro policii, zejména v rámci vyšetřování trestných činů, ale také kriminalistické prevence. Dále se diplomová práce v této části zabývá pojmem informace v trestním zákoně, zejména osobními údaji. Dalším předmětem zájmu práce na tomto místě je i rodné číslo jako prostředek identifikace osob.

Devátá kapitola uvádí základní informace o zdrojích v policejní praxi. Provádí jejich členění na civilně-správní evidence, policejní informační systémy a zdroje otevřené. Zastavuje se i u kriminalistických sbírek. Dalším tématem kapitoly jsou informační zdroje obsahující citlivé údaje. V této souvislosti zmiňuje kapitola americký projekt US-Visit, archivy DNA a daktyloskopické systémy. V této kapitole jsou rozebírány i právní aspekty vedení policejních informačních zdrojů. Kapitola dále podává informace o přístupech do policejních systémů. Pozastavuje se i u informačních činností prováděných v rámci informačních systémů policie. V další

části kapitoly jsou charakterizovány vybrané policejní informační systémy. Zajímavé je i uvedení příkladů systémů pro oblast policie ze zahraničí v další části kapitoly.

Desátá kapitola je věnována nejrozšířenějším civilně-správním evidencím, konkrétně registru občanů, registru vozidel a registru řidičů.

2. BEZPEČNOST STÁTU A OBČANA

Než se začnu věnovat samotné problematice informačních zdrojů využitelných v oblasti bezpečnosti státu a občana, považuji za vhodné vymezit nejprve v této kapitole několik základních pojmů z této oblasti.

2.1. Pojem bezpečnost obecně

S pojmem *bezpečnost* se můžeme setkat v celé řadě oborů (společenskovedních, přírodovědných i technických), v nichž má tento termín vždy svůj specifický význam a charakter. Tento pojem se vyskytuje v ustálených slovních spojeních, v jednotlivých zákonných předpisech, v názvech státních institucí apod. (*bezpečnost práce, požární bezpečnost, bezpečnost (a plynulost) provozu na pozemních komunikacích, bezpečnost leteckého provozu, informační bezpečnost, bezpečnost dat, Státní úřad pro jadernou bezpečnost* apod.).

Pojem *bezpečnost* lze definovat nejen v rámci jednotlivých vědních disciplín, kdy má pokaždé svůj specifický charakter, ale i v obecné rovině. Ve *Slovníku spisovné češtiny pro školu a veřejnost* z roku 2001 je *bezpečnost* vymezena u přídavného jména *bezpečný* (jako synonymum se uvádí slovo *jistota*, respektive *jistý*). *Bezpečný* je ten, kdo není vystaven nebezpečí (být bezpečný před někým, něčím), popř. poskytuje ochranu před nebezpečím (*bezpečný úkryt*) nebo je nepochybný, zaručený, důvěryhodný (*bezpečný pramen informací*). [1]

Bezpečnost lze charakterizovat jako stav absence určitých hrozeb. Spíše se však jedná o ideální stav, neboť většinou je možné v oblasti bezpečnosti dosáhnout pouze určitého rozsahu eliminace hrozeb či ochrany před hrozbami. [1] (viz. také kapitola *Bezpečnostní terminologie v rámci České republiky* a pojem *Běžný stav*).

Obecně se pod pojmem *bezpečnost* rozumí společností (státem) stanovená (garantovaná) schopnost zamezení toho, aby konkrétní riziko překročilo únosnou mez. Pro zajištění bezpečnosti (omezení stávajících i potenciálních hrozeb) se odpovědný subjekt, např. stát, popř. mezinárodní organizace, efektivně připravuje řešit možná ohrožení (např. ve formě různých preventivních opatření). Hrozby mohou směřovat např. vůči obyvatelstvu, svrchovanosti státu, vnitřnímu pořádku, majetku,

životnímu prostředí, plnění mezinárodních bezpečnostních závazků a dalším společenským zájmům. [2]

Pojem *bezpečnost* bývá často doplňován různými adjektivy, která se vztahují především k charakteru (původu):

- a) **hrozeb**, které bezpečnost ohrožují,
- b) **opatření, nástrojů** či **institucí**, které mají bezpečnost zajišťovat a chránit,
- c) **objektů**, jejichž bezpečnost má být chráněna. [1]

Jedním z objektů, jehož bezpečnost je třeba zajišťovat a chránit, je stát. Neboť se tato diplomová práce zabývá informačními zdroji využitelnými v oblasti *bezpečnosti státu* (bezpečnosti státu jako celku i bezpečnosti jednotlivých občanů), je nutné si tento pojem ujasnit.

2.2. Bezpečnost státu – výklad pojmu, typologie

Terminologický slovník z oblasti krizového řízení a plánování obrany státu, který byl zpracován ústředními správními úřady a vydán Ministerstvem vnitra v roce 2004 [2] pojem *bezpečnost* definuje následujícím způsobem:

„Bezpečnost je stav, kdy jsou na efektivní míru omezeny hrozby pro objekt a jeho zájmy a tento objekt je k omezení stávajících i potenciálních hrozeb efektivně vybaven a ochoten při něm spolupracovat.“ [2]

Pojem *bezpečnost státu* pak lze definovat jako *stav, kdy jsou na efektivní míru omezeny hrozby pro stát a jeho zájmy a stát je k omezení stávajících i potenciálních hrozeb efektivně vybaven a ochoten při něm spolupracovat.* [3]

V rámci *bezpečnosti státu* lze rozlišovat *bezpečnost vnější* (jde-li o existenci, potlačování a eliminaci hrozeb, které mají svůj původ vně objektu) a *bezpečnost vnitřní* (jde-li o existenci, potlačování a eliminaci hrozeb, které pochází zevnitř objektu). [3] Vnější bezpečností se rozumí: zajištění územní celistvosti, vnější svrchovanosti a nezávislosti státu, nedotknutelnosti jeho státních hranic a ochrana jeho zastupitelských úřadů, členů diplomatického sboru a dalších občanů (zejména v případě hrozby mimořádné události v zahraničí nebo po jejím vzniku). Vnitřní bezpečnost státu pak v širším významu (užší vymezení viz. dále - Specifika pojmu

vnitřní bezpečnost) znamená zachování a zajištění vnitřních funkcí státu, ochranu jeho demokratických základů, ochranu vnitřního pořádku, bezpečnosti a zákonnosti, ochranu životů a zdraví, majetkových hodnot a životního prostředí před hrozbami majícími původ na území státu. [2]

Slovní spojení *vnější bezpečnost* bylo a je často používáno v podstatě synonymně pro *bezpečnost vojenskou* a pojem *vnitřní bezpečnost* synonymně pro bezpečnost v oblasti policejní (kriminální). Objevuje se i dělení na tzv. *tvrdou* (tj. tradiční vojenskou) a *měkkou bezpečnost* (kriminalita, organizovaný zločin, nevojenské hrozby životnímu prostředí apod.). [1]

Co se týká dělení bezpečnosti státu na bezpečnost vnější a vnitřní, je třeba konstatovat, že pokles mezinárodního napětí ve vojenské oblasti a současně nárůst vlivu transnacionálních aktérů ohrožujících bezpečnost (organizovaný zločin, terorismus), ale i globalizace ekonomiky a celosvětové působení ekologických hrozeb postupně smazávají rozdíly mezi vnější a vnitřní bezpečností. [1]

Dalším zavedeným termínem používaným v bezpečnostní praxi je *bezpečnost kolektivní* (bezpečnost kolektivu aktérů). Do této kategorie spadají pojmy jako *národní bezpečnost* (bezpečnost národního státu), *mezinárodní bezpečnost* (bezpečnost v mezinárodním společenství) nebo *globální bezpečnost* (bezpečnost v rámci celého světa). Protiklad kolektivní bezpečnosti představuje bezpečnost *individuální* (bezpečnost individua). Všechny výše uvedené pojmy jsou zpravidla vzájemně provázány a jejich ohraničení není zcela jednoznačné. Bezpečnost je pojem komplexní. [1]

2.3. Bezpečnostní terminologie v rámci České republiky

V následující části práce budou vymezeny základní pojmy bezpečnostní terminologie (*bezpečnost, bezpečnostní politika státu, bezpečnostní situace, bezpečnostní strategie ČR, bezpečnostní systém státu, běžný stav, hrozba a riziko*).

Pojem bezpečnost

V současné české legislativě ani v odborné literatuře neexistuje žádná jednotná definice pojmu *bezpečnost*. [2] Pojem *bezpečnost* není vymezen ani v ústavním zákoně č.110/1998 Sb., o bezpečnosti České republiky, lze jej pouze odvodit z čl. 2 a čl. 3 (viz. dále) tohoto zákona.

Čl.2

(1) Je-li bezprostředně ohrožena svrchovanost, územní celistvost, demokratické základy České republiky nebo ve značném rozsahu vnitřní pořádek a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí anebo je-li třeba plnit mezinárodní závazky o společné obraně, může se vyhlásit podle intenzity, územního rozsahu a charakteru situace nouzový stav, stav ohrožení státu nebo válečný stav.

(2) Nouzový stav a stav ohrožení státu se vyhláší pro omezené nebo pro celé území státu, válečný stav se vyhláší pro celé území státu.

Čl.3

(1) Bezpečnost České republiky zajišťují ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby.

(2) Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky. Rozsah povinností a další podrobnosti stanoví zákon.

Výkladový slovník krizového řízení a obrany státu, jenž definici pojmu *bezpečnost* podává (byla již zmíněna), rozlišuje *bezpečnost* taktéž na *vnější* a *vnitřní*, kdy:

***Vnější bezpečnost státu** je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby ohrožující stát a jeho zájmy zvnějšku a kdy je tento stát k eliminaci existujících i potenciálních vnějších hrozeb efektivně vybaven a ochoten. Hrozby mohou být vojenské nebo ekonomické povahy, mohou mít charakter migrační vlny apod. Je to také souhrn mezinárodněpolitických, ekonomických a vojenských vztahů státu s okolními státy a koalicemi, jejichž prostřednictvím prosazuje své státní zájmy. [2]*

***Vnitřní bezpečnost státu** je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby ohrožující stát a jeho zájmy zevnitř a kdy je tento stát k eliminaci stávajících i potenciálních vnitřních hrozeb efektivně vybaven a k ní ochoten. Je to rovněž souhrn vnitřních bezpečnostních podmínek a legislativních norem a opatření, kterými stát zajišťuje demokracii, ekonomickou prosperitu a bezpečnost občanů a kterými stanoví a prosazuje normy morálky a společenského vědomí. [2]*

Specifika pojmu vnitřní bezpečnost

Pojem *vnitřní bezpečnost* není v české legislativě jednoznačně definován. Tento pojem lze chápat v jeho širším nebo užším významu.

- V *širším* významu, kdy je nadřazený pojem *bezpečnost* odvozen z čl. 2 a čl. 3 ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR – v tomto případě je termín *vnitřní bezpečnost* definován podle územního hlediska (rizika a hrozby mají svůj původ a působí na území státu). Takto pojatá *vnitřní bezpečnost* obsahuje vedle ohrožení zákonnosti a veřejného pořádku i např. ochranu obyvatelstva včetně záchranných a likvidačních prací a humanitární pomoci, ochranu ekonomiky před vnitřními riziky, ekologii, jadernou bezpečnost, bezpečnost v dopravě apod. [2]
- V *užším* významu (častěji užívaném), kdy pojem *vnitřní bezpečnost* vychází z nadřazeného pojmu *bezpečnost* uvedeném např. u vymezení působnosti MV v zákoně č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy a dále v zákoně č. 283/1991 Sb., o Policii ČR. Pak je pojem *vnitřní bezpečnost* vázán na pojem *veřejný (vnitřní) pořádek* (viz. § 10 odst. 3 zákona č. 240/2000 Sb., o krizovém řízení) a vztahuje se zejména k působnosti Policie ČR (Ministerstva vnitra) a dalších ozbrojených bezpečnostních sborů. [2]

Neboť je tato diplomová práce orientována na využívání informačních zdrojů zpravodajskými službami a Policií České republiky, bude se obsah práce spíše přiklánět k užšímu pojetí pojmu *vnitřní bezpečnost*.

Po vymezení pojmu *bezpečnost* je vhodné seznámit se ještě s dalšími (základními) pojmy bezpečnostní problematiky. Následující definice pocházejí opět z výkladového slovníku krizového řízení a obrany státu.

Pojem bezpečnostní politika státu

Společenská činnost, jejíž základ tvoří souhrn základních státních zájmů a cílů, jakož i hlavních nástrojů k jejich dosažení, směřující k zabezpečení státní svrchovanosti a územní celistvosti státu a jeho demokratických základů, činnosti demokratických institucí, ekonomického a sociálního rozvoje státu, ochrany zdraví a života občanů, majetku, kulturních statků, životního prostředí a plnění mezinárodních bezpečnostních závazků. [3]

Bezpečnostní politiku státu tvoří 5 základních komponentů:

- *zahraniční politika v oblasti bezpečnosti státu,*

- obranná politika,
- politika v oblasti vnitřní bezpečnosti,
- hospodářská politika v oblasti bezpečnosti státu,
- politika veřejné informovanosti v oblasti bezpečnosti státu. [3]

Pojem bezpečnostní situace

Výslednice procesů a vztahů ve sféře nevojenské a vojenské bezpečnosti, je souhrnem vztahů politického, kulturně-sociálního, ekonomického, vojenského a ekologického prostředí jako celku. Bezpečnostní situace je spoluurčena vnitrostátními a mezinárodními bezpečnostními poměry: je ovlivňována parametry vnitřní a vnější bezpečnosti státu a celým souborem aktivit zahraniční politiky, ekonomického rozvoje státu, sociální stability, rozvoje demokracie a respektování lidských práv a souborem bezpečnostních důsledků, které vyplývají z mezinárodních smluvních závazků státu. [3]

Pojem bezpečnostní strategie ČR

Základní koncepční dokument vlády ČR, který specifikuje na základě bezpečnostních hrozeb a z nich plynoucích rizik bezpečnostní zájmy ČR a stanovuje místo a úlohu správních úřadů, orgánů územní samosprávy, ozbrojených sil, ozbrojených bezpečnostních sborů, záchranných sborů, havarijních, záchranných aj. služeb ČR při naplňování její bezpečnostní politiky. Bezpečnostní strategie ČR stanovuje rovněž vojenskopolitické ambice ČR. [3]

Pojem bezpečnostní systém státu

Systém orgánů veřejné správy, ozbrojených sil, ozbrojených bezpečnostních sborů, záchranných sborů a služeb, havarijních a jiných služeb, právnických a fyzických osob, jejich vzájemných vazeb a činností, zabezpečujících koordinovaný postup při zajišťování bezpečnosti státu a jeho obyvatelstva. [3]

Bezpečnostní systém České republiky je možné strukturovat následujícím způsobem:

- *ústřední úroveň: prezident republiky, Parlament České republiky, vláda, Bezpečnostní rada státu a její pracovní orgány, ústřední správní úřady,*

- *územní prvky bezpečnostního systému: hejtman kraje, starosta obce, krajské úřady, obecní úřady obcí s rozšířenou působností a ostatních obcí a jejich pracovní orgány krizového řízení. [2]*

Pojem běžný stav

Období, ve kterém nedochází k narušení života společnosti (fungování systému), nebo ve kterém přípustná míra narušení nevybočuje z rámce přijatých norem. [1]

Pojmy hrozba a riziko

Hrozbou se rozumí objektivní skutečnost, která může znamenat negativní dopad pro chráněný zájem v daném prostředí (ohrožení) – na určitém území, ve vymezeném období apod. Hrozbě lze čelit protiopatřeními. S ohledem na konkrétní objekt či chráněný zájem (jeho důležitost apod.), bývá intenzita opatření odstupňována. [2]

Rizikem se výsledně rozumí to, co stát podstupuje, aby jeho snaha redukovat hrozby nepřekročila únosnou míru. Pro stanovení rizik (míry rizika) je nezbytné analyzovat a kvantifikovat hrozby z hlediska možných dopadů na chráněný zájem (např. pravděpodobnost a rozsah ohrožení osob). [2]

2.4. Subjekty zajišťující bezpečnost České republiky

Podle čl. 3 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky zajišťují bezpečnost České republiky *ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby* (odst. 1). *Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby* jsou povinny se podílet na zajišťování bezpečnosti České republiky (odst. 2). Jmenované subjekty tvoří *bezpečnostní systém České republiky* (tento pojem byl již v předcházející části vymezen).

V rámci České republiky jsou hlavními subjekty zajišťujícími bezpečnost státu *Armáda České republiky a Vojenské zpravodajství* jako představitelé ozbrojených sil a dále *Policie České republiky, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace* a *Vězeňská služba České republiky* jako zástupci ozbrojených bezpečnostních sborů. Na zajištění bezpečnosti se také podílí bezpečnostní sbory *Hasičský záchranný sbor* a *Celní správa České republiky*.

Z hlediska své působnosti sem náleží i další složky dohlížející na bezpečnost jako městská a obecní policie, Horská služba České republiky nebo Vodní záchranná služba. Mezi další složky spadající do problematiky bezpečnosti státu a jejích občanů lze dále řadit zdravotnickou záchrannou službu, různé havarijní, pohotovostní, odborné a jiné služby, záchranné brigády kynologů apod.

3. INFORMAČNÍ ZDROJE V OBLASTI BEZPEČNOSTI STÁTU

Zejména z důvodu rozsáhlosti celé problematiky se budu v diplomové práci blíže zabývat pouze informačními zdroji z oblasti zpravodajských služeb a Policie České republiky. Informačním zdrojům využitelným ostatními bezpečnostními složkami zvýšená pozornost věnována nebude, pokud budou zmíněny, pak jen okrajově. Jedinou výjimkou budou informační zdroje z oblasti obrany. Oproti informačním zdrojům využitelným zpravodajskými službami a Policií České republiky se však bude jednat pouze o stručný nástin dané problematiky. Jedním z důvodů je ta skutečnost, že z hlediska rozsahu by si podle mého názoru problematika informačních zdrojů z oblasti vojenství zaslouhovala zpracování samostatné diplomové práce. Než přejdu k pojednání o informačních zdrojích pro oblast vojenství, zastavím se nejprve u vymezení *využitelnosti* (hlediska záběru) informačních zdrojů, který bude v této diplomové práci uplatňován.

3.1. Využitelnost informačních zdrojů

Využitelnost informačních zdrojů v rámci kterékoliv složky zabývající se oblastí bezpečností státu a občana lze chápat nejenom jako záběr informačních zdrojů potřebných k plnění stanovených úkolů (využitelných pouze v rámci *činnosti* těchto složek). *Využitelnost* informačních zdrojů lze chápat i v širším významu. Toto pojetí bude stručně přiblíženo na příkladech informačních zdrojů z oblasti vojenství a zdrojích vězeňské služby.

V oblasti vojenství nejsou využitelné pouze databáze přímo z oblasti vojenství, (jejichž příklady budou v diplomové práci následně uvedeny). Zájmovou oblastí vojáků z české protichemické jednotky v souvislosti s chemickými zbraněmi používanými nepřátelskými vojsky mohou být např. nejrůznější obecně zaměřené (tedy nejenom pro oblast vojenství) databáze z oblasti chemie, databáze nebezpečných látek apod. Využití v oblasti vojenství naleznou i různé obecné databáze z dalších oblastí jako toxikologie, fyziky, politologie, techniky, matematiky, elektrotechniky. Záběr využitelných informačních zdrojů Armádou České republiky je tak možné vztahovat nejen k databázím věnujícím se přímo oblasti vojenství, ale i k řadě dalších databází. Stejně tak se mohou mezi informační zdroje využitelné Vězeňskou službou České republiky řadit různé informační zdroje z oblasti

psychologie, sociologie, penologie apod., z nichž lze získat obecné poznatky týkající se např. resocializace odsouzených osob v rámci různých států, případně různé statistické přehledy. Dále (v obecné) rovině zasahují nové vědecké objevy svým významem v rámci jednoho vědního oboru také do dalších oborů. Informační zdroje vědy a výzkumu mají vliv na jakoukoliv oblast života lidské společnosti (tedy i oblast vojenství). Těmito aspekty *využitelnosti* se tato diplomová práce blíže zabývat nebude. Předmětem jejího zájmu budou pouze informační zdroje využitelné v rámci *činnosti* bezpečnostních složek státu. Přesto jsem považovala za vhodné, zmínit se i o možném širším pojetí využitelnosti zdrojů pro oblast bezpečnosti státu.

3.2. Informační zdroje z oblasti vojenství

Konkrétními subjekty z oblasti bezpečnosti státu (České republiky), kterých se (z hlediska obsahového zaměření) informační zdroje pro oblast vojenství týkají, jsou Ministerstvo obrany jako ústřední orgán státní správy zabezpečující obranu České republiky, a dále Armáda České republiky, kterou ministerstvo řídí. Působnost Ministerstva obrany definuje zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČSR v § 16.

Jedním z prostředků, který umožňuje Ministerstvu obrany České republiky a Armádě České republiky řádně bránit bezpečnost České republiky a jejích občanů, jsou informace. Bez nich by byla obrana státu nemožná. Informace potřebovali vojáci za dob Napoleonských válek stejně jako je potřebují dnes. Změnil se však charakter informačních zdrojů. Moderní informační technologie umožnily vzniknout řadě informačních zdrojů, např. různým databázím využitelným armádou nebo přímo zaměřených na oblast vojenství.

Příklady databází pro oblast vojenství

- **Gale Military and Intelligence Database**

Obsah: e-journals

Obor: Ekonomické vědy, politologie, technika, technologie, inženýrství, vojenství.

Producent dat: Thomson Gale

Databáze obsahuje kolekci plných textů z více než 600 titulů časopisů s více než 7 mil. článků, z nichž na 80 % je dostupných v plném textu. Databáze je

zaměřena na oblast vojenství a zpravodajských služeb včetně přesahu do souvisejících oblastí jako je letectví, strojírenství, logistika aj. Zároveň je zaměřena i na významná periodika přinášející obecnou geopolitickou informovanost.

- **Global Defence Information**

Obsah: bibliografie

Obor: Vojenství

Producent dat: United Communications Group US Naval Institute TelDan Information Sy

Global Defence Information obsahuje dvě přední světové vojenské databáze DEFENSENET a USNI MILITARY DATABASE.

DEFENSENET obsahuje abstrakty článků, zpráv, rozhovorů a mezinárodních kontraktů z předních světových periodik v oboru obrany od roku 1986. Pokrývá přes 9900 společností a dalších organizací a 35 000 produktů. DefenseNet je aktualizována měsíčně na disketách. Novou součástí GDI je DefenseNet Personal Journal - pomůcka, která umožňuje sestavovat zájmové profily pro automatické vytváření SDI rešerší při každé aktualizaci databáze.

USNI MILITARY DATABASE je rozdělena do dvou částí WEAPONS a NATIONS. Část NATIONS obsahuje detailní popisy vojenských organizací, vojenského vybavení a doktrín USA, SNS a 170 dalších zemí světa. V části WEAPONS je podrobně popsáno přes 4300 dnes používaných zbraňových systémů všech druhů - letadel, lodí, ponorek, dělostřelectva, pozemní techniky, raket a řízených střel, námořních min apod.

- **MILITARYnetBASE**

Obsah: plné texty/obrázky

Obor: Vojenství

Producent dat: CRC Press

Databáze pokrývá všechny otázky vojenství - historii, výzbroj, politiku, boj proti terorismu a další. Obsahuje (říjen 2006) 116 e-books (jejich seznam včetně údajů o editorech je uveden pod odkazem MILITARYnetBASE: Meet our Editors).

- **PROQUEST MILITARY**

Obsah: plné texty/obrázky

Obor: Politologie, vojenství

Producent dat: ProQuest Information & Learning

Součástí PROQUEST ACADEMIC RESEARCH LIBRARY. MILITARY je jedním z 10 doplňkových modulů, které lze volitelně přikoupit k jádru (core database), což je kolekce pokrývající abstrakty 700 periodik (500 v plných textech). Retrospektiva bibliografické části sahá do roku 1987. Plné texty jsou k dispozici od roku 1998.

- **WORLDWIDE GOVERNMENT AND DEFENCE DIRECTORY**

Obsah: adresář

Obor: Biografické a jim příbuzné studie, politologie, vojenství

Producent dat: Worldwide Government Directories

Databáze poskytuje široký záběr informací o světových vládních organizacích a jejich představitelích. Vychází ze tří základních zdrojů:

- *Worldwide Government Directory* obsahuje jména a kontaktní informace o klíčových hráčích světové legislativní a diplomatické komunity a také nejvyšší představitele více než 100 mezinárodních organizací jako jsou OSN, Světová banka nebo Rada Evropy. Jsou zde informace o ministrech, jejich náměstcích, poradcích, klíčových legislativních představitelích a soudech, diplomatických misiích apod. pro 195 zemí.
- *Worldwide Directory of Defence Authorities* je rozsáhlý zdroj kontaktních informací vojenských a obranných organizací celého světa. Záznam o každé zemi začíná přehledem obranné struktury a odpovědnosti různých agentur a ministerstev vč. údajů o počtech pracovníků a ročním rozpočtu. K dispozici jsou adresy vedoucích pracovníků ministerstev obrany, předních důstojníků a struktur taktického velení.
- *Profiles of Worldwide Government Leaders* poskytují detailní biografie hlav států a ministrů vlád z celého světa. Informace jsou získávány z řady zdrojů, velvyslanectví, vlád a vlastní sítě korespondentů po celém světě.

- **MARKET INTELLIGENCE**

Obsah: plné texty/obrázky

Obor: Doprava, vojenství

Producent dat: Forecast International/DMS

Prestižní MARKET INTELLIGENCE od firmy FORECAST INTERNATIONAL/DMS patří k nejdůležitějším informačním zdrojům o trhu s vojenskou a dopravní technikou. Obsahuje plné texty analýz a popisů více než 3 000 civilních a vojenských programů, včetně obrany a leteckého průmyslu v celosvětovém měřítku. Zabývá se též vojenskou výzbrojí, komerčními leteckými společnostmi, helikoptéry, leteckými motory a jejich kontrolou. Specialitou FI/DMS jsou detailní a časem dobře prověřené předpovědi vývoje každé oblasti v nejbližších 10 letech. Aktualizace online v Dialogu je týdenní. CD-ROM verze umožňuje předplatit kompletní sérii nebo jednotlivé tituly (např. COMPLETE AEROSPACE SYSTEMS SERIES, AIRCRAFT FORECAST Civil & Military, CIVIL AIRCRAFT FORECAST, MILITARY AIRCRAFT FORECAST, AIRBORNE RETROFIT & MODERNIZATION FORECAST, SPACE SYSTEMS FORECAST, COMPLETE WEAPONS SYSTEM SERIES, MILITARY VEHICLES FORECAST, MISSILE FORECAST, ORDNANCE & MUNITION FORECAST).

[4]

[popisy databází převzaty z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.]



- **Jane's**

Vydavatelství Jane's patří k celosvětově uznávaným producentům informací z oblasti vojenství. Vydává i referenční příručky a adresáře pro oblast dopravy a poskytuje také světové politicko-ekonomické zprávy. [4]

Hlavními předměty zájmu jsou obrana, doprava, letectví, bezpečnost, obchod a regionální zprávy.

[následující popisy databází převzaty z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.]

Vybrané produkty



INFORMATION WARFARE

Producent: Jane's

Vydavatel: Jane's Information Group Ltd.

Report se zabývá měnícími se principy vojenských informačních technologií a otázkami informační dominance na informačních bitevních polích. Jeho prostřednictvím je možné se dovědět, jak vojenské služby po celém světě využívají komplexní informace. Dále lze například získat informace o nastupujících válečných softwarech apod. K dispozici na CD-ROM a online.

JANE'S AIR-LAUNCHED WEAPONS IMAGE LIBRARY

Obsah: plné texty/obrázky

Databáze obsahující několik tisíců fotografií vzdušných zbraní - střely vzduch-vzduch, vzduch-země, řízené i neřízené střely, rakety, bomby, návrhy munice budoucnosti (fotografie ze zemí jako je Čína, Francie, Německo, Izrael, Rusko, Velká Británie a Spojené státy).

JANE'S ARMOUR AND ARTILLERY

Obsah: faktografie

Nejnovější informace o systémech dělostřelectva a obrněných jednotek armád celého světa. Sekce o obrněných transportérech, samohybných ostřelovacích systémech apod. Tento produkt obsahuje obrázky.

JANE'S DEFENCE WEEKLY

Obsah: faktografie

Jane's Defence Weekly představuje nejpřednější světový týdeník ve svém oboru, s největším množstvím technických detailů a informací ze zákulisí. Poskytuje pravidelné zprávy díky světové síti renomovaných korespondentů a unikátní skupině vlastních novinářů a technických redaktorů. Časopis obsahuje hloubkové zprávy ze zbrojního průmyslu, profily jednotlivých států, příležitosti na trhu, novinky z oblasti

technologického vývoje, rozhovory s klíčovými osobnostmi. Online verze se aktualizuje dvakrát týdně.

JANE'S RADAR AND ELECTRONIC WARFARE SYSTEMS

Obsah: faktografie

Obsáhlý zdroj informací o pozemních, námořních a leteckých radarových, zpravodajských a komunikačních systémech. [4]

3.3. Vězeňský informační systém (VIS)

Další bezpečnostní složkou, která bude na tomto místě uvedena, avšak jen okrajově, je Vězeňská služba České republiky (a její informační systém *VIS*). Důvodem, proč bych se o ní ráda výslovně zmínila, je ta skutečnost, že představuje jakýsi další bezpečnostní stupeň, který navazuje na činnost policie. Po vypátrání pachatele trestného činu (a po jeho pravomocném odsouzení v rámci činnosti soudů) je vězeňská služba dalším bezpečnostním stupněm, který odsouzeného přebírá do své kompetence.

Do působnosti vězeňské služby spadá i vedení evidence osob ve výkonu vazby a trestu odnětí svobody na území České republiky (§ 2 zákona č. 555/1992 Sb., o Vězeňské službě a justiční strážci ČR). Toto zákonné ustanovení dále uvádí, komu je vězeňská služba povinna údaje z evidence poskytovat (orgánům činným v trestním řízení, Bezpečnostní informační službě, celním úřadům, dalším správním úřadům). [5]

Stěžejním informačním zdrojem z oblasti vězeňství je jednotný informační systém *VIS - Vězeňský informační systém*. V současné době je Vězeňskou službou tento systém zaváděn zejména z důvodu sjednocení aplikací v rámci jednotlivých věznic a z důvodu dálkové správy (do té doby měly jednotlivé věznice svoje vlastní databáze, což mělo za důsledek to, že převody dat mezi jednotlivými věznicemi byly značně komplikované). Vězeňský informační systém se skládá z několika modulů (Správy vězňů, Administrativy, Skladového hospodářství, Ekonomiky, Zaměstnávání). Zhotovitelem tohoto projektu je firma Microsoft.

4. INFORMAČNÍ ZDROJE ZPRAVODAJSKÝCH SLUŽEB

4.1. Vybrané termíny z oblasti zpravodajských služeb

4.1.1. Pojem zpravodajská služba

Pouze tehdy, jsou-li ti, kteří rozhodují, *dostatečně informováni*, je možné očekávat, že učiní správné rozhodnutí. [6] Pokud má soud spravedlivě rozhodnout o vině nebo nevině obžalovaného, potřebuje mít dostatek informací (ve formě důkazů). Aby mohl učinit správná rozhodnutí stát, potřebuje taktéž disponovat adekvátními informacemi. Získávání, vyhodnocování a využívání informací důležitých pro národní bezpečnost, obranu, ochranu ústavního zřízení a ochranu významných ekonomických zájmů je nejen právem, ale i povinností státu. Za účelem získávání, shromažďování a vyhodnocování informací důležitých pro rozhodovací činnost státu stát zřizuje zpravodajské služby. [6] Jako synonymum pojmu *zpravodajská služba* je také často používán termín *tajná služba*.

4.1.2. Typologie zpravodajských služeb

Zpravodajské služby lze dělit podle různých hledisek. Za základní hlediska členění lze považovat dělení podle *hlavního pole zájmu* a podle *směru působení*. Podle hlavního pole zájmu se zpravodajské služby člení na **vojenské** a **civilní**. Předmětem zájmu *vojenských zpravodajských služeb* jsou militární záležitosti - obranyschopnost, obranný průmysl, různé aspekty vojenství (početnost, organizace, připravenost, rozmístění, výzbroj vojska). Druhou základní skupinu zpravodajských služeb představují *civilní zpravodajské služby*. Nejsou „jednostranně“ zaměřené jako je tomu v případě vojenských zpravodajských služeb. Civilní služby se zabývají celou řadou problematik. Jejich zpravodajská činnost se týká politických, bezpečnostních i ekonomických záležitostí.

Zpravodajské služby lze dále dělit podle směru působení, a to na služby s **vnitřní působností** (známé zejména pod označením *kontrarozvědky*, případně také *bezpečnostní služby*) a služby s **vnější působností** (známé zejména pod názvem *rozvědky*). Dalšími užívanými synonymy jsou *výzvědné služby*, *špionážní služby* nebo *vnější služby*). [6]

Posláním vnitřního zpravodajství obecně je získat, porovnat a vyhodnotit zpravodajské poznatky (informace) relevantní pro vnitřní bezpečnost státu. Zpravodajská činnost kontrarozvědky se zaměřuje zejména na vnitřní, či z vnějšku pocházející rizika, která však směřují dovnitř vlastní země služby (proto se také používá označení služby *bezpečnostní* – např. *Bezpečnostní informační služba* v České republice). Posláním vnějšího zpravodajství obecně je naopak získat, porovnat a vyhodnotit zpravodajské poznatky (informace) relevantní pro vnější bezpečnost státu. K tomu je potřeba disponovat včas informacemi o úmyslech, schopnostech a aktivitách cizích států, organizací, skupin (či jednotlivců) a jejich činitelů, které znamenají reálnou nebo potenciální hrozbu státu a jeho zájmům. Původ informací je v zahraničí (to však nevylučuje, že by nemohly být tyto informace získány z území České republiky). [6]

4.1.3. Zpravodajské služby České republiky

Podle § 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky jsou zpravodajské služby *státní orgány pro získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky*.

V České republice působí v současnosti tři zpravodajské služby. ***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 a ***Vojenské zpravodajství*** jako součást Ministerstva obrany. V čele služeb stojí ředitelé. Podle používané zpravodajské terminologie, která byla přiblížena v předcházející části, se v případě *Bezpečnostní informační služby* jedná o civilní kontrarozvědku, službu s vnitřní působností. *Úřad pro zahraniční styky a informace* naproti tomu spadá do kategorie civilních rozvědek, služeb s vnější působností. *Vojenské zpravodajství* je zástupcem vojenských zpravodajských služeb. Vojenské zpravodajství představuje zároveň vojenskou kontrarozvědku i vojenskou rozvědku. Ještě donedávna působily v rámci České republiky dvě vojenské zpravodajské služby - *Vojenská zpravodajská služba* a *Vojenské obranné zpravodajství*. První z nich zastávala pozici vojenské rozvědky, druhá vojenské kontrarozvědky. Obě služby však byly sloučeny. Od roku 2005

působí v rámci České republiky jednotná zpravodajská služba – *Vojenské zpravodajství*.

4.1.4. Pojem zpravodajská informace

Zpravodajská informace je informace, která byla získána, zpracována a zaměřena (zúžena) s ohledem na potřebu vědět pro ty, kdo rozhodují. *Zpravodajská informace* může mít přesto ještě několik jemnějších významů, existuje několik možných pojetí co do rozsahu:

- informace získaná pouze operativní cestou (pak zpravodajský = operativní) – nejužší
- informace získaná (všemi) skrytými metodami - širší
- informace získaná všemi skrytými metodami, zpracováním otevřených zdrojů a následnou analytickou prací - nejširší [6]

Další možné vymezení *zpravodajské informace* – termín, který označuje informaci, jež je konečným produktem zpracování informací zpravodajským procesem. [7]

Pohyb informace v rámci zpravodajské služby

Informace jdou nejen směrem ke zpravodajské službě – zpravodajská služba nejen informace sbírá, shromažďuje. Jejím úkolem je také informace podávat, distribuovat. Zpravodajská služba *zpravuje* stát o skutečnostech, které spadají do pole její působnosti. Předané informace jsou důležité pro rozhodovací činnost státu. Veškeré, zpravodajskou službou shromážděné informace tvoří podklad pro *zpravodajské informace*, které služba ve formě výstupů (jako konečný produkt své činnosti) poskytuje dále svým „zákazníkům“. V České republice předávají zpravodajské služby informace těmto adresátům:

podle § 8 zákona č. 153/1994 Sb., o zpravodajských službách České republiky *zpravodajské služby podávají prezidentu republiky a vládě jednou za rok a kdykoliv o to požádají zprávy o své činnosti. Zpravodajské služby předávají prezidentu republiky, předsedovi vlády a příslušným členům vlády v případech zjištění, která nesou odkladu, informace bezprostředně. Zpravodajské služby předávají státním orgánům a policejním orgánům informace o zjištěních, která náleží do oboru jejich*

působnosti; to neplatí, jestliže by poskytnutí ohrozilo důležitý zájem sledovaný příslušnou zpravodajskou službou.

4.2. Zpravodajský cyklus a jeho podobnost s cyklem informačním

Zpravodajský cyklus (angl. intelligence cycle) je řetězec postupných a vzájemně navazujících činností, při nichž jsou informace získávány, shromažďovány, zpracovány do formy zpravodajské informace a dány k dispozici uživatelům. [8]

Ve zpravodajské terminologii je znám i pod označením *zpravodajský proces* (angl. intelligence process)

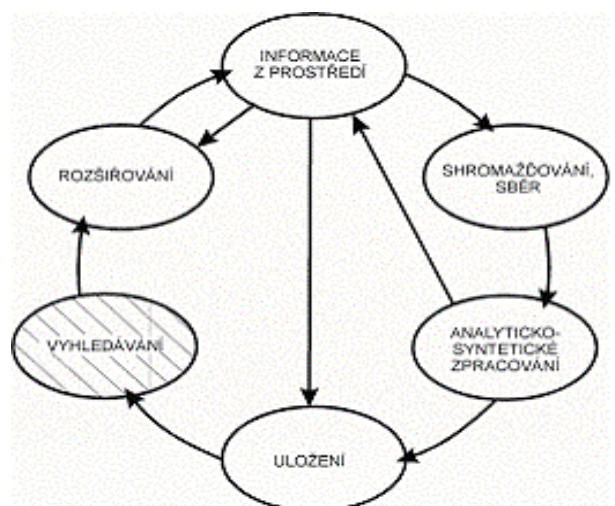
Je složen z následujících 4 fází:

1. *zadání* (a plánování)
2. *sběr informací*
3. *zpracování* (vyhodnocení) informací
4. *distribuce* informací uživatelům

Zpravodajský cyklus má podobný průběh jako klasický informační proces. Podobnost mezi zpravodajským a informačním cyklem vystihují následující obrázky. Fáze zpravodajského procesu spolu dohromady tvoří kruh. Používané názvy jednotlivých fází se mohou v různých vymezeních zpravodajského procesu poněkud lišit.



ZPRAVODAJSKÝ CYKLUS



INFORMAČNÍ CYKLUS

(Obrázky převzaty z PPT prezentace *Jak vyučovat Competitive Intelligence* přístupné na <http://www.konjunktura.cz>)

Charakteristika jednotlivých fází zpravodajského cyklu:

- *Zadání* (na základě kterého zpravodajská služba plní své úkoly) vzniká vznesením požadavku oprávněného žadatele směřujícího na zpravodajskou službu. Zadání může vzniknout i na základě rozhodnutí samotné zpravodajské služby, která zachytí určitý podnět, který spadá do její činnosti – kompetence. Zpravodajská služba pasivně nečeká na zadání, ale také v tomto ohledu aktivně jedná.

Po obdržení zadání následuje *plánování* (v rámci něhož je třeba zohledňovat i dostupnost a kvalitu již existujících relevantních poznatků, které jsou k dispozici již z dřívější doby. Je třeba určit také informační mezery (které informace je třeba ještě získat, aby bylo dosaženo splnění zadání). Je vhodné nejprve prověřit dostupné *otevřené zdroje*. Poté je třeba zvolit adekvátní metody sběru a naplánovat jednotlivé kroky dalšího postupu.

- Rozhodující fází zpravodajské činnosti je *sběr potřebných vstupních informací* (získaných jednotlivými disciplínami sběru zpravodajských informací). Následuje prvotní zpracování nasbíraných informací, které je spíše technické a organizační povahy (technické zpracování, zařazení do databází, třídění informací).
- Fáze *analytického zpracování* vyžaduje nejprve zhodnocení zpráv ze všech dostupných zdrojů, zejména posouzení důvěryhodnosti konkrétního zdroje a hodnověrnosti konkrétní informace v následujících parametrech: vztah k dané otázce, významnost, časovost, úplnost, prověřenost (potvrzení z jiných zdrojů - verifikace). Analýza je dále rozpoznání signifikantních nových faktů, srovnání s dosavadními fakty, vytvoření závěrů; integrace a (syntéza) – spojení veškeré analyzované informace do souvislého obrazu (vzorce); interpretace – rozhodnutí, „co to znamená“, ve smyslu „co se pravděpodobně v budoucnu stane“.
- Výsledkem je zpracovaná zpravodajská informace (*finished intelligence*) vhodná pro napsání výstupní zprávy, která se *distribuuje* oprávněným příjemcům. [6]

Každý jednotlivý článek cyklu zahrnuje zpětné vazby k ostatním částím zpravodajského cyklu (jedná se o učící se proces). Analytické posuzování je komponentou, přítomnou ve všech fázích cyklu. Ve zpravodajské činnosti jsou však zřídka zaplněny všechny informační mezery. Ideálem je nejen popis stavu (zpravodajský odhad), ale i prognóza vývoje a jeho alternativ. [6]

4.3. Využití zpravodajského cyklu v rámci Competitive Intelligence

Aby firmy obstály v silném konkurenčním prostředí, potřebují mít ve správnou dobu správné informace. Na základě včasných a kvalitních informací se mohou správně rozhodnout (správné rozhodnutí zásadním způsobem ovlivňuje úspěšnost firmy na trhu). *Zpravodajský cyklus* nenachází uplatnění pouze v rámci činnosti zpravodajských služeb. Využití nachází i v rámci *Competitive Intelligence*.

V České republice odborná veřejnost překládá většinou pojem *Competitive Intelligence* jako *konkurenční zpravodajství*). Používá se akronym *CI*. [10] Podstatou *Competitive Intelligence* je vytěžování veřejných informačních zdrojů za účelem získání informací o konkurenci. [9] Konkurenční zpravodajství představuje proces monitorování externího prostředí firmy, který zahrnuje získávání, zpracování a analýzu relevantních informací sloužících k získání konkurenční výhody a pro podporu rozhodování. [9] Prostřednictvím zjišťování, sledování a vyhodnocování konkurenčního prostředí lze odhalit slabé a silné stránky konkurence, rozpoznat její strategické záměry. [10]

V oblasti *Competitive Intelligence* jsou informace získávány (v rámci zpravodajského cyklu – fáze sběr informací) pouze z otevřených zdrojů. Zpravodajský cyklus používaný v rámci činnosti zpravodajských služeb počítá nejenom s otevřenými zdroji, ale i utajovanými zdroji informací.

Zpravodajský cyklus v rámci *Competitive Intelligence* je tvořen 4 fázemi:

- plánováním - identifikací informačních potřeb v návaznosti na formulaci zadání
- sběrem informací a jejich verifikací
- analýzou shromážděných informací

- distribucí informací spojenou s praktickou aplikací výsledků do podnikových procesů. [9]

5. METODY SBĚRU ZPRAVODAJSKÝCH INFORMACÍ

5.1. Významy zpravodajského termínu intelligence

Způsobů sběru zpravodajských informací existuje celá řada. V mezinárodní zpravodajské terminologii jsou jednotlivé disciplíny (metody sběru zpravodajských informací) známé pod anglickými zkratkami, které mají (až na jednu výjimku, viz. dále) koncovku *INT*. Zakončení *INT* je zkratkou pro slovo *intelligence* (zpravodajství). Slovo *intelligence* má (kromě použití v označení metod sběru zpravodajských informací) ještě druhý význam. Pod tímto termínem se skrývá i samotný produkt té které metody. Pak jsou slovem *intelligence* míněny zpracované zpravodajské poznatky, které byly získány příslušnou metodou sběru informací (v těchto případech se tedy jedná o zpracované zpravodajské informace).

Jak už bylo zmíněno, způsobů sběru zpravodajských informací existuje celá řada. Tato práce se bude blíže zabírat pouze *zpravodajstvím z otevřených zdrojů* (anglicky *Open Source Intelligence*, známé pod zkratkou *OSINT*, případně *OSCINT*). Přesto je vhodné seznámit se i s ostatními metodami sběru zpravodajských informací. Jejich stručný přehled následuje.

5.2. Stručná charakteristika jednotlivých metod sběru

HUMINT (*Human Intelligence, zpravodajství lidských zdrojů*) - špionážní činnost vedená lidskou bytostí (člověkem), který využívá různých tradičních metod konspirace (mrtvé schránky, šifrování apod.).

TECHINT (*Technical Intelligence, zpravodajství z technických zdrojů*) - technické zpravodajství je obecným protikladem předchozího INTu. Oproti HUMINTu (informace zde pochází od lidských zdrojů) jsou v případě TECHINTu informace získávány pomocí technických prostředků. TECHINT je však velmi obecným označením. Pod tímto pojmem jsou zahrnuty všechny ty zdroje, které nespádají do HUMINTu a OSINTu. Je nutno podotknout, že název TECHINT se v dnešní době už příliš nepoužívá. Jedná se o zastaralé pojmenování. Spíše než s takto obecným termínem se lze totiž setkat s jednotlivými - úžeji vymezenými INTy. Většina

zpravodajských služeb se zmiňuje o konkrétních druzích špionážní činnosti, které spadají pod tento zastřešující termín. Můžeme se setkat s pojmy jako:

SIGINT (*Signals Intelligence, radiové a radiotechnické zpravodajství*) - radiové a radiotechnické zpravodajství představuje špionážní činnost založenou na sledování různých komunikačních kanálů. Tradičně se ještě dělí na některé konkrétnější oblasti:

- **COMINT** (*Communication Intelligence, komunikační zpravodajství*) - komunikační špionáž sleduje všechny veřejně přístupné komunikační zdroje (e-maily, telefony, faxy, rádiový odposlech apod.). Dekódování zašifrovaných informací je také činností této sekce.
- **ELINT** (*Electronic Intelligence, elektronické zpravodajství*) - elektronická špionáž je založena na odposlechu a analýze především rádiové komunikace mezi vojenskými i civilními prostředky (letový provoz, policie, armáda apod.)
- **FISINT** (*Foreign Instrumentation Signals Intelligence, zpravodajství ze signálů vznikajících při používání přístrojů*) - kontrašpionážní činnost zahrnující sledování a neutralizaci / likvidaci zařízení SIGINTu cizích organizací a agentur.

IMINT (*Imagery Intelligence, obrazové zpravodajství*) - optoelektronická špionáž nebo také obrazová špionáž zahrnuje především dvě významné metody, které mohou velmi detailně informovat o aktuálním stavu v dané oblasti - letecké a družicové snímkování. Pro tuto činnost se používá jak špionážních družic, tak bezpilotních prostředků, při nutnosti pokrytí větší oblasti tradičních pilotovaných letadel s kamerovými systémy. Vedle tradičních leteckých snímků jsou mnohdy využívány i různé termovize, infrakamery a další optoelektronické systémy.

- Předchůdcem a zároveň odvětvím IMINTu, s nímž byl sloučen, je **PHOTINT** (*Photographic Intelligence, fotografické zpravodajství*) - zpravodajská činnost založená na analýze fotografií. V mnoha směrech je v dnešní době překonán. Přesto během 2. světové války měl obrovský vliv např. při analýze pobřeží pro vylodění v Normandii. Britská tajná služba žádala lidi, aby jí posílali fotky ze svých dovolených během i před válkou, díky čemuž existovala kvalitní informace o reliéfu v té které oblasti.

- **GEOINT** (*Geospatial Intelligence, geoprostorové zpravodajství*) - geoprůzkum zahrnuje veškeré geologické, hydrologické, geodetické a geografické informace o daném území. Tyto informace má většinou na starosti samostatná sekce - geografická služba, která je buď součástí zpravodajské agentury nebo s ní velmi úzce spolupracuje.

Družicové snímkování a mapování nyní patří minulosti. Vytvořily cestu pro novou disciplínu, satelitní zpravodajství.

- **SATINT** (*Satellite Intelligence, satellite electronic photography, satelitní zpravodajství*) - odvětví IMINTu, elektronické zobrazování snímané špionážními satelity.

MASINT (*Measurement And Signature Intelligence, zpravodajství měření a příznaků*) - špionáž měření a příznaků zahrnuje široký okruh rozmanitých technik sběru a zpracování informací. Zahrnuje veškerý technický zpravodajský sběr kromě zobrazovacího (IMINT) a signálního zpravodajství (SIGINT). Je primárně používáno pro určení technických parametrů cíle. MASINT používá pro účely získávání zpravodajských dat technické nástroje jako je radar, RF antény, lasery, pasivní elektrooptické snímače, jaderné radiační detektory a seizmické nebo akustické snímače. Většinou se jedná o lokaci, identifikaci a popis konkrétních předmětů či jevů odvozených od kvantitativní a kvalitativní analýzy informací, získaných z měření specifického vyzařování (např. podle šíření vln ve vodním prostředí, seizmického vlnění apod.). Při porovnání naměřených informací s databází informací známých zdrojů, lze zařízení či zdroj vyzařování s vysokou pravděpodobností identifikovat.

- Jedním z velkých podsouborů MASINTu je **TELINT** (*Telemetric Intelligence, telemetrické zpravodajství*) – dálkové měření některých signálů, telemetrická špionáž, která je založena např. na sledování elektronických signálů z konkrétního systému čidel satelitů v kosmickém prostoru. Po počítačovém zpracování je přenášena k Zemi.
- **ACINT**, nebo také **ACOUSTINT** (*Acoustic Intelligence, zvukoměrné – akustické zpravodajství*) - zvuková špionáž (zvukoměrný průzkum) k němuž je využíváno informací získaných ze zvukových signálů. Protivníkovy aktivity

jsou sledovány akustickými přístroji a prostředky (např. sledování pohybu a činnosti ponorek).

- **RADINT** (*Radar Intelligence, radarové zpravodajství*) - radarové zpravodajství je typické pro vojenské agentury. Jedná se o zpravodajství založené na informacích získaných pomocí radiolokačního vyzařování. Radar je tradičně používán pro lokalizování pozice cíle, ve vojenském zpravodajství se jedná především o radarové mapování cizích dopravních prostředků). Cílem RADINTu pak mohou být např. satelity, rakety, lodě, letadla, bojová vozidla apod.
- Jako další součásti MASINTu lze jmenovat **LASINT** (*Laser Intelligence*), sběr laserových signálů, **IRINT** (*Infrared Intelligence*), sběr infračervených signálů, **OPTINT** (*Optical Intelligence*), sběr nezobrazovaných optických zpravodajských dat, **NUCINT** (*Nuclear Intelligence*), sběr jaderných odpadů, **EFFLUENT** ((chemical) *Effluents Intelligence*), jakýkoli sběr dat o chemických odtocích nebo odpadech).

OSINT (*Open source intelligence, zpravodajství z otevřených zdrojů*) - špionáž otevřených zdrojů zahrnuje monitoring médií, novin, časopisů a webových stránek (především zpravodajských serverů) a dalších veřejně přístupných informací (knihy, technické dokumentace apod.), které mohou doplňovat a potvrzovat analytické závěry ze sledované oblasti. **LITINT** (*Literature Intelligence*), tedy sběr informací z publikované odborné literatury, je subdisciplínou OSINTu. [11, 12,13]

LIAISON - výjimkou, která byla zmíněna na začátku tohoto oddílu, kde bylo konstatováno, že všechny metody sběru zpravodajských informací (kromě jediné) jsou označovány anglickými zkratkami s koncovkou INT, je zdroj zpravodajských informací zvaný **LIAISON**. Toto anglické slovo znamená v překladu do češtiny *spolupráci*. Ve zpravodajské praxi je to pojmenování pro získávání zpravodajských informací od zahraničních partnerů. [6]

Rozdělení zpravodajských zdrojů tak, jak je provedeno v tomto přehledu, nemá žádnou všeobecnou závaznost, může se od jiných dělení lišit. Zařazení jednotlivých INTů může být odlišné. Příkladem je RADINT, který může být uváděn

jako jedno z odvětví IMINTu (*obrazového zpravodajství*). Jiné prameny jej řadí do radarového SIGINTu (*radiové a radiotechnické zpravodajství*), konkrétně do jeho odvětví ELINTu - *elektronického zpravodajství* - získávání informací sběrem z letadel, družic, lodí i pozemních stanic). Ne vždy je tedy RADINT řazen do MASINTu. To je způsobeno tím, že mnohé INTy se mezi sebou vzájemně prolínají, a proto je nelze mnohdy zcela jednoznačně zařadit.

HACKINT, ASKINT, RUMINT - další specifické metody sběru zpravodajských informací

V žádném případě se nejedná ani o celkový výčet zpravodajských disciplín sběru informací, těch je mnohem více, mnohdy jsou zcela specifického rázu.

Například **HACKINT** (*Hacking Intelligence*) představuje sběr informací zejména vojenského nebo politického charakteru získaných při nabourání se do počítačového systému a použitých k vojenským účelům (Web speak, The Daily Telegraph, October 25, 2001), dále **ASKINT** (*Askink Intelligence - Just Ask, Just Ask Them*) – získání informací využitelných zpravodajskými službami od lidí, kterým je položena otázka (tazatel může obdržet často informace, které nebyly žádány). Mnozí lidé se rádi o informace dělí s ostatními. Dalším příkladem specifické metody sběru zpravodajských informací je **RUMINT, ROUMINT** (*Rumor Intelligence, Rumour Intelligence*) – zpravodajství z informací, které jsou spíše než na faktech založeny na neověřených zprávách, řečech, dohadách, fámách apod. [14]

RUMINT a ASKINT se většinou řadí do zpravodajství lidských zdrojů, tedy HUMINTu. Obsahově by je ale bylo možné za určitých okolností zařadit i do OSINTu. Lidé se nemusí vyjadřovat pouze ústně, ale i písemnou formou či elektronicky.

Role fámy ve zpravodajství

Jelikož fáma může vzniknout v kterékoliv oblasti života člověka, může se objevit i v zájmové oblasti zpravodajských služeb. Fámy se řídí pevnou logikou a mnohdy nahrazují nedostatečnou oficiální informaci. Za jejich zjevným obsahem je možné vysledovat skryté poselství. [15]

V souvislosti s možným uplatněním fám (přesněji řečeno jejich obsahu) u tajných služeb je nutné zdůraznit, že fámou nelze zaměňovat s pojmy lež ani nesmysl, není synonymem ani pro jeden z těchto termínů. Pro veřejnost neexistuje žádná objektivní čára mezi informací a fámou. Za informaci považuje většinou to, co je podle ní pravdivé, a za fámou to, co shledává jako nepravdivé nebo přinejmenším za neověřené. Vždy se jedná o subjektivní názor. [15] To znamená, že ve skutečnosti pravdivá informace může být chybně považována za fámou, a naopak. Z toho je možné dovodit, proč může zpravodajská služba získat poznatky využitelné při své činnosti i z fámy. Zpráva, původně považovaná za fámou, může být ve skutečnosti pravdivou (a posléze i ověřenou informací). Nesmí se zapomínat na to, že existují dvě základní skupiny fám. Za první – fámy, kterým lidé uvěřili, ale které se posléze ukáží být skutečně nepravdivými informacemi, a za druhé – fámy, které jsou ve skutečnosti pravdivými informacemi a jsou využitelné.

5.2.1. Možnosti vzniku nových metod sběru informací

Pokud by bylo cílem této diplomové práce shromáždit veškeré metody sběru zpravodajských informací, které existují, jednalo by se pouze o seznam zdrojů k určitému časovému rozhraní. V souvislosti s pokrokem ve vědě mohou vznikat další metody sběru informací, neboť jsou objeveny nové technologie, kterých lze při shromažďování informací využít. Také pokud dosavadní metody sběru zpravodajských informací nepostačují k získání potřebných informací, je na to třeba zareagovat. Původní metoda je doplněna o nové poznatky, nové postupy nebo vznikne přímo nová disciplína sběru informací (případně její odvětví).

5.2.2. Blog jako zdroj informací pro zpravodajství

Za příklad vzniku zcela nového odvětví dobře poslouží příklad s blogy (neboť se tato diplomová práce z velké části věnuje otevřeným zdrojům a mezi ně patří i blogy).

Blogy představují nový zdroj informací pro zpravodajské služby. Obsahují informace ve formě osobních zpráv, obrázků, fotografií, názorů, postřehů, komentářů apod. Často jsou vytvářeny mobilními zařízeními, které umožňují publikování tohoto druhu informací během několika málo sekund. Význam blogů pro tajné služby nelze prozatím přesně určit. U otevřených zdrojů obecně se dá předpokládat, že se pro ně

budou otvírat stále nové možnosti jejich uplatnění, rozšíří se i jejich pestrost. Zastávám názor, že otevřené zdroje budou pro zpravodajské služby nabývat stále většího významu. Jak velký význam bude mít blog – nový zdroj informací pro zpravodajské služby se teprve ukáže. Nejprve je zapotřebí důkladně zhodnotit jeho výhody (přínos), náklady, rizika, možnosti využití.

Tajné služby se na zpravodajství z otevřených zdrojů spoléhají už dlouho – získávají a analyzují informace shromážděné ze zdrojů veřejnosti volně přístupných (např. z tisku, rádia, televize apod.). Na blogy se dá pohlížet jako na nový zdroj informací vhodný pro zpravodajství. [16]

Americké tajné služby (včetně CIA) i ministerstvo obrany čerpají informace mimo jiné také např. z webových stránek, a svou pozornost obrátily také k informacím pocházejícím z blogů. Blogy slouží např. k identifikování sociálních sítí a vztahů mezi jednotlivými osobami. [17] Z velkého množství blogů, které na internetu vznikají, lze získat řadu užitečných informací využitelných i tajnými službami. Lidé na blogy umisťují často takové informace, které se nikde jinde nenacházejí, říká ředitel *Open Source Center* Douglas J. Naquin. Vyskytují se zde informace vypovídající o sociálních perspektivách, náladách ve společnosti apod. [18]

Pokud bylo řečeno, že CIA získává informace také z blogů, neznamena to, že si může dovolit prohlížet úplně všechny blogy. Vzhledem k jejich velkému množství po celém světě by to ani nebylo proveditelné. Pečlivě si mezi nimi vybírá. Proto není ani důvod k obavám, že by tajné služby četly i neškodné blogy obyčejných lidí. Zpravodajské služby věnují svoji pozornost pouze vytipovaným blogům (např. z určitých zeměpisných oblastí – z Číny, z arabských států apod.). Podle *Washington Times* jsou v hledáčku CIA právě blogy z Číny. Podle sdělení jednoho z představitelů Pentagonu obdržela CIA skrze čínské blogery cenné informace týkající se tajných čínských programů výzbroje armády. [19] Zpravodajství z blogů – **BLOGINT**, **WEBBLOGINT** (*Blog Intelligence, Webblog Intelligence*), získávání informací z blogů, je možné pokládat za novou subdisciplínu OSINTu.

6. OTEVŘENÉ ZDROJE U ZPRAVODAJSKÝCH SLUŽEB

6.1. Úvod do problematiky otevřených zdrojů

Případová úloha – politique fiction

Příznivci špionážních románů mohli číst knihu od spisovatele Jamese Gradyho Šest dnů kondora (známé je i filmové zpracování této knihy Tři dny kondora od režiséra Sidneyho Pollacka). Hrdiny špionážních románů bývají většinou neohrožení agenti tajných služeb, zařazení ve speciálních odděleních zpravodajských služeb. Pracují v terénu a účastní se tajných operací, při nichž plní nebezpečné úkoly. Hlavní postava knihy Jamese Gradyho se v tomto ohledu od těchto „klasických“ agentů liší. Působí v jednom zcela netypickém oddělení CIA, než v jakých obvyklí hrdinové špionážních románů a filmů pracují. Hlavní hrdina je zaměstnán v jedné ze sekcí CIA, jež se zabývá problematikou otevřených zdrojů. Jeho pracovní náplní je čtení literárních děl týkajících se špionáže. Celá tato sekce CIA má za úkol pročítat špionážní romány a detektivky, poté díla zanalyzovat, provést rozbor popisovaných zápletek příběhů a porovnat je se skutečnými událostmi. [20]

V uvedené románové situaci představuje shromažďování a třídění informací hlavní činnost CIA. Dále v knize stojí, že asi 80 % informací, které CIA shromažďuje a třídí, pochází z odborných časopisů, z domácích i zahraničních periodik, z rozhlasového a televizního vysílání z celého světa a z knih, tedy z otevřených zdrojů. V této knize je činnost zpravodajských služeb prezentována také jako práce s informacemi z otevřených zdrojů. O logičnosti vysokého procenta podílu informací pocházejících z *otevřených zdrojů* svědčí ten fakt, že na světě z celkového počtu veškerých existujících informací tvoří tajné informace 1 %, 4 % připadají na informace z šedé zóny a zbytek, tedy 95 % všech informací představují informace veřejně dostupné (včetně informačních zdrojů placených, zdrojů podmíněných členstvím apod.).¹

V *otevřených zdrojích* mohou zpravodajské služby nalézt pro svou činnost velké množství využitelných informací. Robert D. Steel, bývalý zpravodajský důstojník, který mimo jiné působil také jako prezident *Open Source Solutions, Inc.*, neziskové vzdělávací korporace se sídlem v Oaktonu ve Virginii, za dobu svého působení ve zpravodajské praxi objevil, že by dokázal 80 % informací požadovaných

¹ Z přednášek PhDr. Richarda Papíka, Ph. D. konaných na Ústavu informačních studií a knihovnictví v Praze v roce 2005

„zákazníky“ získat pouze za použití otevřených zdrojů. Na utajované zdroje by připadalo zbývajících 20 %. [13]

Zpravodajství z otevřených zdrojů (OSINT) by nemělo být považováno za okrajovou metodou sběru informací, nemělo by být podceňováno. Za příklad zamítavého postoje k otevřeným zdrojům lze považovat prohlášení bývalého prezidenta Nixona. Je nutné podotknout, že jeho prohlášení směřovalo v první řadě k činnosti americké CIA, avšak lze jej vztahovat i na otevřené zdroje. Prezident Nixon prohlásil: „K čemu je vůbec CIA? Mají tam více než 40 000 zaměstnanců, kteří nedělají nic jiného, než čtou noviny.“ Studium otevřených zdrojů (kam spadají i zmíněné noviny) je důležité i pro zpravodajské služby. [21] Názor, že tajné informace jsou nesrovnatelně důležitější než informace získané z otevřených zdrojů, je mylný. Veřejně přístupné informace není na místě podceňovat. Na informace pocházející z otevřených zdrojů a informace pocházející z utajovaných zdrojů by se mělo ve zpravodajských službách pohlížet jako na nerozlučnou dvojici. Lze si je představit jako jednotlivé kousky skládačky. Jestliže nějaká část skládačky chybí, nelze ji nikdy celou složit, zkompletovat.

Britské listy ve svém článku CIA: Chcete-li být dobrým špiónem, čtěte noviny ze dne 1. 11.2005 (ze kterého bylo převzato i výše uvedené prohlášení prezidenta Nixona) uvádí známé případy z minulosti, kdy tajné zprávy byly kompilací novinových výstřižků z různých zemí světa. Podle Britských listů je to umožněno tím, že tisk často publikuje zpravodajství založené na prozrazených důvěrných informacích. [21] Agent CIA James Lilley si před lety uvědomil, že čínští agenti CIA „podvádějí“ jeho kancelář tím, že mu poskytovali údajně důvěrné informace o vývoji v Číně. Ve skutečnosti to však byly vyšperkované překlady článků z regionálního čínského tisku. Podobně i evropští podvodníci v padesátých letech často předávali CIA informace získané ze sovětského tisku. [21]

Britské listy v článku dále uvádí: Za druhé světové války bylo přísně zakázáno informovat v médiích o letech bombardérů B-29. Agent Samuel Halpern vzpomíná na to, jak jednou překvapil jednoho admirála, když ve svém informačním shrnutí informoval o letech těchto bombardérů. „Jak je možné, že to víte?“, ptal se admirál. Halpern ho informoval, že o letech bombardérů se dověděl z monitoringu japonského rozhlasu. To, co bylo v USA utajováno, bylo v Japonsku otevřenými

informacemi. To může vést k absurdní situaci, kdy se cizinci dovídají o akcích CIA z celostátních sdělovacích prostředků, avšak v Americe je to přísně tajné a armáda a CIA vůbec nevědí, že se o těchto akcích otevřeně píše v místním tisku. Vlastně je to potom tak trochu „jednostranně utajovaná zpráva“. [21]

Otevřené zdroje

Představa o tom, že tajné služby pracují pouze s informacemi podléhajícími určitému stupni utajení, by byla mylná. Tvrzení, že veřejně přístupné informace, ke kterým se snadno dostane i běžný uživatel, nemohou přinést tajným službám žádný užitek, by nebylo pravdivé. Zpravodajské služby pro svou práci potřebují a využívají samozřejmě i neutajované informace, které tvoří protiklad informací tajných. Neutajované informace získávají z tzv. *otevřených zdrojů*. Dále zpravodajské služby využívají různé speciální informační zdroje, které jsou však pro běžného uživatele nedostupné. K otevřeným zdrojům (jak už lze z názvu usuzovat) si naopak může zajistit přístup v podstatě kdokoli. Nalézají se v nich řada důležitých informací, které se nikde jinde nenalézají a bez nichž by se v dnešní době tajné služby při své činnosti neobešly. Lze se setkat i s jinými označeními pro tento druh zdrojů informací jako např. *veřejné zdroje* nebo *volně přístupné zdroje*.

Jestliže zde bylo řečeno, že tento druh informačních zdrojů může využít kdokoli, neznamená to, že k nim bude mít přístup každý z nás kdykoliv si vzpomene, bez nutnosti splňovat jakoukoliv podmínku, a že není potřeba vyvinout sebemenší úsilí, aby se zájemce o informaci k takovému zdroji dostal. Představovat si tyto zdroje jako zdroje, které jsou *někde neustále každému* k dispozici, by bylo samozřejmě mylné. Označení *veřejné zdroje* může k tomuto chybnému závěru poněkud svádět. Z tohoto důvodu by asi bylo lepší v označení nepoužít příslovce *veřejně*, ale podstatné jméno *veřejnost* (např. zdroje (určené) pro veřejnost, zdroje veřejnosti přístupné apod.). Ona *otevřenost*, *volnost*, *veřejnost* informačního zdroje spočívá v něčem jiném, než ve způsobu, případně snadnosti přístupu. Znamená především *možnost* pro jakéhokoliv zájemce o informaci(e), zajistit si do informačního zdroje přístup. Tato možnost je tu pro uživatele k dispozici nepřetržitě.

Tím se otevřené zdroje od těch tajných zásadním způsobem odlišují. U utajených zdrojů zde tato možnost – aby měl jakýkoliv člověk k tajným zdrojům

přístup - vůbec neexistuje (myšleno legální cestou). Pokud se k tajným informacím pocházejícím z utajovaných zdrojů informací dostane neoprávněná osoba, jedná se v podstatě o únik informací (způsobený např. vyzrazením tajné informace oprávněnou osobou osobě nepovolané nebo zapříčiněné nedostatečnou ochranou dat). Tímto způsobem přístup k informacím se však tato diplomová práce zabývat nebude.

6.2. Charakteristika otevřených zdrojů ve zpravodajství

Žádná obecně platná a všemi uznávaná definice otevřených zdrojů v současnosti neexistuje. Většinou jsou však za ně považovány zdroje dostupné zdarma nebo za úplatu celé veřejnosti. Jindy jsou mezi ně zahrnovány i zdroje neveřejné, s omezeným přístupem. Stejně tak neexistuje žádná definice otevřených zdrojů, která by byla uznávaná všemi zpravodajskými službami světa. Záleží na každé jednotlivé zpravodajské službě, které zdroje informací bude mezi otevřené řadit.

Otevřených zdrojů informací existuje velké množství, obsahují informace pravdivé i nepravdivé, ne vždy jsou snadno dostupné. Některé z těchto zdrojů jsou dostupné zcela volně, bez omezení, některé jsou přístupné na základě bezplatné registrace, jiné mohou být placené.

Ve zpravodajské praxi by otevřené zdroje měly být první zastávkou při hledání informací. Pokud lze dané informace získat z otevřených zdrojů, je lepší dát přednost této metodě sběru informací. Získání informací z otevřených zdrojů je výhodnější - ať už z hlediska snadnější dostupnosti informací, z hlediska finančních nákladů spojených s pořízením informací či z hlediska bezpečnosti výtěžovatele informace (u jiné metody sběru informací by mohlo hrozit např. prozrazení příslušnosti osoby výtěžovatele ke zpravodajské službě). V *otevřených zdrojích* se nenalézají pouze obvyklé, nepříliš důležité či okrajové informace. Nenacházejí se v nich informace, které může využít jen běžný (všední) uživatel. Hodnotné informace, použitelné pro svou činnost, nacházejí v *otevřených zdrojích* i zpravodajské služby. Konkrétně v nich mohou vojenské zpravodajské služby například sledovat vývoj obranných systémů v rámci nějakého státu nebo z nich výtěžit informace o aktuálním stavu obranných systémů. Stačí sledovat odbornou literaturu, články v odborných časopisech apod. za určité časové období. V těchto zdrojích mohou být zpracovány

různé přehledy, souhrny, srovnání technických parametrů atd. (zpracované odborníky). Z hlediska času je možnost získání požadovaných informací tímto způsobem pro zpravodajské služby velmi výhodná (nejenom z hlediska času, také kvality zpracovaných informací či z hlediska finančních prostředků). Na závěr je třeba zmínit, že *otevřené zdroje* nejsou využitelné ve všech případech. Existují samozřejmě i oblasti, které jsou předmětem zájmu zpravodajských služeb, o nichž se v otevřených zdrojích nepíše.

6.2.1. Možné definice otevřených zdrojů a jejich informací pro oblast zpravodajství

Definic otevřených zdrojů existuje celá řada. Lze se setkat s vymezeními negativními i pozitivními, s vymezeními širokými či úzkými. Následuje několik příkladů možných definic.

- Negativním způsobem lze otevřené zdroje charakterizovat jako *zdroje, které nebyly získány prostřednictvím specifických prostředků získávání informací (viz. ostatní metody sběru zpravodajských informací) a nebyly získány ani v rámci spolupráce se zahraničními partnery.*
- Jiná definice může otevřené zdroje vymezovat pouze jako *běžně přístupné sdělovací prostředky.*
- Další jako *masová, regionální a specializovaná média (například internet).*
- Za otevřené zdroje mohou být také považovány *zdroje, které jsou neutajované a jsou dostupné ve veřejné sféře nebo prostřednictvím komerčních služeb.* [22]
- Další definice otevřené zdroje vymezuje jako *zdroje, které nejsou předmětem utajení, je k nim zpravidla volný přístup, jsou etičtější a rovněž levnější než zdroje speciální a je zde menší riziko konfliktu se zákonem.*

Následují definice informací z otevřených zdrojů:

- *Informace z otevřených zdrojů jsou veřejně dostupné informace a jakékoliv neutajované informace s limitovanou veřejnou distribucí nebo omezeným přístupem (např. za úplatu, s podmínkou registrace), dostupné legálními a etickými prostředky.* [23]

- Jiným označením, které lze použít místo pojmu informace z otevřených zdrojů, jsou volné zpravodajské informace. *Jsou to veřejně dostupné informace (tj. jakýkoliv člen veřejnosti může podle zákona obdržet informace na požádání nebo je může získat zkoumáním), a také další neutajované informace, které mají omezenou veřejnou distribuci nebo přístup.*
- V rámci zpravodajských služeb lze za volné zdroje informací považovat také *jakékoliv informace, které mohou být využity v neutajovaném kontextu bez ohrožení národní bezpečnosti nebo zpravodajských zdrojů a metod.*
- Další negativně pojaté vymezení informací z otevřených zdrojů - *Jestliže informace není veřejně dostupná, mohou se aplikovat určité právní požadavky týkající se shromažďování, zadržování a šíření.*

Možné definování pojmu *zpravodajství z otevřených zdrojů* (OSINT) a jeho informací:

- *Volný zpravodajský zdroj poskytující informace shromážděné z volných zdrojů jako jsou noviny, televizní a rozhlasové vysílání, knihy, zprávy, časopisy, fotografie a jiná média.*
- *Informace získané z rozsáhlých souborů informací v otevřené, neutajované literatuře.*
- *Informace z otevřených zdrojů - materiál, který je veřejně dostupný (noviny, knihy, časopisy atd.). Tato definice se řadí mezi ty úžeji pojaté. Například velké množství informací pocházejících z IMINTu (Optoelektronická špionáž, obrazová špionáž) se stává veřejně dostupným z komerčních zobrazovacích satelitů. Komerční databáze zase obsahují velké množství ekonomických dat, která jsou dostupná za cenu předplatného.*
- *Zpravodajství z otevřených zdrojů - Zpráva určená pro podporu rozhodování, zpracovaná z informací z otevřených zdrojů, bez podpory utajovaných zdrojů. [24]*

Bývalý ředitel Úřadu pro zahraniční styky a informace Petr Zeman se k *otevřeným zdrojům* vyjádřil takto: *Otevřené zdroje nejsou jen obvyklé komerčně*

dostupné tištěné a elektronické sdělovací prostředky, ale celá škála sofistikovaných, málo známých postupů, v nichž jsou často „ukryta“ cenná data, o nichž často dopředu nemáme tušení. S nástupem internetu (a po pádu mnoha diktatur ve světě) se staly otevřené zdroje ještě významnější. Data z otevřených zdrojů tvoří v databázích – informačních fondech zpravodajských služeb obrovský podíl. Na některá témata a při vyšším stupni obecnosti analýz mohou otevřené zdroje poskytnout uspokojivé odpovědi. [6]

6.2.2. Typologie otevřených zdrojů

Dělit otevřené zdroje informací lze z více úhlů pohledu, neexistuje pouze jediné členění.

➤ Z hlediska přístupu lze otevřené zdroje dělit na:

- informační zdroje *přístupné bez omezení, veřejné* (přístupné obecně), určené pro širokou veřejnost, v podstatě pro kohokoliv, kdo o ně projeví zájem.
- Otevřené zdroje informací *s omezeným přístupem, neveřejné* - přístup je pro veřejnost omezen, jedná se především o různé databáze vedené státními orgány a orgány územní samosprávy, veřejnými institucemi hospodařícími s veřejnými prostředky apod. Příkladem jsou informační systémy vedené Policií České republiky, která je podřízena Ministerstvu vnitra.

➤ Dalším hlediskem je například hledisko finanční, tedy zda jsou informace z těchto zdrojů poskytovány zdarma či za úplatu. Pak rozeznáváme informační zdroje

- poskytované zdarma
 - bez nutnosti registrace
 - s podmínkou registrace
- poskytované za úplatu (placené informační zdroje, zdroje komerční)

6.2.3. Výhody a nevýhody otevřených zdrojů

Výhody otevřených zdrojů

Otevřené zdroje jsou velmi cenné z různých důvodů. Jednou z velkých výhod je *rychlost šíření* těchto informací. Pokud dojde v některé části světa k nějaké krizi, dozví se o ní velmi rychle zbytek světa z novin, televize, rádia. [21]

Další výhodou *otevřených zdrojů* je *množství informací*. Kvantitu informací je však třeba za jistých okolností vnímat i jako nevýhodu.

Kvalita informací z otevřených zdrojů představuje další výhodu. V *otevřených zdrojích*, např. v různých komerčních databázích se nacházejí kvalitně zpracované informace využitelné zpravodajskými službami. Na druhou stranu se v *otevřených zdrojích* nalézají i nekvalitní informace, což je třeba zohledňovat. Informační zdroje je nutné z hlediska spolehlivosti a přesnosti hodnotit, vhodné je si danou informaci ověřit z více zdrojů.

Ačkoliv kvalitní informace nejsou většinou zadarmo, vynaložené *náklady* na získání informací z otevřených zdrojů mohou být ve srovnání s náklady vynaloženými na získání informací z utajovaných zdrojů zanedbatelné (příklad: drahý výzvědný satelit poskytující fotografie ponorky patřící nepřátelskému státu kontra zahraniční magazín poskytující stejné informace (fotografie) – stačí si jej předplatit).

Otevřené zdroje jsou relativně *snadno získatelné, rychle dostupné*, jsou *nezávislé na zadání* (*otevřené zdroje* většinou zpřístupňují to, co získaly ve svém zájmu a nejsou - narozdíl od utajovaných zdrojů - závislé na zadání analytika zpravodajské služby). Jejich *sběr obnáší nižší riziko*, nehrozí rozkrytí utajených metod sběru informací (může však být odhalen objekt zájmu). Otevřené zdroje *minimálně zasahují do lidského soukromí a nemusí být utajovány*. [25]

Nevýhody otevřených zdrojů

- Jejich **původ, spolehlivost, důvěryhodnost a rozsah** může být neznámý, mohou být prostředkem dezinformace.
- Jsou **nestrukturované** a velmi **různorodé**.

- Jejich **objem** - přinášejí informační nadbytek, který ztěžuje nalezení relevantní, užitečné informace.
- Jsou **nestabilní**, především na internetu je řada informací dostupná pouze dočasně. [25]

6.2.4. Zřizování specializovaných oddělení zaměřených na otevřené zdroje

Zpravodajské služby celého světa využívají otevřených zdrojů v rámci své činnosti. Informace spadající do této kategorie zdrojů jsou na internetu volně přístupné, ale jsou uloženy také v rozmanitých databázích. Vyhledávání v takových databázích, zvláště v těch, které používají složitější dotazovací jazyky, může obecně nezkušeným uživatelům činit obtíže. V praxi je obvyklé, že zejména větší firmy, které tyto databáze využívají, za tímto účelem zřizují speciální pracoviště s informačními specialisty, kteří se této problematice věnují. Takováto pracoviště vznikají i v nejrůznějších státních úřadech a institucích, a disponují jimi také zpravodajské služby. Pracovníci z takto zaměřených oddělení služeb vyhledávají informace pro analytiku (např. na základě konkrétního informačního požadavku analytika, ale i ve formě průběžné rešerše). Sběr informací je důležitou součástí zpravodajského cyklu. Má podstatný vliv na všechny následující fáze cyklu. O shromážděných informacích platí, že po předání informací musí analytik určit, zda jsou tyto informace užitečné a jak jsou přesné. Analytik by měl také posoudit, zda je dotyčný zdroj znám již z minulosti (zejména zda je znám jako spolehlivý). [7] Analytikem zpracované informace jsou pak v konečné fázi distribuovány zákazníkům ve formě výstupní analytické zprávy.

6.3. Otevřené zdroje z hlediska obsažených informací

Pokud budeme informace dělit do dvou základních skupin na informace *utajované* a *neutajované*, pak obsahem *otevřených zdrojů* budou jediné informace neutajované (nesprávná manipulace s utajovanými informacemi však může toto dělení poněkud zkomplikovat. Je otázkou, do které ze dvou skupin by se řadily informace utajované, které by byly například vyzrazeny a následně zveřejněny, zpřístupněny široké veřejnosti, a naopak, do které ze skupin by případly informace neutajované, které by byly nesprávně klasifikovány jako informace utajované).

6.3.1. Utajované versus neutajované informace

Jedním ze způsobů, jak se pokusit definovat *neutajované informace* pocházející z *otevřených zdrojů* (v rámci České republiky), je seznámit se nejprve s druhem informací, které tvoří jejich pravý opak, tedy s informacemi utajovanými. Na základě vymezení utajovaných informací lze odvodit následně i definici informací neutajovaných. Utajované informace jsou vymezeny v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tento zákon mimo jiné upravuje zásady pro stanovení informací jako *informací utajovaných*, podmínky pro přístup k nim a další požadavky na jejich ochranu.

V paragrafu 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací je objasněn pojem utajovaná informace jako „*informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, 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.*“

Národní bezpečností úřad zpracovává návrh seznamu utajovaných informací. Seznam utajovaných informací pak vydává vláda svým nařízením.

6.3.2. Klasifikace utajovaných informací

Zákon č. 412/2005 Sb., o ochraně utajovaných informací klasifikuje utajované informace podle stupně utajení na:

- a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,
- b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,
- c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,
- d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.

6.3.3. Rozdíly mezi utajovanými a neutajovanými informacemi

Z definice *utajované informace* podle § 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací je důležité povšimnout si zejména této části věty „... jejíž vyobrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací.“ V této větě jsou významné zejména tři charakteristiky utajovaných informací.

Za prvé, pokud může tuto informaci nějaká osoba *vyzradit*, případně *zneužít*, logicky z toho vyplývá, že zřejmě patří do nějaké skupiny lidí, kteří se s touto informací mohou seznamovat (na rozdíl od ostatních lidí). Jinými slovy, že přístup k informaci nemá kterákoliv osoba v České republice (nebo dokonce na světě), pokud by o ni měla zájem. Musí se jednat o oprávněnou osobu, která splňuje podmínky přístupu k utajovaným informacím stanovené zákonem č. 412/2005 Sb., o ochraně utajovaných informací.

Když může informaci člověk snadno získat, případně se k ní dostane za minimálního přičinění se nebo za určitých, ne nepřekonatelných překážek, zřejmě se nebude jednat o utajovanou informaci. Těmito překonatelnými překážkami jsou myšleny například technické záležitosti (např. prozatímní nemožnost připojení se k internetu) nebo různé schopnosti a dovednosti zájemce o informaci (chybějící zkušenosti ve vyhledávání informací apod.). Pokud se bude daná informace nacházet na internetu, stačí se k němu připojit a informace se stane dostupnou. V dnešní době může mít přístup k internetu v podstatě kdokoli (stačí zajít do internetové kavárny, knihovny, pokud její osoba nemá přímo doma, případně k dispozici v práci). Pokud se bude jednat o utajovanou informaci, je situace odlišná. S těmito informacemi se mohou seznamovat pouze *oprávněné osoby*.

Druhou zásadní charakteristikou utajovaných informací je ta skutečnost, že případné vyobrazení nebo zneužití utajovaných informací má ten účinek, že může způsobit újmu zájmu České republiky nebo její vyobrazení může být pro tento zájem nevýhodné. Zájmem České republiky je zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob (§ 2 písm. b) zákona č. 412/2005 Sb., o ochraně utajovaných informací).

Neutajované informace takovýto účinek – způsobení újmy zájmu České republiky - nemají. Samozřejmě i zveřejněním neutajované informace může dojít ke způsobení újmy určitým zájmům. Ne však zájmům České republiky, ale například zájmům nějaké fyzické osoby, pokud o ní někdo napíše - například do novin nebo na internet - nějakou pomluvu, rozšíří fámu apod. Tato osoba bude pociťovat újmu, ne však újmu, která je myšlena v zákoně č. 412/2005 Sb., o ochraně utajovaných informací, ale například újmu morální (nebo je poškozeno dobré jméno nějaké firmy uvedením nepravdivých údajů o ní, což se může projevit např. v tržbách - finanční újma atd.).

Třetí podstatnou charakteristikou utajovaných informací je ta okolnost, že utajovaná informace je uvedena v seznamu utajovaných informací. Informace tak lze jednoduše rozdělit do dvou základních skupin – buď se nějaká informace řadí do existujícího seznamu utajovaných informací nebo ne. Z toho vyplývá, že pokud určitá informace mezi ty utajované (zanesené v seznamu) nespadá, patří mezi informace neutajované. Neberou se zde v potaz případy, kdy by byla nějaká informace (neutajovaná) do seznamu neoprávněně zařazena nebo by se jiná do seznamu nedostala (utajovaná), ač by tam být měla. Stejně platí, jestliže nějaká informace, patřící mezi utajované informace, je někým neoprávněně vyzrazena a dostala by se například do novinového článku nebo na internet, čímž by byla dostupná komukoliv z nás. Neplatil by zde příměr, že utajované informace jsou přístupné jen omezenému okruhu oprávněných osob, jak bylo zmíněno v první charakteristice utajovaných informací.

7. INTERNET VERSUS ZPRAVODAJSKÉ SLUŽBY

Díky tomu, že se na internetu vyskytuje velké množství informací, lze předpokládat, že některé z obsažených informací budou zajímavé i pro zpravodajské služby. Prostřednictvím internetu jsou uživatelům zprostředkovány informace z různých veřejných i komerčních databází. Mnohé z databází jsou využitelné i zpravodajskými službami. Relativně snadný přístup k informacím na internetu se může v určitém směru obrátit i proti zpravodajským službám.

Jestliže se jedná o zpravodajské – v následujícím případě bude vhodné použít termín *tajné služby*, logicky z toho vyplývá, že by příslušnost zaměstnanců k těmto organizacím, s ohledem na jejich bezpečnost a z dalších důvodů, měla být utajena (nepočítaje v to oficiálně známé osobnosti služeb, např. jejich ředitele, mluvčí apod.). Následující případ ukáže, že utajení totožnosti příslušníků k tajným službám v době internetu může být poněkud komplikované.

7.1. Prostřednictvím internetu lze odhalit agenty CIA



Případová úloha

K získání informací o identitě agentů nejznámější americké tajné služby CIA stačí mít podle Chicago Tribune přístup na internet. Americká tajná služba CIA je jednou z nejznámějších zpravodajských služeb světa. Zkratka CIA (Central Intelligence Agency) je pro mnohé synonymem pro pojmy jako uchování v tajnosti, utajení či zachování tajemství. Avšak v době internetu už na to zřejmě nemá nárok. Americký list Chicago Tribune totiž ve svém článku s názvem „Internet blows CIA cover. It's easy to track America's covert operatives. All you need to know is how to navigate the Internet.“ ze dne 12. 3. 2006 napsal, že agenty americké tajné služby CIA lze odhalit přes internet. Na žádost CIA a s ohledem na národní bezpečnost jména agentů list nezveřejnil.

O jaké konkrétní informace se jednalo? Údajně se mu podařilo zjistit totožnost 2653 zaměstnanců CIA. List uvedl, že mezi vypátranými osobami bylo 160 analytiků, představitelů služby (veřejnosti známí), ale patřilo mezi ně i nejméně 24 agentů s utajenou identitou. Aniž by byl navenek zřejmý vztah některého z příslušníků CIA, člověku, který se na internetu dobře vyzná, by zřejmě nečinilo větší problémy (za pomoci správců nejrůznějších dat na internetu), odhalit jeho totožnost

a vztah k této organizaci. Nejednalo se o žádné nabourání se do počítačů CIA, veškeré informace byly získány legálními prostředky, přístupnými komukoliv. K většině zjištěných jmen bylo možné dohledat také adresy, soukromá telefonní čísla, jména rodinných příslušníků, dřívější zaměstnavatele a další informace, které zvláště pro příslušníky CIA pracující v utajení mohou znamenat ohrožení života. Jako příklad jmenoval list údaje o jedné z agentek. Bez problémů bylo možné zjistit, že se jedná o 52letou ženu, která vyrůstala na předměstí Kansas City, nyní žije v rodinném domku ve Virginii se třemi ložnicemi, a že v posledním desetiletí pracovala na několika amerických ambasádách v Evropě.

Podrobnou rešeršní strategii z pochopitelných důvodů autor článku John Crewdson nezveřejnil. Poznamenal však, že odhalení identity agentů CIA bylo záležitostí komplexnějšího charakteru a jednalo se o pouhé zadání jednoduchého dotazu do Googlu (i když i ten byl k vyhledávání informací údajně použit). To však nic nemění na tom, že by stejné informace dokázal vyhledat každý, kdo se na internetu „vyzná“ a umí provádět rešerše např. ve veřejných databázích přístupných přes internet.

Ke zjištění identity agentů CIA listu nebyly použity žádné speciální nepřístupné databáze. K vyhledání informací napomohly pouze bezplatné vyhledávací internetové nástroje (jako příklad uveden Google) a komerční databáze (jako příklad uveden Lexis-Nexis.). Rozmanité online vyhledávací služby v USA (většinou se jedná o placené databáze) nabízejí přístup k nejrůznějším informacím. Zpřístupňují veřejná data týkající se jednotlivých osob nebo institucí. Zpřístupňování takovýchto informací je z obchodního hlediska výhodné. V USA neexistuje žádný jednotný systém na přihlašování obyvatelstva. Jednotlivé databáze poskytují řadu informací – telefonní seznamy, údaje z pozemkových knih, dále různé daňové doklady (např. o dani z pozemků, daňová přiznání), volební seznamy s uvedením povolání, pracovní místa registrované osoby, podklady z obchodu s nemovitostmi, rozsudky soudů, obchodní rejstřík, satelitní snímky (např. obydlí, pracovišť). Za 14 dolarů 95 centů si může zájemce přes podobné služby nechat vyhledat svého bývalého spolužáka. Anebo někoho jiného napadne zkusit vyhledat přes tyto veřejně přístupné informační zdroje příslušníky CIA.

List Chicago Tribune identifikoval agenty CIA právě přes telefonní seznamy, informace o koupích a prodeích nemovitostí, volební seznamy, daňové doklady a další finanční a právní dokumenty. Při svém hledání nenarazil Chicago Tribune pouze na příslušníky CIA. Odhalil také více než 24 tajných objektů a výcvikových středisek patřících CIA, rozmístěných po celých Spojených státech, krycí firmy CIA, 50 interních telefonních čísel nebo informace o 17 soukromých letadlech, které mají vztah k CIA (včetně bližších letových údajů a údajů o oficiálních vlastních těchto letadel). Některá z letadel měla být použita k transportu podezřelých osob z terorismu.

CIA neměla před tím, než je list Chicago Tribune konfrontoval s provedenou rešerší, poněti o tom, že je tak snadnou cestou možné odhalit tolik informací o svých zaměstnancích. Tajná služba byla překvapena, v jakém rozsahu je možné tajné informace nalézt na internetu. Ředitel CIA Porter Goss nařídil (dle vyjádření vydavatele Chicago Tribune) okamžitě celou věc prošetřit. Některé z informací, které redaktoři přes internet našli, byly údajně z webu odstraněny (za několik dnů poté, co Tribune požádala CIA o stanovisko k celé věci, měly z internetu zmizet údaje o firmách majících vztah k zmiňovaným soukromým letadlům).

Příčinou odhalení totožnosti agentů v Americe je podle mluvčího CIA především ta skutečnost, že postupy, které k utajení v minulosti stačily, již v současnosti nefungují. V době internetu je utajení totožnosti agentů mnohem těžší. Celou problematiku s utajováním příslušníků tajných služeb je podle jeho vyjádření nutné brát komplexně, a přizpůsobit ji soudobému stavu. Naproti tomu je nutné podotknout, že sami agenti záležitost s utajováním totožnosti svým chováním negativně ovlivňují.

Případ Camp Peary

Dále se list Chicago Tribune pokusil prostřednictvím internetu nalézt informace o výcvikovém středisku CIA ležícím ve státě Virginia - Campu Peary. Pokud by se někdo v centrále CIA v Langley ptal po Campu Peary, dostal by vyhýbavou odpověď. Do 80. let 20. století CIA popírala existenci tohoto výcvikového střediska, ležícího v blízkosti Williamsburgu ve Virginii. Pokud položíme stejnou otázku Googlu, dostaneme znatelně lepší výsledek. Úspěšný byl i list Chicago Tribune při své rešerši na téma Camp Peary.

Provedením jednoduché rešerše na téma The Farm – Camp Peary, jak uvádí Crewdson z Chicago Tribune, se dají rychle získat informace vedoucí k údajům o 26 osobách, kteří jsou podle získaných dat zaměstnáni na Farmě. V databázích americké civilní letecké dopravy se daly vynalézt informace o leteckém provozu malého letiště náležejícímu ke Campu Peary. U 17 letů bylo možné na základě získaných informací vysledovat to, že se jedná o krycí názvy firem (leteckých společností) za účelem maskování příslušnosti letu k CIA, a dále bylo možné rekonstruovat některé minulé lety těchto letadel.

Pokud budeme prostřednictvím Googlu hledat informace o výcvikovém centru CIA Campu Peary, získáme o něm překvapivě mnoho informací. Dozvíme se například, že tento kamp je mezi příslušníky CIA znám pod přezdívkou Farma, že oficiálně patří americkému ministerstvu obrany, ale už mnoho let je to jedno z nejdůležitějších výcvikových středisek CIA nebo že se jedná o uzavřený tajný vojenský prostor o rozloze 38 km². Existence Farmy však není pro veřejnost žádná nová a ani neznámá věc. O Farmě psal již v roce 1972 list Virginia Gazette, tedy ještě v předinternetové éře bylo možné v otevřených zdrojích nalézt o Campu Peary informace. V různých databázích se všeobecně nacházejí dosti podrobné popisy tohoto tajného zařízení. Prostřednictvím internetu je možné dostat se k údajům o přesném umístění vojenského letiště (zeměpisná šířka, délka) náležejícímu k tomuto středisku (včetně jména a telefonního čísla vedoucího tohoto letiště) nebo se dokonce přímo podívat na satelitní obrázek tohoto výcvikového centra CIA (viz. následující obrázek).



CAMP PEARY – OBRÁZEK PŘEVZAT Z (<http://cryptome.org/peary-eyeball.htm>)

V souvislosti s odhalením identity příslušníků CIA měla být údajně zamlčena ta skutečnost, že celý experiment byl odsouhlasen samotnou CIA. Jestli CIA o celé záležitosti dopředu věděla nebo ne, není v tento okamžik důležité. List Chicago Tribune není bulvární plátek a lze předpokládat, že pokud takovýto článek zveřejnil, zřejmě k tomu musel mít nějaké důkazy a určité informace vedoucí ke konkrétním agentům CIA se mu přes internet opravdu vypátrat podařilo. Svědčil by o tom i ten fakt, že se nejedná o ojedinělý případ, kdy se přes internet podařilo dopátrat se k informacím majícím utajený charakter. Organizace na ochranu lidských práv Human Rights Watch taktéž - zčásti pomocí rešerše provedené na internetu - odkryla letadla, kterými měla CIA převážet údajné teroristy do tajných vězení.

Snadný přístup k informacím tajného charakteru vyvolává řadu otázek. Experti nevylučují, že by si podobné údaje – jména a adresy agentů CIA či tajných zařízení CIA mohli obstarat také jiné státy nebo teroristé. Nejmenovaný vládní úředník k případu udává – „Nevím, jestli by tyto informace mohla získat Al Kajda, ale Číňané toho zcela jistě schopni jsou“.

7.2. Katastr nemovitostí jako nástroj k získání informací



Případová úloha

O tom, že je v dnešní době utajení totožnosti agentů mnohem těžší (nebo naopak odhalení těchto agentů mnohem snazší), se mohla přesvědčit i Česká republika. I u nás jsme zaznamenali podobný případ jako byl případ v Americe. Prostřednictvím veřejně přístupného informačního zdroje byly získány takové informace, na základě nichž se dala následně vypátrat totožnost příslušníků jedné z českých zpravodajských služeb. Stejně jako ve výše uvedeném případě ze zahraničí byli těmi, kdo se o toto odhalení osobně přičinili, novináři. Jediným informačním zdrojem, který k získání těchto informací potřebovali, byl katastr nemovitostí. Díky informacím, které jsou v něm obsaženy, bylo možné po vyčtení potřebných dat vypátrat totožnost příslušníků Bezpečnostní informační služby. Žurnalisté Mladé Fronty Dnes zjistili, že je možné získat v katastru nemovitostí údaje o služebních bytech důstojníků Bezpečnostní informační služby.

Z katastru nemovitostí se dá za mírný poplatek zjistit, kolik nemovitostí a pozemků každý člověk či instituce v celé zemi vlastní - i s konkrétními informacemi, kde se objekt nebo parcela přesně nacházejí. Každý člověk může katastrální úřad požádat o informace, jaké nemovitosti jsou v celé zemi ve vlastnictví zpravodajské služby. Postup MFD byl následující – mezi třicítkou nemovitostí se nacházely i dva rozsáhlé bytové komplexy, v nichž Bezpečnostní informační služba údajně vlastní přes sto bytů (z toho se dá usuzovat, že se s největší pravděpodobností jedná o služební byty důstojníků). Detailní výpis nemovitosti obsahuje nejen číslo popisné vyhledaného objektu, ale i konkrétní číslo bytu, který v daném bytovém komplexu zpravodajská služba vlastní. Poté stačí vyhledat si na mapě přesnou adresu nemovitosti, na tuto adresu se dostavit a podívat se na jména nájemníků.

8. VÝZNAM INFORMACÍ PRO POLICII

Policie České republiky je jedním z ozbrojených bezpečnostních sborů působících na našem území. Policie plní úkoly ve věcech vnitřního pořádku a bezpečnosti a další úkoly v rozsahu a způsobem stanoveným právními předpisy (§ 1 zákona č. 283/1991 Sb., o Policii České republiky, dále jen zákon o policii).

Abychom mohli vést plnohodnotný život, potřebujeme mít přístup k informacím. Stejně tak se i policie neobejde při své činnosti bez dostatečného množství kvalitních informací. Bez nich by nemohla plnit své úkoly stanovené zákonem. Čeho se tyto informace týkají, lze odvodit právě z úkolů, které jsou blíže specifikovány v § 2 zákona o policii (viz. příloha č. 1). Policie České republiky má např. za úkol chránit bezpečnost osob a majetku, vést boj proti terorismu nebo odhalovat trestné činy a zjišťovat jejich pachatele. Dalším úkolem, který svědčí o důležitosti informací pro policii a který je zároveň vhodné v souvislosti s hlavním předmětem této diplomové práce – informačními zdroji - zmínit, je vedení evidencí a statistik potřebných pro plnění svých úkolů (§ 2 písm. l) zákona o policii).

8.1. Informace při odhalování, objasňování a vyšetřování trestných činů

Typickou činností policie je odhalování a vyšetřování trestných činů. Vyšetřování je v podstatě shromažďování informací o spáchaném trestném činu – osobě pachatele, okolnostech spáchání trestného činu apod. Jedním ze způsobů shromažďování těchto informací je jejich získávání z policejních a dalších databází využitelných policií. Zvláštní postavení mezi shromážděnými informacemi zaujímají ty informace, které mají sílu důkazu. Jedná se o informace z výpovědí svědků, z odborných posudků soudních znalců, informace získané ohledáním místa činu atd.

Policie jen nečinně nevyčkává, až se dozví o spáchání trestného činu na základě trestního oznámení. Policie je ze zákona povinná i aktivně jednat v této záležitosti, to znamená odhalovat trestné činy, aniž by ji o jejich spáchání někdo informoval. Toto aktivní jednání představuje vyhledávání informací, jejich získávání, shromažďování a vyhodnocování. Na základě vyhodnocení informací může policie dojít k závěru, že byl trestný čin spáchán, případně že se jeho provedení teprve

chystá, a může podniknout příslušné právní úkony – zajistí důkazy, provede bezpečnostní opatření vedoucí k překažení spáchání trestného činu a dopadení pachatele na místě činu atd.

Informace vzniklé při páchání trestného činu - získané na místě činu

Jak už bylo zmíněno, aby byla policie úspěšná při objasňování a vyšetřování trestných činů, potřebuje mít k dispozici dostatek kvalitních informací. Důležitým zdrojem informací pro vyšetřování je místo činu. Informace zde policie získává ve formě kriminalistických stop. I ten nejopatrnější pachatel nedokáže zabránit tomu, aby na místě činu nezanechal informace o své přítomnosti alespoň ve formě mikrostop. Skrze vlasy, prach, úlomky laku nebo vlákna, které kriminalisté naleznou na místě činu se lze postupně dopátrat k dalším informacím - důkazům, kterými je možné později usvědčit pachatele. V případě informací získaných na místě činu se jedná o zcela nové informace, které před spácháním trestného činu neexistovaly, neboť vznikly právě až při jeho samotném páchání. [26, 27]

Informace vzniklé před spácháním trestného činu

Při objasňování trestných činů se využívají nejen informace nové - informace z místa činu, ale i informace starší, které existovaly již v době před spácháním vyšetřovaného trestného činu. Typickým zdrojem těchto informací jsou různé policejní databáze. Pro aktuálně vyšetřovaný případ je kupříkladu třeba zjistit z databáze střelných zbraní držitele zbraně nalezené na místě činu. Ač tyto informace vznikly v minulosti, tedy v době před spácháním aktuálního skutku, přesto mohou být velmi nápomocny při vyšetřování. [26, 27]

8.2. Informace jako prostředek kriminalistické prevence a policejní statistiky

Informace hrají důležitou roli také v kriminalistické prevenci. Policie může vyhodnocováním informací zjistit problematická místa, kde jsou ve větší míře páchány trestné činy, například kde dochází k častým loupežím nebo ke krádežím vloupáním. Následně zaměří na inkriminovaná místa více svou pozornost – danou oblast častěji kontrolují policejní hlídky nebo je na rizikové místo nainstalována

zabezpečovací technika (např. kamerové systémy), což odradí potencionální pachatele trestných činů. [26, 27]

K účelům kriminalistické prevence jsou vhodné také informace statistického charakteru. Lze z nich usuzovat například na celkovou strukturu kriminality nebo vyvozovat nové trendy v páchání trestné činnosti. [26, 27]

8.3. Pojem informace v trestním zákoně

Informace hrají svou roli při páchání kteréhokoliv trestného činu. V některých skutkových podstatách dokonce o některých specifických informacích zákon přímo hovoří. Patří mezi ně například osobní údaje.

8.3.1. Trestněprávní ochrana osobních údajů

Zákonná definice osobních údajů

„Pro účely zákona se rozumí osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“ (§ 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů).

Pod pojem osobní údaj tedy náleží vše, co nás umožňuje identifikovat. Jméno, adresa, datum narození, pohlaví, informace o našem ekonomickém zázemí... Zvláštní skupinu osobních údajů tvoří *citlivé údaje*. Rozumí se jimi údaje *„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 jakýkoliv biometrický nebo genetický údaj subjektu údajů“* (§ 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů).

Největším opodstatněným shromažďovatelem osobních dat a informací o jednotlivých osobách je samotný stát. Úřady po lidech vyžadují nejrůznější informace, rodným číslem počínaje a výpisem z trestního rejstříku nebo majetkovými a rodinnými poměry konče. Že se v případě osobních údajů nejedná o

žádné *obyčejné informace* dokládá ten fakt, že jejich ochranu upravuje celá řada zákonů, vyhlášek a směrnic. Stát je povinen chránit osobní data občanů před neoprávněnými zásahy. Tyto informace jsou dokonce takového významu, že jsou chráněny i samotným trestním zákonem. V trestním zákoně (zákon č. 140/1961 Sb.) existuje přímo skutková podstata trestného činu „Neoprávněné nakládání s osobními údaji“. Jedná se o § 178, ve kterém stojí:

(1) *Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem.*

(2) *Stejně bude potrestán, kdo osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, byť i z nedbalosti, sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti.*

(3) *Odnětím svobody na jeden rok až pět let nebo zákazem činnosti nebo peněžitým trestem bude pachatel potrestán,*

a) *způsobí-li činem uvedeným v odstavci 1 nebo 2 vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se údaj týká,*

b) *spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem, nebo*

c) *spáchá-li čin uvedený v odstavci 1 nebo 2 porušením povinností vyplývajících z jeho povolání, zaměstnání nebo funkce.*

8.3.2. Další kategorie informací výslovně zmiňované trestním zákonem

Jako další kategorie informací zmiňované trestním zákonem lze jmenovat utajované informace, nepravdivé informace nebo informace v obchodním styku (např. sdělení důležité nepravdivé informace s následkem uvedeným ve skutkové podstatě trestného činu podle § 95 *Teroristický útok*, vyzvídání utajované informace - § 105 *Vyzvědačství*, *Ohrožení utajované informace* - § 106 a 107, neoprávněné užívání informací, které nejsou dosud veřejně přístupné, a jejichž zveřejnění podstatně ovlivňuje rozhodování v obchodním styku, s úmyslem opatřit sobě nebo jinému výhodu nebo prospěch - § 128, *Zneužívání informací v obchodním styku*, sdělení nepravdivé informace, která může ohrozit bezpečnost nebo provoz vzdušného dopravního prostředku za letu nebo civilního plavidla za plavby - 180b *Ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla*, nepravdivé informace, které jsou obsahem poplašné zprávy - § 199 *Šíření poplašné zprávy*, neoprávněné užití informací, jejich zničení, poškození, změna nebo učinění těchto

informací neupotřebitelnými tak, jak je specifikováno v § 257a *Poškození a zneužití záznamu na nosiči informací*).

8.4. Role rodného čísla při individuální identifikaci osob, příklady jeho využití

Jednoduchým způsobem individuální identifikace osoby je znalost jejího rodného čísla. Rozhodně však nelze trvat na tom, že bez rodného čísla nejde osobu identifikovat. Ani samotný občanský zákoník s rodným číslem jako jednoznačným identifikátorem nepočítá. Pro určení fyzické osoby ve smluvním vztahu jsou za takové údaje považovány jméno a příjmení, datum narození a bydliště. [28]

Nikoho nepřekvapí sdělení, že k mnoha osobním údajům, např. k rodnému číslu, případně adrese člověka se dostanou bezpečnostní složky státu přes policejní informační systémy. K některým rodným číslům a adresám mnoha osob se však lze dopátrat i mnohem snadnější cestou. Kdokoli ovládá alespoň trochu práci s internetem, stačí, když si otevře webovou stránku Ministerstva spravedlnosti ČR (<http://www.justice.cz>). Skrze Obchodní rejstřík se může dozvědět rodné číslo a také adresu vyhledávané osoby (jsou-li v databázi obsaženy).

Například když známe pouze její jméno, dostaneme se skrze něj i k rodnému číslu (pokud je v Obchodním rejstříku uvedeno. Některé osoby jsou zde uvedeny včetně rodného čísla, jiné jsou bez tohoto údaje). Známe-li název firmy, po zobrazení výpisu (úplného nebo aktuálního) zjistíme i členy představenstva, dozorčí rady, jednatele apod. včetně jejich rodných čísel, pokud jsou k dispozici. Podle jmen osob si můžeme snadno zjistit i jména obchodních společností, které jsou spojeny s touto osobou.

Existují dokonce speciální programy, které dokáží, pokud jsou nasyceny příslušnými daty, vytvořit přehledné pavoukové grafy, které jsou schopné odpovědět na otázku, s kým dotyčný člověk udržuje kontakty a jaké jsou jeho obchodní aktivity, případně které firmy jsou spolu majetkově provázány. Samozřejmě platí, že pokud takový program není řádně aktualizován a postupně doplňován novými daty, jeho využitelnost rapidně klesá. Je také nutné konstatování, že disponovat stoprocentně nasycenou databází je prakticky nemožné. [29]

Rodné číslo spolu s údajem o místě narození považují soukromí detektivové za vůbec nejcennější údaj. Během chvilky podle nich zjistí spoustu podrobností ze života toho, kterého dostali za úkol sledovat (navazující informace).

Na internetu se dá najít mnoho podstatných údajů, které využije nejen běžný uživatel, ale i soukromý detektiv, policista nebo příslušník zpravodajské služby. Stačí vědět, kde je hledat a jak se skrze tyto údaje dostat k dalším informacím, které potřebujeme k dosažení stanoveného cíle.

9. INFORMAČNÍ ZDROJE V POLICEJNÍ PRAXI

Policejní složky ve své praxi nevyužívají pouze vlastní informační systémy. Široké uplatnění zde naleznou i mnohé další informační systémy, ať už z oblasti státní a veřejné správy nebo různé komerční databáze ze soukromého sektoru, u nichž by se na první pohled mohlo zdát, že s policejní činností nemají nic společného. Ovšem i tyto informační systémy mohou obsahovat důležité poznatky vhodné pro bezpečnostní praxi.

Z tohoto pohledu lze informační systémy využitelné policií rozdělit do těchto tří základních skupin:

- civilně-správní informační systémy
- speciální policejní informační systémy
- obecné informační systémy (informační systémy z oblasti otevřených zdrojů) [27]

Tyto tři základní skupiny informačních systémů lze dále členit do podskupin.

9.1. Civilně-správní informační systémy

Civilně-správní evidence představují základní informační zdroje státní správy. Bez nich by výkon státní správy nebyl možný. Tvoří podklad pro další informační systémy státní správy, ostatní databáze od nich některé z údajů přebírají. Civilně-správní informační systémy slouží zejména k evidenčním účelům a nejsou obecně přístupné veřejnosti. Obsahují identifikační údaje o osobách, motorových vozidlech, občanských průkazech, cestovních pasech, řidičských oprávněních apod. Jedná se zejména o databáze jednotlivých ministerstev. Primárním ministerstvem je zde Ministerstvo vnitra (vede i dva největší informační systémy státní správy – *Centrální registr obyvatel* a *Centrální registr vozidel*). V souvislosti se vstupem České republiky do Evropské Unie přešly některé databáze z Ministerstva vnitra na ostatní – civilní ministerstva. Jako příklad je možné uvést Ministerstvo dopravy, které od 1. 7. 2006 vede *Centrální registr řidičů*. Do té doby jej spravovalo Ministerstvo

vnitru. Registry nejsou veřejnosti obecně přístupné. Identifikační údaje, které obsahují, mají často charakter osobních údajů.

9.2. Policejní informační systémy

9.2.1. Historie a současnost policejních informačních systémů

Shromažďování a ukládání různých informací takovým způsobem, aby bylo možné jejich pozdější vyhledání, není záležitostí posledních desetiletí. Policie shromažďuje informace v různých evidencích po celou dobu své existence. S rozvojem výpočetní techniky se však zásadním způsobem změnila forma policejních evidencí. Dnešní moderní policejní informační systémy mají své předchůdce v podobě různorodých sbírek, evidencí a kartoték, vedených manuálně. Ty s nástupem výpočetní techniky postupně zanikly a byly nahrazeny moderními počítačově vedenými evidencemi (Policie České republiky využívá v současnosti jedinou manuálně vedenou evidenci – *Základní evidenci pachatelů*. Od roku 1993 však už není tato evidence aktualizována, má pouze archivní charakter). Výpočetní technika vytěžování policejních informačních zdrojů velmi ovlivnila.

9.2.2. Předpočítačová éra policejních databází

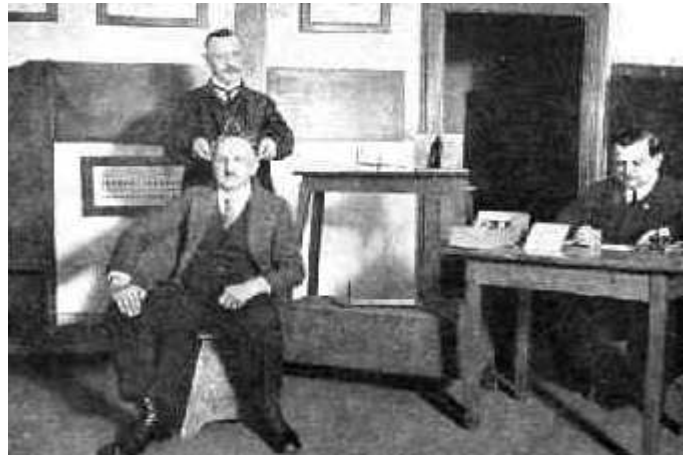
Pokud chtěl kriminalista v předpočítačové éře získat z nějaké evidence informace, znamenalo to manuálně prohlížet velké množství kartiček v kartotéce – obsahující např. informace o jednotlivých pachatelích. Starší druhy policejních evidencí, manuálně vedené, byly většinou nahrazeny svými moderními počítačovými nástupci.

Příkladem z minulosti může být historická metoda z roku 1879, která se později zasloužila o rozvoj moderní portrétní identifikace osob (*obor kriminalistické techniky, který se zabývá zkoumáním a popisováním vnějších znaků člověka s cílem jejich využití při pátrání po osobách a při zjišťování totožností neznámých osob a mrtvol*. [26] Tato metoda je známá pod označením *bertillonáž* (pojmenovaná po francouzském policejní úředníku Alphonse Bertillonovi). Louis Alphonse Bertillon jako první na světě vypracoval použitelnou metodu individuální identifikace pachatele postavenou na vědeckém základě. Jednalo se o systém identifikace osob založeném na antropologické teorii o tom, že po ukončení fyzického vývoje člověka

se jeho určité tělesné rozměry již nemění. Metoda byla postavena na měření jedenácti antropologicky určujících znaků a rozměrů lidského těla. Bertillon byl přesvědčen o tom, že tyto rozměry (například výška a šířka obličeje, obvod hlavy, délka paží a prstů nohou nebo rozměr pravého ucha) mohou být sice u různých lidí stejné, nikdy však čtyři nebo pět rozměrů zároveň. Svou metodu nazval *antropometrií*, novináři ji později přejmenovali na *bertillonáž*. V praxi mohla tato metoda např. přispět k odhalení recidivisty, který se vydával za někoho jiného. Poté, co byl zatčený změřen, byly zjištěné údaje porovnány s údaji v evidenci, jež obsahovala údaje o rozměrech v minulosti měřených osob. *Bertillonáž* byla na přelomu devatenáctého a dvacátého století překonána *daktyloskopií*. [26, 27]



LOUIS ALPHONSE BERTILLON
(1853 – 1914)



ANTROPOMETRICKÉ MĚŘENÍ HLAVY DELIKVENTA

9.2.3. Moderní počítačové informační systémy

Dynamický rozvoj výpočetní techniky měl zásadní vliv na rozvoj policejních informačních systémů. Rozvoj v technice umožnil uživatelům – policistům čerpat potřebné informace z elektronických databází rychleji a efektivněji. Pouhé shromáždění velkého množství informací by k úspěšné práci policie příliš nepřispělo. Pokud by se vůbec požadovanou informací podařilo nalézt, trvalo by to příliš dlouho. Při vyšetřování spáchaného trestného činu je často potřeba reagovat okamžitě. Proto je nutné mít k dispozici informace v co nejkratším možném čase. Pouze v databázi s tříděnými informacemi lze informace efektivně vyhledávat, bez zbytečného časového prodloužení způsobeného neuspořádaností informací.

Uložené informace musí být v pořádku z hlediska jejich aktuálnosti. Aktuálnost spolu s úplností a vhodnou strukturalizací informací v rámci informačního systému jsou základními předpoklady jeho funkčnosti. Pokud tedy některé z uložených informací v databázi pozbyly platnosti, je třeba je z databáze vymazat, pokud došlo k nějaké změně, musí se údaj v informačním systému opravit. Při vzniku nových údajů je třeba je bez zbytečného odkladu do databáze vložit. V některých případech je nutné zařadit údaje do databáze v podstatě okamžitě, bez jakéhokoliv prodlení. Aby se zabránilo vývozu odcizeného uměleckého díla – např. obrazu - přes hranice našeho státu, musí o tom být oprávněné orgány (pohraniční policie, celníci) včas vyrozuměny, neboť jen tak mohou učinit příslušná opatření. Informace o odcizeném obrazu musí být zaevidovány bezodkladně, neboť čas hraje v podobných případech hlavní roli.

V policejních databázích se nacházejí nejrozmanitější informace (např. informace o neobjasněných trestných činech a způsobech jejich spáchání (důležitý údaj pro tzv. *modus operandi systém* pomáhající ve vytipování neznámého pachatele), nejružnější bližší informace o konkrétních pachatelích, kteří již byli dopadeni – např. o jejich fyzických, psychických, odborných a dalších vlastnostech, dále informace o místech a době páchaní zločinů, informace o odcizených věcech, o pohřešovaných osobách a mnoho dalších). [26]

9.3. Kriminologické sbírky

Kriminologické sbírky představují zvláštní policejní evidence, v nichž jsou uloženy informace specifického charakteru. Některé z policií shromážděných informací nelze fyzicky vložit do počítačových informačních systémů, neboť se jedná o hmotné předměty (materiální kriminologické stopy). V informačních systémech lze zanechat pouze záznam o tom, kde se daná informace nachází. Tento druh informací je ukládán do *kriminologických sbírek*. Lze si je představit jako speciální informační fondy obsahující informace v materiální podobě. Tyto informace - kriminologické stopy mají tu vlastnost, že se dají zachovat pouze ve fyzické podobě (in natura), často na původním nosiči informace. Nelze je totiž buď vůbec nebo v dostatečné kvalitě kopírovat. Tato vlastnost způsobuje, že mohou být vedeny pouze na jedné - kupříkladu regionální úrovni. Nemohou být tedy uloženy na několika místech

zároveň. Obsahem těchto kriminalistických sbírek jsou především některé druhy stop z míst neobjasněných trestných činů. Sbírkové jsou děleny podle druhu stop, které obsahují. Policie využívá např. daktyloskopické sbírky z míst neobjasněných trestných činů, daktyloskopické sbírky srovnávacích otisků, sbírky nábojnic a střel, sbírky pachových stop, sbírky trasologických stop a další. Podobný charakter mají i různé expertizní sbírky, obsahující srovnávací materiál pro expertizní, vědeckovýzkumné, výměnné účely a jiné účely. [26, 27]

Systém TRASIS

V kriminalistické trasologii Policie České republiky využívá identifikační systém TRASIS. Struktura systému se skládá z následujících hlavních částí:

- Obrazové a textové databáze otisků podešví (tzv. KATALOG)
- Obrazové a textové databáze trasologických stop podešví (tzv. SBÍRKA STOP)

V databázi KATALOG jsou ukládány obrazy úplných otisků podešví známé obuvi. Otisky jsou předem externě zpracovány za pomoci různých vstupních zařízení, tj. scanneru, kamery apod., a po následné úpravě grafickým programem připraveny k vložení do systému TRASIS. Vedení databáze má za cíl poskytnout maximálně dostupné informace o původu otisku. Proto jsou součástí jednotlivého záznamu databáze textové položky, informující o původu podešve, která otisk vytvořila. V databázi SBÍRKA STOP jsou ukládány úplné i neúplné upotřebitelné trasologické stopy podešví zajištěné na místě činu. Vedení databáze má za cíl aktuální celostátní přehled o trasologických stopách zajištěných na místech trestné činnosti, a proto jsou součástí záznamu i textové informace související se zajištěnou stopou.

Projektový záměr systému TRASIS předpokládá v rámci realizace dalších vývojových etap rozšíření systému o databázové moduly jako např. sbírka stop uší, referenční sbírky vzorů textilií a kůže. Systém TRASIS je koncipován jako uzavřený databázový systém určený výhradně pro expertizní činnost v oblasti trasologického zkoumání, a to pouze vyškoleným pracovníkům, kteří mají k práci se systémem potřebnou kvalifikaci a oprávnění [32] (o těchto pracovnících lze říci, že jsou informačními specialisty).

9.4. Informační zdroje obsahující citlivé údaje

9.4.1. Biologické, biometrické a genetické informace

Přístup k civilně-správním a policejním databázím je povolen pouze oprávněným osobám. Tyto evidence totiž obsahují často osobní údaje, se kterými se nemůže kdokoli bez omezení seznamovat. V souvislosti s ochranou osobních údajů se v posledních letech často mluví o zvláštním druhu osobních údajů – o citlivých údajích a jejich zvláštní podskupině – o biologických, biometrických a genetických informacích. Citlivý údaj obecně je v zákoně č. 101/2000 Sb., o ochraně osobních údajů definován jako „*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 jakýkoliv biometrický nebo genetický údaj subjektu údajů*“.

O genetické, biologické a biometrické informace se budeme zajímat v souvislosti s evidencí průkazů totožnosti, a také ve spojitosti s policejními informačními systémy, zaměřenými na shromažďování biologických a genetických informací (typickými představiteli těchto evidencí jsou např. evidence daktyloskopické a databáze DNA).

Osobní doklady v poslední době dosti změnilu svou podobu. V dnešní době si je již nelze představovat jen jako klasické průkazy ve formě kartičky zapuštěné (zalité) v průhledné folii s vypsányi identifikačními údaji a přilepenou fotografií. Začínají se v nich objevovat další speciální identifikační znaky jako např. otisky prstů. V této souvislosti se o nich dá hovořit jako o biometrických občanských průkazech.

9.4.2. Možnosti oboru biometrie v souvislosti s identifikací osob

Technický rozvoj otevřel nové možnosti pro obor zvaný *biometrie*. Tato vědní disciplína používá ke zjištění totožnosti nebo k ověření zadané identity osob jejich charakteristické znaky, a to takové, na základě nichž lze provést individuální identifikaci osoby (ta je umožněna tím, že tyto znaky jsou zcela jedinečné pro každou osobu). Moderní přístroje dokážou porovnat unikátní rysy každého člověka jakými jsou oční sítnice, geometrie ruky, hlas, tvar obličeje, způsob chování, styl

psaní na klávesnici či podpis. Například po sejmutí otisku prstu, dlaně, tvaru tváře, specifického charakteru duhovky oka nebo prostého podpisu proběhne srovnání získaného materiálu s údaji v databázi, a při shodě je vydán např. povel k vpuštění osoby do objektu nebo odblokování příslušného zařízení. [33]

Biometrické informace jsou velmi detailním popisem těla každého jedince. Umožňují provést individuální identifikaci osoby. Uskutečnit takovou identifikaci je možné díky čtyřem základním charakteristikám biometrických údajů. Za prvé jsou tyto údaje všeobecné v tom smyslu, že kterýkoliv člověk na světě je nositelem těchto biometrických údajů. Druhou předností biometrických je jejich unikátnost. To znamená, že je velmi malá pravděpodobnost, že by dva jedinci byli nositeli totožné biometrické informace (v případě otisků prstů je touto unikátností individuálnost papilárních linií. Na světě *neexistují dvě osoby, které by měly naprosto stejné obrazce papilárních linií*. Tento závěr je podložen matematicko statistickými výpočty, jimiž bylo prokázáno, že variabilnost obrazců papilárních linií je tak vysoká, že není možné, aby na Zemi existovali dva lidé s naprosto stejnými obrazci papilárních linií, a to ani za celou dobu existence člověka na Zemi. [26]

Třetí charakteristikou biometrické informace předurčující ji ke spolehlivé identifikaci osoby je to, že ji máme neustále při sobě. Občanský průkaz můžeme zapomenout doma nebo jej můžeme ztratit, případně je nám odcizen. Naproti tomu identifikace prostřednictvím otisku prstu je možná prakticky kdykoliv, neboť prst si nosíme stále s sebou. Čtvrtou výhodou biometrických informací je to, že zůstávají po celý život člověka stejné, nemění svou podobu. [30] Jedná se o velkou výhodu oproti klasickým osobním údajům jako je jméno nebo adresa trvalého bydliště, neboť tyto osobní údaje lze jednoduše měnit. Necháme se přejmenovat, přestěhujeme se do jiného města apod.

9.4.3. Projekt US-Visit

Projekt *US-Visit (United States Visitor and Immigrant Status Indicator Technology)* vznikl ve spojitosti s teroristickým útokem v New Yorku v září 2001 (zaveden byl v roce 2004). V rámci tohoto projektu jsou pasažérům s vízovou povinností, kteří přijíždějí do USA, snímány otisky prstů a pořizovány jejich digitální fotografie. [31] Toto rozhodnutí vyvolalo velkou vlnu zájmu. Reakce lidí na toto opatření se různily, někteří toto rozhodnutí schvalovali, jiní byli zásadně

proti nebo toto opatření vnímali přinejmenším s jistou obezřetností. Diskutovalo se o tom, zda uchovávání biometrických informací je přiměřené a zda skutečně v tomto projektu USA není ještě skryto něco dalšího, co lidem nebylo řečeno. [34]

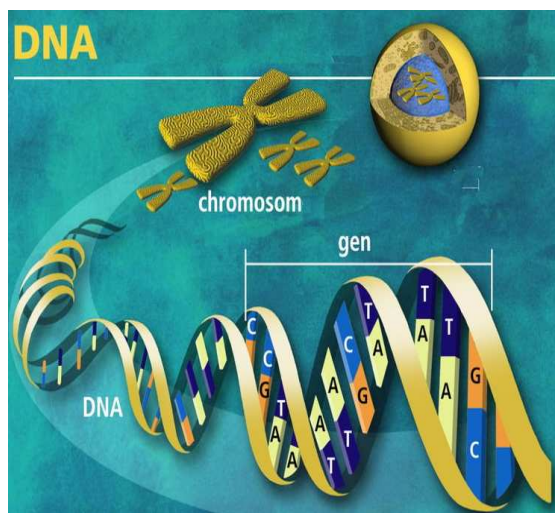
Biometrické informace mohou totiž obsahovat údaje, které by mohly být později zneužity k neoprávněným účelům. Tyto zvláštní údaje zatím sice nedokážeme detekovat, to však neznamená, že to nedokáží třeba příští generace (Spojené státy chtěly původně uchovávat informace o pasažérech padesát let). V roce 2000 proběhla v odborném tisku informace, že z otisku prstů lze vyčíst sexuální orientaci, což byl zcela nový vědecký poznatek. Nikdo nemůže říci, co věda objeví za rok, za dva, za deset let. Pokud někdo bude mít podobnou databázi s biometrickými informacemi, může ji v budoucnu vyhodnocovat jinými metodami, a to například vůči nějaké komunitě či společnosti negativním způsobem. [34]

Tento krok USA lze kritizovat a polemizovat s ním, ale měli bychom se jej snažit i pochopit. Samozřejmě by mohly být otisky prstů (případně jiné biometrické informace) zneužity k neoprávněným účelům (k zneužívání v této době obvyklých osobních údajů dochází ale také). Na problematiku zavádění snímání otisků prstů pro návštěvníky s vízovou povinností je třeba se dívat i z druhé strany, tedy hledat a nalézat přínos podobných opatření (nebo na ně nahlížet alespoň jako na nutnost). Na nárůst teroristických útoků ve světě a na stále častější a důmyslnější praktiky falšování dokladů je třeba reagovat. [33] Pokud již současné bezpečnostní prostředky nejsou schopny dostatečně občany před teroristickými útoky a před trestnou činností ochránit, je na místě tuto situaci řešit za použití zcela nových prostředků. Zavádění a využívání bezpečnostních systémů obsahujících biometrické informace obecně (tedy nejenom otisky prstů) by mohlo přispět ke zvýšení bezpečnosti občanů.

9.4.4. Archivy DNA

Jednou z dalších možností individuální identifikace osob v moderní kriminalistice je identifikace osob pomocí DNA (Deoxyribonukleová kyselina – viz. obrázek).

Technika vytvoření jedinečného genetického profilu jedince se nazývá *DNA fingerprinting*, *genetická daktyloskopie* či *DNA otisky*. [převzato včetně následujícího obrázku z Wikipedie]



Při soudním řízení jsou od roku 1984 využívány otisky DNA (tzv. DNA fingerprints, viz 100+1 ZZ, č. 20/2000). Jakkoli je DNA spolehlivým nástrojem pro dopadení pachatele, shromažďování takto získaných poznatků do databází je značně problematické, zvláště pokud jde o jednotlivce, kteří prokazatelně nikdy nespáchali trestný čin. Projekt takovéto databáze vznikl ve Velké

Británii. Genetické informace získané od podezřelých osob nebo od lidí, kteří byli zproštěni viny, by se místo likvidace začaly uchovávat. Základní myšlenkou bylo urychlit vyšetřování trestných činů tím, že budou předem vyloučeny osoby s odlišným vzorcem DNA. Brzy po zveřejnění této zprávy se objevily odmítavé reakce veřejnosti. Nepomohl ani fakt, že uložení těchto informací by bylo podmíněno souhlasem zúčastněných osob. Mluví organizace na ochranu lidských práv Liberty (Svoboda) Deborah Clarková například tvrdí, že vybudování databáze se vzorky DNA samo o sobě nic nevyřeší. Obává se však, že by měl stát k dispozici stále více osobních údajů. [36]

Výsledky, které dodávají forenzní vědy (tedy i genetika), samozřejmě nepostačují k rozhodnutí o vině. Místo odpovědi ano - ne se používá termín *pravděpodobnost*, která se stanoví podle toho, kolik sekvencí se u porovnávaných vzorků shoduje. K určení viny jsou vždy zapotřebí další důkazy, zejména tehdy, když nejsou dostupné genetické informace dostatečné. V Británii se v současnosti vedou diskuse o problematice ochrany soukromí, kterých se účastní vedle policie i zástupci vědců a ochránců lidských práv. Policie argumentuje tím, že nevinní lidé nemusejí mít z archivace osobních údajů obavy. Zda je její tvrzení pravdivé, ukáže teprve čas. [35]

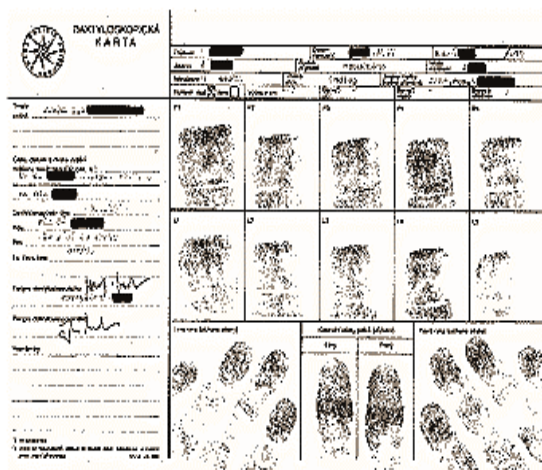
9.4.5. Daktyloskopické systémy

Základní objev, tedy možnost určit identitu podle otisků prstů, byl znám v Číně a Japonsku už před třemi tisíci lety. Právě tímto způsobem se tam pečtily smlouvy. V moderní době zkoumal skotský lékař Henry Faulds jako jeden z prvních otisky prstů na starých keramických nádobách a roku 1880 publikoval své závěry ve

vědeckém časopise Nature. Inspiroval tím britského přírodovědce Francise Galtona, jehož kniha *Fingerprints* (Otisky prstů), kde shrnul výsledky svého studia papilárních linií, vyšla v roce 1892. Prokázal, že u každého člověka vypadají jinak (liší se i u dvojčat) a nejsou dědičné. Na základě Galtonova objevu utřídil sir Edward Henry otisky do *systemu*, který byl v roce 1901 oficiálně přijat Scotland Yardem a stal se východiskem pro moderní daktyloskopii. V Argentině vypracoval podobný *system* policejní úředník Juan Vucetich z Buenos Aires. Je také autorem původního *systemu klasifikace otisků prstů* (vyšel v roce 1904 pod názvem *Dactiloscopía comparada*, Srovnávací daktyloskopie, který se dodnes používá ve španělsky mluvících zemích). [35]

Automatizovaný identifikační systém AFIS 2000

Porovnávání otisků zajištěných např. na místě činu s otisky na daktyloskopických kartách se v minulosti provádělo ručně. Jednalo se o časově náročnou činnost. Za účelem zvýšení efektivity a rychlosti porovnávání otisků byly vypracovány různé klasifikační systémy. V moderní kriminalistice jsou celosvětově zaváděny počítačové automatizované identifikační systémy. AFIS 2000 používaný Policií České republiky je jedním z nich. Jedná se o jeden z nejvýkonnějších systémů využívaných při zpracování otisků a stop vedených v daktyloskopických sbírkách. [36]



DAKTYLOSKOPICKÁ KARTA



VYUŽÍVÁNÍ VÝPOČETNÍ TECHNIKY
V DAKTYLOSKOPII

9.5. Právní aspekty vedení policejních informačních systémů

Vedení policejních evidencí a statistik je jedním ze samostatných úkolů policie (§ 2 odst. 1 písm. l) zákona o policii). Jednotlivé systémy vede policie buď na základě výslovného zákonného zmocnění (např. vedení evidence dopravních nehod dle § 123 zákona o provozu na pozemních komunikacích) nebo je jejich vedení opřeno o obecné zmocnění uvedené v zákoně o policii (§ 2 odst. 1 písm. l). Konkrétní právní úprava týkající se zpracování informací policií je uvedena v hlavě čtvrté zákona o policii (viz. příloha č. 2). Zpracování osobních údajů je pak dále specifikováno v hlavě páté zákona o policii (viz. příloha č. 2).

Informační systémy Policie České republiky spravuje Policejní prezidium České republiky.

Osobní údaje v policejních informačních systémech

Informační systémy provozované policií obsahují často informace charakteru osobních údajů. Osobní údaje podléhají obecně režimu zákona o ochraně osobních údajů. Co se týká zpracování osobních údajů, platí pro policii z tohoto zákona řada výjimek. [31] Obecné zpracování osobních údajů je upraveno v hlavě druhé zákona č. 101/2000 Sb., o ochraně osobních údajů. Na zpracování osobních údajů policií se však některá ustanovení této hlavy nevztahují. V těchto případech se policie při zpracování osobních údajů řídí *Zvláštními ustanoveními o zpracování osobních údajů policií* (hlava pátá zákona o policii, viz. příloha č. 2).

V souvislosti s trestním řízením je například policie oprávněna, na rozdíl od obecné právní úpravy, sdružovat osobní údaje, které byly získány k rozdílným účelům (dle zákona o ochraně osobních údajů lze osobní údaje shromažďovat pouze ke stanovenému účelu). Policie také může zpracovávat osobní údaje nepravdivé, nepřesné a neověřené (dle zákona o ochraně osobních údajů lze zpracovávat pouze pravdivé a přesné údaje). [31]

Zpracování citlivých údajů Policií České republiky

Výjimky platí pro policii i co se týká zpracování citlivých údajů. V zákoně o ochraně osobních údajů jsou uvedeny obecné důvody, za nichž lze citlivé údaje

zpracovávat. Policie může citlivé údaje zpracovávat také při plnění úkolů v souvislosti s trestním řízením a je-li to nezbytné k nalezení osob, po kterých je vyhlášeno pátrání. Policie může tyto citlivé údaje shromažďovat i bez souhlasu osoby, k níž se tyto údaje vztahují, avšak za podmínky, že musí dbát jejího práva na ochranu soukromého a osobního života.

9.6. Přístup do policejních informačních systémů

Z bezpečnostních důvodů platí při přihlašování do informačních systémů určité zásady, se kterými by měl být každý uživatel – policista před prvním přihlášením seznámen. Přístup do většiny informačních systémů včetně těch policejních probíhá skrze konto uživatele (uživatelský účet). Při zřízení konta uživatele (na základě podané žádosti, která je posléze schválena, jestliže je oprávněná) je pro tento účet stanoven rozsah oprávnění nového uživatele pro přístup do jednotlivých evidencí. Přístupové konto každého uživatele musí být nezaměnitelné s účtem jiného uživatele (byla by znemožněna následná identifikace tazatele).

Každý přístupový účet musí být chráněn heslem, které by měl znát jen oprávněný uživatel. Heslo je vhodné z bezpečnostních důvodů v pravidelných intervalech obměňovat.

Pro vyhledávání v policejních informačních systémech dále platí, že každý dotaz musí být v případě potřeby řádně zdůvodnitelný, jinými slovy, uživatel – policista smí provádět dotazy jen v souvislosti s plněním služebních úkolů. [31]

9.7. Informační činnosti v rámci informačních systémů policie

Policie má pro účely plnění svých úkolů k dispozici řadu speciálních informačních systémů. Tyto informační systémy jsou zcela specifické z hlediska svého obsahu. Vznik, získávání a využívání informací lze charakterizovat následujícím způsobem:

- **Vytváření informací** (jedná se o samotný vznik informací jako např. zanechání otisků prstů pachatelem na místě činu, tedy informace ve formě kriminalistické stopy, svědek si zapamatuje popis pachatele – paměťová stopa apod.)

- **Získávání informací** (na základě ohledání místa činu jsou sejmuty otisky prstů, zajištěny další kriminalistické stopy, svědek učiní výpověď na policii apod.)
- **Zpracování informací** (získané informace je nutné zařadit a uložit do příslušného informačního systému. U některých informací je nutné před samotným vložením do systému nejprve tyto informace upravit do vhodné podoby, např. otisky prstů získané na místě činu jsou převedeny do digitální podoby apod. Důležitým aspektem je i udržování aktuálního stavu uložených informací. Kvalita zpracování informací výraznou měrou ovlivňuje následné získávání uložených informací)
- **Zpřístupnění informací** (možnost získání uložených informací v případě potřeby. Snadné vyhledání informací, rychlost získání požadovaných informací závisí nejenom na kvalitně provedeném zpracování informací, ale samozřejmě také na dovednostech uživatele informačního systému) [27]

9.8. Stručná charakteristika vybraných policejních informačních systémů

V následujících odstavcích jsou stručně popsány nejrozšířenější celostátní policejní informační systémy. Nejedná se o celkový výčet policejních informačních systémů.

PATRMV (Pátrání po motorových vozidlech)

Jedná se o centrální celostátní systém pro pátrání po odcizených vozidlech. Za vozidla se pro potřeby tohoto systému pokládají osobní vozidla, speciální stroje, nákladní vozidla, jednostopá motorová vozidla, zemědělské stroje a traktory, tabulky státních poznávacích značek, přívěsy, návěsy, autobusy a obytné přívěsy.

Obsahem databáze jsou identifikační údaje vozidla, popis markantů, datum, čas a místo odcizení. Vedeny jsou taktéž údaje k osobě poškozeného a k útvaru, který pátrání vyhlásil. V případě nalezení vozidla údaje k útvaru, který vozidlo našel, a to včetně místa nalezení.

Systém dále umožňuje rychle získat informaci o tom, zda je po určitém vozidle vyhlášeno pátrání, případně, zda po tomto vozidle bylo již někdy vyhlášeno

pátrání v minulosti a zda bylo zrušeno. Existuje i zkrácená verze tohoto systému, která obsahuje pouze vybrané údaje z celkové databáze.

Údaje z tohoto informačního systému jsou zdrojem dat, která jsou zveřejňována denně na internetovém serveru Ministerstva vnitra.

PATROS (Pátrání po osobách)

Jedná se o informační systém pro pátrání po pohřešovaných a hledaných osobách, po totožnosti osob a totožnosti nalezených mrtvol a kosterních nálezů. Obsahem databáze jsou identifikační údaje osoby, údaje o jejím bydlišti, rodičích a zaměstnání, její podrobný popis, její oblečení a zvláštnosti. K osobě hledané jsou dále informace o její minulé trestné činnosti, operativně taktické údaje, případně údaje ke stykům osoby. Dále je uvedeno datum vyhlášení pátrání, útvar, který pátrání vyhlásil, a důvod a podklad k vyhlášení.

Jako v případě předchozím i u tohoto systému existuje jeho zkrácená verze, která obsahuje pouze vybrané údaje z databáze.

TELEFOTO

Jedná se o informační systém určený pro pátrání po:

- pachatelích trestné činnosti s vysokou společenskou nebezpečností
- po hledaných a pohřešovaných osobách, ke kterým jsou vyhlášena mimořádná opatření
- po identifikaci osob, které nemohou nebo nechtějí prokázat svoji totožnost
- po identifikaci nálezů mrtvol nebo fragmentů lidských těl neznámé totožnosti
- po odcizených věcech, jejichž odcizením vznikla škoda velkého rozsahu
- po odcizených uměleckých předmětech a starožitnostech vysoké umělecké hodnoty
- po původu nalezených nebo zjištěných uměleckých předmětů a starožitností vysoké umělecké hodnoty.

Obsahem databáze jsou obrazové informace, identifikační údaje osob, popis věcí a uměleckých předmětů, popis markantů, datum, místo a čas nalezení/odcizení, aktuální sdělení k pátrání. Dále jsou vedeny údaje k útvaru, který pátrání vyhlásil.

Systém nabízí možnost vyhledávání pátrání, která jsou rozčleňována do různých skupin podle druhu informace:

- **OSOBA** - kategorie informací k osobám, které jsou pohřešované nebo po kterých je vyhlášeno pátrání, obsahuje fotografii, identifikační údaje osoby, údaje o bydlišti, její podrobný popis, druh pátrání a nebezpečnost
- **IDENTIKIT** - tato kategorie se váže k portrétům neznámých osob sestaveným podle popisu a výpovědí svědků, údaje obsahují obrazovou informaci a podrobný popis osoby
- **VĚCI** - uvedená kategorie se váže k odcizeným a nalezeným věcem kromě uměleckých předmětů, obsahuje obrazovou informaci, druh a popis věci, rozměry, její hodnotu a výrobní číslo
- **STAROŽITNOST** - kategorie vážící se k odcizeným nebo nalezeným uměleckým předmětům, obsahuje obrazovou informaci, druh a popis předmětu, autora, rozměry, materiál a hodnotu
- **SDĚLENÍ** - tato kategorie se váže na aktuální sdělení v rámci policie.

UDÁLOST

Představuje celostátní informační systém, který registruje hlášení o závažných porušeních vnitřního pořádku a jiných událostech. Systém umožňuje získávat přehled o všech událostech, které nastaly na příslušném teritoriu. Na úrovni okresního ředitelství je tedy možné získat přehled o událostí na teritorii okresu, na správě kraje události z teritoria všech okresů a v centru je k dispozici přehled událostech z teritoria celé republiky

Událostí se v systému rozumí souhrnná informace, kterou lze rozdělit na vlastní hlášení, popis místa, kde událost nastala, a seznam objektů souvisejících s událostí. Vlastní hlášení se dále dělí na samotný popis události a tzv. doplňkový text, který obsahuje informace o ohledání místa činu, způsobu jeho provedení, seznam nalezených věcí atd.

Opětovně existuje i zkrácená verze tohoto systému, která obsahuje pouze vybrané údaje z databáze. Hlášení z této zkrácené verze mohou být dostupná i pro externí subjekty - např. státní zastupitelství.

ENO (Evidence nežádoucích osob)

Jedná se o informační systém, který obsahuje data cizinců, kterým byl zakázán pobyt na území České republiky. Systém obsahuje informace identifikující takovou osobou, tj. její jména a příjmení, datum narození, státní příslušnost, pohlaví osoby a dále důvod zákazu pobytu, kdo jej a pod jakým číslem vydal.

Při neustálé se zvyšující migraci cizinců ve středoevropském prostoru je tato databáze velmi vítaným pomocníkem zejména pro policisty Služby pohraniční a cizinecké policie.

TUDU (Evidence trvale a dočasně usídlených cizinců)

Na rozdíl od předchozího systému tento obsahuje data cizinců, kterým byl povolen trvalý nebo přechodný pobyt na území České republiky. V evidenci jsou vedeny tyto položky: jméno, příjmení, datum narození, státní příslušnost, rodné číslo (zpravidla jen u občanů Slovenské republiky), číslo pasu včetně platnosti, číslo povolení k pobytu, kdo jej vydal a na jakou dobu, bydliště osoby, místo zaměstnání. Systém taktéž obsahuje i archivní údaje o osobách, kterým byl povolen pobyt v minulosti.

SPPO (Stíhané, podezřelé a prověřované osoby – dříve C-SOV)

Jedná se o informační systém, který obsahuje údaje o osobách ve vyšetřování. Databáze tak vlastně obsahuje kriminální minulost osoby. Údaje z databáze obsahují jména a příjmení osoby, rodné číslo či datum narození, státní příslušnost, adresu bydliště a dále útvar, který vyšetřování vede či vedl, dále číslo vyšetřovacího spisu (přes tento odkaz lze zjistit všechny další spoluobviněné), datum o zahájení řízení, datum sdělení obvinění, datum ukončení, stav rozpracování, způsob ukončení, paragrafy a odstavce trestního zákona, ze kterých byla osoba obviněna, zda je ve vyšetřovací vazbě, od kdy, kde, na základě čeho. Jako jediný policejní

informační systém obsahuje údaje o ukončení trestního řízení z důvodů vyloučení trestní odpovědnosti.

Uvedený systém je velmi intenzivně využíván zejména pracovníky Služby kriminální policie a vyšetřování. Počty dotazů do této databáze se pohybují kolem čtyř až pěti tisíc za pracovní den, jeden až dva tisíce za den pracovního klidu a dokonce i v nočních hodinách je intenzita dotazů kolem stovky za hodinu.

SEUD (Systém evidence uměleckých děl)

Tento informační systém je vlastně centrální evidencí ztracených a odcizených uměleckých předmětů, kdy ve vztahu k těmto předmětům jsou v databázi vedeny stejné údaje jako v Informačním systému Telefoto.

ESSK (Evidenčně statistický systém kriminality)

V uvedeném případě se jedná o nejstarší policejní informační systém (od 15. 9. 1973) známý pod názvem *Evidenčně statistický systém kriminality*. Systém je provozován na krajské a centrální úrovni a jeho účelem je poskytovat statistické informace o kriminalitě a jejich pachatelích zejména pro řídicí analytickou činnost nejen samotné policie, ale i Ministerstva vnitra, a sledovat výsledky trestního řízení v celé jeho šíři. Uvedený systém obsahuje údaje o všech trestných činech, ve kterých policie prováděla trestní řízení.

Základem celé databáze jsou informace pocházející z formulářů o trestném činu, o známém pachateli a z formulářů změn. Formulář o trestném činu vyplňuje každý věcně a místně příslušný policejní orgán k vyšetřování. Formulář se vyplňuje samostatně ke každému spáchanému skutku. Formulář o známém pachateli vyplňuje ten policejní orgán, který uvedené osobě sdělil obvinění. I tento formulář se vyplňuje pro každého pachatele zvlášť. Formulář změn zachycuje veškeré změny, které nastaly v průběhu trestního řízení.

AFIS 2002 (Daktyloskopované osoby)

Jedná se o identifikační systém, který slouží k identifikaci osob a neznámých mrtvol podle otisků prstů a k identifikaci osob na základě zjištěných daktyloskopických stop. [31]

9.9. Příklady zahraničních informačních zdrojů pro policii

9.9.1. Americký projekt National Sex Offender Public Registry

V souvislosti s policejními informačními systémy, které poskytují policistům informace o pachatelích, bych ráda zmínila americký projekt *National Sex Offender Public Registry* (přístup z <http://www.nsopr.gov>). Jedná se o systém, který 20. července 2005 spustilo Ministerstvo spravedlnosti USA (U.S. Department of Justice). Tento systém zpřístupňuje (stejně jako např. zmiňovaný systém SPPO) také informace o pachatelích (konkrétně sexuálních trestných činů). V tomto případě se však jedná o systém přístupný široké veřejnosti.

V USA byla na webu v roce 2005 pro veřejnost zpřístupněna národní databáze pachatelů sexuálních trestných činů. Projekt *National Sex Offender Public Registry* uvedlo do provozu ministerstvo spravedlnosti. Již předtím existovaly na internetu početné databáze obsahující podobné seznamy pachatelů závažných trestných činů. Nejednalo se však o národní systémy, ale databáze, které provozovaly jednotlivé státy, případně města (jako první umožnil online přístup k údajům o odsouzených pachatelích sexuálních trestných činů - včetně fotografií pachatelů, bližších údajů o spáchaných trestných činech nebo informací o současném místě pobytu odsouzeného) stát Florida v roce 1997). Projekt *National Sex Offender Public Registry* umožnil jednotný online přístup k údajům o pachatelích sexuálních trestných činů s celonárodním záběrem. [37]

Jedná se o seskupení záznamů převzatých z původních databází jednotlivých států, která jsou díky vzniku národního systému přístupná skrze jednotné uživatelské rozhraní. Tento fakt však podle kritiků registru zvýšil riziko chybných údajů. Odpovědnost za korektnost dat ministerstvo spravedlnosti řeší tak, že za správnost uložených záznamů odpovídají jednotlivé spolkové státy. [38] Ministerstvo spravedlnosti, jak stojí v podmínkách, za publikované informace neručí (<http://www.nsopr.gov/>).

Občané – uživatelé tohoto registru se v něm mohou podívat, jací odsouzení sexuální delikventi žijí v okolí jejich bydliště. Naleznou zde kupříkladu přesný popis, výšku, váhu, případně zvláštní znamení pachatelů. Výsledky jsou doplněny o aktuální adresu na detailní mapě. Dozví se i základní informace k provinění pachatelů.

Slabinou tohoto kontroverzního webu je fakt, že se do databáze mezi skutečné násilníky doživotně dostávají i 16-ti, 17-ti letí chlapci , kterým se přišlo na románek s jejich příliš mladou přítelkyní (z pořadu *Kosmopolis* vysílaného v říjnu 2006 na ČT).

Před samotným přihlášením se do databáze je nutné akceptovat podmínky, které se nacházejí pod záložkou Conditions of Use (připojen je i seznam podmínek jednotlivých států). Teprve po odsouhlasení podmínek (odkliknutím myši) se uživatel dostane k vyhledávací masce. V databázi není možné zadat takový dotaz, aby bylo možné vyhledat celkový seznam všech pachatelů, možné je pouze konkrétní – cílené vyhledávání podle zadaných kritérií (<http://www.nsopr.gov/>). Databáze obsahuje více než 500.000 záznamů s údaji o jednotlivých pachatelích (jména, adresy, fotografie, bližší popis spáchaných skutků). Kdokoliv má volný přístup k těmto údajům. Uživatel si zde může vyhledat seznam pachatelů, za vyhledávací kritéria může zvolit např. konkrétní stát, lokalitu nebo adresu. [39]



DATABÁZE NATIONAL SEX OFFENDER PUBLIC REGISTRY

Americká databáze sexuálních delikventů vyvolala velkou vlnu zájmu. Tomuto tématu se věnovala nejenom média (včetně těch zahraničních). V sousedním Německu se dokonce rozběhla politická debata o případném zavedení podobné databáze i zde. Co se týká zájmu médií, dá se říci, že zájem o toto téma byl v Německu dokonce větší, než v samotných Spojených státech amerických. Pokud se totiž provedlo srovnání mezi německým a americkým přehledem novinek na Googlu

(Google News), pak v přehledu německých zpráv bylo dohledáno na 90 příspěvků médií na téma *National Sex Offender Public Registry*. Na News.google.com se objevilo pouze 30 příspěvků zabývajících se touto databází. Důvodem tohoto výsledku však mohl být právě ten fakt, že veřejně přístupné databáze pachatelů trestných činů nejsou v USA žádnou novinkou (viz. předešlý text). V převážné většině států USA je možné získat tato data online. [38]

Projekt má své přívržence i odpůrce. Odpůrci projektu zastávají názor, že pokud budou mít občané volný přístup k podobným informacím, mohou nastat situace, kdy občané vezmou spravedlnost do svých rukou. V dubnu 2006 se jejich obavy staly skutečností. Dva pachatelé, jejichž jména databáze obsahovala, byli zastřeleni rozhořčenými občany. [37] Mezi další argumenty odpůrců databáze patří např. to, že je ohrožena resocializace pachatelů, neboť musí žít s nálepkou násilník i po odpykání trestu (což může mít negativní vliv právě na následné začlenění těchto osob zpět do společnosti). V neposlední řadě zde hrozí i to riziko, že vzhledem k chybným údajům (které obsahuje dá se říci každá databáze), mohou být „veřejnému pranýřování“ vystaveny i nevinné osoby.

Z výše uvedeného vyvstává otázka, kdo všechno by k podobným informacím měl mít přístup. Zda by o odsouzených pachatelích - kromě oprávněných úřadů včetně policie - měli vědět i běžní občané, kteří by si tyto informace vyhledali přes internet.

9.9.2. NCJRS Abstracts Database

Dalším zahraničním informačním zdrojem týkajícím se kriminality, a proto využitelným v oblasti kriminalistiky a policejní činnosti (včetně oblasti vědy a výzkumu), je bibliografická online přístupná databáze *NCJSR Abstract Database* (*National Criminal Justice Reference Service Abstracts Database*) (přístup na <http://www.ncjrs.gov/abstractdb/search.asp>) zaměřená na justici a kriminalistiku (především v USA) [převzato z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.] a navazující oblasti (např. viktimologie, kriminologie). Systém produkuje organizace NCJRS [40] prezentující se na webových stránkách <http://www.ncjrs.gov>. Jedním ze sponzorů je Ministerstvo spravedlnosti USA. Jedná se o bibliografický typ zdroje, volně dostupný. [40]

Tento zdroj nabízí ke stažení nejrůznější výzkumy a studie o kriminalitě i dalších sociálně patologických jevech. [41]

Databáze zahrnuje aspekty lokálního, státního a mezinárodního práva, poskytuje rozsáhlé informace o kriminální justici, policii, soudech, trestech, souzení mladistvých, prevenci společensky nebezpečných činů, justičních systémech, zpronevěrách atd. Vychází se z různých druhů (140) primárních amerických a mezinárodních výzkumných zpráv a zdrojů. Retrospektiva sahá do roku 1972, aktualizace probíhá měsíčně, k dispozici je rovněž tezaurus. [převzato z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.]

Aktuálně obsahuje 174 000 záznamů článků, zpráv vládních úřadů, monografií, výzkumných zpráv a výběrově také oficiálně nepublikovaných dokumentů. Roční přírůstek činí cca 5500 záznamů. [převzato z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.]

9.9.3. FORENSICnetBASE a InfoSECURITYnetBASE

Dalším využitelným zdrojem v oblasti kriminalistiky a policejní činnosti je jedna z kolekcí e-books nakladatelství CRS Press (vystavuje okolo 1200 elektronických knih), konkrétně *FORENSICnetBASE*, jež je zaměřena do oblastí soudní lékařství, patologie, kriminalistika a právo. Další využitelnou kolekcí od nakladatelství CRS Press je *InfoSECURITYnetBASE*, jež se zabývá datovou bezpečností, počítačovou kriminalistikou a právem. [převzato z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.]

9.9.4. Ciminal Justice Abstract

Producentem této bibliografické databáze je Willow Tree Press, zaměřena je na obory právo a společenské vědy. Databáze poskytuje odkazy na literaturu z oblasti kriminologie s retrospektivou od roku 1968. Jejími zájmovými oblastmi jsou kriminální trendy, prevence kriminality, kriminalita mladistvých, činnost policie, soudů, trestní otázky apod. 85 000 záznamů pokrývá zprávy vládních i nevládních agentur, knihy, nepublikované přednášky a disertační práce. [převzato z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.]

9.9.5. CRIMINAL JUSTICE PERIODICAL INDEX

Producentem je CJPI, databáze obsahuje plné texty a obrázky, zaměřena je na oblast práva. Zpracovává obsahy periodik, novinek a zpráv z oblasti kriminality, kriminalistiky, justice a práva (komerční kriminalita, drogy, narkotika, rodinné právo, organizovaný zločin, vězeňství, kriminální prevence apod.). Zaměřuje se na USA, Británii a Kanadu. Kompletní seznam excerpovaných zdrojů je dostupný prostřednictvím UMI. Retrospektiva sahá do roku 1975, aktualizace probíhá měsíčně, cca.198 000 záznamů od r. 1993.

CPJI poskytuje bibliografické záznamy o více než 120 světových periodicích z oblasti kriminalistiky, policie, drogové problematiky, rehabilitace a práva od roku 1981 s týdenní aktualizací. Pro cca 40 titulů jsou k dispozici jak abstrakty, tak plné texty (většinou od roku 1996). Od roku 1999 obsahují všechny záznamy abstrakt. Databáze poskytuje více než 3x více záznamů než jiné podobně zaměřené databáze. [převzato z katalogu elektronických zdrojů/databází nabízených společností Albertina icome Praha s.r.o.]

10. NEJROZŠÍŘENĚJŠÍ CIVILNĚ SPRÁVNÍ EVIDENCE

10.1. Registry spravované Ministerstvem vnitra

10.1.1. Registr občanů

Tento centrální registr, spravovaný Ministerstvem vnitra vede informace o občanech České republiky. Dotaz je povolen podle příjmení, jména a data narození (nebo intervalu data narození), podle rodného čísla, rodného i minulého příjmení, podle místa narození, podle místa trvalého pobytu. U občanů jsou vedeny i rodinné vazby (rodič-dítě, případně manžel-manželka).

10.1.2. Registr vozidel

Centrální registr vozidel, taktéž spravovaný Ministerstvem vnitra vede informace o vozidlech registrovaných v České republice. Obsahuje podrobné údaje o jednotlivých vozidlech (např. registrační značku vozidla, číslo VIN, číslo motoru, číslo technického průkazu, typ, barvu a rok výroby vozidla).

10.2. Registr řidičů spravovaný Ministerstvem dopravy

Centrální registr řidičů je od 1. července 2006 spravován Ministerstvem dopravy. Do této doby bylo vedením tohoto registru pověřeno Ministerstvo vnitra. Tento registr vede informace o řidičích, řidičských oprávněních, vydaných řidičských průkazech (včetně mezinárodních), omezeních popř. zákazech řízení, informace o přestupcích včetně přidělených bodů.

11. ZÁVĚR

Pokrok ve výpočetní technice, v telekomunikacích, v přenosu dat podstatně ovlivnil i tak specifickou oblast, jakou je práce zpravodajských služeb nebo policejních složek. Moderní informační technologie otevírají kriminalitě nové cesty ve způsobech páchání trestných činů, pro tajné služby představují například zvýšení rizika úniků informací. V souvislosti s rozvojem vědy a techniky se však bezpečnostním složkám otevřely i nové možnosti ve způsobech sběru informací, jejich zpracování a využívání. Informační technologie rozšířily možnosti lepšího, snadnějšího a kvalitnějšího využívání stávajících zdrojů informací. Umožnily vzniknout i řadě nových informačních zdrojů (např. v podobě různých komerčních databází nebo informačních systémů státní a veřejné správy).

Na změny ve využívání informačních zdrojů neměly vliv pouze nové informační technologie, ale i politický zvrát, ke kterému došlo zejména po skončení studené války. Politické uvolnění mělo za následek mnohonásobné rozšíření objemu volně dostupných informací. Tyto informace jsou přístupné také v rámci různých informačních systémů, z nichž mnohé jsou využitelné také bezpečnostními složkami státu. Informační zdroje měly v oblasti bezpečnosti státu a občana vždy své nezastupitelné místo. V posledních dvaceti letech se však díky moderním informačním technologiím změnil jak způsob přístupu k těmto informacím, tak jejich vyhledávání a zpracování.

V souvislosti s ukončením studené války se v rámci zpravodajských služeb změnil objekt zájmu, ke kterému zpravodajské služby informace vyhledávají, shromažďují a následně zpracovávají. Do konce 80. let 20. století byl nepřítel jednoznačně vymezen. Byl jím Sovětský svaz z pohledu USA (a naopak). V současnosti již situace tak jednoduchá není. Zájmových objektů zpravodajských služeb existuje celá řada – od islámských fundamentalistů, přes různé separatistické skupiny (např. ETA, IRA), až po obchod s vojenským materiálem.

Rozmanitost informačních zdrojů představuje z hlediska různorodosti zájmových objektů velkou výhodu, na druhou stranu si však tato skutečnost zřejmě vyžádá i změny v organizaci zpravodajských služeb. Vzhledem k tomu, že význam využívání informačních zdrojů jako jednoho z prostředků, který se podílí na zajišťování bezpečnosti státu a občana, bude neustále narůstat a budou vznikat zcela

nové informační zdroje (čímž bude docházet ke kvantitativnímu nárůstu zdrojů) se dá předpokládat, že v rámci zpravodajských služeb a stejně tak v rámci policie budou ještě ve větší míře, než je tomu dosud, zapotřebí specializovaní pracovníci – informační specialisté. Orientovat se v množství informačních zdrojů bude totiž vyžadovat dostatečné znalosti a zkušenosti ve využívání těchto zdrojů. Stejně tak bude nezbytné neustálé prohlubování znalostí a zdokonalování se v rámci dynamického vývoje této problematiky.

SEZNAM POUŽITÉ LITERATURY

1. (zak). Evropa a úpadek [online]. *Konkursní noviny*. 2005. [cit. 2006-12-7]. Dostupné také z WWW: <<http://www.konkursni-noviny.cz/clanek.html?ida=1361>>.
2. SOUČEK, V. *Vnitřní bezpečnost a pořádek* [online]. Ministerstvo vnitra. 2005. [cit. 2006-12-7]. Dostupné také z WWW: <<http://www.mvcr.cz/udalosti/prirucky/bezpecnost/bezpecnost.pdf>>.
3. *Výkladový slovník krizového řízení a obrany státu* [online]. Ministerstvo vnitra. 2004. [cit. 2006-12-7]. Dostupné také z WWW: <http://www.mvcr.cz/udalosti/slovník/index_odbor_info.html#xB>.
4. *Produkty a služby* [online]. Albertina icome Praha. 2006. [cit. 2006-12-10]. Dostupný z WWW: <<http://www.aip.cz/produkty.php>>.
5. VSČR. *Podávání informací o vězněných osobách* [online]. VSČR. [cit. 2006-12-7]. Dostupný z WWW: <http://www.vscr.cz/clanky/?cl_id=665>.
6. ZEMAN, P. *UZSI – přednášky, školení a veřejná vystoupení* [online] UZSI. 2005. [cit. 2006-11-13]. Dostupné z WWW: <<http://www.uzsi.cz/index.php@lang=1&show=001001003013.html>>.
7. OPAT, L. *Výkladový slovník analytiky*. 1. vyd. Praha : EUROLEX BOHEMIA, 2005. 191 s. ISBN 80-86861-19-8.
8. HANOUSEK, M. *Zpravodajská terminologie z pohledu současnosti* [online]. Ministerstvo obrany. 2005. [cit. 2006-12-01]. Dostupný také z WWW: <http://www.army.cz/mo/tisk/vojroz/2000_1/hanousek.htm>.
9. BRÁZDILOVÁ, M. Jak moc se firmy zajímají o své konkurenty? [online]. In *INFORUM Praha 2005*. [cit. 2006-12-10]. Dostupný také z WWW: <www.inforum.cz/inforum2005/prispevek.php-prispevek=44.htm>.
10. PAPÍK, R. Competitive Intelligence, informační služby, Internet a informační profese. *Ikaros* [online]. 2001, roč. 5, č. 4 [cit. 2006-06-08]. Dostupný z WWW: <<http://www.ikaros.cz/node/739>>. URN-NBN:cz-ik739. ISSN 1212-5075>.
11. *Druhy špionáže*. Specialista [online]. Web. 2005. [cit. 2006-12-10]. Dostupný z WWW: <<http://www.specialista.info/view.php?cislocclanku=2005090106>>.

12. Lloyd, M. *Guinnessova kniha špionáže*. 1. vyd. Praha : Nakladatelství Olympia, 1996. 255 s. ISBN 80-7033-413-4.
13. *Open source intelligence resources for the military*. The 434th Military Intelligence Detachment. New Haven, 1999. [cit. 2006-11-01]. 85 s.
14. SPITZER, M. *The Man Inside China's Bomb* [online]. CTRL. 2001. [cit. 2006-11-01]. Dostupný z WWW: <<http://www.mail-archive.com/search?l=ctrl@listserv.aol.com&q=askint>>.
15. KAPFERER, J.–N. *Fáma nejstarší médium světa*. 1. vyd. Praha : Vydavatelství a nakladatelství Práce, 1992. 248 s. ISBN 80-208-262-2.
16. FININ, T. *Is the CIA reading your blog?* [online]. UMBC. cit. 2006-12-01]. Dostupný z WWW: <<http://ebiquity.umbc.edu/blogger/2006/04/19/is-the-cia-reading-your-blog/>>.
17. *Big Brothers und das Web 2.0* [online]. Rabenhorst. 2006. [cit. 2006-12-01]. Dostupný z WWW: <rabe.supersized.org/archives/574-Big-Brothers-und-das-Web-2.0.html>.
18. GERTZ, B. *CIA mines 'rich' content from blogs* [online]. *Washington Times*. 2006. [cit. 2006-12-01]. Dostupný z WWW: <<http://www.washtimes.com/national/20060418-110124-3694r.htm>>.
19. KULIK, M. *George W. Bush liest Blogs!* [online]. Blog watch. 2006. [cit. 2006-12-01]. Dostupný z WWW: <blogwatch.germanblogs.de/archive/2006/04/20/15letwm3yx7iy.htm>.
20. GRADY, J. *Šest dnů Kondora*. 2. vyd. Praha : Nakladatelství Svoboda–Libertas, 1993. 113 s. ISBN 80-205-0312-9.
21. CIA: Chcete-li být dobrým špionem, čtěte noviny [online]. *Britské listy*. 2005. [cit. 2006-10-01]. Dostupné z WWW: <<http://www.blisty.cz/2005/11/1/art25590.html>>.
22. KREJCI, Roman. *Open-Source Intelligence in the Czech Military: Knowledge System and Process Design*. Master's Thesis, Naval Postgraduate school, Monterey, California [online]. 2002. 133 s. Dostupné z WWW: <<http://library.nps.navy.mil/uhtbin/cgiisirsi/faSNzTUKrn/213910058/123>>.
23. Director of Central Intelligence Directive 2/12. *Community Open Source Program. I.* [online]. 1994. [cit 2006-12-10]. Dostupné z WWW: <<http://www.fas.org/irp/offdocs/dcid212.htm>>.
24. *Concept paper: creating a bare bones capability for open source support to defense intelligence analysts* [online]. DIA Report 001.1. 1997. 33 s. [cit 2006-12-10]. Dostupné z WWW: <<http://www.oss.net>>.

25. KOUTSKÁ, Marie. *Otevřené zdroje ve zpravodajských službách*. Praha: Studijně rozborová práce. 2003, 24 s.
26. MUSIL, J, Konrád, Z., Suchánek, J. *Kriminalistika*. 1. vyd. Praha : C.H.Beck, 2001. 512 s. ISBN 80-7179-362-0.
27. PORADA, V., BRADÁČ, A., DOGOŠI, M. *Kriminalistika*. Brno : Akademické nakladatelství Cerm, 2001. 746 s. ISBN 80-7204-194-0.
28. MOUČKOVÁ, Miroslava. Jak chránit své osobní údaje. *Haló noviny*, 31. 3. 2004, s. 7.
29. HRBÁČEK, Jan. Očko v obýváku. *Týden*, 30. 10. 2000, s. 18.
30. NEUWIRT, K. *Boj proti terorismu*. Čro 1 – Radiožurnál, 8. 1. 2004, Radiofórum, rozhovor.
31. FRYŠTÁK, M. Ochrana osobních údajů a policejní informační systémy. *Policista*, červenec 2003, č. 7.
Přístupný z WWW:
<<http://www.mvcr.cz/casopisy/policista/2003/07/ochrana.html>>.
32. ŠTRAUS, J. a kol. Identifikační a počítačové systémy v trasologii. *Čtvrtletník kriminalistika*, leden 2005, 4. 1.
Přístupný z WWW:
<http://www.mvcr.cz/casopisy/kriminalistika/2005/01/straus_info.html>.
33. BAUMAN, M. Průkazy totožnosti mění podobu. *Hospodářské noviny*, 18. 11. 2004, s. 8.
34. (lek). Spory o snímání otisků v USA. *Právo*, 9. 1. 2004, s. 3.
35. FOKUS. Na stopě zločinu. *100+1 zahraniční zajímavost*, březen 2001, s. 2.
36. Společnost pro kriminalistiku. *AFIS 2000* [online]. 2002. [cit. 2006-11-16]
Dostupný z WWW: <http://sweb.cz/krimi-pk/02_exper/expertiz/02a_dakt/02_afis.htm>.
37. KREML, S. *Streit um deutsche Online-Datenbank mit Sexualstraftätern*. Heise Online [online]. 2006 [cit. 2006-11-26]. Dostupné z WWW:
<<http://www.heise.de/newsticker/meldung/79426>>.
38. *Unterschiedliches Rechtsverständnis*. intern.de Fachinformationsdienst [online]. 2005 [cit. 2006-11-26]. Dostupné z WWW:
<<http://www.intern.de/news/6924.html>>.
39. ERNST, N. *USA stellen Adressen von Sexualstraftätern ins Netz*. Networld [online]. 2005 [cit. 2006-11-25]. Dostupné z WWW:
<<http://www.golem.de/0507/39389.html>>.

40. Ústřední knihovna UTB. *Volně dostupné databáze. Informační zdroje* [online]. 2006 [cit. 2006-11-25]. Dostupné z WWW: <http://www.knihovna.utb.cz/portal/zakladni_vypis.php?vybrany_druh=5>.
41. Institut pro kriminologii a sociální prevenci. Odkazy. *IKSP* [online]. 2006 [cit. 2006-11-25]. Dostupné z WWW: <<http://www.ok.cu/ik.sp/odkazy:zahranicni5.html>>.
42. Zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů. Sbírka zákonů 1998, částka 39.
43. Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČSR, ve znění pozdějších předpisů. Sbírka zákonů 1969, částka 1.
44. Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů. Sbírka zákonů 1994, částka 49.
45. Zákon č. 555/1992 Sb., o Vězeňské službě a justiční strážní ČR, ve znění pozdějších předpisů. Sbírka zákonů 1992, částka 112.
46. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Sbírka zákonů 2000, částka 32.
47. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, Sbírka zákonů 2005, částka 143.
48. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Sbírka zákonů 1999, částka 39.
49. Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů. Sbírka zákonů 1961, částka 65.
50. Zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů. Sbírka zákonů 1961, částka 65.

PŘÍLOHY

Příloha č. 1

§ 2 zákona č. 283/1991 Sb., o Policii České republiky

§ 2 – Úkoly policie

(1) Policie plní tyto úkoly:

a) chrání bezpečnost osob a majetku;

b) spolupůsobí při zajišťování veřejného pořádku, a byl-li porušen, činí opatření k jeho obnovení;

c) vede boj proti terorismu;

d) odhaluje trestné činy a zjišťuje jejich pachatele;

e) koná vyšetřování o trestných činech;

f) zajišťuje ochranu státních hranic ve vymezeném rozsahu;

g) zajišťuje ochranu ústavních činitelů České republiky a bezpečnost chráněných osob, kterým je při jejich pobytu na území České republiky poskytována osobní ochrana podle mezinárodních dohod;

h) zajišťuje ochranu zastupitelských úřadů, ochranu sídelních objektů Parlamentu, pokud zákon nestanoví jinak, prezidenta republiky, Ústavního soudu, ministerstva zahraničních věcí, ministerstva vnitra a dalších objektů zvláštního významu pro vnitřní pořádek a bezpečnost, které určí vláda na návrh ministra vnitra; rovněž zajišťuje ochranu objektů, pro které taková ochrana vyplývá z mezinárodní dohody, kterou je Česká republika vázána;

i) dohlíží na bezpečnost a plynulost silničního provozu a spolupůsobí při jeho řízení;

j) odhaluje přestupky;

k) projednává přestupky, pokud tak stanoví zvláštní zákon; 2)

l) vede evidence a statistiky potřebné pro plnění svých úkolů;

m) vyhledává celostátní pátrání; přitom je oprávněna zveřejňovat údaje nezbytné k identifikaci hledaných osob;

n) na základě vyzoomění orgány Vězeňské služby České republiky provádí úkony související s bezprostředním pronásledováním osob, které uprchly z výkonu vazby nebo z výkonu trestu odnětí svobody;

o) zadržuje svěřence s nařízenou ústavní nebo uloženou ochrannou výchovou, kteří jsou na útěku, a spolupůsobí při jejich vyhledávání,

p) zajišťuje pohotovostní ochranu jaderných zařízení, která určí vláda České republiky, a podílí se na fyzické ochraně jaderného materiálu při jeho přepravě podle zvláštního zákona,

q) kontroluje doklady o pojištění odpovědnosti za škodu způsobenou provozem vozidla podle zvláštního právního předpisu.

(2) Policie plní též úkoly státní správy, pokud tak stanoví zvláštní zákon.

(3) Policie plní rovněž úkoly při zabezpečování místních záležitostí veřejného pořádku, které jí ukládají příslušné orgány obcí za podmínek stanovených zvláštními předpisy.

Příloha č. 2

Hlava čtvrtá a pátá zákona č. 283/1991 Sb., o Policii České republiky

HLAVA ČTVRTÁ

ZPRACOVÁVÁNÍ INFORMACÍ POLICIÍ

§ 42d

Policie zpracovává v souladu s tímto zákonem a zvláštními právními předpisy 17b) informace včetně osobních údajů, shromážděné při plnění úkolů policie, a to v rozsahu nezbytně nutném pro plnění těchto úkolů.

§ 42e

(1) Policista, který při plnění úkolů policie nemůže získat osobní údaje, umožňující budoucí identifikaci, jiným způsobem, je oprávněn u osob obviněných ze spáchání trestného činu, u osob ve výkonu trestu odnětí svobody za spáchání úmyslného trestného činu, u osob, jimž bylo uloženo ochranné léčení, nebo u osob nalezených, po nichž bylo vyhlášeno pátrání a které nemají způsobilost k právním úkonům v plném rozsahu,

a) snímat daktyloskopické otisky,

b) zjišťovat tělesné znaky,

c) provádět měření těla,

d) pořizovat obrazové, zvukové a obdobné záznamy, nebo

e) odebírat biologické vzorky umožňující získání informací o genetickém vybavení.

(2) Zjišťování vnějších tělesných znaků a měření těla podle odstavce 1 provádí policista stejného pohlaví nebo na jeho žádost odborně způsobilý zdravotnický pracovník, odběr krve nebo odběr jiného biologického materiálu, který je spojen se zásahem do tělesné integrity, provádí na žádost policisty pouze odborně způsobilý zdravotnický pracovník. Obdobně se postupuje i u odběru, který není spojen se zásahem do tělesné integrity, je-li při něm překonáván odpor osoby. Odběr biologických vzorků se provádí způsobem, který nesmí ohrozit zdraví osoby.

(3) Nelze-li úkon podle odstavce 1 pro odpor osoby provést a nejde-li o odběr krve nebo jiný obdobný úkon spojený se zásahem do tělesné integrity, je policista po předchozí marné výzvě oprávněn tento odpor překonat. Způsob překonání odporu musí být přiměřený intenzitě odporu.

§ 42f

(1) Policie je oprávněna, je-li to potřebné pro plnění úkolů policie, pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu služebního úkonu nebo služebního zákroku.

(2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, je policie povinna informace o zřízení takových systémů vhodným způsobem uveřejnit.

HLAVA PÁTÁ

ZVLÁŠTNÍ USTANOVENÍ O ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ POLICIÍ

§ 42g

Zpracovávání osobních údajů při plnění úkolů policie v souvislosti s trestním řízením

(1) Při předcházení a odhalování trestné činnosti, zjišťování pachatelů trestných činů a konání vyšetřování o trestných činech (dále jen "plnění úkolů policie v souvislosti s trestním řízením") je policie při zpracovávání osobních údajů povinna

a) stanovit účel, k němuž mají být osobní údaje zpracovány,

b) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu,

c) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování,

d) zpracovávat osobní údaje podle tohoto ustanovení odděleně od osobních údajů zpracovávaných při plnění jiných úkolů policie,

e) neprodleně ohlásit Úřadu pro ochranu osobních údajů 17c) zřízení každé evidence obsahující osobní údaje; součástí tohoto ohlášení je název útvaru odpovědného za zpracovávání osobních údajů, účel evidence, kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají, a popis opatření k zajištění požadované ochrany osobních údajů.

(2) Policie je při zpracování osobních údajů podle odstavce 1 oprávněna v rozsahu potřebném k plnění úkolů policie v souvislosti s trestním řízením

a) sdružovat osobní údaje, které byly získány k rozdílným účelům,

b) zpracovávat nepravdivé, nepřesné a neověřené osobní údaje; tyto osobní údaje tak musí být označeny.

(3) Policie je při zpracování osobních údajů podle odstavce 1 oprávněna zpracovávat citlivé údaje, 17d) je-li to s ohledem na povahu trestného činu nezbytné pro plnění úkolů policie v souvislosti s trestním řízením.

(4) Policie zpracovává osobní údaje podle odstavce 1 i bez souhlasu osob; přitom je povinna dbát práva na ochranu jejich soukromého a osobního života. Policie je povinna, jakmile tím již není ohroženo plnění úkolů policie v souvislosti s trestním řízením, osobě sdělit, že zpracovává její osobní údaje, nebo provést likvidaci jejich osobních údajů.

(5) Policie neprovede likvidaci osobních údajů v případě, že jde o osobní údaje, které jsou součástí spisového materiálu a nejsou zpracovávány automatizovaně.

(6) Podle ustanovení této hlavy zpracovává policie osobní údaje též při předcházení a odhalování činů, jejichž znaky jsou uvedeny v trestním zákoně 17e) a jejichž pachatelé nejsou trestně odpovědní pro nedostatek věku nebo pro nepřičetnost, a při zjišťování těchto pachatelů.

§ 42h

Zpracovávání osobních údajů při pátrání po osobách

(1) Při pátrání po osobách, po nichž bylo vyhlášeno pátrání, je policie oprávněna

a) v potřebném rozsahu sdružovat osobní údaje získané k rozdílným účelům, a

b) zpracovávat citlivé údaje těchto osob, je-li to nezbytné k jejich nalezení.

(2) Policie provede likvidaci osobních údajů pohřešované nebo hledané osoby bez zbytečného odkladu po jejím nalezení. Likvidace osobních údajů nemusí být provedena,

a) byla-li osoba pohřešována nebo hledána opakovaně,

b) lze-li důvodně předpokládat, že bude opět pohřešována nebo hledána,

c) jsou-li její osobní údaje zpracovávány při plnění úkolů policie v souvislosti s trestním řízením.

§ 42i

Prověřování potřebnosti dalšího zpracovávání osobních údajů

(1) *Policie nejméně jednou za 3 roky prověřuje, jsou-li zpracovávané osobní údaje nadále potřebné pro plnění úkolů policie v souvislosti s trestním řízením nebo při pátrání po osobách. Zjistí-li policie při prověřování nebo v průběhu zpracovávání osobních údajů, že již nejsou potřebné pro plnění úkolů policie v souvislosti s trestním řízením nebo při pátrání po osobách, provede bez zbytečného odkladu likvidaci těchto osobních údajů.*

(2) *Pro potřeby prověřování podle odstavce 1 jsou orgány činné v trestním řízení, Ministerstvo spravedlnosti, Ústavní soud a Kancelář prezidenta republiky povinny policii v mezích své působnosti průběžně informovat o pravomocných rozhodnutích orgánů činných v trestním řízení, promlčení trestního stíhání, výkonu trestu nebo o rozhodnutích prezidenta republiky týkajících se trestního řízení, trestů nebo udělené amnestie.*

§ 42j

Informování o osobních údajích a oprava nepravdivých nebo nepřesných osobních údajů

(1) *Policie na písemnou žádost sdělí žadateli bezplatně osobní údaje vztahující se k osobě žadatele, a to do 30 dnů od jejího doručení.*

(2) *Policie na písemnou žádost provede bezplatně likvidaci nebo opravu nepravdivých nebo nepřesných osobních údajů vztahujících se k osobě žadatele, a to neprodleně po jejím doručení.*

(3) *O žádostech podle odstavců 1 a 2 rozhoduje Policejní prezidium České republiky; novou žádost lze podat nejdříve po uplynutí jednoho roku od podání žádosti předchozí.*

(4) *Policie žádostem podle odstavců 1 a 2 nevyhoví, pokud by tím došlo k*

a) ohrožení plnění úkolů policie v souvislosti s trestním řízením, nebo

b) ohrožení oprávněných zájmů třetí osoby;

nevyhovuje-li se žadateli, musí být rozhodnutí o žádosti písemně odůvodněno.

(5) *Nezpracovává-li policie žádné osobní údaje vztahující se k žadateli nebo pokud by sdělením odůvodněného rozhodnutí došlo k ohrožení plnění úkolů policie v souvislosti s trestním řízením, žadatel se písemně vyrozumí o tom, že policie nezpracovává žádné osobní údaje vztahující se k žadateli.*

(6) *Na postup při vyřizování žádosti se nevztahuje správní řád.*

§ 42k

Předávání osobních údajů

(1) *Policie předá osobní údaje jiným orgánům nebo osobám,*

a) stanoví-li tak tento nebo zvláštní zákon,

b) je-li to ve prospěch osoby, k níž se osobní údaje vztahují, a tato osoba dala k předání souhlas nebo lze její souhlas na základě okolností důvodně předpokládat, nebo

c) je-li předání osobních údajů nezbytné k odstranění bezprostředního závažného ohrožení bezpečnosti osob nebo veřejného pořádku.

(2) *Policie předá podle odstavce 1 osobní údaje na základě písemné žádosti, která musí obsahovat účel, pro který mají být osobní údaje předány. V případě podle odstavce 1 písm. a) a c) lze předat osobní údaje i bez žádosti.*

(3) *K předávaným osobním údajům musí být připojeny 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 musí být při předávání označeny a musí být uvedena míra jejich spolehlivosti. Dojde-li k*

předání nepravdivých nebo nepřesných osobních údajů, je policie povinna bez zbytečného odkladu informovat všechny příjemce údajů, kterým byly takové osobní údaje předány.

(5) Příjemce údajů je oprávněn zpracovávat osobní údaje k jinému účelu, než ke kterému byly předány, pouze za podmínky, že by mu i pro tento účel mohly být osobní údaje předány, a pouze s předchozím souhlasem policie.

(6) Do zahraničí lze předat osobní údaje mezinárodní organizaci Interpol nebo za podmínek stanovených v odstavci 1 písm. a) až c) mezinárodní policejní organizaci nebo zahraničnímu bezpečnostnímu sboru, a to i bez žádosti.

§ 42l

Zveřejňování osobních údajů

Policie je oprávněna zveřejňovat osobní údaje v rozsahu nezbytném k plnění úkolů policie v souvislosti s trestním řízením nebo při pátrání po osobách.

§ 42m

Zpracování osobních údajů útvarem inspekce

(1) Na zpracovávání osobních údajů útvarem inspekce při plnění úkolu podle § 2 odst. 4 se použijí ustanovení této hlavy obdobně.

(2) O žádostech podle § 42j odst. 1 a 2 rozhoduje ministerstvo.

§ 42n

Zpracovávání osobních údajů v souvislosti s vykázáním ze společného obydlí a zákazem vstupu do něj

(1) Podle ustanovení této hlavy zpracovává policie též osobní údaje ohrožené osoby a vykázané osoby (§ 21a); v případě, že ve společném obydlí, na které se vztahuje vykázáni (§ 21a odst. 3), bydlí nezletilá osoba, zpracovává policie též osobní údaje této osoby.

(2) Osobní údaje osob uvedených v odstavci 1 se zpracovávají podle zásad stanovených v § 42g.

