



UNIVERZITA KARLOVA V PRAZE

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

Mgr. Jaroslav Hora

**Utajované informace jako jeden z prostředků zákonného
omezení svobodného přístupu k informacím v České republice**

Rigorózní práce

Praha 2007

Prohlášení:

Prohlašuji, že jsem rigorózní práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Praze dne 23. května 2007

A handwritten signature in black ink, consisting of several fluid, connected strokes, positioned above a horizontal dotted line.

podpis rigorózanta

Poděkování:

Rád bych poděkoval konzultantovi mé rigorózní práce Stanleyemu KALKUSOVI, Ph.D. a řediteli ÚISK PhDr. Richardu PAPÍKOVI, Ph.D. za podnětné náměty a připomínky. Za cenné rady a konzultace děkuji také Mgr. Františku KORBĚLOVI, Ph.D.

Identifikační záznam

HORA, Jaroslav. *Utajované informace jako jeden z prostředků zákonného omezení svobodného přístupu k informacím v České republice [Classified information as one of instruments of legal restriction of free access to information in Czech republic]*. Praha, 2007. 122 s. Rigorózní práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2007. Konzultant rigorózní práce Stanley KALKUS, Ph.D.

Abstrakt

Tématem rigorózní práce, která aktualizuje a doplňuje diplomovou práci autora, je zmapování a zhodnocení postavení institutu „utajovaných informací“ ve smyslu zákona číslo 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, jako jednoho z nejvýznamnějších současných nástrojů zákonného omezení svobodného přístupu k informacím v České republice. Na konkrétní problémy, nepřesnosti a nedostatky této problematiky je nahlíženo z několika zorných úhlů. Na příkladech z praxe jsou pak jednotlivé sporné otázky a možnosti jejich řešení demonstrovány a vysvětleny.

Rigorózní práce je rozčleněna do tří částí. První část je věnována aspektům obecného přístupu k informacím, druhá část pak možnostem jeho zákonného omezení, zejména při uplatnění zákona číslo 106/1999 Sb., o svobodném přístupu k informacím. Část třetí, která je pro účel práce stěžejní, pak obrací svou pozornost k institutu utajovaných informací. Ve všech částech je poukázáno na historický vývoj, popis a analýzu současného stavu. Dále pak jsou jednotlivé aspekty a hlediska problematiky detailně analyzovány a demonstrovány prostřednictvím praktických příkladů.

Klíčová slova

Informace, svobodný přístup k informacím, utajované informace, bezpečnostní řízení, poskytování informací, obchodní tajemství, lhůty, práva občanů, omezení práva na informace, praktické zkušenosti.

OBSAH

OBSAH.....	8
PŘEDMLUVA.....	11
1. ÚVOD.....	14
2. SVOBODNÝ PŘÍSTUP K INFORMACÍM.....	16
2.1 ZÁKLADY PRÁVA NA INFORMACE.....	16
2.2 HISTORIE SVOBODY INFORMACÍ V ČR.....	17
2.3 PRÁVNÍ ÚPRAVA POSKYTOVÁNÍ INFORMACÍ.....	18
2.3.1 Současná obecná právní úprava poskytování informací v ČR.....	18
2.3.2 Formálnost stávající právní úpravy.....	20
2.4 ZÁKON O SVOBODNÉM PŘÍSTUPU K INFORMACÍM.....	21
2.4.1 Zajištění práva občanů na informace.....	21
2.4.2 Pojem „informace“ z hlediska zákona č. 106/1999 Sb.....	21
2.4.3 Subjekty práva na informace.....	22
2.4.4 Povinné subjekty.....	22
2.4.5 Další subjekty.....	22
2.4.6 Žadatel.....	23
2.4.7 Vymezení pojmu zveřejňované informace.....	23
2.4.8 Nepravdivá informace.....	24
2.5 RESTRIKCE PRÁVA NA INFORMACE.....	25
2.5.1 Formulace omezení ve zvláštních zákonech.....	26
2.5.2 Další omezení práva na informace.....	29
2.5.3 Technická podoba omezení přístupu k vybraným informacím.....	29
2.5.4 Osobní údaje a jejich ochrana.....	30
2.5.5 Omezení přístupu k písemnostem osobní povahy.....	31
2.5.6 Obchodní tajemství.....	32
2.5.7 Ochrana duševního vlastnictví.....	34
2.5.8 Ochrana důvěrnosti majetkových poměrů.....	35
2.5.9 Podmíněně předané informace.....	35
2.5.10 Časové omezení odepření informací.....	36
2.5.11 Priorita vyššího zájmu.....	36
2.6 VZTAH ZÁKONA Č. 106/1999 SB. K JINÝM ZÁKONŮM.....	36
2.7 ŽÁDOST O PŘÍSTUP K INFORMACÍM A MOŽNOSTI JEJICH ODEPŘENÍ.....	39
2.8 POSKYTOVÁNÍ A ODPÍRÁNÍ INFORMACÍ V PRAXI.....	40
2.8.1 Právo na informace nepodléhající režimu utajení.....	40
2.8.2 Nevědomost o možnosti požadovat některé informace.....	41
2.8.3 Umělé překážky v přístupu k informacím v praxi.....	42
2.9 PRÁVO STÁTU NA INFORMACE OBČANŮ.....	44
2.10 KAM PRÁVNÍ NORMY NEDOSÁHNOU.....	45

3.	UTAJOVANÉ INFORMACE.....	47
3.1	HISTORIE „STÁTNÍHO TAJEMSTVÍ“.....	48
3.2	STÁTNÍ TAJEMSTVÍ.....	48
3.2.1	Průlom v právní úpravě státního tajemství.....	49
3.2.2	Zavedení nových pojmů.....	50
3.2.3	Rozšíření klasifikace utajovaných skutečností.....	51
3.2.4	Působnost NBÚ a úkoly pro další subjekty.....	51
3.2.5	Vývoj současné právní úpravy.....	52
3.3	PLATNÁ PRÁVNÍ ÚPRAVA V ČR.....	53
3.4	NĚKTERÉ OTÁZKY OBECNĚ ZÁVAZNÉ PRÁVNÍ ÚPRAVY OCHRANY UTAJOVANÝCH INFORMACÍ.....	54
3.4.1	Co se rozumí utajovanými informacemi.....	56
3.4.2	Klasifikace utajovaných informací stupněm utajení.....	58
3.4.3	Změna nebo zrušení stupně utajení.....	59
3.4.4	Členění újmy způsobené zájmu ČR.....	60
3.4.5	Příklady skutečností, které mohou mít za následek mimořádně vážnou újmu zájmu ČR.....	61
3.4.6	Příklady, které mohou mít za následek vážnou újmu zájmu ČR.....	61
3.4.7	Příklady skutečností, které mohou mít za následek prostou újmu zájmu ČR.....	62
3.4.8	Příklady skutečností, které mohou mít za následek nevýhodnost pro zájmy ČR.....	62
3.4.9	Zajištění ochrany utajovaných informací (6 druhů).....	62
3.4.10	Bezpečnostní ředitel.....	64
3.5	PŘÍSTUP K UTAJOVANÝM INFORMACÍM.....	64
3.5.1	Vydání oznámení a osvědčení.....	65
3.5.2	Bezpečnostní řízení.....	66
3.5.3	Osobnostní způsobilost.....	69
3.5.4	Kdo má přístup k utajované informaci.....	70
3.5.5	Ověření splnění podmínek a bezpečnostní řízení.....	74
3.5.6	Bezpečnostní spolehlivost.....	79
3.5.7	Personální bezpečnost.....	81
3.5.8	Princip věcného určení a poučení.....	82
3.5.9	Problémy současné právní úpravy.....	83
3.5.10	Přístup k utajované informaci bez platného osvědčení.....	85
3.5.11	Jednorázový přístup k utajované informaci.....	86
3.6	DALŠÍ VÝZNAMNÉ OBLASTI ZAJIŠTĚNÍ OCHRANY UTAJOVANÝCH INFORMACÍ.....	87
3.6.1	Administrativní bezpečnost.....	87
3.6.2	Fyzická bezpečnost.....	90
3.6.3	Kryptografická ochrana utajovaných informací.....	91
3.6.4	Výkon státní správy v oblasti ochrany utajovaných informací (NBÚ, ZS, MV, Policie ČR).....	92

3.6.5	Státní dozor v oblasti ochrany utajovaných informací	92
3.7	SEZNAM UTAJOVANÝCH INFORMACÍ	93
3.7.1	Příklady z obecné části a seznam resortů a jiných státních orgánů, u kterých byl stanoven seznam utajovaných informací.....	93
3.7.2	Vztah obecné a zvláštní části seznamu utajovaných informací	94
3.7.3	Aplikace obecné části seznamu utajovaných informací	95
3.7.4	Původce a adresát utajovaných informací.....	96
3.7.5	Porovnání s dřívější právní úpravou	96
3.8	PŘIPRAVOVANÁ NOVELA ZÁKONA 412/2005 SB.	97
3.8.1	Důvody navrhovaných změn	97
3.8.2	Řešení komplikací při zániku platnosti osvědčení fyzické osoby	97
3.8.3	Jednotný průběh bezpečnostního řízení	98
3.8.4	Formální důvody zániku platnosti osvědčení fyzické osoby	99
3.8.5	Zjednodušení opětovného vydání osvědčení fyzické osoby	100
3.8.6	Změny ve vedení bezpečnostních svazků.....	100
3.9	POROVNÁNÍ OBECNĚ ZÁVAZNÉ PRÁVNÍ ÚPRAVY S KAŽDODENNÍ REALITOU.....	101
3.9.1	Prevence a informovanost veřejnosti	101
3.9.2	Zásadní povinnosti při ochraně utajovaných informací	101
3.9.3	Porušování základních povinností.....	102
3.10	PŘÍKLADY PORUŠOVÁNÍ OCHRANY UTAJOVANÝCH INFORMACÍ V MEDIÁLNÍ OBLASTI	105
3.10.1	Příklad podle článku „Poznatky, tvrzení a žvásty“ v týdeníku Euro ze dne 12.6.2006, autor Jan Schneider [58]	105
3.10.2	Příklad podle článku „Zabijačka na Seychelách“ v týdeníku Euro ze dne 16.10.2006, autor Jiří Pšenička [59]	107
3.10.3	Příklad podle článku „Proč BIS odposlouchávala Grosse“ v Respektu ze dne 14.4.2003, autor Jaroslav Spurný [60]	107
3.10.4	Příklad podle uveřejněných informací v kauze tzv. „Kubiceho zprávy“ na internetových stránkách ČRo1–Radiožurnálu [61].....	108
4.	ZÁVĚR	113
	EVIDENCE VÝPŮJČEK	122

PŘEDMLUVA

Tato rigorózní práce je aktualizovanou verzí mé diplomové práce, kterou jsem v lednu 2006 obhájil na Ústavu informačních studií a knihovnictví s hodnocením výborně.

Cílem této práce je především seznámení s komplexní problematikou omezení svobodného přístupu k informacím s důrazem na informace utajované. Vzhledem k velkému rozsahu tohoto tématu je práce formulována ze dvou úhlů pohledu. Prvním je celkový pohled na obecné souvislosti spojené se svobodným přístupem k informacím a zákonné možnosti jeho omezení v České republice. Druhým hlediskem je podrobný rozbor omezení přístupu k informacím prostřednictvím institutu utajovaných informací.

Rigorózní práce je proto rozčleněna do tří částí. První část je věnována aspektům obecného přístupu k informacím, druhá část pak možnostem jeho zákonného omezení, zejména při uplatnění zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Část třetí, která je pro účel práce stěžejní, pak obrací svou pozornost k institutu utajovaných informací. V této části, podobně jako v části druhé, jsou jako příklady z praxe použity a analyzovány případy uveřejněné v denním tisku.

Současný stav v oblasti utajovaných informací je poměrně málo zmapovaný a před veřejností mnohdy zbytečně tabuizovaný. Zároveň jde o sféru nebezpečně náchylnou k případnému zneužití. V obou částech jsem se zároveň pokusil o pohled do historie a základní analýzu současného stavu. Důraz je kladen na informační aspekt zároveň provázaný s právní teorií a praxí. Všeobecné informovanosti veřejnosti o existenci a zákonitostech týkajících se utajovaných informací by měla být v našem každodenním životě věnována větší pozornost.

Výběr tématu se odvíjel jak z mé dosavadní praxe v bezpečnostních složkách státu, tak z mých každodenních zkušeností

a poznatků jako obyčejného občana ČR. Některé otázky svobodného přístupu k informacím jsem konzultoval s uznávaným odborníkem na tuto problematiku, právníkem Mgr. Františkem KORBELEM, Ph.D.

Jedním z hlavních přínosů této rigorózní práce je rozbor jednotlivých povinností, oprávnění a možných důsledků jejich nedodržení, v oblasti utajovaných informací vycházejících z běžného života. V oblasti utajovaných informací není publikována téměř žádná aktualizovaná literatura a též informovanost veřejnosti je v tomto směru na velmi špatné úrovni.

V průběhu přepracování a revize mé diplomové práce na práci rigorózní, došlo k určitým doplněním a změnám, zejména co se týče části hlavní, zabývající se utajovanými informacemi. Celý text prošel podrobnou aktualizací, doplněním a úpravou daného tématu. V době dokončování textu rigorózní práce byla v závěrečném schvalovacím procesu novela zákona číslo 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tyto nejnovější změny byly v textu zohledněny.

Některé konkrétní otázky týkající se podrobností daného tématu nebylo možné detailně prozkoumat, neboť podléhají režimu utajení, případně se jedná o záležitosti řešené interními předpisy určenými jen pro vnitřní potřebu odpovědných institucí. Jako příklad mohu uvést specifické činnosti v oblasti utajovaných informací stanovené pro případy ohrožení státu.

Při zpracovávání tématu rigorózní práce jsem čerpal z dostupných informačních zdrojů, jako jsou odborné články (jak internetové, tak tradiční tištěné), knihy, právní normy, údaje ze serverů jednotlivých odpovědných institucí a v neposlední řadě z vlastních praktických zkušeností.

Použitá literatura je citována v souladu s normou ISO 690 a ISO 690-2. V textu jsou použity formulace právního jazyka a jako

hlavní informační pramen sloužily převážně zákony ČR uvedené ve sbírce zákonů ČR. Vzhledem ke značné nepřehlednosti a ztížené „čitelnosti“ textu při citaci jednotlivých právních ustanovení metodou uvedení autora a roku publikace, nebyla tato metoda použita. Citované zdroje jsou proto uvedeny metodou číselných citací v pořadí, v němž byly poprvé uvedeny, a to pomocí čísla odkazu, které odpovídá číslu záznamu v soupisu citací umístěném na konci této práce.

1. ÚVOD

Na počátku byla informace, ta informace byla všech, ta informace byla přístupná – nikoli však vždy a pro každého.

Parafrází první věty Evangelia svatého Jana s následným dovětkem, poukazují na skutečnost, že fenomén přístupu k informaci, ať už na tento pojem nahlížíme z jakéhokoli z možných úhlů pohledu, je starý jako lidstvo samo.

Šíření informací procházelo v průběhu staletí různými etapami. V těchto etapách byl přenos informací přímo i nepřímo ovlivňován jednotlivými složkami tohoto procesu: dostupností informace pro jednotlivce, rychlostí přenosu informace, jednotlivými informačními zdroji, formou informací, jejich významem a v neposlední řadě i věrohodností.

S vývojem výměny a přijímání jednotlivých sdělení vznikla i potřeba některé informace z této procedury vyloučit a omezit vybraným jedincům přístup k nim.

V proudu informací existuje několik mezistupňů, kterými musí tyto projít, než se dostanou od původce k příjemci.

Z historie známe mnoho případů, kdy bylo třeba přístup k údajům regulovat, ať už se to dělo z jakéhokoli důvodu. Pravěcí lidé chránili své poznatky před nepovolanými členy ostatních společenství zejména z důvodu vlastního přežití – informace o důležitých zdrojích potravy nebo o strategicky umístěných příbytcích byly životně důležité. V pozdějších dobách si například církve udržovala kontrolu nad informačním tokem především tím, že „kódovala“ informace do latinského jazyka a přitom ovládala proces vzdělávání. Nikdo neproověřený se latinsky učit nemohl a negramotný poddaný se

k citlivým informacím nedostal. Byl pak zcela závislý na informacích sdělených duchovními představiteli církve. Dále bychom mohli pokračovat příklady přísně střeženého tajemství výroby hedvábí ve staré Číně či balzamování mrtvých ve starém Egyptě. V moderní historii byly pak hlavními prostředky omezení informovanosti cenzura, policejní režim, informační monopoly státních tiskových agentur a v současné době hrozící absolutistická monarchie globálních mediálních konglomerátů. Dalším důvodem filtrace informací byly a jsou zájmy ochrany osobních údajů, obchodní, etické a zejména strategicko-bezpečnostní.

V následujícím textu se však budu věnovat současným zásadním způsobům a důvodům zákonného omezení svobodného přístupu k informacím v České republice, přičemž největší pozornost bude kladena na utajované informace a jejich ochranu.

„Právo na informace je nepochybně subjektivním právem každého občana. Odmítnout poskytnutí informace je možné pouze v případech zákonem výslovně stanovených. Takové odmítnutí je podle názoru Ústavního soudu rozhodnutím správního orgánu, které podléhá soudnímu přezkumu.“ [1]

[Usnesení Ústavního soudu sp. zn. III.ÚS 28/96]

2. SVOBODNÝ PŘÍSTUP K INFORMACÍM

2.1 Základy práva na informace

Právo na informace bylo poprvé zakotveno ve Všeobecné deklaraci lidských práv v roce 1948 [2]. Již v její preambuli je zmínka o významu svobody projevu přesvědčení. Dále její článek 19 zaručuje každému právo na svobodu přesvědčení a projevu, nepřipouští, aby někdo trpěl újmu pro své přesvědčení a zahrnuje právo vyhledávat, přijímat a rozšiřovat informace a myšlenky jakýmkoli prostředky a bez ohledu na geografické hranice.

Velkým průkopníkem v této oblasti byly Spojené státy americké (dále jen USA). V roce 1966 podepsal tehdejší americký prezident Lyndon Johnson zákon o svobodě informací pojmenovaný Freedom of Information Act (dále jen FOIA), od kterého se odvíjí současné pojetí práv občana na přístup k informacím správních orgánů nejen v USA, ale možno říci, i v celém zbývajícím demokratickém světě [3]. V roce 1996 podepsal prezident Bill Clinton novelu informačního zákona, podle níž musejí být všechny vládní a obdobné informace přístupné v digitální podobě, a to v režimu online. Na základě výše zmíněných dokumentů má každý občan USA právo získat, až na zákonem

vymezené výjimky, jakákoli data od všech institucí placených z veřejných prostředků. Týká se to nejen vládních či městských úřadů, ale i policie, nejrůznějších nevládních organizací nebo dobročinných nadací.

„Právo svobodně vyhledávat, přijímat a šířit informace bez ohledu na státní hranice je přinejmenším v pasivním smyslu elementární součástí ideálu lidské svobody“ [4, s. 46]. Právo na informace v tomto smyslu proto někteří autoři nazývají raději svobodou informací, než právem, čímž je lépe vyjádřen subjektivní poměr k jejímu nositeli a třetím osobám, případně svobodou komunikace, pokud chceme do jednoho pojmu zahrnout svobodu projevu, svobodu získávání informací a svobodu rozšiřování informací [5].

2.2 Historie svobody informací v ČR

V zemích dřívější Rakousko-uherské monarchie ani v novodobé historii českého státu, počínaje obdobím první a druhé republiky, německého protektorátu, let 1945 – 1948 a doby komunistického režimu až do konce 20 století, neexistovala komplexní právní úprava práva na informace a povinnosti státních orgánů, orgánů samosprávy, případně jiných osob informace poskytovat.

Teprve změna politické a společenské situace po roce 1989 nastolila do popředí otázky svobodného přístupu k informacím, a to s ohledem na předchozí deficit možná silněji, než kde jinde.

Tento trend byl ve filozofické a státoprávní rovině započat zejména přijetím ústavního zákona Federálního shromáždění č. 23/1991 Sb., uvozujícího Listinu základních práv a svobod s účinností od 8.2.1991. Tímto zákonem bylo poprvé v síle ústavního, resp. nadústavního zákona deklarováno právo veřejnosti na informace, jimiž disponují orgány veřejné moci [6, s. 16-17].

2.3 Právní úprava poskytování informací

2.3.1 Současná obecná právní úprava poskytování informací v ČR

Svoboda projevu a právo na informace je v Listině základních práv a svobod (dále jen Listina), která byla usnesením předsednictva ČNR začleněna do ústavního pořádku ČR, zařazeno na první místo mezi právy politickými (článek 17 odst. 1 Listiny). Společným znakem politických práv a svobod je umožnit zejména fyzickým osobám účast na správě věcí veřejných v celostátním i místním měřítku. Žádné ze zakotvených politických práv se nenachází v režimu čl. 41 odst. 1 Listiny (omezující některá práva) a lze je proto v zásadě realizovat bezprostředně, již na základě ústavní úpravy. Pro právo na informace to platí bezvýhradně [7].

Všem státním orgánům a orgánům územní samosprávy Listina v čl. 17 odst. 5 ukládá, aby přiměřeným způsobem poskytovaly informace o své činnosti. Podrobnosti a podmínky poskytování informací dále upravují zvláštní zákony, jako například Zákon č. 123/1998 Sb., o právu na informace o životním prostředí [8] a zákon č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen zákon č. 106/1999 Sb.). Před přijetím těchto zákonů existovala jen dílčí úprava v některých oblastech, která však platí povětšinou i v současnosti. Jde např. o ustanovení § 8a trestního řádu [9], který stanoví, že orgány činné v trestním řízení mají prostřednictvím hromadných sdělovacích prostředků poskytovat veřejnosti informace o své činnosti. Přitom však nesmí ohrožovat zejména objasnění věci v trestním řízení. Zákon ČNR č. 6/1993 Sb., o České národní bance [10], ve znění pozdějších předpisů, ukládá tomuto orgánu, aby nejméně jednou za tři měsíce informoval veřejnost o měnovém vývoji a zpravidla dvakrát ročně podávat Poslanecké sněmovně zprávu o měnovém vývoji. Českému statistickému úřadu je v zákoně č. 89/1995 Sb., o statistické službě [11], ve znění pozdějších předpisů, mimo jiné uloženo, aby seznamoval veřejnost prostřednictvím

hromadných sdělovacích prostředků, vlastními publikacemi a jinými médii s výsledky statistických zjišťování, a to ve lhůtách, rozsahu a způsobem, které předem oznámí ve sdělovacích prostředcích, vlastních publikacích a jiných médiích.

Obdobně podle zák. č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů [12], ve znění pozdějších předpisů, má Státní úřad pro jadernou bezpečnost přiměřeným způsobem informovat veřejnost o výsledcích své činnosti a jednou ročně vypracovat zprávu o své činnosti, kterou předkládá vládě a veřejnosti.

Výroční zprávu o vlastní kontrolní a jiné činnosti vypracovává také Nejvyšší kontrolní úřad a předkládá ji Parlamentu, vládě a uveřejňuje ve svém Věstníku (zák. č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, ve znění pozdějších předpisů [13]). Podobně je upravena informační povinnost Úřadu pro ochranu osobních údajů, který je povinen Poslanecké sněmovně, Senátu a vládě podávat výroční zprávu o kontrolní činnosti a zhodnocení stavu v oblasti ochrany zpracování a ochrany osobních údajů a publikovat ji ve svém Věstníku (zák. č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů [14]).

Povinnost informovat veřejnost o své činnosti má také Veřejný ochránce práv (zákon č. 349/1999 Sb. [15]), který má kromě vypracování výroční zprávy pro příslušné státní orgány (Poslanecká sněmovna, Senát, prezident republiky, vláda, ministerstva a jiné správní úřady) soustavně seznamovat veřejnost se svou činností a poznatky, které z ní vplynuly. Všeobecně pak ministerstva a jiné ústřední správní úřady mají povinnost přiměřeným způsobem informovat veřejnost o návrzích závažných opatření.

Dále např. dle zákona č. 309/1991 Sb., o ochraně ovzduší před znečišťujícími látkami (zákon o ovzduší), mají orgány ochrany ovzduší povinnost zpřístupňovat včasné a úplné informace o kvalitě ovzduší

a podílu jednotlivých zdrojů na jeho znečištění a vždy jsou povinny informovat veřejnost v případě smogové situace [16].

2.3.2 Formálnost stávající právní úpravy

Zmíněná ustanovení jsou však podle některých názorů většinou spíše jen formální, protože nikde není stanoveno, jaký právní důsledek bude mít nedodržení informační povinnosti. V krajním případě by snad mohla být vůči vedoucímu činiteli uplatněna odpovědnost politická, pracovněprávní či služební, tedy jeho odvolání z funkce, rozvázání pracovního poměru nebo disciplinární postih. Je ale málo pravděpodobné, že by se tak stalo, zvláště půjde-li o ojedinělý případ.

Podle ojedinělých názorů zde nepřichází v úvahu možnost podání opravného prostředku k vyšší instanci, tím méně pak žaloba podle předpisů o správním soudnictví. Tento názor je však v rozporu s usnesením Ústavního soudu vedeného pod spisovou značkou III.ÚS 28/96 [1].

2.4 Zákon o svobodném přístupu k informacím

2.4.1 Zajištění práva občanů na informace

Nejvýznamnější průlom do zajištění práva občanů na informace mělo přinést přijetí zákona č. 106/1999 Sb., o svobodném přístupu k informacím [17], ve znění pozdějších předpisů. Schvalování této zákonné normy bylo velmi komplikovaným procesem. Výsledkem byl předpis, dle názorů části odborné veřejnosti, poměrně nedokonalý jak po stránce obsahové, tak z hlediska legislativně-technického. Jde o zákon, který má povahu obecné úpravy, a použije se tedy pouze tam, kde není stanovena úprava zvláštní.

Tento zákon je komplexním předpisem, který upravuje všechny základní aspekty práva na informace, tj. především povinnost aktivní publikace informací a poskytování informací na žádost. Vedle povinnosti poskytovat informace stanoví úplným výčtem i důvody pro odepření informací, a tím naplňuje prakticky celé právo na informace [4, s. 42].

2.4.2 Pojem „informace“ z hlediska zákona č. 106/1999 Sb.

V § 3 zákona č. 106/1999 Sb. byl novelou tohoto zákona zpřesněn pojem informace (nejde však o definici tohoto pojmu). Stanoví se, že *„za informaci se považuje jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního“* [17]. Toto ustanovení má vést k odstranění dosavadních obstrukcí některých úřadů odepírat zvukové či obrazové záznamy

s odůvodněním, že nejde o informace. Současně je výslovně stanoveno, že počítačové programy informacemi ve smyslu tohoto zákona nejsou.

2.4.3 Subjekty práva na informace

Jak vyplývá již z čl. 42 odst. 2 Listiny, oprávněným subjektem práva na informace se rozumí každá fyzická či právnická osoba, pokud se na ni jakýmkoli způsobem vztahuje právní řád České republiky (např. dle zásady teritoriality) [18]. Zákon nijak dále způsobilost oprávněného neupravuje, takže lze dovodit, že povinný subjekt (viz níže) má povinnost vyhovět žádosti osoby v jakémkoli postavení i věku (tedy i nezletilému).

2.4.4 Povinné subjekty

Povinným subjektem se podle tohoto zákona rozumí předně státní orgány a orgány územní samosprávy, které mají podle zákona 106/1999 Sb. povinnost poskytovat informace vztahující se k jejich působnosti.

2.4.5 Další subjekty

Povinnými subjekty jsou rovněž ti, jimž zákon svěřil rozhodování o právech, právem chráněných zájmech a povinnostech fyzických či právnických osob v oblasti veřejné správy. Na rozdíl od předchozích, je jejich informační povinnost výslovně omezena toliko na rozhodovací činnosti. Těmito dalšími subjekty mohou být soukromé fyzické a právnické osoby, jimž zákon svěřil rozhodování (např. tzv. veřejné strážce, soukromé školy nebo Český normalizační institut), orgány zájmové samosprávy (vysoké školy, profesní komory) a jiné. Zákon se výslovně nevztahuje na poskytování osobních údajů

a informací podle zvláštního zákona. Z toho plyne, že pokud jsou údaje poskytovány podle zvláštního zákona (např. obligatorně zveřejňovány nebo jsou součástí evidencí veřejně přístupných), úprava zákona č. 106/1999 Sb. nepřichází v úvahu. Jde-li o osobní údaje, platí pro jejich poskytování režim podle zákona č. 101/2000 Sb.

2.4.6 Žadatel

Žadatelem je dle zákona č. 106/1999 Sb. každá fyzická a právnická osoba žádající o informaci. Stejně jako předchozí, ani tento zákon nerozlišuje mezi tím, zda jde o českého státního občana nebo cizince, resp. českou nebo zahraniční právnickou osobu. Také zde platí, že žádost nemusí být nijak odůvodněna a nemusí být prokazováno, k jakému účelu je informace požadována.

2.4.7 Vymezení pojmu zveřejňované informace

Zveřejněná informace je zde vymezena jako taková, která může být vždy znovu vyhledána a získána, zejména vydaná tiskem nebo na jiném nosiči dat, který umožňuje zápis a uchování informace, vystavená na úřední desce, informace dosažitelná dálkovým přístupem nebo umístěná ve veřejné knihovně. Obecná definice samotné zveřejňované informace, případně definice informace, která má být poskytnuta, v zákoně chybí.

V doslovném významu termínu "*informace*" lze spatřovat např. jednotku znalosti (vědomosti), která je pravdivá *per definitionem*, tj. vždy. Jak však uvádí V. Pavlíček v komentáři publikace Ústava a ústavní řád České republiky: „*Nepřavdivá nemůže být informace, ale jen zpráva. Taková zpráva však nepřináší informaci, ale dezinformaci*“ [19, s. 181].

Z ustanovení, které vymezuje množinu povinných subjektů, je však zřejmé, že informací, jež má být po splnění zákonných předpokladů poskytnuta, je jakákoli informace vztahující se k působnosti těchto povinných subjektů, případně k jejich činnosti rozhodovací [20, s. 62].

Všem povinným subjektům je uloženo, aby za účelem informování veřejnosti zveřejnily ve svém sídle a úřadovnách, na místě všeobecně přístupném, stanovený okruh informací. Velmi názorně tento institut popisuje J. Hřebejk v díle Ústava a ústavní řád ČR, kde na straně 185 uvádí: „*Pojetí odst. 5 čl. 17 Listiny znamená i právo veřejnosti očekávat, že jí informace o činnosti orgánů veřejné moci bude poskytnuta, že tyto informace si najdou veřejnost samy, nikoli tak, že veřejnost musí tyto informace aktivně vyhledávat*“ [21, s. 185].

V zákoně 106/1999 Sb. je tato povinnost definována následovně:

„Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon“ [17].

Tento odstavec tak stanoví, že úřady musejí samy od sebe (aniž jsou dotázány) poskytovat informace o své činnosti. Přiměřený způsob tohoto automatického poskytování stanoví zákon č. 106/1999 Sb. v § 5.

2.4.8 Nepravdivá informace

Subjekty práva na informace však často nemají příliš možností, jak si ověřit, je-li informace, kterou obdržely, pravdivá. Existuje několik případů, kdy povinný subjekt poskytne informace nepravdivé. Jedná se například o případy, kdy mají tyto informace zakrýt protiprávní chování. Pokud občan při získání lživé informace rozpozná její nepravdivost, může to považovat za neposkytnutí informace a postupovat podle zákona č. 106/1999 Sb.

2.5 Restrikce práva na informace

Ústavní omezení práva na informace je vyjádřeno v čl. 17 odst. 4 Listiny tak, že právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro:

- ochranu práv a svobod druhých,
- bezpečnost státu,
- veřejnou bezpečnost,
- ochranu veřejného zdraví,
- ochranu mravnosti.

Jakékoli omezení práva na informace musí tedy splňovat formální a materiální podmínky, přičemž formální podmínkou je konkrétní ustanovení zákona, materiální podmínkou je nezbytnost příslušného omezení v demokratické společnosti pro některý z taxativně, leč co do obsahu značně všeobecně, vyjmenovaných účelů. Obě podmínky musí být splněny kumulativně [4].

Výjimkou z posuzování formálních a materiálních podmínek jsou některá ustanovení samotné Listiny, která sledují opačný zájem než čl. 17 Listiny, tj. ochranu před nežádoucím vyhledáváním a šířením informací, kterými jsou zejména:

- čl. 7 odst. 1 (nedotknutelnost osoby a jejího soukromí),
- čl. 10 odst. 1, 2 (obecná ochrana osobnosti),
- čl. 10 odst. 3 (ochrana osobních údajů),
- čl. 12 odst. 3 (nedotknutelnost obydlí),
- čl. 13 (listovní tajemství).

Poskytování, šíření a jiné operace s informacemi, které by se mohly se dotknout výše uvedených ústavně chráněných zájmů, jsou a priori nepřípustné [4].

V každém případě ale platí, že veškerá omezení práva na informace musí mít formu zákona. Jinými slovy, neexistuje-li zákon, který zakazuje veřejné moci poskytovat informace z důvodů obsažených buď v Listině, nebo v mezinárodních smlouvách, není veřejná moc oprávněna informace neposkytnout s odkazem kupř. na Listinu základních práv a svobod samotnou, nebo na omezovací klauzule v mezinárodních smlouvách, neboť tyto omezovací klauzule nejsou tzv. *selfexecuting*, tedy *samovykonávací*. Právě omezovací klauzule musí být zásadně provedeny zákonem, a to na rozdíl od práva na informace jako subjektivního veřejného práva, které je podle moderní poválečné teorie (a v některých poválečných ústavách je to explicitně stanoveno), přímo použitelným právem [22].

2.5.1 Formulace omezení ve zvláštních zákonech

Formulace ve zvláštním zákonu jsou dvojího typu: buď pozitivní (když se určité informace poskytnou určitému okruhu osob, určitým způsobem apod.), anebo negativní (když se určité informace za určitých okolností neposkytnou).

Pozitivní formulace

Neomezují rozsah poskytnutých informací podle obecného zákona, naopak ho buď rozšiřují anebo mění a doplňují způsob poskytnutí informací (proces, technický způsob poskytnutí).

Jako příklad uvádějí autoři publikace *Svoboda informací: Svobodný přístup k informacím v právním řádu České republiky*, Oldřich KUŽÍLEK a Michael ŽANTOVSKÝ následující situaci:

Správní řád (zde v postavení zvláštního zákona) stanoví, že „*účastníci řízení mají právo nahlížet do spisů*“. Z toho však nelze dovodit, že ostatním žadatelům o informaci (ne-účastníkům řízení) budou všechny informace ve spise odepřeny z titulu „*neúčastnictví*“ [23]. Mohou jim být odepřeny jen ty informace, u kterých to plyne z jejich vlastní charakteristiky (například jde o osobní údaje anebo o informace nehotové). Správní řád zde jen rozšiřuje právo účastníka správního řízení tak, že se může s informací seznámit přímo nahlédnutím, zatímco běžný žadatel o informaci se musí spokojit s takovým způsobem poskytnutí, který zvolí úřad (například předání fotokopie či opisu části určitého dokumentu ze spisu).

Podle těchto autorů nelze účastníka řízení také omezit při přístupu k informacím z hlediska těch charakteristik informací obsažených ve spise, které jsou jinak chráněny v zájmu nestranného průběhu řízení (tedy zejména informace charakterizované jako nehotové, „*nově vznikající*“ anebo jako osobní údaje samotného účastníka. Je to pochopitelné, protože každý zákon musíme posuzovat z hlediska jeho účelu. Účelem zákona o správním řízení je zajištění nestranného a spravedlivého procesu účastníků (dává jim tedy záruky co do možnosti nejen nahlížet do spisu, ale i přidávat do něj další dokumenty, mít zajištěný režim doručení písemností a další procesní záruky). „*Jeho účelem však není úprava přístupu k informacím. Proto nelze k tomuto nesprávnému účelu překrucovat jeho některé pasáže*“ [23, s. 25].

Negativní formulace

Negativní formulace zvláštního zákona znamenají, podle autorů publikace Svoboda informací: Svobodný přístup k informacím v právním řádu České republiky, něco jiného. „*Jedině ony mohou omezit rozsah poskytnutých informací podle obecného zákona pro dané podmínky (například pro oblast informací z daňového řízení)*“ [23].

Praktický příklad nesprávného omezení svobody informací

K výše uvedenému je třeba uvést ilustrativní příklad aplikace zmíněného omezení základních lidských práv na informace. Jedná se o situaci kolem výkladu úředníků ministerstva dopravy ČR a dopravní policie ČR k používání „pasivních“ antiradarů (tzn. takových, které svou funkcí nemohou fyzikálně ovlivnit jakékoli elektromagnetické, optické či jiné technické prostředky), kteří se snaží po svém interpretovat ustanovení silničního zákona [24], kde se v § 3 odst. 4 stanovuje:

„Nikdo nesmí používat technické prostředky a zařízení, která znemožňují nebo ovlivňují funkci technických prostředků používaných policií nebo Vojenskou policií při dohledu na bezpečnost provozu na pozemních komunikacích (dále jen antiradar)“.

Podle názoru výše zmíněných úředníků se funkcí technických prostředků nemyslí pouze funkce technická, ale také funkce kontrolní. Taková logika však při podrobnějším zkoumání neobstojí.

Velmi pěkně v článku „Chodí pešek okolo... antiradaru“ v Mladé frontě Dnes tuto situaci popisuje O. KUŽÍLEK, spoluautor zákona 106/1999 Sb. o svobodném přístupu k informacím a poradce pro otevřenost veřejné správy:

„Podívejme se na pasivní antiradar očima základních občanských svobod. Jde o jedno ze stovek technických zařízení, která monitorují fyzikální či chemické prostředí okolo nás a zjištěné informace činí vnímatelné nedokonalými lidskými smysly. Například teploměr, barometr, měřič emisí, ale pro některé lidi také obyčejné brýle či naslouchátko. Jde tedy jen o pomůcku umožňující přijímat různé typy informací z vnějšího prostředí, na které smysly nestačí. Listina základních práv a svobod uvádí tři formy ‘pohybu’ informací: každý má právo je vyhledávat, přijímat a rozšiřovat. Ovšem jen dvě z nich – právo vyhledávat a šířit informace – lze za velmi úzkých

podmínek omezit zákonem. To třetí, právo informace přijímat, omezit nelze vůbec nijak a nikdy. Zákon, který by omezil občana ve svobodě přijímat informace, které už k němu putují, by byl protiústavní“ [25, s. 6].

2.5.2 Další omezení práva na informace

Dále pak zákon č. 106/1999 Sb. obsahuje jistá omezení práva na informace. Veřejnost nemá nárok na utajované informace, informace podléhající ochraně osobnosti a soukromí, obchodní tajemství (neplatí tam, kde jde o použití prostředků ze státního rozpočtu, rozpočtů územních celků nebo fondů zřízených zákonem, jakož i nakládání s majetkem těchto subjektů, a to pokud se týká informací o rozsahu a příjemci těchto prostředků) a informace o důvěrných majetkových poměrech osob.

Kromě toho není možno poskytnout informace, které vznikly bez použití veřejných prostředků, a které byly předány osobou, jež takovou povinnost podle zákona nemá, ledaže by k tomu dala souhlas. Neposkytují se také informace o probíhajícím trestním řízení, rozhodovací činnosti soudů (nikoli však správních orgánů), plnění úkolů zpravodajských služeb a přípravě, průběhu a projednávání výsledků kontrol Nejvyššího kontrolního úřadu.

2.5.3 Technická podoba omezení přístupu k vybraným informacím

Omezení lze provést jedině tak, že úřad z informací vypustí nejužší oddělitelnou část informace, která skutečně nese znaky, díky kterým ji lze odepřít (např. osobní údaj, obchodní tajemství). Zbytek musí poskytnout. Pokud tedy určitý dokument, třeba usnesení obecní rady, obsahuje osobní údaje konkrétní osoby, musí úřad tuto pasáž

z celého usnesení vypustit (usnesení překopírovat po zakrytí citlivé pasáže, nebo ostatní text přepsat s vynecháním chráněných údajů) a zbylé informace poskytnout.

Není možné odepřít celý širší dokument jen proto, že v něm na některém místě je chráněný údaj.

Přípustný je však takový rozsah omezení, který bere ohled na možnost doplnit vypuštěnou chráněnou informaci bez zvláštního úsilí pomocí jiných, veřejně přístupných souborů informací. Pak je přijatelné rozšířit okruh omezení tak, aby takové snadné doplnění nebylo možné. Na druhé straně zákon bere v úvahu nesnadnost rekonstrukce odepřené informace ustanovení § 4 písmo a) zákona č. 101/2000 Sb., o ochraně osobních údajů: „*O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků*“ [26].

2.5.4 Osobní údaje a jejich ochrana

Zákon č. 101/2000 Sb., o ochraně osobních údajů, definuje „*osobní údaje*“ jako jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu.

Osobním údajem může být jedna informace nebo i kombinace více informací najednou (v případech, kdy není možné zjistit totožnost osoby z jediného údaje).

Nejtypičtějším osobním údajem je jméno, příjmení, trvalé bydliště, podobenka a rodné číslo, pokud je z jejich vzájemného kontextu nebo ze situace určený či určitelný jejich nositel (subjekt).

Zvláštním druhem osobních údajů jsou „*citlivé údaje*“. Jedná se o osobní údaje vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích,

náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě.

Ustanovení § 2 odst. 3 zákona č. 106/1999 Sb. stanoví, že se zákon nevztahuje na poskytování osobních údajů a informací podle „*zvláštního právního předpisu*“. Tímto zvláštním právním předpisem vůči zákonu o svobodném přístupu k informacím je právě zákon č. 101/2000 Sb., o ochraně osobních údajů, v platném znění [26].

2.5.5 Omezení přístupu k písemnostem osobní povahy

Specifickou kapitolu tvoří právo přístupu k „*písemnostem osobní povahy*“. Jako příklad lze uvést právo na získání kopií lékařských zpráv zemřelého pozůstalým příbuzným. Na ochranu lékařské dokumentace se vztahuje ustanovení § 67 odst. 9 písm. b zákona č. 20/1966 Sb., o péči o zdraví lidu: „*Práva a povinnosti při zpracování osobních údajů souvisejících se zajišťováním zdravotní péče se řídí zvláštním zákonem*“. Zároveň § 12 Občanského zákoníku stanoví, že: „*Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejich projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením*“.

Po smrti fyzické osoby se však totožný údaj ve zdravotní dokumentaci mění z „*osobního údaje*“ chráněného zákonem č. 101/2000 Sb., v „*písemnost osobní povahy*“, chráněnou ustanovením § 15 Občanského zákoníku: „*Po smrti fyzické osoby přísluší uplatňovat právo na ochranu její osobnosti manželu a dětem, a není-li jich, jejím rodičům*“. Fakticky tedy jde o uplatňování práva na ochranu osobnosti zemřelého, do kterého spadá i souhlas s použitím písemností osobní povahy.

Jak k uvedené problematice připomíná autor článku Právo na kopie zdravotní dokumentace [27]: „*Nelze oponovat ani § 67b odst 10*

zákona o zdraví lidu, v němž se vyjmenovává, kdo smí do zdravotnické dokumentace nahlížet, přičemž pozůstali zde uvedeni nejsou. Zde je nutno zdůraznit, že v zásadě jde o právní vztah, kterým se realizuje základní právo dle čl. 17 Listiny – přístup k informacím – za velmi specifických okolností, kdy je úzce vymezena nejen informace, ale i osoba, jejíž přístup k informaci se posuzuje (pozůstalý). Obecně platí, že omezení přístupu k informacím musí mít povahu negativního výroku, vylučujícího přístup dané osoby (okruhu osob) k dané informaci (okruhu informací). Musí jít o tzv. negativní formulaci (neposkytne se, neumožní se přístup, nesmí nahlížet, anebo poskytne se jen (výhradně) tomu, kdo... apod.) Naopak tzv. pozitivní formulace, umožňující přístup k informaci určitého okruhu osob, nemůže znamenat omezení přístupu pro ostatní“ [27].

Ve výše uvedeném případě tedy omezení přístupu k „písemnostem osobní povahy“, které představuje zdravotnická dokumentace, je pro všechny osoby dáno uvedeným ustanovením Občanského zákoníku § 12 odst. 1, a je tedy vázáno na souhlas osoby. U zemřelé osoby tento souhlas může dát jen manžel a děti, a není-li jich, rodiče. To je tedy základní omezovací klauzule. Vůči ní, jako rozšíření možnosti nahlížet, stojí jako speciální ustanovení uvedený § 67b odst. 10 zákona o zdraví lidu, umožňující i bez tohoto souhlasu pozůstalého nahlížet do dokumentace lékařům a dalším vyjmenovaným, v zásadě zdravotnickým osobám [27]. Aplikace pojmu „osobní údaj“ v souvislosti s poskytováním informací zůstává však v mnoha směrech otevřenou otázkou.

2.5.6 Obchodní tajemství

Obchodní tajemství je definováno v zákoně č. 513/1991 Sb., obchodní zákoník [28]. Informace může být oprávněně označena za obchodní tajemství, jen když splní zároveň všechny stanovené znaky podle § 17 obchodního zákoníku:

- jde o skutečnosti obchodní, výrobní či technické povahy, které mají alespoň potenciální materiální či nemateriální hodnotu,
- nejsou v příslušných obchodních kruzích běžně dostupné a mají být podle vůle podnikatele utajeny,
- podnikatel odpovídajícím způsobem jejich utajení zajišťuje.

Ve vztahu k náležitostem obchodního tajemství však žadatel o poskytnutí informací nemá možnost efektivně zkontrolovat, zda údajné obchodní tajemství skutečně znaky uvedené v zákoně má. Pokud se tedy chce bránit proti odepření informace, odůvodněnému ochranou obchodního tajemství, má šanci odstranit všechny pochybnosti až v případném soudním řízení.

Povinnosti podnikatele

Při uplatnění práva přístupu k informacím ve veřejné správě je prvořadá povinnost podnikatele aktivně a z vlastní iniciativy předmět svého obchodní tajemství chránit. Například při uzavření smlouvy s povinným subjektem (orgánem veřejné moci, který má uloženou informační povinnost) musí označit skutečnosti zmíněné ve smlouvě a dokumentaci, které pokládá za obchodní tajemství.

Charakteristika obchodního tajemství z pohledu zákona č. 106/1999 Sb. tedy vyžaduje, v návaznosti na znění § 17 obchodního zákoníku, že informace bude pro oprávněné omezení přístupu k ní z důvodu ochrany obchodního tajemství podnikatelem takto označena.

Povinnosti úřadu

Každý úřad má obecnou povinnost postupovat na základě skutečných ověřených faktů, v rámci které musí např. při uzavírání smluv prověřit pravdivost podnikatelem deklarovaných skutečností. Je tedy odpovědný za to, že uvedené obchodní tajemství splňuje všechny náležitosti podle § 17 obchodního zákoníku.

Označit obsah obchodní smlouvy za obchodní tajemství, které svědčí ve prospěch daného podnikatele, v žádném případě nemůže tedy úřad.

2.5.7 Ochrana duševního vlastnictví

Mnoho informací může také podléhat ochraně duševního vlastnictví. Jde především o ochranu autorskou, ale také o ochranu průmyslových vzorů a další typy ochrany. Povinný subjekt potom při poskytování informací nesmí porušit takto stanovenou ochranu informace.

Ustanovení zákona č. 106/1999 Sb. před poslední novelizací uskutečněnou v loňském roce, neumožňovalo poskytnout informaci, která je předmětem ochrany podle autorského zákona [29]. Nyní platí omezení jen u taxativně vymezeného výčtu povinných subjektů, zejména provozovatelů rozhlasového a televizního vysílání, veřejných knihoven a kulturních a vědeckých institucí (u nich by takový postup vlastně suploval či obcházel jejich běžnou formu poskytování, jako je půjčování knih v knihovnách či vysílání filmů v televizi). Ostatní povinné subjekty jsou omezeny ve výdeji informací tohoto druhu, pouze pokud by tím byla porušena ochrana práv třetích osob. Jestliže však povinný subjekt sám vykonává práva, která mu umožňují nakládat s informací chráněnou podle autorského práva, pak je povinen tuto informaci poskytnout.

Způsob poskytování informací tohoto druhu upravuje jednak nově doplněné ustanovení § 14a o licenční nebo podlicenční smlouvě zákona č. 106/1999 Sb. a v ostatním autorský zákon. V zásadě to znamená, že úřad uzavře se žadatelem smlouvu o poskytnutí těchto autorsky chráněných informací. Obsahem smlouvy bude zpravidla požadavek, aby žadatel tyto informace dále nešířil komerčně. Úhrada by měla být v zásadě stejná, jako při běžném poskytování informací, tedy jen za materiálové náklady. Zákon však připouští, aby byla požadována i úhrada, odpovídající nákladům, které povinný subjekt vynaložil na získání majetkových práv k autorsky chráněným informacím [30].

2.5.8 Ochrana důvěrnosti majetkových poměrů

Všechny informace, které úřady získaly od fyzických či právnických osob (např. občanů, firem) v rámci daňového řízení, řízení o výběru poplatků, v rámci řízení o penzijním nebo zdravotním pojištění či sociálním zabezpečení, nelze poskytnout. U fyzických osob je část těchto informací již chráněna jako osobní údaje. V § 10 zákona č. 106/1999 Sb. se obdobná ochrana rozšiřuje i na právnické osoby, ale nikoli z hlediska vlastní charakteristiky informace jako osobního údaje, ale z hlediska způsobu, jak byla informace získána.

2.5.9 Podmíněně předané informace

Úřad nesmí poskytnout informaci, kterou mu někdo „dobrovolně“ předal (aniž mu to zákon ukládal), a přitom nedal souhlas s jejím dalším předáváním. Jako příklad lze uvést stížnost občana na podnik, poškozující životní prostředí. Úřad pak nemůže sdělit (podle zákona č. 106/1999 Sb.), kdo tuto stížnost podal.

2.5.10 Časové omezení odepření informací

Trvání jakéhokoliv odepření informací je ohraničeno dobou, po kterou trvá důvod odepření informací. Neexistuje-li v době vyřizování žádosti o informace důvod pro jejich odepření, informace musí být poskytnuty bez ohledu na to, že takový důvod v minulosti existoval. Často se může jednat například o poskytování informací, které byly v minulosti odepírány z důvodu ochrany obchodního tajemství. Existence obchodního tajemství totiž není konstantní, neboť se může měnit během času v souvislosti s vědeckotechnickým pokrokem i změnami ve společnosti či úplně zaniknout [4].

Existenci konkrétního obchodního tajemství nelze dovodit pouze z § 9 zákona č. 106/1999 Sb., ale musí být posuzována především z hlediska § 17 obchodního zákoníku, zda jsou kumulativně splněny všechny uvedené náležitosti.

2.5.11 Priorita vyššího zájmu

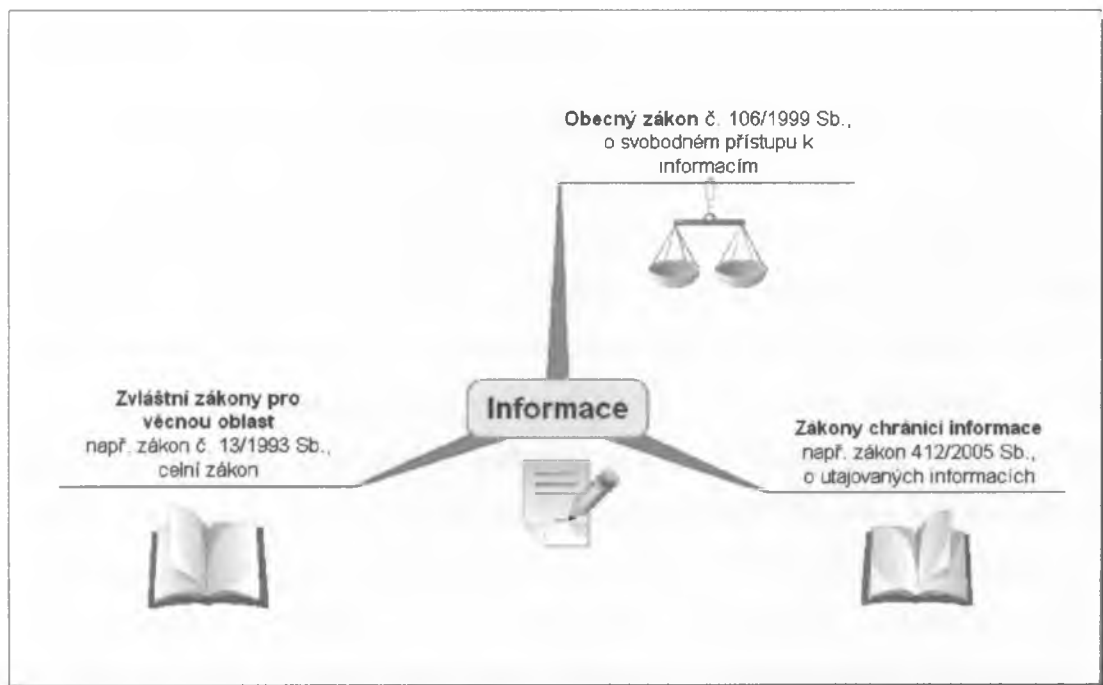
Pokud jde o vztah mezi utajovanými a zvláštními skutečnostmi (informacemi), popř. jinými instituty, které mají charakter skutečností podléhajících režimu tajemství (např. obchodní tajemství), nelze vyloučit případy, kdy určitá skutečnost (informace) bude splňovat oba znaky a bude současně jak informací utajovanou, tak např. obchodním tajemstvím nebo zvláštní skutečností. V takovém případě bude ochrana a zabezpečení informace prováděna způsobem a podle předpisů, které upravují utajované informace, neboť zde platí priorita vyššího zájmu [31].

2.6 Vztah zákona č. 106/1999 Sb. k jiným zákonům

Podle právního názoru autorů publikace Svoboda informací: Svobodný přístup k informacím v právním řádu České republiky,

Oldřicha Kužílka a Michaela Žantovského, musíme s ohledem na zásady uvedené výše a při rozboru toho, zda konkrétní informace má či nemá být poskytnuta, uvážit alespoň tři hlediska (viz obr. 1):

1. hledisko obecného zákona (č. 106/1999 Sb.),
2. vliv zvláštního zákona (nebo ustanovení zákona) upravujícího ochranu některých informací před volným přístupem k nim (např. zákona o ochraně utajovaných informací, o ochraně osobních údajů, ustanovení o obchodním tajemství obchodního zákoníku, ustanovení o telekomunikačním tajemství zákona o telekomunikacích [32], ustanovení o bankovním tajemství zákona o bankách [33]),
3. vliv zákona upravujícího danou věcnou problematiku, kterých je téměř nekonečné množství (např. posouzení přístupu k informaci z činnosti celní služby podle zákona celního k informaci z činnosti Senátu to bude podle jednacího řádu Senátu, k informaci o veřejné zakázce zákon o zadávání veřejných zakázek apod.) [23].



obr. 1: Vztahy jednotlivých druhů zákonů

© 2006 Jaroslav Hora

Při tomto posouzení platí zásada, že zvláštní zákon má přednost před obecným zákonem. Tuto přednost však nelze přehnaně vyložit tak, že by zvláštní zákon omezil přístup k informacím jen na rozsah, upravený zvláštním zákonem. To by bylo možné jen tehdy, pokud by tento zvláštní zákon výslovně vyloučil jakékoliv jiné poskytnutí informací v dané oblasti [23].

Charakteristika informace podle obecného zákona č. 106/1999 Sb.

Základní charakteristiky informací, kvůli kterým může být jejich poskytnutí omezeno, jsou uvedeny v omezovacích ustanovení zákona, tedy v §§ 7–11 základního (obecného) zákona č. 106/1999 Sb. Tato omezovací ustanovení buď formulují požadované charakteristiky informace přímo, anebo se odkazují na tyto charakteristiky ve zvláštních zákonech chránících informace.

Charakteristika informace podle zvláštního zákona chránícího informace

Některé charakteristiky informací, kvůli kterým je možno či nutno omezit jejich poskytování, jsou obsaženy ve zvláštních omezujících zákonech, jako je například zákon č. 101/2000 Sb., o ochraně osobních údajů, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákon č. 40/1964 Sb., občanský zákoník [34] v ustanovení o ochraně osobnosti, zákon č. 513/1991 Sb., obchodní zákoník [28] v ustanovení o obchodním tajemství, zákon č. 151/2000 Sb., telekomunikační zákon v ustanovení o telekomunikačním tajemství, zákon č. 21/1992 Sb., o bankách [33] v ustanovení o bankovním tajemství a podobně. Obecný zákon č. 106/1999 Sb. na ně často přímo odkazuje. Při odepření informace na ně úřad musí poukázat ve zdůvodnění svého rozhodnutí.

Charakteristika informace podle zvláštního zákona pro věcnou oblast

Na informaci se vztahuje také režim podle oblasti, v níž se informace vyskytuje, např. stavební řízení, potravinářská inspekce apod. [23].

2.7 Žádost o přístup k informacím a možnosti jejich odepření

Výlukami z poskytování informací však nejsou dotčena ustanovení zvláštních zákonů o poskytování informací (např. podle § 8a trestního řádu) [9]. Veškerá omezení práva na informace je však třeba uplatňovat v co možná nejmenším rozsahu. Požadované informace, a to včetně doprovodných, které úzce souvisí s požadovanými informacemi, mají být poskytnuty po vyloučení těch informací, o nichž je to stanoveno.

Stejně jako u zákona č. 123/1998 Sb., o právu na informace o životním prostředí [8] i zde platí, že právo odepřít informace trvá pouze tak dlouho, dokud existuje důvod odepření.

Žádost o poskytnutí informace se činí ústně nebo písemně, přičemž za písemné se považuje i podání učiněné telekomunikačním zařízením, tj. fax nebo e-mail. Pro vyřízení ústní žádosti nejsou předepsány žádné formality ani lhůty. Platí pouze, že není-li na ústní žádost poskytnuta odpověď (podle doslovného výkladu zákona by měla být vždy poskytnuta písemně) nebo žadatel nepovažuje odpověď za dostatečnou, musí žádost podat písemně.

Z podání musí být zřejmé, kdo je činí a komu je určeno a také přesné vymezení informace, o niž je žádáno, u podání učiněného telekomunikačním zařízením je třeba provést identifikaci žadatele. Protože se na podávání žádostí nevztahuje správní řád, nepřichází jiná

forma podání v úvahu, zejména tedy není možno podat žádost ústně do protokolu.

Proti případnému rozhodnutí o odepření informace se lze odvolat do 15 dnů ode dne, kdy uplynula lhůta pro vyřízení žádosti. Odvolání se podává u povinného subjektu, který rozhodnutí vydal či vydat měl. Ten může odvolání buď zcela vyhovět, a neučiní-li tak, postoupí je k rozhodnutí nejbližší vyššímu orgánu. Odvolací orgán musí rozhodnutí vydat do 15 dnů, jinak se má za to, že odvolání zamítl.

Zákon však nepamatoval na případ, kdy povinný subjekt žádný nadřízený orgán nemá (např. prezident republiky nebo ředitel soukromé školy).

2.8 Poskytování a odpírání informací v praxi

2.8.1 Právo na informace nepodléhající režimu utajení

Nejvyšší správní soud v Brně potvrdil v únoru 2004 právo ekologických sdružení na informace o jihočeské jaderné elektrárně Temelín, které nepodléhají režimu obchodního tajemství či utajovaných informací. Na soud se obrátily v různých věcech tři jihočeská ekologická sdružení - Calla, Občanská iniciativa pro ochranu životního prostředí a sdružení V havarijní zóně jaderné elektrárny Temelín. Jak tehdy uvedl na tiskové konferenci v Českých Budějovicích právní zástupce ekologických sdružení Mgr. František KORBEL: *„Státní úřad pro jadernou bezpečnost na žádosti o informace v zákonem stanovených lhůtách vůbec nereagoval“*.

Stejně postupovala i předsedkyně tohoto sdružení ohledně odvolání proti nečinnosti úřadu. Teprve s dlouhým zpožděním úřad vydával rozhodnutí o odepření informací. Šlo přitom o obecné informace o dopadech a rizicích provozu elektrárny na její okolí. Nejvyšší správní soud konstatoval, že ve všech případech byl porušen

zákon o svobodném přístupu k informacím a žalobám všech sdružení vyhověl. Podle názoru soudu byla tři napadená rozhodnutí předsedkyně Státního úřadu pro jadernou bezpečnost nezákonná a porušila práva žalobců na včasné informace o elektrárně Temelín [35].

2.8.2 Nevědomost o možnosti požadovat některé informace

Někdy naopak mohou občané požadovat informace, o které by je žádat mnohdy ani nenapadlo. Jen hrstka motoristů například ví, že se může policistů písemně dotázat, kde jsou na konkrétních úsecích umístěny mobilní radary. Jak uvedl tábořský policejní mluvčí Pavel Hanták: „*Jsmo schopni uvést i jejich počet, poznávací značku a typ vozu, ve kterém je umístěn*“ [36, s.16].

Aplikaci práva na informace v praxi uskutečnili občané sjednocení pod hlavičkou Občanského sdružení Auxilium legis. Okresní ředitelství Policie ČR v Pardubicích od nich dostalo tři dotazy. Nevalnou naději na úspěch vystřídala přesná a vyčerpávající odpověď. Přibližně po měsíci skutečně přišla. Na otázku, kolik radarů pro měření rychlosti nyní pardubická policie využívá, se v oficiálním dopise praví: „...*má k dispozici na území své působnosti tři měřicí zařízení*...“.

Velice podrobně je zodpovězen dotaz na typy, značky, barvy a registrační značky vozidel, v nichž jsou instalovány zmíněné radary pro měření rychlosti. „*Policisté používají vozidlo Škoda Felicia - služební barevné provedení - registrační značka PUN 12 - 84, měřicí zařízení Ramer 7 M; Škoda Felicia - služební barevné provedení - registrační značka PUM 79 - 81, měřicí zařízení Ramer 7 M; VW Passat - modré barvy - registrační značka PUM 79 - 84, měřicí zařízení Ramer 7 CCD*“ uvádí se v odpovědi [37, s. 6].

2.8.3 Umělé překážky v přístupu k informacím v praxi

Na druhou stranu bývají úředníci ve snaze bojkotovat žádost o zpřístupnění údajů mnohdy velmi nápadití. Třeba zneužívají poplatky, které žadatel musí zaplatit za vyhledání a případné okopírování dokumentů. A tak je-li byrokrat zlovolný, může žadateli o informace jeho snahu pořádně znepříjemnit.

Jako ilustrativní lze uvést případ jednání pražského magistrátu z roku 2000. Když chtěl redaktor časopisu *Týden* po tamním památkovém odboru vysvětlení, proč byla na pražském Alšově náměstí zbourána kvůli stavbě hotelu *Four Seasons* památkově chráněná klasicistní budova, dočkal se bezmála výsměchu. Úřad zaprvé trojnásobně přetáhl zákonnou patnáctidenní lhůtu na zodpovězení dotazu a zadruhé se doslova vyřádl na poplatcích za vyhledání a zpracování dokumentů. Elaborát, jež vyhotovil, sestával z 31 řádků plných vágních, a jak se později ukázalo, mnohdy nepravdivých údajů, za něž redakce zaplatila 474 korun 40 haléřů [38, s.32].

Kromě územních a stavebních dokumentací, kde může jít často o snahu zakrýt korupční chování, se v Česku tají některé informace bezdůvodně. Redakci časopisu *Týden* se například nepodařilo získat oficiální cestou ceny jídel v jídelně Poslanecké sněmovny a údaje o množství spotřebované potravy a alkoholu za měsíc tamtéž.

Kromě výše uvedených způsobů kladení překážek v přístupu k informacím jsou některé povinné subjekty ještě vynalézavější. V jednom konkrétním případě požadoval povinný subjekt po žadateli zaplacení zálohy několika desítek tisíc korun za 452 hodin kancelářské práce, údajně potřebných k prostudování správních spisů za účelem zjištění, zda požadované informace netvoří předmět obchodního tajemství. Po případném zjištění, že jejich poskytnutí brání zákonná překážka, by požadované informace nakonec ani nemusel poskytnout.

Takovému jednání však po následném soudním sporu učinil přítrž rozsudek Nejvyššího správního soudu ze dne 10.10.2003, vedený

pod spisovou značkou 5 A 119/01: „Zálohu ve smyslu § 17 odst. 3 zákona č. 106/1999 Sb. lze požadovat pouze za úkony spadající pod vymezení v § 17 odst. 1 tohoto zákona, tedy za úkony vykonané v souvislosti s poskytováním informací a v žádném případě ne za úkony směřující pouze ke zjištění, zda lze informace poskytnout, neboť je koneckonců věcí povinného subjektu, aby měl informace natolik strukturované a přehledné, aby fakt, zda je může poskytnout, mohl být zjištěn jednodušeji, než zaměstnáním úředníka na 56 pracovních dní plodně strávených procházením spisů“.

Z nejnovějších případů omezování toku informací směrem od státu k občanovi je třeba zmínit zejména podrobnosti vládou sjednávaného smíru s Japonskou společností *Nomura*, utajení části smlouvy o zřízení dálničního mýtného systému mezi Ministerstvem dopravy a firmou *Kapsch* a selekci informací o pronájmu billboardů podél dálnic. U všech těchto případů se projevila právní neznalost některých úředníků i ministrů. Alespoň tak tuto situaci popsal ve svém článku „Státní smlouva nesmí být tajná“, Oldřich Kužilek:

„Veřejné úřady mohou konat pouze v zákonných mezích. Pokud zákon nedovoluje státu omezit informace o své činnosti, nemůže ani ministr o své vůli omezit poskytování informací nad zákonný rámec“.

Konkrétně k případu sjednávání smíru s bankou *Nomura* výše jmenovaný autor poznamenává: „Bez ohledu na rozsah veřejných peněz (či na něčí dojem o mimořádnosti řešené věci) nikdo nemůže sebe ani stát zavázat k něčemu, co odporuje zákonům. Tak jako ředitel okresní policie nemůže ve smlouvě o opravě střechy strážnice slíbit pokrývači beztretnost, nemůže ani ministr slíbit *Nomuře*, že s ní něco ujedná, a utají to před občany“ [39, s. 10]. Tyto základní zásady jsou však, dle mého názoru, stále v nedostatečné míře veřejně presentovány a odpovědnými orgány uplatňovány.

Stejně tak jako následující zásady: „Uzavírá-li někdo smlouvu se státem, převažuje omezení státní moci nad volností soukromých

subjektů. Neznalost zákona neomlouvá ani ministry. Smluvní ujednání, překračující zákonný rámec pro výkon státní moci, nemůže vést k omezení práva na informace. A státní orgán se na takové smluvní ujednání nemůže odvolávat“ [39, s. 10]. Pokud podobné případy nebudou veřejně pranýřovány a veřejnost nebude trvat na řádném informování o činnosti veřejných činitelů, hrozí všem daňovým poplatníkům, že případné důsledky neoprávněného utajování zaplatí ze své kapsy.

Ačkoli je v poslední době trend směřující spíše k odstraňování překážek volnému přístupu k informacím, v České republice mají tyto tendence oproti zahraničí trochu zpoždění.

2.9 Právo státu na informace občanů

Zcela jinou kapitolou, která není v literatuře o svobodě informací zmiňována, je podle mého názoru právo státu na informace od občana. Jedná se o trochu nezvyklý pohled na problematiku, domnívám se však, že v současném stavu, jaký v ČR panuje, stojí za zmínku.

Jako příklad lze uvést oprávnění Bezpečnostní informační služby žádat od telekomunikačních operátorů poskytnutí informací z databáze účastníků telekomunikačního provozu. Tato žádost musí být řádně odůvodněná a navíc schválena předsedou senátu Vrchního soudu. Některé společnosti ale toto oprávnění zpochybňují a požadované údaje svévolně neposkytují. Jako důvod uvádějí domnělou dvojsmyslnost příslušných ustanovení platných zákonných předpisů (zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů [42] a zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů [43]).

Za tohoto stavu, kdy kontrarozvědná zpravodajská služba demokratického státu nemá reálnou jistotu, že informace, na které má

zákonné právo, skutečně dostane, není možné hovořit o skutečné svobodě informací. Nedávný pokus o nápravu tohoto stavu cestou návrhu novely zákona č. 127/2005 Sb. v Poslanecké sněmovně potřebnou podporu pro přijetí nenašel.

2.10 Kam právní normy nedosáhnou

Za zvláštní kapitolou v přístupu k informacím lze považovat zpovědní tajemství. Povinnost mlčenlivosti kněze z něj vyplývající není upravena světskými právními normami, a není tedy součástí právního řádu. Jde o institut církevního práva obsažený v Kodexu kanonického práva (*Codex iuris canonici*) [44]. Jedná se o církevní zákoník, přijatý v roce 1917, vyjadřující centralizační tendence Vatikánu. Plyne z něj, že povinnost mlčenlivosti kněží je nadřazena světským předpisům. Zpovědní tajemství by podle něj nemělo být prolomeno ani příkazem světského soudu. Konkrétně se ve zmiňovaném dokumentu praví:

Kánon 983:

1: Zpovědní tajemství je neporušitelné, proto není dovoleno zpovědníkovi slovy nebo jakýmkoliv způsobem a z jakékoliv příčiny cokoli vyrazit na kajícího.

2: Povinností zachovat zpovědní tajemství je vázán i tlumočník, má-li účast při zpovědi, a také všichni ostatní, kteří jakýmkoliv způsobem znají něco o hříších ze zpovědi.

a následně

Kánon 984:

1: Zpovědníkovi se naprosto zakazuje užít vědomosti získané ve zpovědi ke škodě kajícího, i když je vyloučeno jakékoliv nebezpečí vyrazení.

2: Představený nesmí nijak použít pro vnější řízení vědomosti, kterou získal o hříšících vyznaných kdykoliv ve svaté zpovědi [44].

Zmíněný Kodex má však povahu vnitro-církevního předpisu. Právní dokumenty papeže a římské kurie se podle některých názorů mohou týkat pouze práva církevního, protože sekulární, čili světské, právo jednotlivých států by mělo být mimo jejich působnost. Podle jiného právního názoru však ustanovení §7 odst. 1 písm. f/ zákona č. 3/2002 Sb., o svobodě náboženského vyznání a postavení církví a náboženských společností a o změně některých zákonů [45] svědčí v tomto ohledu ve prospěch církve. Podle tohoto ustanovení *„Registrovaná církev a náboženská společnost může za podmínek stanovených tímto zákonem k plnění svého poslání získat oprávnění...“*. K výkonu tohoto zvláštního práva *„... zachovávat povinnost mlčenlivosti duchovními v souvislosti s výkonem zpovědního tajemství nebo s výkonem práva obdobného zpovědnímu tajemství, je-li tato povinnost tradiční součástí učení církve a náboženské společnosti nejméně 50 let; tím není dotčena povinnost překazit trestný čin uložená zvláštním zákonem“* [45].

V církevním dokumentu Codex iuris canonici se však s možností prolomení povinnosti mlčenlivosti v případě informací o trestném činu nepočítá.

3. UTAJOVANÉ INFORMACE

Název republika pochází z latinského res publica, což znamená věc veřejná.

Nikoli tedy utajovaná...

Jakékoli ohrožení tajemství je vždy chápáno jako přímá hrozba dosavadní kvalitě existence jednotlivce, ať už je jím fyzická či právnická osoba, instituce nebo stát. Proto se každý, kdo chce utajené informace ochránit před vyzrazením, snaží učinit konkrétní opatření, která k utajení objektivně vedou. Tuto svou vůli většinou projeví veřejným prohlášením, že má zájem určitý druh informací utajovat.

Právní pořádek většiny demokratických zemí na tyto potřeby reaguje vydáním odpovídajících předpisů. V rámci platného právního řádu je pojem „*tajemství*“ označováno různými termíny a přívlastky, např. poštovní tajemství, obchodní tajemství, citlivé údaje, důvěrné informace, bankovní tajemství nebo utajované informace. Tyto instituty se vzájemně liší především druhem obsažených informací, způsobem a mírou jejich ochrany a zájmem, pro který jsou tyto informace chráněny.

Ve veřejném zájmu je jak ochrana svobod a práv jedinců, tak i ochrana utajovaných informací ze strany státu. V tomto případě je tato stránka veřejného zájmu silnější než zájem na publikaci takových informací.

V následujících kapitolách bude věnována pozornost fenoménu utajovaných informací v rámci právní úpravy ČR.

3.1 Historie „státního tajemství“

Institut utajovaných skutečností, častěji nazývaný státní tajemství, se v novodobé historii českého státu poprvé objevil v zákoně na ochranu republiky z roku 1923 [46]. Úprava v tomto zákoně, byť zdůvodňovaná existencí úkladů o republiku, představovala výrazný zásah do demokratických práv občanů nové republiky, zejména co se týkalo svobody projevu (ve znění novelizací z třicátých let) a svobody tisku [47].

S účinností od ledna 1972 byl přijat federální zákon č. 102/1971 Sb., o ochraně státního tajemství, který upravil institut státního tajemství, vymezil způsob jeho určení i ochrany před vyjádřením a zneužitím proti společenskému a státnímu zřízení ČSSR a jejím zájmům. Základní zásady tohoto zákona platily přiměřeně i pro úpravu ochrany hospodářského a služebního tajemství.

3.2 Státní tajemství

Státním tajemství se rozumělo vše, co v důležitém zájmu republiky, zejména v zájmu politickém, vojenském nebo hospodářském má zůstat utajeno před nepovolanou osobou.

Hospodářským tajemstvím se rozumělo vše, co je důležité pro hospodářskou činnost a v obecném zájmu má zůstat utajeno před nepovolanou osobou.

Služebním tajemstvím se rozuměla důležitá skutečnost, která souvisela s činností národního výboru, soudu, ozbrojených sil nebo ozbrojeného sboru nebo jiného státního orgánu, státní, hospodářské, družstevní nebo společenské organizace a v obecném zájmu má zůstat utajena před nepovolanou osobou.

Bližší úpravu ochrany hospodářského a služebního tajemství stanovilo nařízení vlády ČSSR č. 148/1971 Sb.

Poté vláda ČSSR (nařízením vlády č. 149/1971 Sb.) stanovila základní skutečnosti tvořící předmět státního tajemství a ministr vnitra ČSSR, v souladu s těmito skutečnostmi, vydával a doplňoval seznam skutečností tvořících předmět státního tajemství pro jednotlivé obory nebo odvětví, a to včetně seznamů skutečností tvořících předmět hospodářského a služebního tajemství v Ústředním věstníku ČSSR.

Federální ministerstvo vnitra vykonávalo při ochraně státního tajemství činnost metodickou (vydávalo pokyny nebo směrnice), odbornou (zejména pro vedoucí organizací) a kontrolní.

Jako důležité z hlediska současné klasifikace dokumentů podle stupňů utajení lze uvést, že podle původní „*Manipulační směrnice*“ (Směrnice FMV ze dne 23.12.1971 pro manipulaci a dopravu písemných a jiných materiálů obsahujících skutečnosti tvořící předmět státního, hospodářského a služebního tajemství) byly utajované skutečnosti tvořící předmět státního tajemství označovány pouze jediným stupněm utajení Přísně tajné, a utajované skutečnosti tvořící předmět hospodářského nebo služebního tajemství byly označovány jednotně (stupeň utajení nerozlišoval hospodářské nebo služební tajemství) a také jediným stupněm utajení Tajné.

Kromě toho lze pro srovnání uvést, že výše uvedená právní úprava z roku 1971, po několika novelizačních změnách počátkem devadesátých let, přetrvala až do druhé poloviny devadesátých let (do 1.11.1998), kdy v souvislosti s přijetím nového zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, byla zrušena.

3.2.1 Průlom v právní úpravě státního tajemství

Právní úprava ochrany utajovaných skutečností podle zákona č. 148/1998 Sb. přinesla kvalitativní průlom v dosavadní právní úpravě institutu státního tajemství, neboť reflektovala nové společenské

zřízení a uspořádání státu, a položila základy pro výkon státní správy v oblasti ochrany utajovaných skutečností v nových podmínkách.

Zároveň zákon zřídil Národní bezpečnostní úřad (dále jen „NBÚ“), jako ústřední správní úřad v této oblasti, na jehož činnost dohlížel předseda vlády. Ředitel NBÚ byl jmenován, po projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti státu, vládou, a vláda ho mohla též z funkce odvolat. Předseda vlády byl služebně nadřizen řediteli NBÚ.

Kromě toho zákon vymezil skutečnosti, které je nutno v zájmu ČR utajovat, způsob jejich ochrany, působnost a pravomoc orgánů státu při výkonu státní správy v oblasti ochrany utajovaných skutečností, povinnosti orgánů státu, práva a povinnosti fyzických a právnických osob a odpovědnost za porušení povinností stanovených v zákoně.

3.2.2 Zavedení nových pojmů

Za utajovanou skutečnost označil zákon takovou skutečnost, se kterou by neoprávněné nakládání mohlo způsobit újmu zájmům ČR nebo zájmům, k jejichž ochraně se ČR zavázala, nebo by mohlo být pro tyto zájmy nevýhodné, a která je uvedena v seznamu utajovaných skutečností.

V souvislosti s pojmem utajované skutečnosti zákon stanovil, co se rozumí zájmem ČR (zachování ústavnosti, svrchovanosti, územní celistvosti, zajištění obrany státu, veřejné bezpečnosti, ochrana důležitých ekonomických a politických zájmů, práv a svobod fyzických a právnických osob a ochrana života nebo zdraví fyzických osob) a co se rozumí újmou zájmu ČR (poškození nebo ohrožení zájmu ČR nebo zájmu, k jehož ochraně se ČR zavázala, jehož následky nelze odstranit nebo je lze zmírnit pouze následnými opatřeními).

3.2.3 Rozšíření klasifikace utajovaných skutečností

Ve srovnání s předchozím zákonem č. 102/1971 Sb., zákon č. 148/1998 Sb. zavedl klasifikaci skutečností, které tvoří předmět státního tajemství podle čtyř stupňů – Přísně tajné, Tajné, Důvěrné, Vyhrazené, a to v návaznosti na možné následky neoprávněného nakládání s takovou skutečností. Dřívější jediný stupeň utajení pro oblast státního tajemství byl tedy rozdělen na čtyři stupně utajení, což v praxi znamenalo citlivější přístup k posuzování utajovaných skutečností, založený na zkušenosti, neboť zákon považoval za neoprávněné nakládání s utajovanou skutečností též neoznačení utajované skutečnosti stupněm utajení nebo nesprávné stanovení stupně utajení utajované skutečnosti.

3.2.4 Působnost NBÚ a úkoly pro další subjekty

Pokud jde o výkon státní správy v oblasti ochrany utajovaných skutečností, zákon stanovil především působnost NBÚ - zajišťovat jednotné provádění ochrany utajovaných skutečností, vykonávat státní dozor a metodickou činnost, vést ústřední registry utajovaných skutečností poskytovaných v rámci mezinárodních styků, zajišťovat a koordinovat výzkum a vývoj v určitých oblastech, zajišťovat certifikaci, provádět bezpečnostní prověrky, vydávat osvědčení, potvrzení, certifikáty, bezpečnostní standardy a plnit další úkoly, které zákon vymezil taxativně.

Kromě toho zákon stanovil úkoly v této oblasti státní správy i pro ministerstvo obrany, zpravodajské služby ČR (dále jen „zpravodajské služby“), Policii ČR, včetně propojení činnosti těchto subjektů s činností NBÚ při výkonu státní správy v oblasti ochrany utajovaných skutečností.

Klasifikace utajovaných skutečností čtyřmi stupni utajení, včetně členění způsobené újmou zájmu ČR podle významu zájmu a závažnosti

způsobené újmy a nevýhodnosti pro zájmy ČR, přetrvává do současné doby, kdy ochranu utajovaných skutečností upravuje nový zákon č. 412/2005 Sb. Rovněž tak pokračuje v modifikované podobě výkon státní správy v oblasti ochrany utajovaných skutečností v rámci NBÚ, zpravodajských služeb, ministerstva vnitra a policie.

Dnes již činnost NBÚ kontroluje Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán. Ředitel NBÚ předkládá tomuto orgánu zprávu o činnosti NBÚ, zprávu o jednotlivých řízeních o žádosti fyzické osoby nebo podnikatele podle § 137 písm. a) zákona č. 412/2005 Sb., návrh rozpočtu NBÚ, včetně podkladů potřebných ke kontrole plnění rozpočtu, a vnitřní předpisy NBÚ.

3.2.5 Vývoj současné právní úpravy

V souvislosti s vývojem ochrany utajovaných skutečností nastal kvalitativní posun též v oblasti bezpečnostního řízení, neboť nový zákon č. 412/2005 Sb. umožňuje soudní přezkum rozhodnutí ředitele NBÚ, který rozhodoval o tzv. rozkladu, který podal účastník bezpečnostního řízení proti rozhodnutí NBÚ vydanému v bezpečnostním řízení. Při dokazování v rámci tohoto soudního řízení je respektována povinnost zachovávat mlčenlivost o utajovaných informacích.

Nový zákon též umožňuje i soudní přezkum rozhodnutí odpovědné osoby zpravodajské služby, která rozhodovala o rozkladu, který podal příslušník nebo zaměstnanec zpravodajské služby jako účastník bezpečnostního řízení proti rozhodnutí zpravodajské služby vydanému v bezpečnostním řízení, a rovněž tak zákon umožňuje soudní přezkum rozhodnutí ministerstva vnitra, který rozhodoval o rozkladu, podaný příslušníkem policie, vybraný v zájmu plnění závažných úkolů policie, jako účastník bezpečnostního řízení proti rozhodnutí ministra vnitra vydanému v bezpečnostním řízení.

Při přípravě nového zákona č. 412/2005 Sb. tak byly zohledněny několikaleté zkušenosti z oblasti ochrany utajovaných skutečností, neboť i samotný zákon č. 148/1998 Sb. procházel četným novelizačním procesem v roce 1999, 2000, 2001, 2002, 2003, 2004, 2005 a jeho původní znění bylo změněno a doplněno 16 novelami.

Torzo zákona č. 148/1998 Sb. je v účinnosti i současné době, avšak jeho ustanovení upravující ochranu utajovaných skutečností a bezpečnostní způsobilosti fyzických osob byla zrušena zákonem č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Zákon č. 412/2005 Sb., který předmětnou úpravu ochrany utajovaných skutečností a bezpečnostní způsobilosti obsahuje, nabyl účinnosti 1.1.2006, tedy ve shodný den jako zákon č. 413/2005 Sb., neboť stěžejním důvodem bylo zachování kontinuity činnosti NBÚ v oblasti výkonu státní správy. V souvislosti s novou právní úpravou institutu státního tajemství došlo též ke změně pojmu „*utajovaná skutečnost*“ na pojem „*utajovaná informace*“, a tato změna pojmu se prolíná do celého nového zákona, včetně jeho názvu.

Úprava z roku 1971 dala poprvé potřebnou zákonnou formu vymezení státního tajemství i povinností vyplývajícím z něj pro občany a jako taková představuje krok vpřed, pokud jde o právní jistoty a efektivnost správy státního tajemství, a to přestože byl zákon přijímán v podmínkách nastupující normalizace.

3.3 Platná právní úprava v ČR

V současnosti platný zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti [48] je obecně závazný právní předpis v oblasti správního práva, který upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro

stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy, vymezení utajovaných informací, režim nakládání s nimi, kompetence Národního bezpečnostního úřadu a dalších orgánů na tomto úseku, procesní pravidla a stanovuje sankce.

Na rozdíl od minulé právní úpravy, kdy byla několikrát provedena novelizace, a to zejména z důvodu několika nálezů ústavního soudu, lze předpokládat, že tento zákon je v souladu s ústavním pořádkem ČR, zejména s článkem 17 Listiny základních práv a svobod, který upravuje právo na informace a přípustné výjimky z něj: „*Svoboda projevu a právo na informace jsou zaručeny*” (odst. 1) a „*Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti*” (v odstavci 5 je zároveň stanoveno, že podrobnosti stanoví zákon). Existence zákona o utajovaných informacích je pak umožněna díky výjimce v odstavci 4, která připouští omezení těchto práv „*jde-li o opatření v demokratické společnosti nezbytná pro... ..bezpečnost státu, veřejnou bezpečnost...*”.

V současné době je před schválením novela zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, které se ještě v této práci budu věnovat.

3.4 Některé otázky obecně závazné právní úpravy ochrany utajovaných informací

V návaznosti na následující rozbor obecně závazné právní úpravy ochrany utajovaných informací je nutné přesně definovat alespoň některé základní pojmy, tak jak je vymezuje v § 2 zákon č. 412/2005 Sb.:

Pro účely tohoto zákona se rozumí

a) utajovanou informací 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 v § 139,

b) zájmem České republiky 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,

c) porušením povinnosti při ochraně utajované informace porušení povinnosti uložené tímto zákonem nebo na základě tohoto zákona,

d) neoprávněnou osobou fyzická nebo právnická osoba, která nesplňuje podmínky přístupu k utajované informaci stanovené tímto zákonem [48].

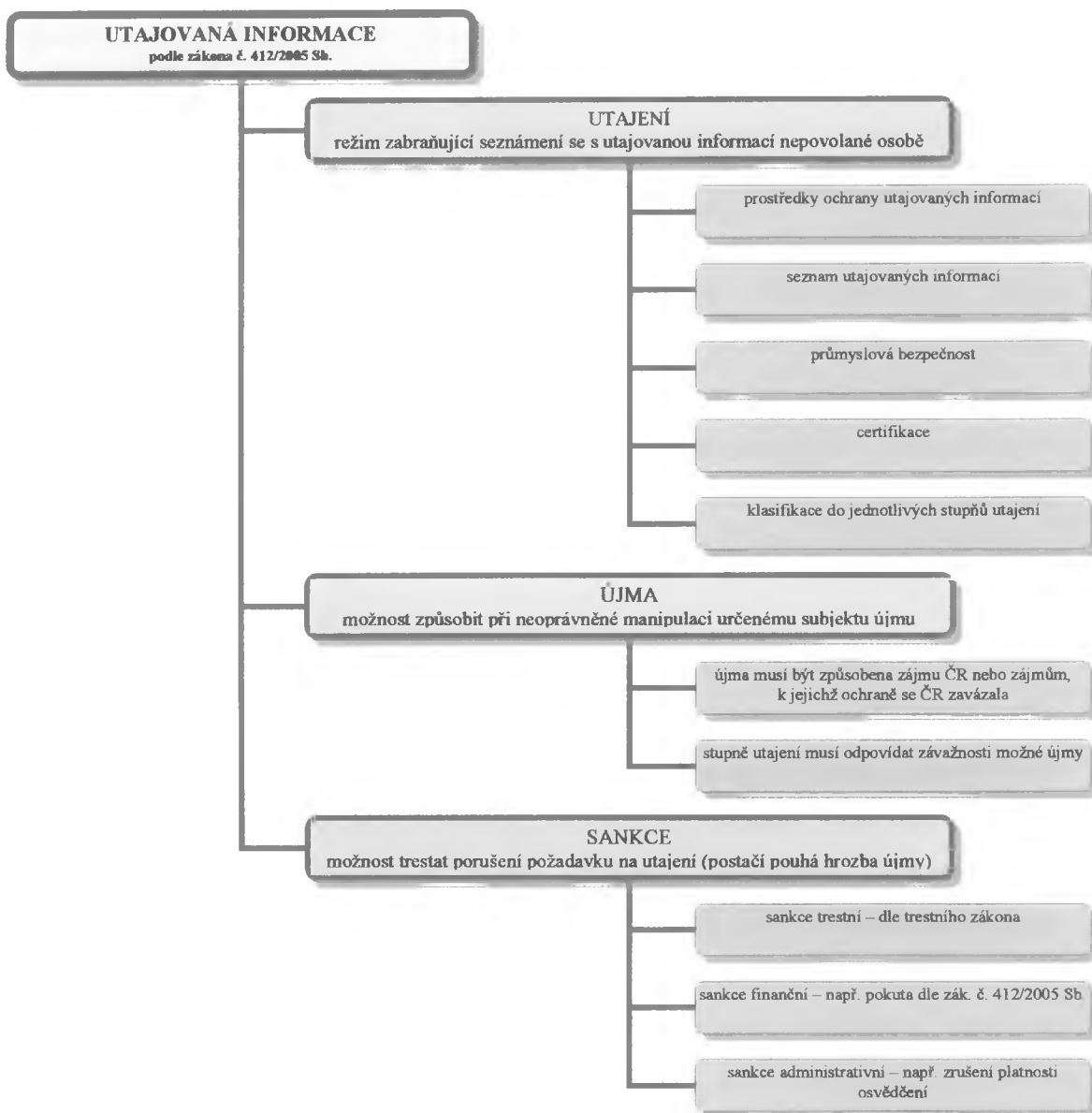
K výše uvedenému lze konstatovat, že ani Národní bezpečnostní úřad, kterému je svěřen výkon státního dozoru nad dodržováním povinnosti v oblasti ochrany utajovaných informací, není imunní proti vzniku nedostatků při výkonu své činnosti. V období od 1. prosince 2004 do 30. června 2005 proběhla na tomto úřadu kontrola postupu při provádění bezpečnostních prověrek fyzických osob. Komise mimo jiné zjistila vážné nedostatky při administrativním zpracování bezpečnostních prověrek a vedení bezpečnostních spisů. V protokole o kontrole se mimo jiné uvádí: „*Docházelo k neoprávněnému označení stupně utajení na některých listinách bezpečnostního spisu (nepřesně, formálně nesprávně) – to se týká zejména neoprávněného utajování podkladových materiálů poskytnutých navrhovanou osobou. Jsou utajovány písemnosti, které v žádném případě nejsou utajovanými (žádost o vydání osvědčení, výpis z Rejstříku trestů apod.). Naopak některé písemnosti, které by měly být utajovány, utajeny nejsou (vyhodnocení bezpečnostní prověrky, kde jsou citovány utajované informace zpravodajských služeb apod.)*“ [49].

3.4.1 Co se rozumí utajovanými informacemi

Utajované informace mohou být nejen fakta vyskytující se v působnosti orgánů státu a veřejné správy, ale i informace týkající se činnosti podnikajících fyzických osob. Jde například o agendu provozu podniků, informací společností poskytující služby v počítačové bezpečnosti apod. Utajované informace mohou být zároveň předmětem ochrany obchodního tajemství či duševního vlastnictví.

Definice utajované informace má materiální i formální složku. Materiálně (hmotně-právně) je utajovaná informace vymezena v první části věty v § 3 odst. 1 zákona: „*Utajovanou informací je informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tyto zájmy nevýhodné*“. Formální složkou je, že tato informace „*je uvedena v seznamu utajovaných informací*“. Obě tyto složky musí být splněny současně.

Nelze proto za utajovanou informaci pokládat skutečnost, jejíž zveřejnění by mohlo přivodit újmu zájmu ČR, ale která není uvedena v seznamu. Zákon tak motivuje orgány, které se podílí na zpracování seznamu (NBÚ, který seznam kompletuje, ústřední úřady, které mu dodávají podklady, a vládu, která je vydává v podobě nařízení) k průběžnému racionálnímu vyhodnocování rizikových informací. Stejně tak není možné zařadit na seznam informací, jejíž vyzrazení nebo zneužití nemůže způsobit újmu zájmu České republiky nebo by nebylo pro tyto zájmy nevýhodné – nešlo by o utajovanou informaci, neboť by chyběl materiální znak. Ustanovení § 2 písm. b/ zákona č. 412/2005 Sb., pak blíže vymezuje, co se rozumí zájmem ČR a § 3 odst. 1 tohoto zákona vymezuje, co se rozumí újmou (poškození nebo ohrožení zájmu České republiky) [48]. Základní znaky utajované informace názorně popisuje obr. 2.



© 2006 Jaroslav Hora

Obr 2: Utajovaná informace a její základní znaky

Na podobu zákona mají rovněž fakticky vliv mezinárodní smlouvy, a to jak právně závazné, tak nezávazné. V neposlední řadě pak i bezpečnostní politika NATO, resp. její klíčové dokumenty. Podle názoru Heleny Svatošové z *Iuridicum remedium, o.s.* však nelze tento vztah vzhledem k jejich spíše faktickému než právnímu působení v žádném případě považovat za ekvivalentní působení závazků ČR v oblasti mezinárodních smluv o lidských právech. Toto faktické

působení kontroverzní a kritizované bezpečnostní politiky Severoatlantické aliance [50] bylo právně dodatečně stvrzeno mnohostrannou tzv. dohodou o bezpečnosti informací v roce 2001. Ta obsahuje vůči státu závazek utajovat všechny informace, které samo NATO na základě své bezpečnostní politiky označí za utajené. Zásadní obtíží přitom je, že základní dokumenty této politiky (C-M(55)15(Final) z roku 1955 a C-M(2002)49 z června 2002) nemá veřejnost k dispozici. Ačkoli ani jeden z dokumentů není klasifikován jako utajovaná informace, NATO je od padesátých let odmítá zpřístupnit veřejnosti a instruuje i členské státy, aby je – v rozporu se závazky států v oblasti práva na informace – občanům neposkytovaly [47].

Některé definice informací, které je nutno utajovat, jsou však stanoveny velmi obecně, takže se utajování někdy ve skutečnosti prohloubí dále i tam, kde to není potřeba. Na toto často upozorňují různí právníci a novináři, jako např. právnička Helena Svatošová, která vypracovala podrobnou analýzu zákona o ochraně utajovaných informací pro mezinárodní organizaci *Transparency International*, zabývající se korupcí. Ve zprávě k problematice přílišného utajování píše: „*Odůvodnění tuzemského trendu zahraničními normami není na místě. Na západě se vedou o způsobu utajování, které má kořeny v době studené války, odborné diskuse a očekává se revize zákonů*“ [51, s. 6].

3.4.2 Klasifikace utajovaných informací stupněm utajení

Utajovaná informace se podle § 4 zákona číslo 412/2005 Sb. klasifikuje stupněm utajení [48]:

- a) **Přísně tajné**, jestliže její vyobrazení 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.

Toto ustanovení vymezuje jednotlivé stupně utajení v závislosti na intenzitě újmy, která by mohla vzniknout zájmům ČR při neoprávněném nakládání s utajovanou informací. Klasifikaci provádí původce této utajované informace, kterým je orgán státu, právnická nebo podnikající fyzická osoba, u nichž utajovaná informace vznikla nebo úřad průmyslového vlastnictví podle § 70 odst. 4 tohoto zákona.

Výše uvedené členění klasifikace utajovaných informací je v souladu s členěním utajovaných informací užívaným ve státech Evropské unie i Organizace Severoatlantické smlouvy.

3.4.3 Změna nebo zrušení stupně utajení

Změnu nebo zrušení stupně utajení upravuje především § 22 zákona č. 412/2005 Sb. a dále pak vyhláška NBÚ č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Výše uvedené předpisy vymezují případy, kdy může dojít ke změně nebo zrušení stupně utajení, definují přesný postup a stanovují podmínky, za kterých k tomuto může dojít.

Stupeň utajení se na utajované informaci vyznačí při jejím vzniku, nestanoví-li zákon č. 412/2005 Sb. jinak. Vyznačení stupně utajení na utajované informaci musí být zachováno po celou dobu

trvání důvodů utajení. Bez souhlasu původce nebo poskytující cizí moci nesmí být stupeň utajení změněn nebo zrušen.

Vyžaduje-li to charakter utajované informace, musí původce utajované informace vyznačit na utajované informaci dobu, po kterou bude informace utajována. Stupeň utajení pak zaniká uplynutím vyznačené doby.

Původce stupeň utajení neprodleně zruší nebo změní po zjištění, že pominul důvod pro utajení informace, důvody pro utajení neodpovídají stanovenému stupni utajení nebo byl-li stupeň utajení stanoven neoprávněně. Toto zrušení nebo změnu stupně utajení je pak povinen na utajované informaci vyznačit. Dále pak je původce povinen zrušení nebo změnu stupně utajení oznámit neprodleně adresátům utajované informace, a to písemně. Adresáti utajované informace oznámí neprodleně tuto skutečnost všem dalším adresátům, kterým utajovanou informaci zpřístupnili. O změně nebo zrušení stupně utajení bude ještě podrobněji pojednáno v kapitole zabývající se administrativní bezpečností.

3.4.4 Členění újmy způsobené zájmu ČR

Podle závažnosti poškození nebo ohrožení zájmu České republiky se újma člení na mimořádně vážnou újmu, vážnou újmu a prostou újmu. Nevýhodností pro zájmy České republiky se rozumí poškození nebo ohrožení zájmu České republiky, jehož závažnost nedosahuje ani prosté újmy.

Ustanovení § 3 odst. 2,3,4 a 5 tohoto zákona vymezuje újmu a nevýhodnost pro zájmy České republiky s ohledem na intenzitu újmy a způsobených následků. Vymezení újmy (vedle uvedení v seznamu utajovaných informací) je základním předpokladem pro klasifikaci utajované informace do příslušného stupně utajení [52].

3.4.5 Příklady skutečností, které mohou mít za následek mimořádně vážnou újmu zájmu ČR

- bezprostřední ohrožení svrchovanosti, územní celistvosti nebo demokratických základů České republiky,
- značnou škodu České republiky ve finanční, měnové nebo hospodářské oblasti,
- rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení zdraví obyvatel,
- mimořádně vážné ohrožení činnosti nebo existence Organizace Severoatlantické smlouvy, Evropské unie nebo členského státu,
- mimořádně vážné ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie.

3.4.6 Příklady, které mohou mít za následek vážnou újmu zájmu ČR

- ohrožení svrchovanosti, územní celistvosti a demokratických základů České republiky,
- značnou škodu České republiky ve finanční, měnové nebo hospodářské oblasti,
- ztráty na lidských životech nebo ohrožení zdraví obyvatel.
- vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb,

3.4.7 Příklady skutečností, které mohou mít za následek prostou újmu zájmu ČR

- zhoršení vztahů České republiky s cizí mocí,
- ohrožení bezpečnosti jednotlivce,
- zmaření, ztížení anebo ohrožení prověřování nebo vyšetřování zvláště závažných trestných činů nebo usnadnění jejich páchaní,
- vznik nezanedbatelné škody České republice,
- závažné narušení ekonomických zájmů České republiky.

3.4.8 Příklady skutečností, které mohou mít za následek nevýhodnost pro zájmy ČR

- zmaření, ztížení anebo ohrožení prověřování nebo vyšetřování ostatních trestných činů než uvedených v odstavci 4 písm. f) nebo usnadnění jejich páchaní,
- poškození významných ekonomických zájmů České republiky nebo Evropské unie nebo jejího členského státu,
- narušení bezpečnostních nebo zpravodajských operací.
- narušení důležitých obchodních nebo politických jednání České republiky s cizí mocí.

3.4.9 Zajištění ochrany utajovaných informací (6 druhů)

V § 5 zákona 412/2005 Sb. jsou vymezeny jednotlivé druhy ochrany utajovaných informací a způsoby, jakými je ochrana zajišťována. Jednotlivé druhy se při realizaci vzájemně prolínají

a doplňují. Vznikl tak ucelený systém opatření, resp. činností, jejichž realizací a dodržováním dochází k zajištění maximální míry ochrany utajovaných informací v souladu s mezinárodními závazky České republiky:

a) personální bezpečností, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,

b) průmyslovou bezpečností, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,

c) administrativní bezpečností, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,

d) fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,

e) bezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému a

f) kryptografickou ochranou, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.

3.4.10 Bezpečnostní ředitel

Orgán státu, u kterého utajovaná informace vzniká nebo kterému je poskytnuta, a dále právnická osoba a podnikající fyzická osoba, které mají přístup k utajované informaci, jsou povinni zřídit a obsadit funkci bezpečnostního ředitele. Bezpečnostní ředitel je osobou jmenovanou. Zodpovídá dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, za problematiku oblasti utajovaných informací v rámci působnosti zřizujícího subjektu.

Funkci bezpečnostního ředitele může vykonávat i odpovědná osoba sama; jinak je bezpečnostní ředitel přímo podřízen odpovědné osobě. Orgán státu, právnická osoba a podnikající fyzická osoba jsou povinni do 15 dnů ode dne obsazení funkce bezpečnostního ředitele oznámit písemně NBÚ jméno, příjmení a rodné číslo osoby, vykonávající tuto funkci.

Funkci bezpečnostního ředitele může vykonávat pouze fyzická osoba, která splňuje podmínky přístupu k utajovaným informacím takového stupně utajení, ke kterým bude mít při výkonu této funkce přístup. [48]

3.5 Přístup k utajovaným informacím

Zákon číslo 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti stanoví, že přístup k utajovaným informacím lze umožnit fyzické osobě, jestliže jej nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti a je držitelem oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené nebo držitelem osvědčení pro stupně utajení Důvěrné, Tajné nebo Přísně tajné.

3.5.1 Vydání oznámení a osvědčení

Oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené vydává fyzické osobě osoba odpovědná (zpravidla zaměstnavatel - viz definice v ustanovení § 2 písm. e) zákona č. 412/2005 Sb.). Osvědčení pak vydává po provedení bezpečnostního řízení NBÚ, dále pro své příslušníky zpravodajské služby a pro vybrané příslušníky Policie ČR Ministerstvo vnitra (fyzická podoba osvědčení – viz obr. 3). Bezpečnostní řízení se zahajuje na základě žádosti fyzické osoby (účastníka řízení). Vzory těchto dokumentů jsou stanoveny vyhláškou NBÚ.



Obr 3: Osvědčení vydané Národním bezpečnostním úřadem

3.5.2 Bezpečnostní řízení

Ze zákona číslo 412/2005 Sb. vyplývá, že Bezpečnostní řízení je proces vedený NBÚ nebo jiným ze zákona oprávněným subjektem. V oblasti ověřování bezpečnostní způsobilosti slouží k ověření, zda fyzická osoba splňuje podmínky pro vydání dokladu o bezpečnostní způsobilosti. Řízení je neveřejné a v jeho průběhu musí být šetřena čest a důstojnost osob dotčených řízením. Jednacím jazykem je čeština (vyjma zákonného výkonu práva příslušníka národnostní menšiny). Písemnosti v jiných jazycích musí být v rámci řízení předkládány jak v originále, tak v úředně ověřeném překladu do českého jazyka. Kromě osobních úkonů se může účastník řízení nechat zastupovat advokátem nebo zvoleným zástupcem, kterému udělil písemnou plnou moc. V průběhu řízení je účastník a jeho zástupce oprávněn nahlížet, před vydáním rozhodnutí, do neutajované části bezpečnostního svazku. Úřední osoba, která se řízení účastní, může být z řízení vyloučena na základě svého oznámení nadřízenému nebo na základě námítky podjatosti vznesené účastníkem řízení.

Bezpečnostní řízení se v současné době již řídí zásadami správního práva, a to se odrazilo rovněž v zavedení lhůt pro provedení jednotlivých jeho kroků. Délka bezpečnostního řízení se odvíjí od druhu řízení.

Například bezpečnostní řízení o žádosti o doklad je 3 měsíce. Lhůtu může ředitel NBÚ prodloužit maximálně o dobu stanovenou pro řízení stupně a to v případech, kdy nemůže zpravodajská služba nebo policie sdělit výsledky šetření ve stanovených lhůtách, nebo orgán státu, právnická osoba nebo podnikající fyzická osoba nemůže poskytnout ve stanovené lhůtě informaci požadovanou v rámci řízení.

Bezpečnostní řízení začíná (dle § 93 zákona č. 412/2005 Sb.):

- dnem doručení žádosti o vydání dokladu o bezpečnostní způsobilosti fyzické osoby nebo
- dnem doručení písemného oznámení o zahájení řízení o zrušení platnosti dokladu anebo
- dnem doručení rozhodnutí o rozkladu.

V případě, že bude účastník po zahájení řízení vyzván, aby upřesnil údaje uvedené v žádosti, učiní tak do 14 dnů od doručení výzvy (§103/1 zákona č. 412/2005 Sb.). Jestliže tak neučiní, vystavuje se tomu, že NBÚ bezpečnostní řízení zastaví (§ 113/1h zákona č. 412/2005 Sb.). Tento institut může být použit kdykoli v průběhu řízení, nikoli pouze bezprostředně po podání žádosti.

Cílem a smyslem řízení je zjistit stav věci v rozsahu, který je nezbytný pro rozhodnutí o vydání či nevydání dokladu o bezpečnostní způsobilosti fyzické osoby. Úkony, které jsou za tímto účelem prováděny, směřují k ověření pravdivosti údajů poskytnutých účastníkem bezpečnostního řízení. Ve svém rozhodování, zda účastník řízení splňuje podmínky pro vydání dokladu, pak NBÚ vychází nejen z údajů od účastníka řízení, ale také z informací, které si vyžádal od příslušných orgánů státu, právnických nebo podnikajících fyzických osob. V případě, že takto získané informace nepostačují pro zjištění úplného stavu věci, lze je ověřit nebo doplnit provedením dalších úkonů, tj. například šetřením zpravodajské služby nebo policie k účastníkovi řízení, k osobám starším 18 let žijícím s účastníkem řízení ve společné domácnosti nebo v prostředí, v němž se účastník řízení pohybuje. V takovém případě je provedení těchto úkonů podmíněno písemným souhlasem účastníka řízení. Důležitými instituty

v průběhu řízení jsou dále svědek, pohovor s účastníkem řízení a znalec.

Svěddek

Jedná se o standardní institut správního řízení. Ustanovení týkající se svědka stanovuje práva, povinnosti a postavení svědka v bezpečnostním řízení. Výslech svědka nenahrazuje šetření zpravodajských služeb, opačně však tento institut slouží k urychlení řízení v těch případech, kdy jednoduchým vyjádřením svědka lze objasnit ty skutečnosti, které by jinak vyžadovaly další úkony jiných orgánů státu pro objasnění skutečného stavu věci. Platná úprava připouští standardní možnost odmítnutí podat svědeckví a stejně jako jiné procesní předpisy přiznává svědkovi právo na náhradu nezbytných výdajů, které mu v souvislosti se splněním této povinnosti vzniknou.

Svědkiem může být každá fyzická osoba (vyjma příslušníků policie a zpravodajských služeb podílejících se na řízení). Z dikce zákona vyplývá (§ 104 zákona č. 412/2005 Sb.), že vyslechnout nelze osobu, která by porušila ochranu utajovaných informací nebo povinnost mlčenlivosti (není – li jí zproštěna). Jako svědek je povinen vypovídat každý, a to za účelem zjištění skutečného stavu věci a zjištění možných bezpečnostních rizik. Svědek má zároveň povinnost dostavit se na předvolání ze zákona oprávněného subjektu. Případné odepření výpovědi se řídí ustanovením § 100 trestního řádu. Následkem nedostavení se či nepravdivé či neúplné výpovědi, může být pořádková pokuta až do výše 50 000, - Kč (v úhrnu 100 000,- Kč). O výpovědi je pořízen protokol, který se stává součástí bezpečnostního svazku.

Pohovor s účastníkem řízení

Pohovor s účastníkem řízení (§ 105 zákona) se provádí, je – li třeba objasnit některé skutečnosti v průběhu řízení. Opětovné nedostavení se k pohovoru bez omluvy má za následek zastavení řízení. Stejný účinek má také nepravdivá nebo neúplná výpověď při pohovoru. O výpovědi je pořízen protokol, který se stává součástí bezpečnostního svazku a v případě, že o to účastník požádá, stane se součástí bezpečnostního svazku i obrazový nebo zvukový záznam z pohovoru.

3.5.3 Osobnostní způsobilost

Z hlediska ochrany utajovaných informací je nezbytné, aby osoba, která má mít přístup k utajovaným informacím, splňovala určité osobnostní předpoklady. V ustanovení o osobnostní způsobilosti se vymezují potíže psychické povahy, které mohou negativně ovlivnit úsudek nebo chování prověřované osoby. Cílem posuzování osobnostní způsobilosti je zjistit, zda u této osoby neexistují poruchy v chování nebo jiné obtíže psychického charakteru, které by mohly mít vliv na její schopnost odpovídajícím způsobem zajistit ochranu utajovaných informací.

Jednou z podmínek pro vydání dokladu o bezpečnostní způsobilosti fyzické osoby je proto osobnostní způsobilost. Pokud je v některých případech v rámci řízení zjištěna pochybnost o osobnostní způsobilosti ze zákona oprávněným subjektem, je stanoven znalece (§ 106 zákona č. 412/2005 Sb.). Účastník řízení se pak podrobí vyšetření a ze zákona oprávněnému subjektu předloží odborný posudek. V rámci řízení si může subjekt provádějící bezpečnostní řízení vyžádat znalecký posudek i z jiné oblasti za účelem odborného posouzení skutečností důležitých pro rozhodnutí (psychiatrie, oceňování majetku, atd.). Náklady na takto vypracované znalecké posudky hradí subjekt, který bezpečnostní řízení provádí.

Zpravodajská služba u svých příslušníků, zaměstnanců a uchazečů o zaměstnání nebo o přijetí do služebního poměru a Ministerstvo vnitra ve zvlášť vymezených případech, ověřuje osobnostní způsobilost na základě prohlášení k osobnostní způsobilosti nebo na základě psychologického vyšetření psychologickým pracovištěm zpravodajské služby nebo Ministerstva vnitra. Pro účely žádosti podle § 94 zákona č. 412/2005 Sb. na stupeň utajení Přísně tajné se osobnostní způsobilost ověřuje na základě psychologického vyšetření.

3.5.4 Kdo má přístup k utajované informaci

Fyzická osoba, která svým podpisem stvrdila platné poučení fyzické osoby, je oprávněna se seznamovat s utajovanými informacemi v rozsahu nepřesahujícím rámec poučení (tzn. co do stupně a rozsahu utajované informace), který potřebuje k výkonu své funkce, pracovní nebo jiné činnosti.

Fyzická osoba musí být poučena před prvním přístupem k utajované informaci určitého stupně.

Poučena může být fyzická osoba, která pro stupeň VYHRAZENÉ má platné oznámení o splnění podmínek pro přístup k utajované informaci, nebo je držitelem platného dokladu o bezpečnostní způsobilosti nebo platného osvědčení fyzické osoby. Pro stupeň DŮVĚRNÉ, TAJNÉ a PŘÍSNĚ TAJNÉ pak může být poučen držitel platného osvědčení fyzické osoby.

Zánik platnosti poučení fyzické osoby

Platnost poučení fyzické osoby končí zánikem platnosti oznámení o splnění podmínek pro přístup k utajované informaci nebo osvědčení fyzické osoby.

Platnost dalších certifikátů

Platnost oznámení o splnění podmínek pro přístup k utajované informaci je povinen ten, kdo jej vydal, ověřovat každé tři roky ode dne jeho vydání.

Platnost dokladu o bezpečnostní způsobilosti je 5 let.

Platnost osvědčení fyzické osoby se pak odvíjí od stupně utajení, pro které bylo vydáno a činí:

- pro DŮVĚRNÉ 9 let od dne vydání
- pro TAJNÉ 7 let od dne vydání
- pro PŘÍSNĚ TAJNÉ 5 let od dne vydání.

	Přístup k utajovaným informacím stupně Vyhrazené	Přístup k utajovaným informacím stupňů Důvěrné nebo Tajné nebo Přísně tajné
Typ dokumentu nebo veřejné listiny nutný k přístupu či výkonu	Oznámení o splnění podmínek pro přístup k utajované informaci	----
	Osvědčení fyzické osoby	Osvědčení fyzické osoby
	Doklad o bezpečnostní způsobilosti	----

Tabulka 1: Dokumenty potřebné k přístupu k utajované informaci určitého stupně utajení

Přístup k utajovaným informacím lze umožnit také osobě, která byla poučena v případech, kdy NBÚ uzná bezpečnostní oprávnění vydané úřadem cizí moci.

Jaké podmínky musí být splněny

Fyzická osoba, které má být vydáno oznámení o splnění podmínek pro přístup k utajované informaci nebo osvědčení fyzické osoby (případně doklad o bezpečnostní způsobilosti), musí splnit určité podmínky. Jejich výčet je stanoven zákonem a jejich splnění se (kromě podmínek pro stupeň utajení Vyhrazené) ověřuje v bezpečnostním řízení. Definice jednotlivých podmínek jsou stanoveny zákonem č. 412/2005 Sb., a to v ustanoveních § 6 odst. 2 (způsobilost k právním úkonům, věk, bezúhonnost), v §§ 12, 13, 14 (státní občanství ČR, členské země EU nebo NATO, osobnostní způsobilost, bezpečnostní spolehlivost) a v §§ 81, 82, 83 a 84 (způsobilost k právním úkonům, věk, bezúhonnost, osobnostní způsobilost a spolehlivost). Poměrně přehledně jsou podmínky pro přístup k utajované informaci, vyžadované podle zákona č. 412/2005 Sb., znázorněny v tabulce 2.

	Oznámení V	Osvědčení D,T,PT	Doklad
Způsobilost k právním úkonům	X	X	X
Věk alespoň 18 let	X	X	X
Bezúhonnost	X	X	X
Státní občanství ČR, členské země EU nebo NATO		X	
Osobnostní způsobilost		X	X
Bezpečnostní spolehlivost		X	
Spolehlivost			X

Tabulka 2: Podmínky pro přístup k utajované informaci

Doklady potřebné pro vydání oznámení nebo osvědčení

Rozsah dokladů, které fyzická osoba předkládá, závisí na stupni utajení, pro který žádá vydání oznámení (pro Vyhrazené) nebo osvědčení (pro Důvěrné, Tajné nebo Přísně tajné).

Pro stupeň utajení Vyhrazené je třeba:

- platný občanský průkaz,
- výpis z evidence Rejstříku trestů (ne starší 3 měsíců) a
- prohlášení o způsobilosti k právním úkonům (vzor je stanoven vyhláškou o personální bezpečnosti).

Pro ostatní stupně je třeba:

- žádost (vzor je stanoven vyhláškou o personální bezpečnosti),
- vyplněný dotazník v listinné (spolu s fotografií) i elektronické podobě (vzor je stanoven vyhláškou o personální bezpečnosti),
- prohlášení o osobnostní způsobilosti (vzor je stanoven vyhláškou o personální bezpečnosti),
- prohlášení o způsobilosti k právním úkonům (vzor je stanoven vyhláškou o personální bezpečnosti),
- originály nebo ověřené kopie písemností dosvědčující správnost údajů uvedených v dotazníku.

Písemnostmi dosvědčujícími správnost údajů uvedených v dotazníku, které budou předkládány spolu se žádostí o vydání osvědčení jsou vždy:

- rodný list,
- doklad o nejvyšším dosaženém vzdělání,

- potvrzení zaměstnavatele o příjmech s uvedením jejich výše, v případě jiného druhu příjmu daňové priznání nebo jiný doklad potvrzující tento příjem, a to 5 let zpětně v případě první žádosti o vydání osvědčení nebo za období, které uplynulo od posledního předložení těchto dokladů v bezpečnostním řízení, má-li mít fyzická osoba přístup k utajované informaci i po skončení doby platnosti prvního osvědčení fyzické osoby.

V individuálních případech, tzn. je-li to relevantní, se předkládá dále:

- v případě studia v zahraničí potvrzení o studiu včetně doby trvání studia,
- rozhodnutí orgánů činných v trestním řízení ve věcech trestních podle zákona o trestním řízení,
- doklady o právech třetích osob zatěžujících vlastnictví žadatele (např. výpis z Katastru nemovitostí, pokud obsahuje zřízení zástavního práva),
- doklady dokumentující rozdíl mezi zápisem ve veřejném seznamu soudu nebo jiného státního orgánu a skutečností a
- rozhodnutí příslušného orgánu o nařízení výkonu rozhodnutí.

3.5.5 Ověření splnění podmínek a bezpečnostní řízení

Pro stupeň utajení Vyhrazené bude ověřovat splnění podmínek ten, kdo je vůči fyzické osobě v rámci služebního poměru nebo pracovněprávního, členského či obdobného vztahu odpovědnou osobou. Ten také následně zajistí poučení fyzické osoby a periodicky (každé 3 roky) ověřuje opětovně splnění podmínek.

U ostatních stupňů utajení (Důvěrné, Tajné a Přísně tajné) je po podání řádně vyplněné a zdůvodněné žádosti o vydání osvědčení

fyzické osobě (předložené spolu se všemi požadovanými podklady) zahájeno bezpečnostní řízení. Po jeho ukončení bude účastník vyrozuměn o jeho výsledku. Držitel osvědčení nebo oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené je v případě potřeby před prvním přístupem k utajované informaci poučen.

Účastník bezpečnostního řízení

Účastníkem bezpečnostního řízení je fyzická osoba, která žádá nebo pro kterou je žádáno o vydání osvědčení, další účastníci řízení nejsou stanoveni.

Dotčeným subjektem může v průběhu řízení být kterýkoli orgán státu, právnická nebo podnikající fyzická osoba, kteří jsou povinni na základě žádosti NBÚ poskytnout potřebnou informaci k ověření pravdivosti údajů poskytnutých účastníkem řízení, pokud s takovou informací nakládají. V průběhu řízení může být použito institutu svědka a znalce, kteří však nejsou účastníky řízení. Účastník řízení se může dát zastupovat advokátem nebo jiným zástupcem, kterého si zvolí. Zastoupení je vyloučeno pouze u osobních úkonů.

Lhůty pro ověření splnění podmínek

Lhůta pro ověření splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené není stanovena.

Lhůta pro provedení bezpečnostního řízení závisí na stupni utajení, pro který má být vydáno osvědčení a činí:

- pro Důvěrné 3 měsíce,

- pro Tajné 9 měsíců,
- pro Přísně tajné 12 měsíců.

Tuto lhůtu může ředitel NBÚ prodloužit maximálně o dobu stanovenou pro řízení daného stupně a to v případech, kdy nemůže zpravodajská služba nebo policie sdělit výsledky šetření ve stanovených lhůtách nebo orgán státu, právnická osoba nebo podnikající fyzická osoba nemůže poskytnout ve stanovené lhůtě informaci požadovanou v rámci řízení. Lhůty neběží po dobu přerušení řízení a je-li doručováno do zahraničí.

Opravné prostředky

Proti rozhodnutí NBÚ vydanému v bezpečnostním řízení má účastník řízení právo podat rozklad, pokud se tohoto práva po doručení rozhodnutí písemně nevzdal nebo pokud zákon nestanoví jinak.

Rozklad lze podat proti těmto rozhodnutím NBÚ:

- rozhodnutí NBÚ o nevydání osvědčení fyzické osoby,
- rozhodnutí NBÚ o zrušení platnosti osvědčení fyzické osoby,
- rozhodnutí NBÚ o zastavení řízení,
- rozhodnutí NBÚ o rozkladu a
- opravnému rozhodnutí NBÚ.

Rozklad se podává u NBÚ do 15 dnů ode dne doručení rozhodnutí. Podání rozkladu proti rozhodnutí o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele nebo dokladu nemá odkladný účinek. Náležitosti rozkladu jsou specifikovány v § 127 zákona č. 412/2005 Sb. Pokud rozklad nemá předepsané náležitosti, je

účastník řízení písemně vyzván k odstranění nedostatků a řízení je přerušeno.

Pokud je rozklad podle zákona nepřipustný nebo byl podán po uplynutí lhůty, NBÚ jej zamítne rozhodnutím, proti němuž lze dále podat rozklad. Shledá-li pro to důvody, vyhoví NBÚ rozkladu v plném rozsahu a napadené rozhodnutí zruší. Proti takovému rozhodnutí lze opět podat rozklad. Pokud NBÚ nerozhodne ani jedním z výše uvedených způsobů, předloží rozklad spolu se svým stanoviskem a veškerým spisovým materiálem do 15 dnů od doručení rozkladu řediteli NBÚ.

Ředitel NBÚ rozhoduje o rozkladu na základě návrhu rozkladové komise. O rozkladu musí rozhodnout do 3 měsíců ode dne jeho doručení. Řízení může být v této fázi zastaveno, rozhodnutí může být potvrzeno nebo rozkladu může být vyhověno a napadené rozhodnutí zrušeno. Tehdy je věc vrácena k novému projednání a rozhodnutí, pokud byl výrok vydán v rozporu s právními předpisy, nebo je jinak nesprávný nebo je zjištěno, že po vydání napadeného rozhodnutí nastaly skutečnosti, které mají vliv na rozhodnutí. V případě, že se ředitel NBÚ nerozhodne zastavit řízení či vyhovět rozkladu, rozklad zamítne a napadené rozhodnutí potvrdí.

Proti rozhodnutí ředitele NBÚ o rozkladu lze podat žalobu dle zákona č. 150/2002 Sb., soudního řádu správního. Proti rozhodnutí ředitele NBÚ o zastavení řízení lze podat žalobu pouze v případě, kdy je podle § 113 odst. 4 zákona č. 412/2005 Sb. proti důvodu zastavení řízení přípustný rozklad. Žaloba se podává ve lhůtě 30 dnů ode dne doručení rozhodnutí NBÚ, a to příslušnému krajskému soudu rozhodujícímu ve správním soudnictví - Městskému soudu v Praze.

Zánik platnosti osvědčení

Tato problematika je upravena v § 56 zákona č. 412/2005 Sb. Zde se mimo jiné praví, že:

- 1) *Platnost osvědčení fyzické osoby nebo osvědčení podnikatele zaniká*
 - a) *uplynutím doby jeho platnosti,*
 - b) *dnem vykonatelnosti rozhodnutí (§ 123 odst. 3, § 126 odst. 4 zákona č. 412/2005 Sb.) o zrušení jeho platnosti (§ 101 zákona č. 412/2005 Sb.),*
 - c) *úmrtím fyzické osoby, nebo byla-li prohlášena za mrtvou,*
 - e) *ohlášením jeho odcizení nebo ztráty,*
 - f) *takovým poškozením, že zápisy v něm uvedené jsou nečitelné nebo je porušena jeho celistvost,*
 - g) *změnou údajů v něm obsažených, nebo*
 - h) *skončením služebního poměru příslušníka zpravodajské služby nebo pracovního poměru zaměstnance zpravodajské služby, nebo přestane-li být fyzická osoba osobou uvedenou v § 141 odst. 1. zákona č. 412/2005 Sb. [48]*

Z citace zákona je patrné, že ne všechny důvody mají stejnou právní sílu a rovněž jsou též fakticky spojeny s různými důsledky. Zatímco skončení doby platnosti osvědčení a rozhodnutí o zrušení jeho platnosti mají tak říkajíc důsledky absolutní, poškození, ztráta či změna údajů mají dopad pouze relativní a znamenají, že původní osvědčení bude pouze vyměněno za osvědčení nové.

3.5.6 Bezpečnostní spolehlivost

Této oblasti je oproti ostatním potřeba věnovat větší pozornost, jelikož často není správně interpretována. Zvláště pokud jde o bezpečnostní rizika jako taková

V § 14 zákona č. 412/2005 Sb. jsou bezpečnostní rizika vymezena následovně:

(1) *Podmínku bezpečnostní spolehlivosti splňuje fyzická osoba, u níž není zjištěno bezpečnostní riziko.*

(2) *Bezpečnostním rizikem je: (a nemůže být posouzeno jinak, tedy že rizikem není!)*

a) *závažná nebo opakovaná činnost proti zájmům České republiky (co je zájem ČR je uvedeno v zákoně), nebo*

b) *činnost, spočívající v potlačování základních práv a svobod, anebo podpora takové činnosti.*

(3) *Za bezpečnostní riziko lze též považovat (a tedy je volba v posuzování - ten, kdo posuzuje, může rozhodnout tak, že formální projev v zákoně uvedený je nebo není bezpečnostním rizikem !!)*

a) *zařazení do složky bývalé Státní bezpečnosti s rozvědným nebo kontrarozvědným zaměřením, zpravodajské správy Generálního štábu Československé lidové armády nebo odboru vnitřní ochrany Sboru nápravné výchovy anebo prokazatelnou spoluprací s bývalou Státní bezpečností nebo zpravodajskou správou Generálního štábu Československé lidové armády nebo odborem vnitřní ochrany Sboru nápravné výchovy,*

b) *užívání jiné identity,*

c) *úmyslné porušení právních předpisů, na jehož základě může nastat újma zájmu České republiky,*

d) *chování, které má vliv na důvěryhodnost nebo ovlivnitelnost osoby a může ovlivnit její schopnost utajovat informace,*

e) *styky s osobou, která vyvíjí nebo vyvíjela činnost proti zájmu České republiky,*

f) *pravomocné odsouzení pro trestný čin,*

g) *uvedení nepravdivé informace nebo zamlčení informace rozhodné pro objektivní zjištění skutečného stavu věci v řízení podle části čtvrté nebo nenahlášení změny údajů uvedených v příloze k této žádosti o vydání osvědčení fyzické osoby (§ 94) nebo v jiném materiálu poskytnutém Úřadu v příloze k této žádosti,*

h) *porušení povinnosti při ochraně utajovaných informací, nebo*

i) *zřejmě nepřiměřené finanční nebo majetkové poměry vzhledem k řádně přiznaným příjmům fyzické osoby.*

(4) *Bezpečnostní rizika uvedená v odstavci 2 a odstavci 3 písm. a) se v případě žádosti podle § 94 zjišťují za období od 15 let věku; bezpečnostní rizika uvedená v odstavci 3 písm. b) až i) se zjišťují 10 let zpětně od podání žádosti pro stupeň utajení Důvěrné, 15 let zpětně pro stupeň utajení Tajné a 20 let zpětně pro stupeň utajení Přísně tajné, nebo za období od 15 let věku podle toho, které z nich je kratší.*

(5) *K bezpečnostnímu riziku uvedenému v odstavci 3 písm. b) se nepřihlíží, pokud fyzická osoba užívala jinou identitu ze zákonného důvodu.*

(6) *Při posuzování, zda skutečnost uvedená v odstavci 3 je bezpečnostním rizikem, se přihlíží k tomu, do jaké míry může ovlivnit schopnost utajovat informace, k době jejího výskytu, k jejímu rozsahu, charakteru a k chování fyzické osoby v období uvedeném v odstavci 4.*

(7) *Zpravodajská služba u svých příslušníků, zaměstnanců a uchazečů o zaměstnání nebo o přijetí do služebního poměru může při*

posuzování bezpečnostního rizika podle odstavce 3 provést fyziodetekční vyšetření, pokud zjištěné skutečnosti vyvolávají pochybnosti o schopnosti fyzické osoby utajovat informace.[48]

Při porovnání ustanovení o bezúhonnosti a bezpečnostní spolehlivosti je důležité věnovat pozornost následujícímu podstatnému rozdílu – zatímco bezúhonnost umožňuje považovat za bezúhonnou osobou, na kterou (i v případě, že byla v minulosti trestána) se pohlíží jako na netrestanou (osvědčení, zahlazení atd.), bezpečnostní spolehlivost tuto benevolenci nezná a pravomocné odsouzení za trestný čin **může** být posouzeno jako bezpečnostní riziko.

3.5.7 Personální bezpečnost

Vzhledem k tomu, že v následující část této rigorózní práce je zaměřena zejména na problematiku vztahující se k personální bezpečnosti, jako jednomu z druhů ochrany utajovaných informací, pokládám za nezbytné tuto oblast podrobněji specifikovat a detailně popsat.

Vymezení pojmu

Dva zákony, které tuto oblast upravovaly po roce 1998, tedy zákon č.148/1998 Sb. a zákon č.412/2005 Sb., užívaly pro tuto oblast poněkud odlišné vymezení, v zásadě však používaly oba zákony tento pojem ve shodném slova smyslu :

1/ zákon č.148/1998 Sb. definoval personální bezpečnost jako „systém opatření, jehož cílem je, aby se s utajovanými skutečnostmi seznamovala pouze fyzická osoba, která to nezbytně nutně potřebuje

k výkonu své činnosti, bylo jí vydáno osvědčení a je osobou určenou“, zatímco

2/ zákon č. 412/2005 Sb. hovoří o personální bezpečnosti v souvislosti s podmínkami přístupu fyzické osoby k utajovaným informacím, který umožňuje tehdy, jestliže fyzická osoba takové informace potřebuje nezbytně nutně k výkonu své funkce, pracovní nebo jiné činnosti, je držitelem platného osvědčení příslušného stupně a je poučena.

Koncepce personální bezpečnosti

Vidíme tedy, že až na několik detailů a jedné podstatné změny, o které se zmíníme dále (určení – poučení), je koncepce personální bezpečnosti stejná a je ovládána:

a) zásadou nezbytnosti přístupu k objektu utajování (tzv. „need to know“, čili „potřeba, nutnost vědět“) a

b) formálním povolením ze strany státu setkávat se v tomto nezbytném rámci s takovým objektem utajování, tedy osvědčením, které stát vydává fyzické osobě po určité proceduře (bezpečnostní řízení, dříve, podle zák.č.148/1998 Sb., bezpečnostní prověrka)

3.5.8 Princip věcného určení a poučení

Existuje však jeden zásadní rozdíl mezi oběma právními úpravami, a sice v tom, že zákon číslo 148/1998 Sb. stál při umožnění styku s utajovanou skutečností na principu věcného určení (to znamenalo v praxi, že držitel osvědčení se mohl stýkat pouze s utajovanou skutečností, pro kterou byl věcně určen), zatímco zákon číslo 412/2005 Sb. stojí na principu poučení (tzn. v praxi, že ten, kdo je jednou poučen, se může stýkat, samozřejmě při zachování zásady nezbytnosti, s jakoukoliv utajovanou informací, pokud má odpovídající

stupeň osvědčení). Vidíme tedy, že princip „*need to know*“ je zde oslaben, byť formálně je zásada nezbytnosti zachována.

3.5.9 Problémy současné právní úpravy

Předchozí právní úprava nebyla ideální. Trpěla vážnými nedostatky, které byly postupnými novelizacemi postupně řešeny. Nový zákon číslo 412/2005 Sb. některé nedokonalosti vyřešil, jiné však bohužel přinesl. Porovnáním obou právních úprav zjišťujeme v té dnešní problémy, které spočívají zejména v následujícím:

- je umožněn trvalý přístup k utajovaným informacím skupině osob, které se nemusí podrobit bezpečnostnímu řízení a nemusí tedy být držiteli platného osvědčení pro přístup k utajovaným informacím (§ 58 zákona č. 412/2005 Sb (osoby, které mají zvláštní přístup k utajované informaci). Rozsah stanovený v naší právní úpravě je neúnosně široký a je v rozporu s mezinárodními závazky, které republika přijala.
- je umožněn přístup k utajovaným informacím skupině osob, které se nemusí podrobit bezpečnostnímu řízení a nemusí tedy být držiteli platného osvědčení pro přístup k utajovaným informacím, aniž by tyto osoby byly uvedeny v § 58 zákona č. 412/2005 Sb.– jde o advokáty, u kterých Ústavní soud rozhodl, že po nich český stát nemůže vyžadovat bezpečnostní prověrku podle zákona
- problematickým se jeví přístup k utajovaným informacím tehdy, když se takové informace dotýkají soudního řízení a osob zde zúčastněných (§ 58 odst. 4,5 zákona č. 412/2005 Sb.) – tyto osoby se pak seznamují s utajovanými informacemi bez jakéhokoliv prověření (v praxi : předseda senátu zúčastněné osoby poučí, že se bude projednávat utajovaná informace a seznámí je s jejím obsahem)

- zákon zrušil institut tzv. věcného určení fyzické osoby (jak jej znala předchozí právní úprava), který zajišťoval lepší aplikaci zásady „*need to know*“ – předchozí právní úprava zajišťovala kompatibilitu se směrnicemi NATO (C-M(55)15(Final) z roku 1955 a C-M(2002)49 z června 2002) o tom, že fyzické osobě lze povolit přístup k utajované informaci až po vydání osvědčení a rozhodnutí o tom, že se musí s utajovanou informací nutně seznamovat a vymezení oblasti takového styku. Dnešní právní úprava zásadu věcného určení (tj. zdůvodnění nutnosti přístupu ke konkrétní informaci či konkrétní oblasti utajovaných informací) opustila a zavedla institut „poučení“. Toto poučení se však provádí pouze před prvním přístupem k utajované informaci a v praxi to znamená, že vydané osvědčení a prvé poučení zajišťuje přístup k utajované informaci vždy a všude, tedy alespoň po dobu platnosti osvědčení. Ten, kdo je držitelem platného osvědčení a je poučen, se bude vždy s utajovanou informací stýkat oprávněně, ať se s ní setká v jakémkoliv rozsahu a ať se jedná o informaci jakéhokoliv druhu. Podmínkou je pouze odpovídající stupeň osvědčení a poučení. Zásada nezbytnosti je sice deklarována, ale v praxi je problematicky uplatnitelná
- zákon velice zvolnil kritéria pro posuzování toho, co je či není bezpečnostní riziko – je v tomto ohledu velmi benevolentní. Jako příklad lze uvést, že je-li pro směrnicí NATO rizikem těžko vysvětlitelný finanční nadbytek, pak podle českého zákona může být tato skutečnost hodnocena jako riziko pouze tehdy, jestliže současně ovlivňuje schopnost utajovat informace. Stejně je pak podvázána většina možných bezpečnostních rizik (§ 14 odst. 2, 6 zákona č. 412/2005 Sb.).
- v zásadě je možné soudní cestou přinutit stát jako držitele utajované informace k vydání osvědčení pro přístup k utajované informaci. Zákon sice správnímu soudu, který provádí přezkum

rozhodnutí státu, tuto možnost přímo nedává, ale z jiných zákonů vyplývá, že tato možnost existuje. Namísto toho, aby se soud zabýval pouze tím, zda byly dodrženy formální předpisy a nebyla krácena formální práva fyzické osoby, tj. zda v řízení bylo vše podle zákona, je mu dána možnost přezkumu vlastního obsahu a důvodnosti rozhodnutí státu. Protože správní orgán (což je v řízení podle zákona o přístupu k utajovaným informacím NBÚ či zpravodajská služba) je rozhodnutím soudu vázán, lze dovodit, že fyzická osoba se může na státu přístupu k utajované informaci soudní cestou domoci.

3.5.10 Přístup k utajované informaci bez platného osvědčení

§ 58 zákona č. 412/2005 Sb. upravuje okruh osob, které vzhledem k jejich specifickému postavení mají přístup k utajované informaci bez platného osvědčení a poučení, a zároveň se stanoví postup pro jejich přístup k utajované informaci. Mají-li se ovšem tyto osoby seznamovat s utajovanými informacemi cizí moci, musí se podrobit bezpečnostnímu řízení podle navrhovaného zákona, což ovšem neplatí pro prezidenta republiky, předsedy Poslanecké sněmovny a Senátu Parlamentu České republiky, předsedu vlády, ministra zahraničních věcí a soudce (§ 58 odst. 11 zákona č. 412/2005 Sb.). To vše samozřejmě při dodržení principu "potřeby znát".

Přístup k utajovaným informacím bez platného osvědčení fyzické osoby pak lze například umožnit i fyzické osobě jednající ve prospěch zpravodajské služby, informátorovi nebo fyzické osobě, které je poskytována zvláštní ochrana podle zvláštního právního předpisu, nebo příslušníku zpravodajské služby, který je zařazen v záloze zvláštní. Poučení této osoby pak provede ten, kdo jí přístup k utajované informaci umožní. Výše uvedené osoby jsou přesně specifikovány v příslušných zákonech.

Osoby, které mají zvláštní přístup k utajované informaci

Osobami, které mají přístup k utajované informaci všech stupňů utajení bez platného osvědčení fyzické osoby a poučení, jsou

- a) prezident republiky,
- b) poslanci a senátoři Parlamentu,
- c) členové vlády,
- d) Veřejný ochránce práv a zástupce Veřejného ochránce práv,
- e) soudci a
- f) prezident, viceprezident a členové Nejvyššího kontrolního úřadu.

3.5.11 Jednorázový přístup k utajované informaci

Na základě písemné žádosti odpovědné osoby může NBÚ ve výjimečných a odůvodněných případech vydat souhlas s jednorázovým přístupem k utajované informaci se stupněm utajení o jeden vyšším, než na který je vydáno platné osvědčení fyzické osoby nebo osvědčení podnikatele, a to na dobu nezbytně nutnou, nejdéle však na dobu 6 měsíců.

3.6 Další významné oblasti zajištění ochrany utajovaných informací

3.6.1 Administrativní bezpečnost

Administrativní bezpečnost je stěžejní oblastí bezpečnosti, jejímž prostřednictvím je zajišťována ochrana utajované informace. Především je zde řešeno vyznačování údajů na utajované informaci a evidence utajované informace. Dále jsou zde řešena opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi.

Vyznačování údajů a evidence utajovaných informací

Jednou ze základních a zcela nezbytných zásad je, že každá utajovaná písemnost musí být zaevidována v příslušné administrativní pomůcce, kterou je např. jednací protokol. Na každé utajované informaci, resp. na jejím nosiči, musí být vyznačen příslušný stupeň utajení. Nebude-li možné takto učinit, bude se příslušný stupeň utajení deklarovat jiným způsobem. Na nosiči utajované informace bude možné vyznačit i dobu, po kterou se bude informace utajovat. Tento princip přispívá k omezení utajování v případech, kdy důvod utajení již pominul. Ustanovení upravuje i odpovědnost NBÚ a ostatních ze zákona odpovědných subjektů v případě, kdy zanikne původce utajované informace.

Utajovaná informace cizí moci

Příslušným stupněm utajení se rovněž označuje utajovaná informace cizí moci poskytnutá České republice nebo utajovaná informace cizí moci, k jejíž ochraně se Česká republika zavázala.

Takto se neoznačují všechny strany, ale pouze první strana, kde se vyznačí český ekvivalent příslušného stupně utajení. Povinnost tohoto označení má ten, kdo takovou utajovanou informaci zaeviduje v České republice jako první. Podrobnosti tohoto označování stanoví prováděcí předpis. Převodníky stupňů utajení jsou obsaženy v jednotlivých mezinárodních smlouvách, týkajících se oblasti ochrany utajovaných informací.

Ustanovení § 21 zákona č. 412/2005 Sb. dále vymezuje případy, kdy může dojít ke změně nebo zrušení stupně utajení a stanovuje podmínky, za kterých k tomuto může dojít.

Prováděcí právní předpis stanoví podrobnosti zabezpečení administrativní bezpečnosti včetně podrobností, týkajících se vyznačování stupňů utajení.

Pořizování opisů, kopií nebo překladů utajovaných informací

Co se týče pořizování opisů, kopií nebo překladů utajovaných informací stupně utajení Přísně tajné nebo výpis z nich, mohou být vyhotoveny pouze na základě písemného souhlasu původce; jde-li o utajovanou informaci stupně utajení Tajné nebo Důvěrné, mohou být vyhotoveny pouze s písemným souhlasem přímo nadřízené osoby.

Přeprava či přenos utajované informace

Přeprava či přenos utajované informace je umožněn pouze v přenosných schránkách nebo v uzavřeném obalu v závislosti na jejím stupni utajení a na jejím nosiči; přepravovat ji lze pouze prostřednictvím kurýrní služby nebo držitele poštovní licence (podle vyhlášky č. 397/2000 Sb., kterou se mění vyhláška č. 245/1998 Sb., o osobnostní způsobilosti a vzorech tiskopisů používaných v oblasti personální bezpečnosti).

Vyznačování stupňů utajení

Ustanovení § 22 zákona č. 412/2005 Sb. se týká povinností při vyznačování stupňů utajení. Podle tohoto ustanovení se stupeň utajení na utajované informaci vyznačí při jejím vzniku, nestanoví-li zákon jinak (§ 70 zákona č. 412/2005 Sb.). Dále pak je stanoveno, že vyznačení stupně utajení na utajované informaci musí být zachováno po celou dobu trvání důvodů utajení. Bez souhlasu původce nebo poskytující cizí moci nesmí být stupeň utajení změněn nebo zrušen. Vyžaduje-li to charakter utajované informace, musí původce vyznačit na utajované informaci dobu, po kterou bude informace utajována. Stupeň utajení zaniká uplynutím vyznačené doby.

Zrušení nebo změna stupně utajení

Stupeň utajení původce neprodleně zruší nebo změní po zjištění, že pominul důvod pro utajení informace, důvody pro utajení neodpovídají stanovenému stupni utajení nebo byl-li stupeň utajení stanoven neoprávněně, a na utajované informaci toto zrušení nebo změnu jejího stupně utajení vyznačí. Původce je povinen prověřit, zda důvod pro utajení informace trvá, a to nejméně jednou za pět let ode dne jejího vzniku. Toto zrušení či změna musí být původcem utajované informace oznámena neprodleně adresátům utajované informace, a to písemně. Adresáti utajované informace oznámí neprodleně písemně tuto skutečnost všem dalším adresátům, kterým utajovanou informaci zpřístupnili.

Výše uvedená povinnost se nevztahuje na předávání utajované informace do stupně utajení Tajné mezi zpravodajskými službami a obdobnými službami cizí moci, uskutečňované v rámci spolupráce podle zvláštního právního předpisu, a to v případech, kdy výše

zmíněný postup nelze dodržet (s výjimkou utajovaných informací vyžadujících zvláštní režim nakládání).

Prováděcí právní předpis pak stanoví např. způsob vyznačování náležitostí na utajované informaci, druhy administrativních pomůcek, náležitosti souhlasu k pořizování opisu, kopie, výpisu a překladu utajované informace nebo podrobnosti k přepravě, přenášení, převzetí a zapůjčování utajované informace.

3.6.2 Fyzická bezpečnost

Dalším významným druhem zajištění ochrany utajovaných informací je fyzická bezpečnost. Zákon v této oblasti definuje základní pojmy používané v této oblasti a stanovuje základní bezpečnostní opatření při projednávání, zpracování a ukládání utajovaných informací.

Podle nejvyššího stupně utajení ukládaných utajovaných informací se stanoví kategorie zabezpečených oblastí. Zabezpečené oblasti se zde dále podle možnosti seznámení s utajovanou informací člení do jednotlivých tříd.

Jednotlivá ustanovení zákona č. 412/2005 Sb. týkající se fyzické bezpečnosti, upravují zejména projednávání utajovaných informací, stanoví povinnosti odpovědné osobě při realizaci bezpečnostních opatření v této oblasti, aby při jednáních nedocházelo k ohrožení nebo k úniku utajovaných informací. Dále obsahují výčet opatření fyzické bezpečnosti, jejichž prostřednictvím je realizováno zabezpečení ochrany utajované informace. Je zde například upraven způsob provádění ostrahy, definována režimová opatření a vyjmenovány technické prostředky, které se při provádění fyzické bezpečnosti zpravidla používají.

Zajištění fyzické bezpečnosti spočívá v kombinaci těchto opatření, např. ostrahou se tak rozumí nejen fyzická přítomnost osob

v místě střežení, ale též kombinace dalších opatření fyzické bezpečnosti užitých pro tento účel. Přítomnost zákonem stanoveného počtu osob přímo ve střeženém objektu není podmínkou. Podrobnosti realizace opatření fyzické bezpečnosti stanoví prováděcí předpis. Stanovuje se také povinnost kontroly aktuálního stavu fyzické bezpečnosti [52].

3.6.3 Kryptografická ochrana utajovaných informací

Kryptografická ochrana je specifickým druhem zajištění ochrany utajovaných informací. Při její realizaci jsou využívány zcela specifické prostředky, materiály, metody a postupy. Kryptografickou ochranu tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací [48].

Zákonem jsou nejprve definovány pojmy používané v této oblasti. Pro účely této práce není tato oblast příliš významná, proto se o ní zmiňuji spíše na okraj.

V zákoně se stanovuje povinnost certifikace kryptografického prostředku a pracoviště. Stanovuje se povinnost vedení evidencí v oblasti kryptografické ochrany, činnosti spadající do oblasti kryptografické ochrany a podmínky pro jejich výkon. Na osoby, které je budou realizovat jsou kladeny požadavky nejen z oblasti personální bezpečnosti, ale i zvláštní požadavky z oblasti odborné.

Zákon č. 412/2005 Sb. stanoví podmínky pro výkon kryptografické ochrany. Kromě obecných podmínek pro přístup k utajovaným informacím je další podmínkou pro výkon této činnosti i zvláštní odborná způsobilost. Tato se bude prokazovat osvědčením o zvláštní odborné způsobilosti, které bude vydáváno na základě úspěšně vykonané zkoušky. Vykonání zkoušky o zvláštní odborné způsobilosti bude zajišťovat NBÚ nebo jím pověřený orgán státu.

Jedná se zejména o pracoviště Ministerstva vnitra nebo Ministerstva obrany, kde jsou již tato pracoviště vybavena příslušným technickým zázemím.

Cílem těchto opatření je dosáhnout stavu, aby příslušné osoby, které budou plnit řadu důležitých úkolů v oblasti kryptografické ochrany utajovaných informací měly patřičné znalosti a dovednosti, což by mělo přispět ke zvýšení celkové kvality provádění ochrany utajovaných informací.

3.6.4 Výkon státní správy v oblasti ochrany utajovaných informací (NBÚ, ZS, MV, Policie ČR)

Výkon státní správy v oblasti ochrany utajovaných informací je nadále svěřen NBÚ, který má již vybudované materiální i personální podmínky pro zabezpečování svých činností.

Zákon též stanoví základní úkoly a oprávnění NBÚ, které jsou nezbytné při realizaci celého systému ochrany utajovaných informací a bezpečnostní způsobilosti fyzických osob.

3.6.5 Státní dozor v oblasti ochrany utajovaných informací

Výkon státního dozoru nad dodržováním povinnosti v oblasti ochrany utajovaných informací je svěřen NBÚ. K tomu, aby mohl být vykonáván, jsou jeho kontrolním pracovníkům přiznána potřebná oprávnění, z nichž nejvýznamnější je oprávnění přístupu k utajovaným informacím v rozsahu prováděné kontroly, a to pokud se kontrolní pracovníci prokáží platným osvědčením fyzické osoby pro příslušný stupeň utajení. Při výkonu státního dozoru se postupuje přiměřeně podle zákona o státní kontrole ve znění pozdějších předpisů. Ustanovením je rovněž řešena kontrola utajovaných informací, poskytnutých ČR cizí mocí, kdy vlastní výkon státního dozoru zůstává

svěřen NBÚ, přičemž právo účastnit se kontroly se přiznává pracovníkům úřadu cizí moci.

Z důvodu specifického postavení a činnosti v oblastech, kde mají obdobnou působnost jako NBÚ, jsou zpravodajské služby a Ministerstvo vnitra vyňaty ze státního dozoru prováděného NBÚ.

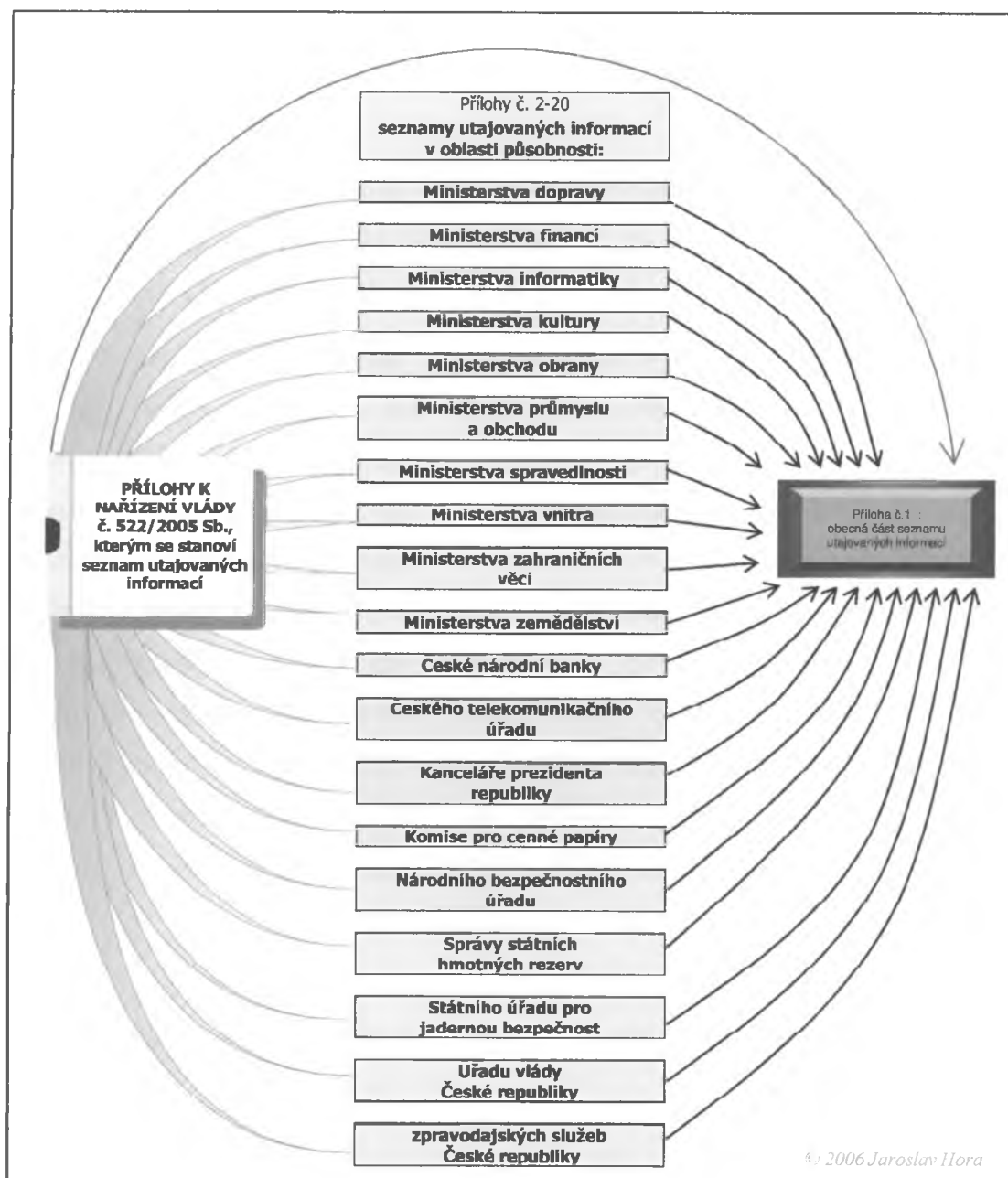
Při zjištění porušení právních předpisů v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti jsou kontrolní pracovníci oprávněni přijímat potřebná opatření k odstranění následků způsobených nedodržováním uložených povinností. Každý je povinen vyhovět pokynům kontrolního pracovníka při provádění neodkladných opatření. V opačném případě je NBÚ oprávněn uložit pořádkovou pokutu za nesplnění povinností.

3.7 Seznam utajovaných informací

3.7.1 Příklady z obecné části a seznam resortů a jiných státních orgánů, u kterých byl stanoven seznam utajovaných informací

Nařízením vlády č. 522/2005 Sb., ze dne 7. prosince 2005, se stanoví seznam utajovaných informací. Toto nařízení stanoví mimo jiné dvě části seznamu utajovaných informací – obecnou část, a část, kterou lze nazvat částí zvláštní.

Podle přílohy č. 1 k tomuto nařízení klasifikuje původce utajovanou informaci tehdy, není-li v přílohách č. 2 až 20 k tomuto nařízení stanoveno jinak. Souvislosti mezi jednotlivými přílohami jsou přehledně zobrazeny na obr. 4. a dále je tato problematika rozvedena v následujících odstavcích.



obr. 4: Vztahy mezi jednotlivými přílohami seznamu utajovaných informací

3.7.2 Vztah obecné a zvláštní části seznamu utajovaných informací

Původce klasifikuje utajovanou informaci v rámci rozsahu stupňů utajení uvedených v přílohách č. 1 až 20 k tomuto nařízení tím

stupněm utajení, který v případě jejího vyzrazení nebo zneužití odpovídá závažnosti možného způsobení újmy zájmu České republiky, anebo nevýhodnosti pro zájem České republiky.

Jak je výše uvedeno, seznamy utajovaných informací podle nařízení vlády č. 522/2005 Sb. lze členit na část obecnou (v příloze č. 1) a část zvláštní (v příloze č. 2 až 20).

V praxi to znamená, že u ministerstva nebo jiného státního orgánu, v jehož působnosti byl stanoven seznam utajovaných informací, který byl vydán ve zvláštní části, v příloze č. 2 až 20, k nařízení vlády č. 522/2005 Sb., se předpokládá vznik utajovaných informací, konkretizovaných v seznamu. V rámci těchto státních orgánů je proto třeba při klasifikaci utajované informace podle stupně utajení vycházet ze seznamu obecného (v příloze č. 1) a ze seznamu zvláštního současně, přičemž státní orgán si volí konkrétní přílohu nařízení vlády č. 522/2005 Sb., podle své působnosti. Oba tyto seznamy jsou tak vodítkem při posuzování informací z hlediska ochrany utajovaných informací podle zákona č. 412/2005 Sb.

3.7.3 Aplikace obecné části seznamu utajovaných informací

Pokud však ve zvláštní části, v příloze č. 2 až 20, k nařízení vlády č. 522/2005 Sb. nebyl pro působnost daného ministerstva nebo jiného státního orgánu vydán seznam utajovaných informací, lze předpokládat, že u těchto státních orgánů buď utajované informace nevznikají, anebo vznikají, ale pouze utajované informace, které stanovila obecná část seznamu utajovaných informací, v příloze č. 1, k nařízení vlády č. 522/2005 Sb.

3.7.4 Původce a adresát utajovaných informací

Jestliže u ministerstev nebo jiných státních orgánů utajované informace vznikají, ať tedy na úrovni obecné nebo zvláštní podle nařízení vlády č. 522/2005 Sb., stávají se tyto státní orgány původci utajovaných informací. Pokud by u některých státních orgánů utajované informace nevznikaly, mohly by se ale stát adresáty utajovaných informací v případě, že by jim poskytl utajované informace jiný původce.

3.7.5 Porovnání s dřívější právní úpravou

Srovnáme-li seznam utajovaných informací podle nařízení vlády č. 522/2005 Sb. se seznamem utajovaných skutečností podle nařízení vlády č. 246/1998 Sb., zjistíme, že zvláštní část nařízení vlády č. 522/2005 Sb. na jedné straně již neobsahuje seznam v působnosti některého státního orgánu (ministerstva zdravotnictví a Nejvyššího kontrolního úřadu) a na druhé straně obsahuje seznam jiného státního orgánu (Český telekomunikační úřad, Správa státních hmotných rezerv), v jehož působnosti seznam utajovaných skutečností dříve vydán nebyl.

Z tohoto srovnání je patrný vývoj na straně subjektů, u nichž vznikají utajované informace, přičemž původci utajovaných informací mohou nejen vznikat, ale i zanikat. Rovněž tak je patrný vývoj u charakteristiky utajovaných informací podle jednotlivých položek seznamů utajovaných informací, a to v obecné i ve zvláštní části, v příloze č. 1 až 20, k nařízení vlády č. 522/2005 Sb., kde zaznamenáváme jejich zpřesnění a konkretizaci.

Názorně vývoj na straně subjektů, u nichž vznikají utajované skutečnosti a vývoj charakteristiky utajovaných skutečností, vidíme u seznamů utajovaných skutečností podle nařízení vlády č. 246/1998 Sb., kde zaznamenáváme změny a doplňky podle šesti novelizačních

úprav. Lze proto předpokládat, že i seznamy utajovaných informací podle nařízení vlády č. 522/2005 Sb. nebudou neměnné, ale mohou časem doznat novelizačních úprav [53].

3.8 Připravovaná novela zákona 412/2005 Sb.

3.8.1 Důvody navrhovaných změn

Legislativní proces je v České republice již delší dobu v takovém stavu, že ve velice krátké době po schválení nového zákona se projeví potřeba tento zákon novelizovat. Ani v případě poměrně nového zákona o utajovaných informacích tomu není jinak. Hlavním důvodem a cílem předkládané novely zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, je nezbytnost urychlené nápravy ustanovení, které umožňuje širokému okruhu osob mít přístup k utajovaným informacím NATO bez platného osvědčení (§ 58 zákona č. 412/2005 Sb.). Pro NATO je tato situace a princip zcela nepřijatelný.

3.8.2 Řešení komplikací při zániku platnosti osvědčení fyzické osoby

Zároveň se touto novelou odstraňuje problém, který komplikoval činnost zpravodajských služeb a Ministerstva vnitra. Tento problém se týká zániku platnosti osvědčení fyzické osoby z důvodů uvedených v § 56 odst. 1 písm. h) zákona. Návrh odstraňuje neodůvodněnou nerovnost příslušníků a zaměstnanců zpravodajských služeb ve srovnání s ostatními držiteli osvědčení fyzické osoby, která vyplývá ze stávajícího znění, a tím vyhovuje principu rovnosti, který je základním principem ústavního pořádku České republiky a předchází možným

stížnostem před Ústavním soudem. Dále se v návrhu upřesňují některé další instituty, u kterých praxe ukázala potřebu jejich změny.

3.8.3 Jednotný průběh bezpečnostního řízení

Jak sám zákonodárce v návrhu novely uvádí, zákon nově upravuje průběh bezpečnostního řízení jednotně, tedy bez ohledu na to, který z příslušných orgánů státu (NBÚ nebo např. zpravodajská služba) jej provádí. Z tohoto důvodu je třeba považovat rozhodnutí o žádosti fyzické osoby vydaná kterýmkoli z těchto orgánů státu na základě řádně provedeného bezpečnostního řízení za rovnocenné správní akty, které se stejnou mírou spolehlivosti určují, zda daná fyzická osoba splňuje podmínky personální bezpečnosti, či nikoli.

Z výše uvedeného vyplývá, že osvědčení fyzické osoby vydaná kterýmkoli z příslušných orgánů státu jsou ekvivalentními veřejnými listinami. Současně je však nevhodné, aby fyzická osoba, která je držitelem osvědčení fyzické osoby a přešla z hlediska předmětu úpravy zákona z působnosti jednoho z příslušných orgánů státu do působnosti jiného (tj. např. pokud se stala příslušníkem či zaměstnancem zpravodajské služby), nadále disponovala osvědčením fyzické osoby vydaným orgánem státu, jenž k tomu byl původně příslušný.

Takováto situace by mohla vést k určitým nežádoucím důsledkům, např. pokud by fyzická osoba přestala splňovat podmínky fyzické bezpečnosti: v takovém případě by v důsledku ustanovení § 137 písm. a), resp. § 140 odst. 1 písm. a) zákona č. 412/2005 Sb., rozhodoval o zrušení platnosti jejího osvědčení jiný správní orgán, než který toto osvědčení vydal. Kromě toho by vznikaly nejasnosti i ohledně plnění některých povinností fyzických osob, např. povinnosti vrátit osvědčení fyzické osoby, jehož platnost skončila. V případech, kdy fyzická osoba přechází z působnosti zpravodajské služby do

působnosti NBÚ, je navíc nutné respektovat i bezpečnostní hlediska vyplývající z její dřívější příslušnosti ke zpravodajské službě.

Nový návrh změny zákona tedy počítá s tím, že pro všechna osvědčení fyzické osoby vydaná kterýmkoli z oprávněných orgánů státu bude platit shodný režim, tj. jejich platnost zanikne v okamžiku, kdy fyzická osoba přejde z hlediska zákona do působnosti jiného orgánu státu oprávněného vydávat osvědčení fyzické osoby.

3.8.4 Formální důvody zániku platnosti osvědčení fyzické osoby

Z hlediska spolehlivosti zjištění, zda fyzická osoba splňuje podmínky fyzické bezpečnosti, není rozhodné, který z příslušných orgánů státu provedl bezpečnostní řízení. Pokud tedy zaniká platnost osvědčení fyzické osoby v případech podle navrhovaného ustanovení § 56 odst. 1 písm. h) a i), dochází k tomu především z důvodů formálních (procesních), tedy aniž by uplynula doba platnosti původního osvědčení fyzické osoby a aniž by dotčená fyzická osoba přestala splňovat materiální podmínky přístupu k utajovaným informacím (tj. zejména podmínku osobnostní způsobilosti a bezpečnostní spolehlivosti).

Zákonodárce proto navrhuje, aby v případě, že fyzická osoba dotčená takovýmto zánikem platnosti osvědčení fyzické osoby potřebuje mít i nadále přístup k utajovaným informacím, jí bylo nově příslušným orgánem státu vydáno osvědčení nové, nahrazující původní osvědčení fyzické osoby, pokud jde o nejvyšší stupeň utajení utajované informace, pro přístup k ní opravňuje a dobu platnosti. Orgán státu, který této fyzické osobě nové osvědčení vydal, bude vůči ní vykonávat všechna práva a povinnosti vyplývající ze zákona č. 412/2005 Sb. Obdobně bude tato fyzická osoba plnit své povinnosti stanovené tímto zákonem vůči orgánu státu, jenž jí nové osvědčení vydal.

3.8.5 Zjednodušení opětovného vydání osvědčení fyzické osoby

Nové osvědčení by mělo být fyzické osobě vydáno v podstatě automaticky, tj. především bez provádění nového bezpečnostního řízení. Návrh přesto obsahuje určité procedurální odlišnosti v případě, kdy je příslušným vydat nové osvědčení NBÚ. Tyto odlišnosti však vyplývají pouze z povahy skutečnosti odůvodňující vydání nového osvědčení: zatímco v případě zpravodajských služeb je rozhodnou skutečností pro jeho vydání právní úkon učiněný samotnými těmito orgány (tj. přijetí do služebního či pracovního poměru, resp. ustanovení policisty na příslušnou funkci), v případech, kdy je k vydání příslušný NBÚ, bude potřeba vydání nového osvědčení zpravidla vycházet ze skutečností, o nichž se NBÚ nemůže bez součinnosti dané fyzické osoby dozvědět.

3.8.6 Změny ve vedení bezpečnostních svazků

Co se týče vedení dokumentace k bezpečnostnímu řízení, tedy bezpečnostního svazku, navrhuje zákonodárce poměrně výraznou změnu oproti stávajícímu stavu. Tato úprava je však, vzhledem k výše uvedeným změnám, nezbytná. Jedná se o to, že bezpečnostní svazek povede po zániku platnosti příslušného osvědčení fyzické osoby nadále orgán státu, který jej vydal. Bude-li však fyzické osobě vydáno nové osvědčení, musí být, z důvodu řádného plnění povinností stanovených zákonem, orgánu státu, který nové osvědčení vydal, předán i příslušný bezpečnostní svazek. Předání bezpečnostního svazku proběhne na písemné vyžádání orgánu státu, který vydal nové osvědčení fyzické osoby [54].

3.9 Porovnání obecně závazné právní úpravy s každodenní realitou

3.9.1 Prevence a informovanost veřejnosti

V oblasti ochrany utajovaných informací je důležité klást důraz na prevenci, a to zejména prostřednictvím větší informovanosti veřejnosti, aby každému bylo zřejmé, jak je důležité chránit utajované informace. Podle mého názoru by tak nedocházelo ve velké míře k porušování povinností při ochraně utajovaných informací uložené zákonem č. 412/2005 Sb., a to zejména prostřednictvím médií.

3.9.2 Zásadní povinnosti při ochraně utajovaných informací

Zákon č. 412/2005 Sb. stanoví povinnosti při ochraně utajovaných informací, a to v obecné rovině, tj. každé fyzické osobě, a v rovině zvláštní, tj. zejména fyzické osobě, která má přístup k utajované informaci, popř. je-li pouze držitelem osvědčení fyzické osoby, nebo podnikateli, který je držitelem osvědčení podnikatele, anebo právnické osobě a podnikající fyzické osobě, které mají přístup k utajované informaci, a orgánu státu.

Vzhledem k tomu, že v další části této práce jsou uvedeny příklady porušování povinnosti ochrany utajovaných informací v mediální oblasti, považuji za důležité porovnat obecně závaznou právní úpravu těchto otázek:

a) Pokud jde o zákon č. 412/2005 Sb., v obecné rovině stanoví povinnost pro každého, aby neprodleně odevzdal nalezenou utajovanou informaci, tj. dokument, jeho část, popř. jednotlivý list, označený stupněm utajení, a to NBÚ, Policii ČR nebo zastupitelskému

úřadu ČR. Stejně tak si má počínat každý, kdo utajovanou informaci získá v rozporu se zákonem č. 412/2005 Sb. Kromě toho zákon ukládá každému, kdo měl nebo má přístup k utajované informaci, povinnost zachovávat o ní nejen mlčenlivost, ale i neumožnit přístup k utajované informaci neoprávněné osobě. Právě vyzrazení utajované informace je jednou z forem neoprávněného nakládání, které může mít za následek i trestněprávní sankci.

b) Při srovnávání těchto ustanovení zákona č. 412/2005 Sb. s čl. 17 Listiny zaručující svobodu projevu a právo na informace, nelze neuvést ustanovení odst. 4 tohoto článku Listiny, který stanoví, že svobodu projevu a právo šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná mimo jiné pro ochranu práv a svobod druhých nebo pro bezpečnost státu. V obecné rovině ustanovení zákona č. 412/2005 Sb. tedy plně korespondují s odst. 4 čl. 17 Listiny.

c) Srovnáme-li výše uvedená ustanovení zákona č. 412/2005 Sb. se zákonem č. 106/1999 Sb., zjistíme, že také tento zákon respektuje ochranu utajovaných informací a v některých případech stanoví omezení práva na informace (pokud je informace jako utajovaná označena tak subjekt, který je podle zákona povinen poskytnout informaci, ji žadateli neposkytne v případě, že žadatel nemá k informaci oprávněný přístup). Také v tomto případě nejsou uvedena ustanovení *contra legem*, tj. protiprávní.

3.9.3 Porušování základních povinností

Přestože tedy existuje výše uvedená obecně závazná právní úprava sledovaných otázek, neustále dochází ke zveřejňování utajovaných informací v médiích a tím k porušování povinností při

ochraně utajovaných informací stanovených zákonem č. 412/2005 Sb. V případech úniku utajované informace v médiích se veškeré subjekty, které jsou zainteresovány na poskytnutí, předání a dalším zveřejnění utajované informace, nechovají tak, jak předepisuje zákon.

Kromě toho existuje možnost, že ve většině případů se subjekty takto chovají účelově. Například v článku „Právní stát po Česku aneb Zákony musí platit pro všechny“ v Právu ze dne 11.10.2006, se autorka, bývalá nejvyšší státní zástupkyně Marie Benešová, vyjadřuje k otázkám úniku tajné zprávy dvou policejních důstojníků do médií takto: „Dovolím si říci, že postup obou důstojníků zakládá minimálně podezření ze zneužití pravomoci veřejného činitele. A nejen to. Jejich postup destabilizuje policejní sbor. Poškozuje prestiž české policie a České republiky v zahraničí. Vytváří nebezpečný precedens, že vysocí policejní důstojníci budou moci svévolně a beztrestně vstupovat do politického a předvolebního dění“ [55, s. 6].

V zásadě lze druhy úniků utajovaných informací podle Jana Schneidera rozdělit následovně [56, s. 9]:

a) Cílený a načasovaný únik vybraných informací do médií je zaranžován jako „náhodný“ v rámci legální zpravodajské hry nebo v intencích vyšetřovací taktiky. Tento specifický „modus operandi“ je užíván zřídka a pouze v důležitých případech (tedy nikoliv vůči politikům).

b) Vybrané informace jsou diskrétně a draho poskytnuty kriminálním klientům nebo subjektům zpravodajského zájmu (aniž by byly zveřejňovány). Jde o nebezpečný kriminální delikt.

c) Vybrané informace jsou cíleně a za úplatu poskytovány ve vhodném čase médiím, s cílem ovlivnit privátní, skupinové, hospodářské či bezpečnostní zájmy. Jde opět o kriminální delikt.

d) Různé informace unikají nahodile a neúmyslně indiskrecí a nesprávnou manipulací; náhodný příjemce či nálezce je pak poskytnut tisku. Tento jev lze omezit, nikoliv však vymýtit: svou roli tu hraje lidský faktor. Jde o trestně postižitelné, avšak nedbalostní jednání.

e) Vybrané informace o vnitřní situaci v bezpečnostních složkách jsou zveřejněny bez ohledu na příhodný čas, spontánně a gratis tak, aby vybudily reakci politického vedení státu. Takové jednání je postižitelné z hlediska ochrany utajovaných informací a porušení zákonem uložené mlčenlivosti.

Jak je z rozdělení patrné, způsob a motivy při vyzrazování utajovaných informací mohou být různé. Kromě prvního případu, kdy jsou zveřejňované informace pečlivě vybrány a při výběru jsou zvaženy případné negativní následky, se vždy jedná o překročení zákona.

Přesto existují názory novinářů, že ve sporu o možné trestání novinářů uniká jádro problému. Např. Petruška Šustrová v *Lidových novinách* ze dne 16.10.2006, uvedla: „*Odpovědnost za to, že tajný dokument opravdu zůstane tajný, spočívá jednoznačně na těch, kdo k němu mají zákonný přístup. Ti také mohou – a mají – být za porušení této odpovědnosti trestáni. Jak ale může někoho napadnout trestat novináře za to, že dělá svou práci, tedy že informuje veřejnost?*“ [57, s. 2].

3.10 Příklady porušování ochrany utajovaných informací v mediální oblasti

Úvodem je třeba předeslat, že každé zveřejnění informací prostřednictvím médií ve věci údajných utajovaných informací, většinou neověřených a nepotvrzených subjektem, kterého se předmětná věc týká, má zřejmě nežádoucí vypovídací schopnost z následujících důvodů:

- Pokud by zveřejněná informace měla utajovaný charakter, rozkrytí informací by ve svém důsledku způsobilo újmu zájmu ČR nebo by bylo pro tento zájem nevýhodné. Zároveň by zřejmě způsobilo ohrožení nebo zmaření určité činnosti státního orgánu, v jehož působnosti je informace utajována.
- Kromě toho každé rozkrytí informací vysílá nepochybně signál pro údajně sledované subjekty a poté způsobuje jejich jiné (a tím nežádoucí) chování než tomu bylo dosud, zejména přechod ke konspirativní činnosti.
- Zveřejnění informací však může mít význam i pro jiné subjekty, které dosud nebyly předmětem zájmu konkrétního státního orgánu, neboť by jim zřejmě poskytlo oporu pro další nežádoucí konání, a jistotu, že nejsou předmětem sledování tohoto státního orgánu.

3.10.1 Příklad podle článku „Poznatky, tvrzení a žvásty“ v týdeníku Euro ze dne 12.6.2006, autor Jan Schneider [58]

Autor tohoto článku, bývalý ředitel Kanceláře Rady vlády ČR pro zpravodajskou činnost, věnoval svou pozornost zejména analýze

utajovaného materiálu, který byl projednáván na jednání Branně-bezpečnostního výboru Poslanecké sněmovny Parlamentu, z něhož následně unikly informace prostřednictvím médií.

Vzhledem k tomu, že v souvislosti s tím se autor článku zabýval manipulací s utajovanými informacemi v praxi, uvádíme jeho postřehy.

Autor článku uvedl především dva příklady ochrany utajovaných informací při jejich předávání:

- bývá zvykem redukovat rozsah utajovaných informací na nezbytně nutnou míru a současně zkoumat důsledky případného úniku informací,

- bývá nepsaným pravidlem, že utajované dokumenty, distribuované ve větším počtu výtisků, mívají nenápadné markanty, které umožňují případně publikované faksimile přiřadit k číslu výtisku, aby bylo možno najít viníka.

Dále autor uvedl, že pokud by byl postup při předávání informací neprofesionální, popř. ze strany pachatele by bylo s únikem předem kalkulováno, byly by kriminálnímu podsvětí elegantně předány citlivé informace, například relevantní poznatky o směrech a stavu operativního rozpracování.

Kromě toho, pokud by se uniknuvší údajně utajované informace nezakládaly na pravdě, podle názoru autora by měl každý takový únik znamenat vysoké riziko pro pachatele, neboť v takovém případě je utajení informací v rozporu se zákonem a posloužilo by pouze ke zvýšení „*důvěryhodnosti*“ podvržených informací.

3.10.2 Příklad podle článku „Zabijačka na Seychelách“ v týdeníku Euro ze dne 16.10.2006, autor Jiří Pšenička [59]

Příklad tohoto článku byl vybrán proto, že v jeho rámci byly zveřejněny dva listy materiálu z údajné „operace Lomikar“ v údajném režimu „Přísně tajné“, které analyzoval bývalý ředitel české civilní rozvědky (Úřadu pro zahraniční styky a informace) a historik, specializující se na tajné služby.

Vzhledem k tomu, že v předchozím článku jsou uvedeny příklady manipulace s utajovanými informacemi v praxi, uvádím příklad zveřejnění zřejmě nedůvěryhodného materiálu. Podle historika specializujícího se na tajné služby, je z jazyka zveřejněného materiálu zřejmé, že jeho autor „*nahlédl pod pokličku polistopadových tajných služeb – StB užívala jiného žargonu -, nicméně detailně seznámen s prací rozvědky zřejmě není. Dokumentu chybějí některé formální náležitosti a zároveň si dovoluji pochybovat, že by takovou operací, jejímž cílem je zabití člověka, dal někdo na papír. Tajné služby by plán maskovaly například kryptonymem zvláštní opatření. Také je nelogické, že by přidělili kódové označení až v rámci tohoto dokumentu*“ [59].

Podle bývalého ředitele české civilní rozvědky se materiál skutečně nijak přesvědčivě nejeví, ač mu kódová označení některých aktérů mohou dodat na autenticitě. Osoby, které mají akci přímo řídit, jsou začerněny.

3.10.3 Příklad podle článku „Proč BIS odposlouchávala Grosse“ v Respektu ze dne 14.4.2003, autor Jaroslav Spurný [60]

Jestliže zkoumáme vypovídací schopnost článku „*Proč BIS odposlouchávala Grosse*“, který se zabývá problematikou údajných odposlechů jednou ze zpravodajských služeb, zjistíme, že autor v něm

uvádí jména údajně odposlouchávaných subjektů a polemizuje s otázkou, proč tomu tak v konkrétních případech bylo. Lze předpokládat, že pokud údaje v článku deklarují použití zpravodajské techniky zpravodajskou službou za určitých, zákonem vymezených předpokladů a se souhlasem předsedy senátu příslušného soudu, představují únik utajovaných informací v působnosti zpravodajské služby.

Tyto závěry však nelze učinit samovolně, bez zkoumání obsahu článku a bez posouzení zveřejněných sdělení z hlediska ochrany utajovaných informací, v tomto případě zpravodajskou službou. Tím však zřejmě vznikne problém, neboť jakékoli potvrzení, částečné potvrzení, popř. nepotvrzení zveřejněných informací ze strany zpravodajské služby bude zřejmě určeno pouze pro potřeby orgánů činných v trestním řízení a chráněno před zveřejněním. A tak veřejnost, která mohla být zveřejněnými informacemi znepokojena bude jejich prostřednictvím dezinformována, neboť ji nebude možno seznámit s výsledky posouzení informací zpravodajskou službou. V každém případě obsah předmětného článku bude mít nežádoucí dopad pro činnost zpravodajské služby, a to ve výše uvedeném smyslu.

3.10.4 Příklad podle uveřejněných informací v kauze tzv. „Kubiceho zprávy“ na internetových stránkách ČRo1–Radiožurnálu [61]

V měsíci květnu minulého roku předložil ředitel ÚOOZ Jan Kubice výboru pro obranu a bezpečnost Poslanecké sněmovny zprávu ÚOOZ o prorůstání organizovaného zločinu do státní správy. Ještě téhož dne zpravodajsko-publicistická stanice veřejnoprávního rozhlasu ČRo1–Radiožurnál zpřístupnila na svých internetových stránkách fragmenty z údajně utajované části této zprávy. Zveřejněny byly

úryvky 24 stran dokumentu ve formě digitalizovaných obrázků. Důležitá je pro tento příklad skutečnost, že pod každou takto zveřejněnou stránku byla uvedena redakční poznámka: „*Radiožurnál obdržel tyto materiály v podobě, v jaké je zveřejňuje na internetových stránkách. Jednotlivé listy nebyly označeny žádným razítkem, podpisem, ani stupněm utajení*“ [61].

Pro následující rozbor je významná přesná definice utajované informace. Ustanovení § 2 písm. a) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti definuje utajovanou informaci následovně: „*pro účely zákona se rozumí utajovanou informací informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, 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 (§ 139)*“ [48].

Zákonodárce tedy určité informaci poskytuje ochranu jako informaci utajované, pokud tato informace splňuje kumulativně čtyři podmínky:

1. informace je zaznamenaná na nějakém nosiči,
2. je jako utajovaná informace označená v souladu se zákonem,
3. její vyobrazení nebo zneužití může způsobit újmu zájmu České republiky nebo být pro tento zájem nevýhodné a
4. je uvedena v seznamu vydaném nařízením vlády.

Původce utajované informace je při jejím vzniku povinen podle § 21 odst. 1 v souvislosti s § 22 odst. 1 zákon č. 412/2005 Sb. vyznačit na utajovanou informaci taxativně vyjmenované náležitosti, mezi něž patří též stupeň utajení. Závazný způsob vyznačování stupně utajení a dalších administrativních náležitostí na nosiče utajovaných informací předepisuje prováděcí předpis, vydaný na základě zákonného zmocnění

NBÚ (vyhláška NBÚ č. 529/2005 Sb). Nesplnění uvedené podmínky, navenek projevené absencí vyznačeného stupně utajení na nosiči informace, např. na písemném dokumentu, vede k tomu, že obsah příslušného dokumentu není chráněn ustanoveními zvláštního zákona, a to ani kdyby splňoval ostatní tři zákonné podmínky pro zařazení mezi utajované informace.

Nová definice utajované informace (na rozdíl od dřívější definice utajované skutečnosti) však rozsah pojmu výrazně zužuje doplněním dalších dvou formálních znaků. V praxi může mít toto zúžení definičního oboru utajované informace zásadní vliv zejména při posuzování situací, kdy jsou utajované informace zpřístupněny mimo okruh osob, které vyhověly zákonným podmínkám pro přístup k utajované informaci. Právní odpovědnost za zpřístupnění utajované informace neoprávněné osobě se uplatní u osoby, která svým jednáním (nepochybně protiprávním, jež podle skutkových okolností a pohnutek pachatele bude posuzováno jako správní delikt, nebo dokonce jako trestný čin) předá utajovanou informaci neoprávněné osobě poté, co ji pozměnila např. odstraněním vyznačeného stupně utajení tak, že informace na daném nosiči (v tomto případě písemnosti) již nesplňuje všechny znaky utajované informace stanovené zákonem č. 412/2005 Sb. V případě že jiná osoba získá přístup k dokumentu, neoznačenému v souladu se zákonem jako utajovaná informace, není vázána režimem ochrany utajovaných informací. Nesplnění této podmínky znamená totiž nenaplnění kumulativně vyjádřených zákonných formálních znaků, a takový dokument pak nepodléhá ochraně příslušného zákona, přestože informace v něm zaznamenané nadále vykazují ostatní znaky utajované informace [62].

Podrobně se tímto problémem zabývá Daniel HAVRÁNEK ve svém článku *Ochrana utajovaných informací a riziko zpřesňování zákonných definic* a dále k uvedenému dodává: „Při vymezení nových

pojmu se uplatňuje obecná zásada, že s rostoucím počtem rozlišovacích znaků pojmu se zužuje rozsah (extenze) pojmu, tzn. třída všech objektů, které pojem designuje, a naopak – nižší počet znaků pojmu vymezuje širší třídu objektů. Stejná logicko-sémantická zákonitost ovládá instalaci nových právních pojmů do textů právních předpisů prostřednictvím legálních definic a rovněž jejich explikace: s rostoucím počtem znaků – druhových rozdílů, kterými normotvůrce odliší zaváděný nebo vysvětlovaný pojem od pojmu obecnějšího (významově nadřazeného), se prohlubuje distance mezi zaváděným pojmem (v daném případě utajovaná informace) a nadřazeným rodem (obecný pojem informace), a zužuje se tak jeho rozsah.“ [62].

Celý komplex institutu ochrany utajovaných informací tím ale dostává nový rozměr a zasahuje též do posuzování odpovídajících trestných činů. Výstižně tuto situaci dále popisuje Daniel HAVRÁNEK: *„Definice utajované informace v zákoně č. 412/2005 Sb. je součástí dispozice trestněprávních norem. Trestní zákon v ustanoveních § 106 a 107 nadepsaných společnou rubrikou „Ohrožení utajované informace“ vymezuje skutkovou podstatu trestných činů, jejichž objektivní stránka spočívá ve vyzvidání, vyzrazení nebo sbírání údajů obsahujících utajovanou informaci (§ 106 trestního zákona) anebo nedbalostní způsobení vyzrazení utajované informace klasifikované třemi vyššími stupni utajení (§ 107 trestního zákona). Obdobně je spojeno s pojmem utajované informace vymezení skutkové podstaty trestného činu „Vyzvědačství“ (§ 105 trestního zákona). Citovaná ustanovení trestního zákona odkazují použitím obratu „informace utajovaná podle zvláštního zákona“ v současném právním stavu na zákon č. 412/2005 Sb“ [62].*

Publikované dokumenty zprávy ÚOOZ o prorůstání organizovaného zločinu do státní správy obsahují informace, které utajované pravděpodobně jsou. Pokud však při získání pracovníky

redakce Radiožurnálu nebyly řádně označené (na nosiči utajované informace), není tak splněn požadavek zákona. Proto obsah dokumentu zveřejněný na stránkách Radiožurnálu v podstatě již není utajovanou informací podle zákona o ochraně utajovaných informací. Ten, kdo tedy takovou informaci zveřejnil, nemusel nutně vědět, že se jedná o informaci utajovanou. Z jednání odpovědných pracovníků redakce Radiožurnálu, kteří k informaci připojili i upozornění na nedostatek jednoho z obligatorních znaků, je však zřejmé, že si uvědomovali skutečnost, že původně tato informace jako utajovaná označena být mohla.

4. ZÁVĚR

Posuzovat, kde jsou hranice svobodného přístupu k informacím, je velmi problematické. Na straně jedné stojí občan, který chce vědět o všem, co se ho týká. Na straně druhé pak stojí se svými zájmy stát, obec, policie, armáda, nemocnice, soudy a další instituce, které mohou mít zájem určité informace nezveřejňovat, případně tajit.

Z obsahu této práce je zřejmé, že obecně závazné předpisy, které upravují poskytování informací v ČR, představují pouze teoretický předpoklad pro záruku práva na informace podle čl. 17 Listiny základních práv a svobod. Totéž lze říci i o zvláštních zákonech, omezujících právo občanů na informace, které pokud upravují opatření nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti v ČR, jsou v souladu s Listinou základních práv a svobod.

Důležitým prvkem pro zabezpečení práva občanů na informace je však lidský faktor a chování jedince, jehož činnost, popř. nečinnost, se promítá do celého systému zabezpečujícího zejména svobodný přístup k informacím, ochranu osobních údajů, ochranu obchodního tajemství, ochranu duševního vlastnictví, ochranu důvěrnosti majetkových poměrů a ochranu státního tajemství.

Lidský faktor má v systému ochrany utajovaných informací podle zákona č. 412/2005 Sb. na jedné straně postavení fyzické osoby, která nemá přístup k utajovaným informacím ani není držitelem osvědčení fyzické osoby, a na druhé straně má postavení fyzické osoby, která má přístup k utajovaným informacím nebo fyzické osoby, která je pouze držitelem osvědčení fyzické osoby. Kromě toho má lidský faktor podle tohoto zákona postavení „odpovědné osoby“, odpovídající za dodržování povinností stanovených zákonem č. 412/2005 Sb. na úrovni státního orgánu, orgánu územní samosprávy

nebo jiných právnických osob, anebo má postavení podnikající fyzické osoby, která má přístup k utajované informaci.

Fyzické osoby, které mají mít přístup k utajovaným informacím, jestliže jej nezbytně potřebují k výkonu své činnosti, jsou prověřovány, aby mohly být držitelem oznámení nebo osvědčení fyzické osoby, popř. osvědčení podnikatele, a které musí být poté poučeny o právech a povinnostech v oblasti ochrany utajovaných informací a s následky jejich porušení. Je tomu tak proto, že ne každé fyzické osobě lze umožnit přístup k utajovaným informacím, a to v zájmu co nejúčinnější ochrany státního tajemství.

S ohledem na důležitost ochrany těchto informací je též v zákoně č. 412/2005 Sb. stanoven rozsáhlý výčet správních deliktů, kterých se dopustí fyzická osoba, právnická osoba, podnikající fyzická osoba nebo státní orgán, který nesplní určitou, zákonem stanovenou povinnost. Výčet pokut představuje desetitisícové nebo statisícové částky, popř. i částky několika miliónů, za tyto přestupky.

Správnou aplikací všech zmíněných institutů a praktických poznatků je možné docílit nejdůležitějších úkolů v oblasti utajovaných informací – zásadně zvýšit ochranu utajovaných informací, snížit jejich objem a zvýšit jejich kvalitu. V neposlední řadě pak zvýšit jejich analytický potenciál, včetně návrhů řešení pro zvýšení vymahatelnosti zákona v této oblasti.

Najít vyvážený poměr mezi ideálním stavem, legislativním rámcem a praxí je úkol velmi obtížný. Základní kámen v rámci právního řádu ČR byl však v obecné rovině již položen a tato oblast je nadále rozvíjena.

SEZNAM POUŽITÉ LITERATURY

1. Usnesení Ústavního soudu sp. zn. III.ÚS 28/96 ze dne 16.5.1996 publikované ve Sbírce nálezů a usnesení Ústavního soudu, svazek č. 5, usnesení č. 5, s. 557.
2. Usnesení Valného shromáždění OSN č. DE01/48 ze dne 10.12.1948. [cit. 2006-11-05]. Dostupný také z WWW: <<http://www.smop.cz/bezpec/zakony/1948-DE01.txt>>.
3. VLASÁK, Rudolf. *Informační politika: základní východiska a současnost ve vyspělých demokraciích*. In *Informační studia a knihovnictví v elektronických textech I.* [elektronický zdroj]. Ed. Richard Papík, Martin Souček, Anna Stöcklová. Praha : Univerzita Karlova, c 2001.
4. KORBEL, František. *Právo na informace : zákon o svobodném přístupu k informacím, zákon o právu na informace o životním prostředí ; komentář*. Praha : Linde, 2004. 295 s. ISBN 80-7201-465-X.
5. SCHMIDT-JORTZIG, E. in Isensee, J., Kirchhof, P.: *Handbuch des Staatsrechts der Bundesrepublik Deutschland*. C. F. Müller Verlag. 2000, § 141, Rn. 3.
6. KORBEL, František. *Svobodný přístup k informacím podle zákona č. 106/1999 Sb. vybrané problémy*. Tábor, Brno 2004/2005. 244 s. Disertační práce., Masarykova univerzita v Brně, Právnická fakulta, Katedra správní vědy a správního práva a finančního práva.
7. PAVLÍČEK, Václav a kol. *Ústavní právo a státověda. II. díl : Ústavní právo České republiky, Část 1*. Praha : Linde, 2001. 551 s. ISBN 80-7201-273-8.
8. Zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů. Sbírka zákonů 1998, částka 42, s. 5442-5445. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1998/sb042-98.pdf>>.
9. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). Sbírka zákonů 2004, částka 184, s. 10059-10085. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2004/sb184-04.pdf>>.

10. Zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů. Sbíрка zákonů 1993, částka 3, s. 35-42. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1993/sb03-93.pdf>>.
11. Zákon č. 89/1995 Sb., o statistické službě, ve znění pozdějších předpisů. Sbíрка zákonů 2002, částka 82, s. 4850-4854. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2002/sb082-02.pdf>>.
12. Zákon č. 18/1997 Sb., o mírovém využití jaderné energie a ionizujícího záření a o změně a doplnění některých zákonů, ve znění pozdějších předpisů. Sbíрка zákonů 1997, částka 5, s. 82-106. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1997/sb005-97.pdf>>.
13. Zákon č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, ve znění pozdějších předpisů. Sbíрка zákonů 1993, částka 11, s. 243-244. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2006/sb011-06.pdf>>.
14. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Sbíрка zákonů 2000, částka 32, s. 1521-1532. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2000/sb032-00.pdf>>.
15. Zákon č. 349/1999 Sb., o Veřejném ochránci práv, ve znění pozdějších předpisů. Sbíрка zákonů 2005, částka 133, s. 7103-7106. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2005/sb133-05.pdf>>.
16. Zákon č. 309/1991 Sb., o ochraně ovzduší před znečišťujícími látkami, ve znění pozdějších předpisů. Sbíрка zákonů 1991, částka 57, s. 1343-1347. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1991/sb057-91.pdf>>.
17. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Sbíрка zákonů 1999, částka 39, s. 2578-2582. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1999/sb039-99.pdf>>.
18. MALENOVSKÝ, J.: *Mezinárodní právo veřejné: jeho obecná část a poměr k vnitrostátnímu právu, zvláště právu českému*. Brno: Masarykova univerzita, 2004, str. 116.

19. PAVLÍČEK, Václav a kol.: *Ústava a ústavní řád České republiky. Komentář. 2. díl. Práva a svobody. 2. vydání.* Praha : Linde, 2002. 1164 s. ISBN 80-7201-391-2.
20. ŠPAČEK, David. *Právo na informace ve veřejné správě.* Disertační práce. Fakulta ekonomiko-správní Univerzity Pardubice. 85 s.
21. HŘEBEJK, Jiří. *Ústava a ústavní řád ČR. Komentář. 2. díl. 2. vydání.* Praha : Linde, 1999. 772 s. ISBN 80-7201-455-2.
22. BREJCHA, Aleš. *Právo na informace a povinnost mlčenlivosti v českém právním řádu,* Praha : ODEX Bohemia, 1998, s. 15-17. ISBN 80-8596-347-7.
23. KUŽÍLEK, Oldřich; ŽANTOVSKÝ, Michael. *Svoboda informací : Svobodný přístup k informacím v právním řádu České republiky.* Praha : Linde, 2002. 182 s. ISBN 80-7201-318-1.
24. Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu), ve znění pozdějších předpisů. Sbírka zákonů 2000, částka 98, s. 4570-4615. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2000/sb098-00.pdf>>.
25. KUŽÍLEK, Oldřich. Chodí pešek okolo... antiradaru. *Mladá fronta Dnes.* 23.08.2006, roč. 17, č. 196, s. 6. ISSN 1210-1168.
26. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Sbírka zákonů 2000, částka 32, s. 1521-1532. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2000/sb032-00.pdf>>.
27. *Právo na kopie zdravotní dokumentace.* [online]. Otevrete.cz. c2004. [cit. 2006-11-06]. Dostupný také z WWW: <<http://otevrete.cz/index.php?akce=clanek&id=521>>.
28. Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů. Sbírka zákonů 1991, částka 98, s. 2474-2565. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1991/sb098-91.pdf>>.

29. Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Sbírka zákonů 2000, částka 36, s. 1658-1685. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2000/sb036-00.pdf>>.
30. *Popis změn v zákonu o svobodě informací*. [online]. 27.2.2006 [cit. 2006-11-05]. Dokument dostupný na: <<http://www.otevrete.cz/index.php?akce=clanek&id=617>>.
31. MUSIL, Rudolf. *Ochrana utajovaných skutečností*. Praha : Eurounion, 2001, s. 379. ISBN 80-85858-93-2.
32. Zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů. Sbírka zákonů 2000, částka 47, s. 2183-2219. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2000/sb047-00.pdf>>.
33. Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů. Sbírka zákonů 1992, částka 5, s. 98-105. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1992/sb005-92.pdf>>.
34. Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů. Sbírka zákonů 2002, částka 57, s. 3216-3218. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2002/sb057-02.pdf>>.
35. POKORNÝ, Petr. Ekologové mají právo na informace o Temelínu. *Novinky : rubrika Domáci* [online]. 2004 [cit. 2006-06-12]. Dostupný také z WWW: <http://www.novinky.cz/domaci/soud--ekologove-maji-pravo-na-informace-o-temelinu_25502_2inos.html>.
36. HAVLŮJOVÁ, Martina. Motoristé se mohou policistů zeptat, kde používají radary. *Táborské listy*. 2003, s. 16. ISSN 1210-5031.
37. ŠAFÁŘ, Jan. Utajený radar? Není potřeba. *Hradecké noviny*. 2003, s. 6. ISSN 1210-602X.
38. SKOČDOPOLE, Petr. České tajnosti. *Týden*, 23.6.2003, s. 32. ISSN 0862-7495.
39. KUŽÍLEK, Oldřich. Státní smlouva nesmí být tajná. *Hospodářské noviny*. 7.12.2006. č. 237, s. 10. ISSN 0862-9587.

40. *New Attorney General FOIA Memorandum Issued*. [online]. United States : Department of Justice. 2001. [cit. 2006-02-09]. Dostupný také z WWW: <<http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>>.
41. *Report on Cost Estimates for Security Classification Activities*. [online]. Information Security Oversight Office. 2004. [cit. 2006-02-09]. Dostupný také z WWW: <<http://www.archives.gov/isoo/reports/2004-cost-report.html>>.
42. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Sbírka zákonů 2005, částka 43, s. 1330-1400. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2005/sb043-05.pdf>>.
43. Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů. Sbírka zákonů 1994, částka 49, s. 1605-1629. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/1994/sb49-94.pdf>>.
44. POLÁŠEK, František. *Codex iuris canonici*, překlad z latiny, Olomouc: Matice Cyrilometodějská, 1991. 227 s.
45. Zákon č. 3/2002 Sb., o svobodě náboženského vyznání a postavení církví a náboženských společností a o změně některých zákonů. Sbírka zákonů 2002, částka 2, s. 83-95. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2002/sb002-02.pdf>>.
46. Zákon č. 50/1923 Sb., zákon na ochranu republiky. Sbírka zákonů 1923, částka 23, s. 207. Dostupný také z WWW: <<http://spcp.prf.cuni.cz/lex/50-23.doc>>.
47. SVATOŠOVÁ, Helena. *Utajování versus základní práva a demokratické standardy včetně problematiky zbraní* [online]. Iuridicum remedium. 2005. [cit. 2006-12-01]. Dostupný také z WWW: <<http://www.iure.org/534579>>.
48. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Sbírka zákonů 2005, částka 143, s. 7526-7576. Dostupný také z WWW: <<http://www.mvcr.cz/sbirka/2005/sb143-05.pdf>>.

49. JORDANOVÁ, Iveta. Kontrola postupu NBÚ při provádění bezpečnostních prověrek. *Neviditelný pes*. [online]. 2006. [cit. 2006-12-09]. Dostupný také z WWW: <http://neviditelnypes.zpravy.cz/p_politika.asp?r=p_politika&c=A060405_194241_p_politika_wag>. ISSN 1212-673X.
50. ROBERTS, A. *Nato's Security of Information Policy and the Right to Information, in: National Security and Open Government: Striking the Right Balance*. New York : The Maxwell School of Syracuse University. 2003, s. 152.
51. SPURNÝ, Jaroslav. Tajnosti českých úředníků. *Respekt*, 15.3.2004, č. 5, s. 6. ISSN 0862-6545.
52. Důvodová zpráva k návrhu zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. PSP : tisk 880/0. [cit. 2006-02-09]. Dostupný také z WWW: <<http://www.micr.cz>>.
53. HORA, Jaroslav. *Svobodný přístup k informacím a možnosti jeho omezení*. Praha, 2006. 22 s. Seminární práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví.
54. Vládní návrh na vydání zákona, kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, PSP, 25.10.2006
55. Právní stát po česku aneb Zákony musí platit pro všechny. *Právo*. 2006, roč. 16, č. 237 , s. 6. ISSN 1211-2119.
56. SCHNEIDER, JAN. Chvála úniku informací. *Euro*. 27.2.2006, č. 9, s. 50. ISSN 1212-3129.
57. ŠUSTROVÁ, Petruška. A znovu odposlechy. *Lidové noviny*. 16.10.2006, roč. 19, č. 241, s. 2. ISSN 0862-5921.
58. SCHNEIDER, Jan. Poznatky, tvrzení a žvásty : KUBICOVA ZPRÁVA: Materiál ve výsledku diskredituje vlastní podezření. *Euro*. 12.6.2006, č. 24, s. 50. ISSN 1212-3129.

59. PŠENIČKA, Jiří. Zabijačka na Seychelách. *Euro*. 16.10.2006, č. 42, s. 50. ISSN 1212-3129.
60. SPURNÝ, Jaroslav. Proč BIS odposlouchávala Grosse *Respekt*. 14.4.2003, č. 7, s. 5. ISSN 0862-6545.
61. *Dokumenty odhalují prorůstání podsvětí do státní správy* [online]. 29.8.2006 [cit. 2007-05-08]. Dokument dostupný na: <http://www.rozhlas.cz/izurnal/cesko/_galerie/249481?type=image&pozice=2>.
62. HAVRÁNEK, Daniel. *Ochrana utajovaných informací a riziko zpřesňování definic*. Právní zpravodaj. 20.11.2006, č. 11, s. 10 - 12.