

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Ochrana utajovaných informací v právním řádu České republiky

Bakalářská práce

Protection of classified information in the legal system of Czech Republic

Bachelor thesis

VEDOUCÍ PRÁCE

doc. JUDr. Ladislav POKORNÝ Ph.D.

AUTOR PRÁCE

Matěj VÁCHA

PRAHA
2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 13. 3. 2023

Matěj Vácha

Poděkování

Rád bych tímto způsobem vyjádřil poděkování vedoucímu mé bakalářské práce doc., JUDr. Ladislavovi Pokornému Ph.D. za jeho ochotu, cenné rady a trpělivost při vedení mé bakalářské práce.

ANOTACE

Tato bakalářská práce se zabývá ochranou utajovaných informací v právním řádu České republiky. Struktura postupuje od obecných pojmů a vývoje utajovaných informací v českém právním řádu směrem k platnému legislativnímu zakotvení utajovaných informací v České republice. Dále se zabývá ochranou utajovaných informací z pohledu zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a prováděcích právních předpisů Národního bezpečnostního úřadu. Tato část upravuje jednotlivé způsoby ochrany podle výše zmíněných právních předpisů a přestupky podle tohoto zákona. Závěr této práce je věnován ochraně utajovaných informací podle zákona č. 40/2009., trestní zákoník.

KLÍČOVÁ SLOVA

Informace * utajovaná informace * stupně utajení * Národní bezpečnostní úřad * zájem České republiky * újma * druhy zajištění ochrany utajovaných informací * přestupky * trestné činy

ANNOTATION

This bachelor thesis deals with protection of classified information in the legal system of the Czech Republic. The structure proceeds from general concepts and the development of classified information in the Czech legal system towards the valid legislative anchoring of classified information in the Czech republic. I also deal with the protection of classified information from the point of view of Act No. 412/2005 Coll., on the protection of classified information and security competence and the implementing legal regulations of the National Security Agency. This part regulates individual methods of protection according to the above-mentioned legal regulations and offenses according to this law. The conclusion of this work is devoted to the protection of classified information through Act No. 40/2009, Criminal Code.

KEY WORDS

Information * Classified information * degrees of secrecy * National Security Agency * interest of the Czech republic * damage * types of protection of classified information * offences * crimes

OBSAH

ÚVOD.....	7
1. Obecná část.....	9
1.1 Pojem informace	9
1.2 Pojem utajovaná informace v právním řádu České republiky	12
1.3 Historie utajovaných informací v legislativní historii České republiky	14
1.3.1 Komparace částí zákona č. 148/1998 Sb. a zákona č. 412/2005 Sb.	15
1.3.2 Důvody vedoucí k nahrazení zákona č. 148/1998 Sb.	17
2. Zakotvení utajovaných informací v právním řádu České republiky	18
2.1 Zákonné právní předpisy související s utajovanými informacemi	18
2.2 Podzákonné právní předpisy související s utajovanými informacemi	20
3. Ochrana utajovaných informací v právním řádu České republiky	22
3.1 Pojmy související s ochranou utajovaných informací	22
3.2 Ochrana podle zákona č. 412/2005 Sb. a vyhlášek NBÚ	24
3.2.1 Personální bezpečnost	25
3.2.2 Průmyslová bezpečnost	41
3.2.3 Administrativní bezpečnost	44
3.2.4 Fyzická bezpečnost	46
3.2.5 Bezpečnost informačních a komunikačních systémů	49
3.2.6 Kryptografická ochrana	52
3.2.7 Přestupky podle tohoto zákona	53
3.3 Ochrana podle zákona č. 40/2009 Sb., trestní zákoník	58
3.3.1 Vyzvědačství	58
3.3.2 Ohrožení utajované informace	59
3.3.3 Ohrožení utajované informace z nedbalosti	60
ZÁVĚR.....	61
SEZNAM POUŽITÉ LITERATURY.....	63

ÚVOD

Člověk v průběhu svého dne vědomě i nevědomě zachytí nepředstavitelné množství informací. Vědomě získané informace následně hodnotí a využívá s cílem snížit nejistotu ve světě, který se odehrává mimo něj. Přírozenou lidskou vlastností je zvědavost, zvědavost, která člověku poskytuje orientaci v tak komplexním světě, jako je ten náš. Informace je tedy dle mého názoru údaj o světě kolem nás, tedy o reálném světě. Dovolím si tvrdit, že již naši dávní předci dokázali klasifikovat a posoudit informaci na základě její vlastní hodnoty. Ty nejhodnotnější informace mohli v krajních situacích rozhodovat o životě a smrti a jejich znalost tedy měla nevyčíslitelnou hodnotu. Jako lidstvo jsme ušli dlouhou cestu a v mnohém se od svých předků lišíme, ale hodnota hodnověrných a význačných informací je dle mého názoru ve 21. století cennější než kdy předtím.

Právo na informace nám v České republice zaručuje Listina základních práv a svobod.¹ Jsou ale takové informace, které právě díky své hodnotě vyžadují určitý stupeň ochrany a těmito informacemi jsou utajované informace. Utajované je synonymem ke slovu tajné, co je tajné, je pro nás záhadné a co je záhadné přirozeně stimuluje výše zmiňovanou lidskou zvědavost a touhu po vědění. Domnívám se, že právě nejistota z neznámého v tomto případě není pejorativním popisem našeho vztahu k utajovaným informacím, ale jakýmsi prekurzorem pro naši vrozenou touhu neznámé poznat. Znalost takových informací je klíčová pro ochranu zájmů institucí, které s utajovanými informacemi pracují a poskytují seznámeným osobám značnou výhodu při řešení těch nejdůležitějších úkolů. Na stranu druhou mohou osobu obeznámenou s těmito informacemi vystavit riziku, neboť znalost a následné využití takových informací může poškodit druhou stranu. Tato strana poté může mít zájem na odstranění informace nebo přímo nositele dané informace. Riziko platí i v případě, že by se utajované informace dostali do rukou nepovolaných osob a tyto osoby by následně mohli způsobit škodu té straně, která má na utajení zájem. Pro mnou zmíněné a mnohé další důvody dochází k utajování některých informací.

¹ Čl. 17. ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod.

Tématem mé bakalářské práce je právě ochrana utajovaných informací, a to v té podobě, jak ji chápe aktuálně platný právní řád České republiky. Má práce bude systematicky rozdělena do tří částí tak, aby čtenáře postupně a srozumitelně dovedla k pochopení problematiky utajovaných informací v právním řádu České republiky. První, obecná část seznámí čtenáře s pojmy informace a utajovaná informace z pohledu právního řádu České republiky a dále s historií utajovaných informací v legislativní historii České republiky. Druhé části je věnováno platné legislativní zakotvení utajovaných informací v právním řádu České republiky. Tato část je rozdělena na dvě podkapitoly, přičemž první je věnována zákonným právním předpisům a druhá podzákonným právním předpisům. První podkapitola využije primárních zákonných právních předpisů, ale poukáže i na skutečnost, že se s utajovanou informací setkáme napříč celým zákonným spektrem. Druhá podkapitola například uvede vybrané vyhlášky Národního bezpečnostní úřadu, jakožto podzákonné právní předpisy vztahující se k této problematice.²

Nejobsáhlejší třetí kapitola upravuje samotnou ochranu utajovaných informací v právním řádu České republiky. V první podkapitole uvedu pojmy s touto problematikou související. Druhá a co do své délky nejobsáhlejší podkapitola nás provede ochranou utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a vyhlášek NBÚ.³ Obsahem této podkapitoly jsou jednotlivé druhy ochrany utajovaných informací, přičemž nejvíce prostoru bude věnováno personální bezpečnosti. Třetí a poslední podkapitolou se dostaneme k ochraně tak jak ji chápe zákon č. 40/2009 Sb., trestní zákoník. V této podkapitole budou rozebrány jednotlivé trestné činy, vztahující se k utajovaným informacím.

Cílem mé bakalářské práce je seznámit a čtenáři vysvětlit problematiku ochrany utajovaných informací v právním řádu České republiky.

² Dále jen NBÚ

³ Dále jen zákon č. 412/2005 Sb.

1. Obecná část

Tato část bakalářské práce se bude pohybovat v rovině obecných pojmů a krátkého legislativního historického exkurzu. Čtenáři se zde pokusím nastínit, co dané pojmy znamenají a dále mu vysvětlit, jak se utajovaná informace v průběhu let měnila v legislativním prostoru. Znalost těchto informací je dle mého názoru důležitým předpokladem pro pochopení ochrany utajovaných informací v celém svém rozsahu.

1.1 Pojem informace

Informace je slovem, které je v běžné komunikaci hojně využíváno a konsenzuálně chápáno, ačkoliv je pravý význam tohoto slova komplexní a multidisciplinární záležitostí. Samotné slovo informace má původ v latinském slovesu *informare*, jehož významem je utváření, či zpravování něčeho.⁴ S existencí mnoha vědeckých disciplín přichází rovněž existence mnoha různých významů tohoto slova. „V biologii je v souvislosti s genetickým kódem informace chápána jako základní biologická vlastnost a přenos informací patří k základním projevům života.“⁵ V informační technice jsou pro změnu informace chápány jako „přesná a včasná data, které mají svojí specifikaci a jsou organizována za účelem prezentace v takovém kontextu, který dává smysl a význam.“⁶ Slovo informace je tedy širokospektrálním slovem a jeho jednotnou a výstižnou definici jen těžko nalezneme. Uvedu zde alespoň obecnou definici, která je dle mého názoru výstižná. Dle této definice je informací „podnět, pocházející z jednoho systému, který ovlivňuje interpretaci vztahu druhého systému k prvnímu nebo vztah, který oba systémy sdílejí s daným prostředím.“⁷

Cílem této práce ale není čtenáře unavit sáhodlouhým výkladem všech možných definic slova informace, ale přiblížit mu problematiku utajovaných informací

⁴ REJZEK, Jiří. *Český etymologický slovník*. Voznice: Leda, 2001. ISBN 80-85927-85-3, s. 237.

⁵ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8, s. 9.

⁶ IT-slovník.cz: Co je to informace [online]. [cit. 2023-01-27]. Dostupné z: <https://it-slovník.cz/pojem/informace>.

⁷ MADDEN, A.D. *A definition of information* [online]. Aslib Proceedings. 2000, vol. 52, no. 9, pp. 343-349 [cit. 2023-01-27]. Dostupné z: doi: <https://doi.org/10.1108/EUM0000000007207>. In: str. 348.

v právním řádu České republiky. Pro účel této kapitoly zde tedy uvedu pro tuto práci relevantní definice informace, tak jak je chápe legislativa České republiky.

V platném právním řádu České republiky nalezneme dva zákony, které přímo souvisejí s informací jako takovou. V obecnější rovině jde o zákon č. 106/1999 Sb. o svobodném přístupu k informacím. Druhý zákon č. 123/1998 Sb. o právu na informace o životním prostředí vytyčuje práva a povinnosti při získávání informací o životním prostředí. Definicí informace se dle zákona č. 106/1999 Sb. o svobodném přístupu k informacím rozumí *„jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaná na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního.“*⁸ Další zákon poskytující nám vodítko k pochopení pojmu informace jako takové je výše zmíněný zákon č. 123/1998 Sb. o právu na informace o životním prostředí. Tento zákon stanoví že informacemi o životním prostředí je informace v jakékoliv technicky proveditelné podobě, a to zejména vztahující se ke stavu životního prostředí, využívání přírodních zdrojů a vlivů staveb na životní prostředí.⁹

Výše uvedené zákony vztahující se k definici informace obsahují široký záběr a pro lepší ukotvení a pochopení významu daného slova zde uvedu i jiné právní předpisy vyjadřující se k dané problematice.

Směrnice Evropského parlamentu a Rady 2003/98/ES o opakovaném použití informací veřejného sektoru zavádí pojem dokument. Tento pojem je k nalezení v bodě jedenáctém preambule této směrnice. Definice pojmu dokument se tedy vztahuje na *„veškeré záznamy jednání, skutečností nebo informací – a všechny soubory takových jednání, skutečností nebo informací – bez ohledu na formu nosiče (psaný či tištěný na papíře či uložený v elektronické formě nebo jako zvuková, vizuální nebo audiovizuální nahrávka), které mají subjekty veřejného*

⁸ § 3 odst. 3. zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

⁹ § 2 zákona č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů.

sektoru v držení. Dokument v držení subjektu veřejného sektoru je dokument, u něhož má subjekt veřejného sektoru právo povolit opakované použití.“

Směrnice je závazným právním předpisem pro každý stát Evropské unie, kterému je určen. Jeho implementace do vnitrostátního práva tedy musí být jednotlivými státy Evropské unie naplněna, pokud se jich týká.

Česká republika mezi tyto státy patřila a implementace dané směrnice byla naplněna skrze novelizaci zákona č. 106/1999 Sb. o svobodném přístupu k informacím prostřednictvím zákona č. 61/2006 Sb. Definice pojmu dokument byla tedy do českého právního řádu transponována spolu se směrnicí. Rozsudek Nejvyššího správního soudu sp. zn. 1 As 17/2008-67 ze dne 7. 5. 2008 dovodil, že *„Záměrem zákonodárce jednoznačně bylo, aby “informace” v pojetí zákona o svobodném přístupu k informacím byla totožná s pojmem “dokument” v transponované směrnici.“*¹⁰ Přičemž vycházel ze sněmovního tisku č. 991, vládního návrhu zákona k zákonu č. 61/2006 Sb.¹¹ Výše zmiňovaný rozsudek NSS rovněž uvádí, že *„poskytováním informací je především poskytování jejich obsahu (tedy zpravidla textu).“*¹²

Problematikou výkladu pojmu informace se dále zabýval například Městský soud v Praze, který ve svém rozsudku uvedl, že *„podstatou každé informace je právě její slovně vyjádřitelný obsah. Ten umožňuje konkrétní informaci reprodukovat, šířit, poskytnout ji žadateli.“*¹³

Dle dostupných zdrojů je patrné, že legislativní definice slova informace není pevně a konkrétně dána. Pojem informace je abstraktním konceptem a dle výše zmiňovaných multidisciplinárních pohledů na tento fenomén, je patrné, že co definice to jiný význam pro danou oblast. Mnou uvedené rozsudky soudů ve svém

¹⁰ Str. 4, rozsudku Nejvyššího správního soudu ze dne 7.5. 2008, sp. zn. 1 As 17/2008-67. Dostupné z: www.nssoud.cz.

¹¹ tamtéž

¹² tamtéž

¹³ Str. 6, rozsudku Městského soudu v Praze ze dne 27. 9. 2016, čj. 9A 117/2013-34, Dostupné z: www.nssoud.cz.

obsahu jasně ukazují, že právě nekonkrétnost pojmu informace otevírá možnost pro právní „napadení“ tohoto konceptu. V důsledku obecné definice informace tedy v minulosti docházelo a v budoucnosti může docházet k nepotřebnému namáhání soudní moci.

1.2 Pojem utajovaná informace v právním řádu České republiky

Zákon výlučně se zabývající utajovanými informacemi je zákon č. 412/2005 Sb. Definici tohoto pojmu nalezneme ve druhém § písmene a.) základního ustanovení. Zákon zde stanoví, že *„utajovanou informací je 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.“*

Utajovaná informace je specifickým druhem informace a abychom ji mohli za utajovanou považovat, musí dle zákonné definice splňovat tři formální a jeden znak materiální. Absence, byť jednoho z těchto znaků znamená, že se o utajovanou informaci nejedná.¹⁴

Prvním formálním znakem je zde skutečnost, že utajovaná informace musí být zaznamenána. Zákon v tomto případě uvádí, že za utajovanou informaci považuje *„informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči.“*¹⁵

K naplnění druhého formálního znaku dochází, pokud je informace označena v souladu se zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti.¹⁶ Legislativní úpravu vztahující se k problematice označování utajovaných informací nalezneme v části druhé, hlavě IV. zákona č. 412/2005 Sb. a ve vyhlášce č. 275/2022 Sb., o administrativní bezpečnosti a o registrech

¹⁴ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 9.

¹⁵ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 11.

¹⁶ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 12.

utajovaných informací. Administrativní bezpečnosti a obsáhlejšímu rozboru této problematiky se budu věnovat v části třetí této bakalářské práce.

Posledním formálním znakem utajované informace je nutnost uvádět tyto informace v seznamu utajovaných informací. Zákon č. 412/2005 Sb. ve své páté části § 139 zmocňuje NBÚ ke zpracování návrhu seznamu utajovaných informací a vládu, která svým nařízením vydá seznam utajovaných informací. Seznam utajovaných informací společně se stupněm utajení nalezneme v nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.¹⁷

Materiálním znakem utajované informace je poté ta část zákonné definice, která stanoví, že utajovanou informací je ta informace, *„jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodná.“*¹⁸ Část druhá § 3 zákona č. 412/2005 Sb. jasně stanoví, co je myšleno pod pojmem újma zájmu České republiky. Dle obsahu zákona jde o poškození či ohrožení zájmu České republiky. Zákon zde rovněž člení újmu v závislosti na poškození, nebo ohrožení na mimořádně vážnou, vážnou a prostou. V první části tohoto zákona nalezneme i vymezení pojmu zájem České republiky. Zájmem České republiky se tedy rozumí, *„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.“*¹⁹

Pojmy, kterými jsou újma a zájem budou podrobněji rozpracovány v části třetí této bakalářské práce.

¹⁷ DVORÁK, Jan a JIŘÍ CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 13.

¹⁸ § 2 písm. a). zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁹ § 2 písm. b). zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

1.3 Historie utajovaných informací v legislativní historii České republiky

V roce 1989 proběhla v Československu Sametová revoluce, která zapříčinila pád komunistické vlády a nástup demokratického státního zřízení. Mezi lety 1990 až 1992 byla Česká republika členským státem České a Slovenské Federativní Republiky a vykazovala se demokratickým zřízením. Je nutno podotknout, že přechod z komunistického do demokratického zřízení byl obecně velmi náročným procesem a legislativní změny probíhající mezi výše zmiňovanými lety byly postupné, nikoliv absolutní a okamžité. Vznik České republiky tak jak ji známe dnes datujeme do 1. ledna 1993. Tento krátký dějinný exkurz, nám usnadní celkové pochopení historie utajovaných informací v právním řádu České republiky.

První zákonné opatření vztahující se primárně k problematice utajovaných informací po období Sametové revoluce byla novelizace zákona č. 102/1971 Sb. o ochraně státního tajemství prostřednictvím zákona č. 383/1990 Sb. Nahrazeno bylo nařízením vlády Československé socialistické republiky č. 149/1971 Sb. o základních skutečnostech tvořících předmět státního tajemství, a to stejnojmenným nařízením vlády České a Slovenské Federativní Republiky č. 419/1990 Sb. Další legislativní změnou zaštiťující utajované informace byl zákon č. 558/1991 Sb., kterým se mění a doplňuje trestní řád a zákon o ochraně státního tajemství. První velmi výrazný legislativní posun v oblasti utajovaných informací nastal, až v roce 1998 a to přijetím zákona č. 148/1998 Sb., o ochraně utajovaných skutečností, kterým byl nahrazen leč novelizovaný tak zastaralý zákon č. 102/1971 Sb. Zákon z roku 1998 byl první vzniknuvší a přes své nedostatky přijatý zákon zabývající se touto problematikou a přizpůsobený pro demokratickou společnost, kterou v té době Česká republika byla. Tento zákon ve své hlavě třetí zadal vzniku NBÚ, který dodnes plní funkci ústředního správního orgánu pro oblast utajovaných informací. Rovněž stanovil pozici ředitele, který je jmenován a odvoláván vládou a je služebně podřízen Předsedovi vlády.²⁰

²⁰ § 7 zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.

Aktuální platná právní úprava zabývající se výhradně utajovanými informacemi je uvedena v zákoně č. 412/2005 Sb. Tento zákon nabyl platnosti k 18. 10. 2005 a nahradil tak předchozí zákon č. 148/1998 Sb., o ochraně utajovaných skutečností.²¹

1.3.1 Komparace částí zákona č. 148/1998 Sb. a zákona č. 412/2005 Sb.

Část zákona	Zákon č. 148/1998 Sb.	Zákon č. 412/2005 Sb.
Předmět úpravy	Utajované skutečnosti	Utajované informace
Stupně utajení	Přísně tajné (PT) Tajné (T) Důvěrné (D) Vyhrazené (V)	Přísně tajné (PT) Tajné (T) Důvěrné (D) Vyhrazené (V)
Přístup FO	Bezpečnostní prověrky (I., II., III., IV., stupeň)	Oznámení Osvědčení FO Doklad
Zvláštní přístup	Prezident republiky Předseda PS Předseda Senátu Členové vlády Prezident NKÚ Soudci	Prezident republiky Poslanci a senátoři Členové vlády Veřejný ochránce práv Zástupce Veřejného OP Soudci Prezident NKÚ Viceprezident NKÚ Členové NKÚ

Tabulka 1: komparace zákonů

²¹ Dále jen zákon č. 148/1998 Sb.

Nyní se společně podíváme na jednotlivé části, které tabulka uvádí. **Předmětem úpravy** podle § 1 zákona č. 148/1998 Sb. jsou utajované skutečnosti. Utajované skutečnosti jsou podle zákona č. 412/2005 Sb. považovány za utajované informace. Nový zákon tento konflikt pojmů upravuje a stanoví, že *„utajovaná skutečnost podle dosavadních právních předpisů se považuje za utajovanou informaci podle tohoto zákona. Pokud se v dosavadních právních předpisech mluví o utajovaných skutečnostech nebo o státním a služebním tajemství, rozumí se tím utajovaná informace podle tohoto zákona.“*²² Dle mnou uvedené tabulky je patrné, že **stupně utajení** se u jednotlivých zákonů nezměnily. Nahrazený zákon tuto problematiku upravuje ve svém § 5, odstavci prvním a u zákona č. 412/2005 Sb. je tato problematika upravena v § 4. Pojmu stupeň utajení podle platného zákona bude věnována hlubší pozornost v části třetí této bakalářské práce.

Přístup fyzických osob k utajovaným informacím se podle § 25 zákona č. 148/1998 Sb. prováděl ve čtyřech stupních bezpečnostních prověrek. První stupeň bezpečnostní prověrky prováděl autorizaci fyzické osoby pro stupeň utajení vyhrazené. Druhý stupeň byl určen pro stupeň utajení důvěrné, bezpečnostní prověrka třetího stupně umožňovala přístup k utajovaným informacím ve stupni tajném a nejvyšším čtvrtým stupněm bezpečnostní prověrky byl fyzické osobě umožněn přístup k informacím ve stupni přísně tajném. Zákon č. 412/2005 Sb. ve svém obsahu v podstatě uvádí tři druhy oprávnění pro fyzické osoby, které se mají dostat do kontaktu s utajovanou informací.²³ Obdobně jako stupni utajení bude této problematice věnován prostor v části třetí této práce.

Obdobu **zvláštního přístupu** u zákona č. 148/1998 Sb. nalezneme v dílu třetím tohoto zákona. Zákon zde ve svém § 43 uvádí určené osoby ze zákona, které mají z činnosti své funkce právo na přístup k informacím všech stupňů ochrany. Dle výčtu subjektů u jednotlivých zákonů je patrné, že přechází zákon v této oblasti a v § 58 stanovil menší počet osob, které byly většinou postaveny nejvýše v hierarchii dané instituce.

²² § 157 odst. 1. zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

²³ Část druhá, hlava II a část třetí zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

1.3.2 Důvody vedoucí k nahrazení zákona č. 148/1998 Sb.

Důvodů k této změně bylo hned několik, předchozí zákon vykazoval hrubé nedostatky jak vnitrostátního, tak i mezinárodního charakteru.²⁴

Vnitrostátní nedostatky předchozího zákona se projevovaly například v absenci zákonných opatření, které by umožňovaly úřadu provádějícímu bezpečnostní prověrku získat údaje vedené v informačních systémech veřejné správy. Tyto údaje by pověřený úřad mohl využít ke kontrole správnosti údajů u žadatelů, kteří tyto údaje uvedly při provádění bezpečnostních prověrek. Nedostatek právní úpravy se projevil i při určování osob, jenž mají mít přístup k utajovaným informacím. Právní úprava zde nejednoznačně stanovila, kdo má tyto osoby určovat a kdo má stanovit jejich stupeň bezpečnostní prověrky. Mezi další nedostatky patřila například nedostatečnost právní úpravy v oblasti průmyslové bezpečnosti, nedostatečnost právní úpravy při uznávání zahraničních prověrek fyzických osob a absence jakýchkoliv zákonných lhůt vztahujících se k tomuto právnímu předpisu.²⁵

Mezinárodní nedostatky předchozího zákona vedli české zákonodárce k takové právní úpravě této problematiky, která by zvýšila právní jistotu České republiky jakožto člena Evropské unie a Organizace Severoatlantické smlouvy. Nový zákon byl plně v souladu s doposud uzavřenými mezinárodními smlouvami, upravujícími oblast utajovaných informací. Kompatibilita tohoto zákona se projevila například u bezpečnostních standardů NATO, konkrétně s rozhodnutím směrnice C-M (2002)49 – Bezpečnost v rámci NATO z dubna 2002. Dále s právem Evropských společenství skrze rozhodnutí Rady Evropské unie 2001/264/EC, rozhodnutím Komise Evropských společenství 2001/844/EC a s nařízením Rady č. 1958/3. V poslední řadě byla nová zákonná úprava slučitelná s Evropskou Úmluvou o ochraně lidských svobod z roku 1950.²⁶

²⁴ Str. 87–91, důvodová zpráva sněmovního tisku: Vládní návrh k zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. SN, 880/0.

²⁵ tamtéž

²⁶ tamtéž

2. Zakotvení utajovaných informací v právním řádu České republiky

Tato část mé bakalářské práce bude zaměřená na zmapování současných právních norem více, či méně souvisejících s utajovanými informacemi.

2.1 Zákonné právní předpisy související s utajovanými informacemi

Zákon, který bude čtenáře provázet po většinu času mé bakalářské práce je výše zmiňovaný zákon č. 412/2005 Sb. Již z podstaty názvu tohoto zákona je patrné, jaké oblasti jsou tímto zákonem upravovány. Tento zákon plní v českém právním řádu funkci základního pilíře v oblasti utajovaných informací a tuto funkci bude rovněž plnit v mé práci.

Zákon č. 412/2005 Sb. je rozčleněn na devět částí s celkovým počtem 161 §. Část první je základní ustanovení, které upravuje předmět úpravy a vymezení pojmů. Ochrana utajovaných informací je částí druhou a je co do svého obsahu nejobsáhlejší. Tato část má 12 hlav a vymezuje stupně utajení, jednotlivé druhy ochrany utajovaných informací, certifikace státní správy v této oblasti, ale například i poskytování utajovaných informací v mezinárodním styku. Částí třetí je bezpečnostní způsobilost, ve které například nalezneme problematiku citlivé činnosti, bezúhonnosti, osobnostní způsobilosti, ale i povinnosti fyzické osoby, právnické osoby a fyzické osoby podnikající. Část čtvrtá tohoto zákona upravuje průběh a zásady bezpečnostního řízení. Pátá část je zde vedena jako výkon státní správy a vymezuje práva a povinnosti jednotlivých složek státní správy v oblasti utajovaných informací. Částí šestou je státní dozor, částí sedmou kontrola činnosti úřadu, v části osmé nalezneme přestupky a v části deváté přechodná a závěrečná ustanovení.²⁷

²⁷ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Leč je tento zákon nejdůležitějším právním předpisem v oblasti utajovaných informací, není jediným. Přijetí zákona č. 412/2005 Sb. s sebou neslo velké množství změn napříč širokým spektrem, do té doby platných zákonných opatření. Zákonem upravujícím nám tyto změny je zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací. Tento podpůrný zákon ve svém obsahu upravuje změny například v oblasti trestního řádu, zákona o bankách, zákona o svobodném přístupu k informacím, zákona o obcích a zákona o krajích.²⁸

Ačkoliv by se mohlo zdát, že pojem utajovaná informace je v právním řádu České republiky specifickým termínem vázaným na vybrané zájmové oblasti, není tomu přímo tak. S problematikou utajovaných informací se setkáme napříč celým legislativním spektrem České republiky. Pro potřeby této kapitoly zde uvedu výčet zákonných právních norem z různých oblastí, které více, či méně souvisí s touto problematikou.

Dalším zákonným předpisem souvisejícím s ochranou utajovaných informací je zákon č. 40/2009 Sb., trestní zákoník, který ve svém obsahu vymezuje skutkové podstaty trestných činů vztahujících se k utajovaným informacím.²⁹ Z logiky věci vyplývá, že pokud je tato problematika upravena trestním zákoníkem, musí být upravena i zákonem č. 141/1961 Sb., trestní řád. Tento zákon upravuje procedurální postup při řešení trestných činů spojených s utajovanými informacemi.³⁰ Zákon mnou výše zmiňovaný v kontextu informace jako takové byl zákon č. 106/1999 Sb., o svobodném přístupu k informacím. Spojitost s utajovanými informacemi zde nalezneme například v části první § 7 tohoto zákona. Dle tohoto paragrafu je například povinný subjekt oprávněn neposkytovat informace, pokud jsou tyto informace označeny za utajované. S utajovanými informacemi se setkáme i například v části osmé § 85h zákona č. 49/1997 Sb., o civilním letectví, která upravuje ochranu civilního letectví před protiprávními činy.

²⁸ Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

²⁹ § 316 až § 318 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

³⁰ § 8, § 16, § 51b, § 65, § 99, § 111a, § 200 a § 201 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

Poslední mnou zmíněný zákon související s utajovanými informacemi je zákon č. 90/2012 Sb., o obchodních korporacích zmiňující například práva jednatelů, kteří mohou zcela nebo z části odmítnout společníkovu žádost o požadování informací o společnosti, pokud jsou tyto informace utajovanými podle jiného právního předpisu.³¹

2.2 Podzákonné právní předpisy související s utajovanými informacemi

Důležitým a v této práci již jednou zmíněným ústředním správním orgánem, dohlížejícím na ochranu utajovaných informací a bezpečnostní způsobilost je NBÚ. Ve své činnosti se řídí zákonem č. 412/2005 Sb. Tento úřad má rozsáhlé pravomoci v oblasti utajovaných informací a z toho důvodu nemůžeme opomenout ani prováděcí právní předpisy kterými upřesňuje tento zákon.³²

Jako první zde uvedu vyhlášku č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, která ve svém obsahu například stanovuje seznamy a vzory písemností vztahujících se k osvědčení fyzických osob a bezpečnostní způsobilosti.³³

Další vyhláškou upravující problematiku zabezpečení utajovaných informací je vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti. Obdobně jako u předchozí vyhlášky zde nalezneme seznamy písemností, vzory těchto písemností a způsoby jejich podání. Tato vyhláška ovšem upravuje podmínky pro vydání osvědčení podnikajících osob, nikoliv osob fyzických nepodnikajících.³⁴

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků je další sekundární právní normou provádějící upřesnění zákona č. 412/2005 Sb. „*Tato vyhláška stanoví bodové ohodnocení jednotlivých opatření*

³¹ § 156 zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů.

³² *Národní bezpečnostní úřad: O NBÚ* [online]. [cit. 2023-02-05]. Dostupné z: <https://www.nbu.cz/cs/o-nas/>.

³³ Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti.

³⁴ Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti.

*fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku.*³⁵

Poslední prováděcí předpis Národního bezpečnostního úřadu, který zde uvedu, je vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Vyhláška ve svém předmětu úpravy stanoví například druhy administrativních pomůcek včetně jejich náležitostí a technických požadavků na jejich vedení. Způsob, jakým se vyznačují náležitosti na utajované informace, náležitosti souhlasu k pořizování kopie utajované informace, logistické záležitosti ve formě přepravy, přenášení a zapůjčování utajovaného dokumentu. V poslední řadě pak stanoví organizaci a činnosti registrů utajovaných informací.³⁶

Poslední mnou zmíněný, ale neméně důležitý podzákonný právní předpis související s utajovanými informacemi je výše zmíněné nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.³⁷

Všechny tyto doposud zmíněné podzákonné právní předpisy budou komplexněji využity v té části práce, která se zabývá ochranou utajovaných informací v právním řádu České republiky.

³⁵ § 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

³⁶ Vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

³⁷ Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.

3. Ochrana utajovaných informací v právním řádu České republiky

Tato část mé práce bude stěžejním bodem, který bude upravovat instituty ochrany utajovaných informací z pohledu souvisejících právních předpisů. Využiji zde primárně zákon č. 412/2005 Sb. a prováděcí předpisy Národního bezpečnostního úřadu, které jsou s tímto zákonem spjaty. Dále rozeberu ochranu utajovaných informací tak, jak ji vnímá zákon č. 40/2009 Sb., trestní zákoník. Abychom ovšem mohli všechny tyto druhy ochrany řádně pochopit, musíme nejdříve znát pojmy s tím související.

3.1 Pojmy související s ochranou utajovaných informací

Pojmy, které budou v této části práce rozpracovány jsou stanoveny a upraveny zákonem č. 412/2005 Sb. Těmito pojmy jsou újma, zájem a stupně utajení.³⁸ K obecnému vysvětlení prvních dvou pojmů, tedy újma a zájem došlo v té části mé bakalářské práce, která byla věnována pojmu utajované informace jako takové. Rovněž jsem čtenáře seznámil s členěním újmy podle závažnosti na mimořádně vážnou, vážnou a prostou újmu. S újmou je v zákoně spjato i jednání, které je nevýhodné pro zájmy České republiky.³⁹

V závislosti na hypoteticky způsobené újmě zájmu České republiky, klasifikujeme utajované informace stupněm utajení.⁴⁰

Za **přísně tajnou** se považuje ta informace, která by mohla v případě prozrazení či zneužití způsobit České republice mimořádně vážnou újmu. Zákon zde obecně uvádí, že tímto poškozením je myšleno například bezprostřední ohrožení svrchovanosti anebo demokratických základů České republiky.⁴¹

³⁸ § 2 písm. b), § 3 odst. 1. a § 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

³⁹ § 3 odst. 5. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁴⁰ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 35.

⁴¹ § 3 odst. 2, písm. a). zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Konkrétní příklad bychom našli ve výše zmiňovaném nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. Se stupněm utajení informace jako přísně tajné, se ku příkladu můžeme setkat u dokumentů souvisejících se zabezpečením bojové a mobilizační pohotovosti z oblasti Ministerstva obrany.⁴²

Informace dle zákona klasifikovaná jako **tajná**, by v případě zneužití mohla České republice způsobit vážnou újmu. Touto újmou je myšleno například „*narušení vnitřního pořádku a bezpečnosti České republiky*“.⁴³ Seznam utajovaných informací stanoví, že informaci označenou jako tajnou můžeme nalézt například u seznamů rádiových kmitočtů sloužících k obranyschopnosti a bezpečnosti České republiky. Informace tohoto druhu spadá do oblasti působnosti Českého komunikačního úřadu.⁴⁴

Informaci, která má schopnost České republice způsobit prostou újmu například skrze „*ohrožení bezpečnostních operací nebo činnosti zpravodajských služeb*“⁴⁵ klasifikujeme jako **důvěrnou**. Konkrétním příkladem důvěrné informace může být plán zpravodajské činnosti spadající do oblasti působnosti zpravodajských služeb České republiky.⁴⁶

Informaci klasifikovanou jako **vyhrazenou** stanovuje zákon v případě, že by její vyzrazení a případné zneužití mohlo být nevýhodné pro zájem České republiky.⁴⁷

⁴² Příloha č. 5, pořadové č. 16. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

⁴³ § 3 odst. 3, písm. a) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁴⁴ Příloha č. 12, pořadové č. 1. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

⁴⁵ § 3 odst. 4, písm. d) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁴⁶ Příloha č. 18, pořadové č. 3. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

⁴⁷ § 4, písm. d) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

S informací ve stupni utajení označeném jako vyhrazená se například setkáme u obchodně politických a strategických záměrů České republiky.⁴⁸

3.2 Ochrana podle zákona č. 412/2005 Sb. a vyhlášek NBÚ

Předchozí podkapitola nám dala zřetelně najevo, že zneužití utajované informace by mohlo mít dalekosáhlé důsledky pro celou naši společnost. Zákonodárci tedy z logiky věci důsledně upravili postup při ochraně těchto informací. Zákonnou úpravu této problematiky nalezneme primárně v části druhé zákona č. 412/2005 Sb. Zákon v této části stanoví celkem šest druhů ochranných opatření, kterými jsou personální bezpečnost, průmyslová bezpečnost, administrativní bezpečnost, fyzická bezpečnost, bezpečnost informačních nebo komunikačních systémů a v poslední řadě kryptografická ochrana. Dále se budu věnovat ochranné funkci přestupků uvedených v tomto zákoně.⁴⁹ Část druhá tohoto zákona je upřesněna jednotlivými prováděcími předpisy Národního bezpečnostního úřadu, které v této části práce rovněž využiji.⁵⁰

Ve stručnosti zde musím zmínit i právní institut povinnosti mlčenlivosti, který nám rovněž poskytuje ochranu utajovaných informací. V tomto případě, jde o státem uloženou povinnost mlčenlivosti a zákon 412/2005 Sb. tento institut zmiňuje v § 7. O uložené povinnosti mlčenlivosti se mluví v případě, že je tato povinnost uložená například zákonem.⁵¹

⁴⁸ Příloha č. 6. pořadové č. 7. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

⁴⁹ Část druhá a část osmá zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁵⁰ Národní bezpečnostní úřad. Prováděcí právní předpisy [online]. [cit. 2023-02-09]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/>.

⁵¹ § 124 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

3.2.1 Personální bezpečnost

Tento druh ochrany spočívá ve vymezení okruhu fyzických osob, kterým je umožněn přístup k utajovaným informacím na základě předem stanovených zákonných podmínek. Podmínky přístupu se rozlišují na dvě skupiny, a to na základě stupně utajení dané informace. První skupinou jsou utajované informace ve stupni utajení vyhrazené. K těmto informacím lze umožnit přístup fyzické osobě, která je držitelem oznámení o splnění podmínek, osvědčení fyzické osoby anebo dokladu.⁵² Druhou skupinu tvoří stupeň utajení důvěrné, tajné a přísně tajné. V tomto případě je postup k přístupu komplikovanější a fyzická osoba musí být držitelem platného osvědčení fyzické osoby příslušného stupně utajení, jehož vydání předchází bezpečnostní řízení.⁵³

3.2.1.1 Podmínky přístupu k utajovaným informacím ve stupni utajení Vyhrazené

Zákonem stanovené podmínky pro fyzickou osobu, které má být umožněn přístup k utajované informaci ve stupni utajení Vyhrazené nalezneme v části druhé, hlavě druhé tohoto zákona. Zákon zde stanoví, že podmínkou k tomuto přístupu je nezbytná potřeba utajovanou informací disponovat pro výkon funkce, pracovní nebo jiné činnosti. Dále pak nutnost, aby fyzická osoba byla držitelem oznámení o splnění podmínek k přístupu k utajované informaci stupně utajení Vyhrazené, nebo držitelem osvědčení fyzické osoby nebo dokladu, a k tomu musí být řádně poučena.⁵⁴

K tomu, aby bylo fyzické osobě vydáno **oznámení umožňující jí přístup k utajované informace ve stupni utajení Vyhrazené**, musí tato osoba splnit zákonem stanovené podmínky. Osoba žádající o oznámení musí být za prvé, plně

⁵² § 6 odst. 1. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁵³ § 11 odst. 1. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁵⁴ § 6 odst. 1. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

svéprávná, za druhé musí dosáhnout minimální hranice 18 let věku a k tomu musí být bezúhonná.⁵⁵

Podmínku plné svéprávnosti osoba prokáže prohlášením o svéprávnosti.⁵⁶ Vzor tohoto prohlášení bychom našli ve vyhlášce NBÚ č. 363/2011., o personální bezpečnosti a bezpečnostní způsobilosti.⁵⁷ Druhou podmínkou je dosažení minimální hranice 18 let věku, kterou splní ta fyzická osoba, která předloží identifikační kartu. Předloženou identifikační kartou, která sleduje splnění podmínky věku se dle tohoto zákona rozumí občanský průkaz nebo cestovní doklad fyzické osoby.⁵⁸ Poslední zákonem stanovenou podmínkou pro vydání oznámení je bezúhonnost. Tuto podmínku dle zákona „*splňuje fyzická osoba, která nebyla pravomocně odsouzena za spáchání úmyslného trestného činu nebo trestného činu vztahujícího se k ochraně utajovaných informací, anebo se na ni hledí, jako by odsouzena nebyla.*“⁵⁹ Bezúhonnost se prokazuje výpisem z rejstříku trestu.

Ověření a vydání oznámení má na starosti ta osoba, která je vůči žadateli odpovědnou osobou v rámci pracovněprávního či obdobného vztahu. Odpovědná osoba má dle zákona rovněž právo určit jinou osobu, která ověření a vydání oznámení učiní za ní.⁶⁰ Zákon ve své první části přímo uvádí, kdo je odpovědnou osobou myšlen. Například u ministerstva je odpovědnou osobou ministr, u kraje se jedná o ředitele krajského úřadu a u České národní banky je odpovědnou osobou guvernér.⁶¹ V případě, že fyzická osoba nemá odpovědnou osobu dle věty první, ověřuje a oznámení vydá odpovědná osoba, či touto osobou určená osoba,

⁵⁵ § 6 odst. 2. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁵⁶ § 7 odst. 1. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁵⁷ Příloha č. 1 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti.

⁵⁸ § 7 odst. 1. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁵⁹ § 8 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁶⁰ § 6 odst. 3. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁶¹ § 2, písm. e). zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

kteřá fyzické osobě umožní přístup k utajované informaci ve stupni utajení Vyhrazené. V ostatních případech, na základě písemné a odůvodněné žádosti probíhá ověření a vydání oznámení skrze NBÚ.⁶²

Vzor oznámení bychom rovněž našli ve vyhlášce č. 363/2011 Sb., o personální bezpečnosti a bezpečnostní způsobilosti, a to konkrétně v příloze třetí této vyhlášky. Tento vzor obsahuje identifikační údaje fyzické osoby, které má být umožněn přístup k utajované informaci ve stupni utajení Vyhrazené. Těmito údaji jsou jméno a příjmení, rodné příjmení, datum narození, místo narození a státní občanství. Další náležitostí tohoto vzoru je datum a místo kdy bylo oznámení vydáno a kdo na základě splnění zákonných podmínek oznámení vydal. Subjekt, který oznámení vydal zde rovněž uvádí své jméno a příjmení, které následně potvrzuje podpisem a otiskem razítka.

Dalším prvkem ochrany v přístupu k utajované informaci ve stupni utajení Vyhrazeném je **poučení**. Zákon ve svém § 9 a odstavci prvním ukládá odpovědné osobě povinnost zajistit fyzické osobě poučení před prvním přístupem k utajované informaci. Vzor poučení, které se váže k tomuto aktu nalezneme ve čtvrté příloze výše zmiňované vyhlášky č. 363/2011 Sb., o personální bezpečnosti a bezpečnostní způsobilosti. Poučení se provádí na dva výtisky a obsahuje podpis fyzické osoby a osoby, která poučení provedla. Jeden výtisk si ponechává fyzická osoba a druhý výtisk se ukládá.

Subjekt vydávající oznámení je povinen každých pět let ověřovat splnění podmínek ze strany fyzické osoby, které bylo oznámení vydáno. V případě existujícího důvodného podezření, že fyzická osoba nesplňuje některou z výše uvedených podmínek, je vydávající subjekt oprávněn podmínky ověřit i před uplynutím pěti let.⁶³

⁶² § 6 odst. 3. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁶³ § 9 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Zákonná právní úprava ve svém § 9 a odstavci třetím rovněž předkládá skutečnosti, které předcházejí zániku platnosti tohoto oznámení. Platnost oznámení tedy zaniká:

- a.) Doručením písemného vyrozumění fyzické osobě, které stanoví, že tato osoba přestala splňovat podmínku pro vydání oznámení.
- b.) Ukončením pracovněprávního nebo obdobného vztahu, který fyzické osobě umožňoval přístup k utajované informaci.
- c.) Vznikem pracovněprávního či obdobného vztahu, ve kterém má být fyzické osobě umožněn přístup k utajované informaci.
- d.) *„Úmrtím nebo prohlášením osoby za mrtvou.“*
- e.) *„Ohlášením jeho odcizení nebo ztráty.“*
- f.) Nečitelností nebo porušením celistvosti oznámení v důsledku poškození.
- g.) Doručením písemného vyrozumění fyzické osobě, že tato osoba nesplnila v zákonné lhůtě svou povinnost vázající se na držení oznámení.
- h.) Vracením oznámení té osobě, která ho vydala, případně Národnímu bezpečnostnímu úřadu.
- i.) *„Patnáctým dnem od doručení osvědčení fyzické osoby nebo dokladu.“*
- j.) *„Změnou některého z údajů v něm obsažených.“*

U písmena a.) a g.) písemně vyrozumí fyzickou osobu vydavatel oznámení a toto vyrozumění řádně odůvodní. V těchto dvou případech je rovněž fyzická osoba povinna odevzdat oznámení do 15 dnů ode dne doručení písemnosti a to subjektu, který oznámení vydal. O zániku oznámení podle písmena b.), c.), d.), f.), h) a i.) je vydavatel oznámení povinen učinit písemný záznam, který následně uloží. Dále je u písmen b.), c.) a h.) držitel oznámení povinen odevzdat oznámení do 15 dnů ode dne zániku platnosti a to subjektu, který oznámení vydal. Písmenem e.), f.) a j.) vzniká držiteli neplatného oznámení možnost, písemně požádat vydavatele oznámení o vydání oznámení nového. Lhůta na tuto žádost je 15 dnů ode dne zániku platnosti. Ten, kdo v těchto případech oznámení vydal, vydá do 5 dnů ode dne přijetí žádosti oznámení nové, nahrazující tak to předchozí.⁶⁴

⁶⁴ § 9 odst. 3 až 6 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Držitel oznámení má rovněž i mnoho povinností vztahujících se k držení samotnému. Podmínka plné svéprávnosti a bezúhonnosti musí být ze strany fyzické osoby splňována po celou dobu přístupu k utajované informaci. Jakékoliv změny, týkající se těchto podmínek, je fyzická osoba povinna sdělit subjektu, který vydání oznámení provedl. Další povinností fyzické osoby je oznámit odcizení, ztrátu, případně poškození oznámení. Pokud je fyzické osobě doručeno osvědčení fyzické osoby nebo dokladu, pak je držitel oznámení rovněž povinen sdělit tuto skutečnost subjektu, který oznámení vydal. Sdělení ze strany fyzické osoby musí dle zákona proběhnout v den doručení osvědčení nebo dokladu. V neposlední řadě je fyzická osoba povinna nahlásit vznik pracovněprávního nebo obdobného vztahu, ve kterém má být této osobě umožněn přístup k utajované informaci. Poslední zákonem stanovenou povinností fyzické osoby je ohlášení změny některého z údajů, obsažených v oznámení. 15denní lhůta na sdělení těchto skutečností běží ode dne, kdy některá z těchto změn nastala, nebo ode dne, kdy se o této změně fyzická osoba dozvěděla.⁶⁵

Osvědčení fyzické osoby je další zákonnou možností, jak fyzické osobě umožnit přístup k utajované informaci ve stupni utajení Vyhrazené.⁶⁶ Osvědčení bychom mohli pochopit jako přístup k utajovaným informacím, který v porovnání s oznámením a dokladem může svému držiteli hypoteticky umožnit přístup k utajovaným informacím ve všech stupních utajení. Osvědčením fyzické osoby se budu komplexněji zabývat v další části personální bezpečnosti dle zákona č. 412/2005 Sb.

Další možností stanovenou tímto zákonem, která umožňuje fyzické osobě přístup k utajované informaci ve stupni utajení Vyhrazené je **doklad o bezpečnostní způsobilosti fyzické osoby**.⁶⁷ Úpravu tohoto dokladu nalezneme v třetí části

⁶⁵ § 10 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁶⁶ § 6 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁶⁷ § 6 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

zákona č. 412/2005 Sb., která upravuje bezpečnostní způsobilost. Právní úprava této části v podstatě stanoví podmínky pro citlivou činnost podle tohoto zákona, přičemž touto činností se například rozumí ta činnost, která by v případě zneužití mohla způsobit ohrožení zájmu České republiky.⁶⁸ Citlivá činnost jako taková ale není výhradou pouze tohoto zákona. S citlivou činností se setkáme například v § 162 zákona č. 263/2016 Sb., atomový zákon a § 2a zákona č. 312/2006 Sb., o insolvenčních správcích. Fyzická osoba vykonávající citlivou činnost musí být bezpečnostně způsobilá, přičemž se za takovou osobu považuje osoba, která je držitelem výše zmiňovaného dokladu o bezpečnostní způsobilosti. Citlivou činnost podle zákona může vykonávat i osoba, která je držitelem platného osvědčení fyzické osoby.⁶⁹ Pro potřeby této části práce se omezím pouze na výklad vztahující se k dokladu.

Doklad jako takový vydává NBÚ, a to jen té fyzické osobě, která splňuje zákonem stanovené podmínky. Těmito podmínkami jsou plná svéprávnost, dosáhnutí věku minimálně 18 let, bezúhonnost, osobnostní způsobilost a spolehlivost.⁷⁰ V kontrastu s vydáním oznámení je patrné, že nám zde přibila osobnostní způsobilost a spolehlivost. V následujícím textu tedy doplním čtenářovi znalosti o tyto dvě podmínky a podmínku bezúhonnosti, která je touto částí definována odlišně od identické podmínky vztahující se k oznámení. Zbylé podmínky jsou chápány obdobně jako je tomu u oznámení.

„Podmínku bezúhonnosti pro účely bezpečnostní způsobilosti splňuje fyzická osoba, která nebyla pravomocně odsouzena za spáchání úmyslného trestného činu, anebo se na ní hledí, jako by odsouzena nebyla.“⁷¹ Prokázání této podmínky probíhá identicky s prokázáním bezúhonnosti u oznámení.

⁶⁸ § 80 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁶⁹ § 80 odst. 2 a 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁷⁰ § 81 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁷¹ § 82 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

„Podmínku osobnostní způsobilosti pro účely bezpečnostní způsobilosti splňuje fyzická osoba, která netrpí poruchou či obtížemi, které mohou mít vliv na její spolehlivost vykonávat citlivou činnost.“⁷²

Poslední mnou zmíněnou podmínkou vázající se na bezpečnostní způsobilost a s tím spojené vydání dokladu bude spolehlivost. Spolehlivost pro účely bezpečnostní řízení nalezneme v § 84 zákona č. 412/2005 Sb. Přičemž tuto podmínku splňuje ta osoba, u které dle zákona nebyla zjištěna negativní okolnost. Zákonná úprava této části uvádí celkem dvě skutečnosti, které jsou považovány za negativní okolnosti a pět skutečnosti, které mohou být považovány za negativní okolnost. Za negativní okolnosti tento zákon považuje činnost fyzické osoby, která jedná proti zájmu České republiky a dále skutečnost, že majetkové poměry fyzické osoby jsou nepřiměřeně zjevné oproti přiznaným příjmům. Mezi možné negativní okolnosti zákon řadí například osobnostní rysy fyzické osoby, které by mohly vést ke zneužití výkonu citlivé činnosti a styky této osoby s osobou, která v minulosti vyvíjela, nebo i vyvíjí činnost proti zájmu České republiky. Všechny tyto negativní okolnosti se zjišťují s přihlédnutím k 10letému období, které se váže na minulost ověřované osoby anebo za období od dosažení věku 15 let, a to podle toho, které z těchto období je kratší.⁷³ *„Z toho vyplývá, že podá-li žádost o doklad osoba, která dosáhla věku 25 let a více, budou se tyto skutečnosti zjišťovat za období 10 let zpětně. Podá-li žádost osoba mladší, budou se tyto skutečnosti zjišťovat za období od 15 let jejího věku.“⁷⁴*

S výjimkou prvních dvou zmiňovaných okolností se ověřuje, zda okolnosti uvedené v zákoně jsou negativními okolnostmi. Zákon zde uvádí určitá kritéria, kterými se rozhodne. Prvním je skutečnost, jak moc může uvedená okolnost

⁷² § 83 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁷³ § 84 odst. 2, 3 a 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁷⁴ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 258.

ovlivnit výkon citlivé činnosti. Dále je to doba výskytu, rozsah a charakter okolnosti a v poslední řadě chování osoby v době, která se prověřuje.⁷⁵

Vzor dokladu bychom našli v příloze č. 11 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a bezpečnostní způsobilosti. Na dokladu se nacházejí identifikační údaje žadatele, kterými jsou například jméno a příjmení, datum narození a rodné číslo. Dále vzor obsahuje datum vydání, dobu platnosti a podpis oprávněného zástupce Národního bezpečnostního úřadu a otisk razítka tohoto úřadu. Podmínka otisku razítka není potřeba, pokud je doklad vydán v elektronické podobě.⁷⁶

Obecně řečeno je platnost dokladu pět let a jeho platnost zaniká uplynutím jeho platnosti. Zákon zde ale uvádí i další faktory, které předcházejí zániku platnosti. Platnost oznámení dále zaniká rozhodnutím Národního bezpečnostního úřadu o zrušení jeho platnosti. Úmrtím, nebo prohlášením držitele dokladu za mrtvého. V případě ztráty, odcizení nebo poškození, které způsobilo nečitelnost nebo celistvost dokladu. Změnou údajů v něm vedených. Vracením dokladu ze strany držitele a to subjektu, který ho vydal. Poslední skutečnost stanovující zánik platnosti dokladu je v den, kdy byl fyzické osobě vydán nový doklad nebo jí bylo doručeno osvědčení fyzické osoby.⁷⁷ V případě krizového stavu je stanovena výjimka pro držitele neplatného dokladu, který žádá o doklad nový, a to pouze v případě zániku platnosti dokladu z důvodů uplynutí jeho platnosti. Pokud tato osoba žádá v období krizového stavu o vydání nového dokladu, pak je oprávněna v tomto mezidobí vykonávat citlivou činnost a je jí umožněn přístup k utajované informaci ve stupni utajení Vyhrazené. Nejdéle však po dobu 12 měsíců.⁷⁸

Část zákona věnující se bezpečnostní způsobilosti ve svém závěru, konkrétně v § 86, §87 a §88 upravuje práva a povinnosti jednotlivých subjektů, které mají

⁷⁵ § 84 odst. 5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁷⁶ § 85 odst. 2, písm. f) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁷⁷ § 85 odst. 1 a 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁷⁸ § 80a zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

spojitost s citlivou činností. Příkladem povinnosti fyzické osoby je neprodleně ohlásit ztrátu nebo odcizení dokladu Národnímu bezpečnostnímu úřadu. Příkladem povinnosti právnické osoby, podnikající fyzické osoby a orgánu státu je vést evidenci fyzických osob, vykonávajících citlivou činnost a majících k tomuto subjektu pracovněprávní či obdobný vztah. Poslední 88. § upravuje výkon citlivé činnosti v oblasti zpravodajských služeb. Příkladem z tohoto § nám může být skutečnost, že podmínky bezpečnostní způsobilosti u fyzických osob vykonávajících citlivou činnost pro zpravodajské služby si ověřuje sama zpravodajská služba.

Doteď jsem probral podmínky, které musí fyzická osoba splňovat, aby mohla žádat o doklad, dále jsem nastínil negativní okolnosti, které mohou mít vliv na spolehlivost ověřované osoby. Čtenáře jsem seznámil s formálním obsahem dokladu a uvedl jsem, v jakých případech zaniká platnost dokladu. Na následujících řádcích bude hrát zásadní roli NBÚ, který byl mnou rovněž zmíněný v kontextu vydávání dokladu jako takového.

Fyzická osoba, žádající o vydání dokladu musí projít **bezpečnostním řízením**. Toto řízení bychom našli v části čtvrté zákona č. 412/2005 Sb. Bezpečnostní řízení pro žadatele o doklad začíná dnem doručení písemné žádosti NBÚ.⁷⁹ Písemné náležitosti, které tato osoba úřadu zasílá jsou primárně uvedeny ve vyhlášce č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti.

Mezi tyto písemné náležitosti zákon řadí žádost o doklad, kdy vzor nalezneme v příloze č. 11 této vyhlášky. Dále dotazník, vzor nalezneme v příloze č. 6. Žádající osoba musí dále prohlásit osobnostní způsobilosti skrze písemnost, která je přílohou č. 2 a písemnostmi, které dosvědčují hodnověrnost údajů uvedených v dotazníku. Těmito dosvědčujícími písemnostmi je dle vyhlášky myšlen například křestní, rodný list a dokumenty dosvědčující finanční stav žadatele.⁸⁰

⁷⁹ § 93 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸⁰ § 6 odst. 1 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti.

Další písemnou náležitostí k vydání dokladu je prohlášení o zproštění mlčenlivosti, který je přílohou č. 13 a prohlášení o svéprávnosti, který je přílohou č. 1 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti. Součástí příloh je i jedna fotografie viditelně zachycující žadatele. V případě žádosti ze strany cizince, je tato osoba povinna zaslat doklad obdobný výpisu z evidence Rejstříku trestů. Tato obdoba musí pocházet ze státu jehož je cizinec státním příslušníkem, případně ze států, ve kterých v uplynulých 10 letech pobýval minimálně šest měsíců v řadě. Tento doklad nesmí být starší tří měsíců.⁸¹

Proces, který následuje, pokud fyzická osoba takto o doklad zažádá, je rovněž stanoven v bezpečnostním řízení k tomuto zákonu. NBÚ si po přijetí žádosti ze strany žadatele vyžádá dodatečné informace od subjektů, které s nimi nakládají.⁸² Tento úřad je následně povinen ukončit řízení o vydání dokladu do 75 dnů od počátku řízení.⁸³ Doklad je následně doručen žadateli o doklad, přičemž se jedna kopie dokladu uloží do bezpečnostního svazku.⁸⁴

Bezpečnostní řízení bude komplexněji probráno v následující části.

3.2.1.2 Podmínky přístupu k utajovaným informacím ve stupni utajení Přísně tajné, Tajné a Důvěrné

Přístup fyzické osoby k utajovaným informacím ve stupni utajení Důvěrné a vyšší je z logiky věci složitějším procesem, neboť v případě, že by se tyto informace dostaly do nepovoláných rukou mohly by způsobit dalekosáhlejší újmu zájmu České republiky. Tak tedy, přístup k utajovaným informacím ve stupni utajení Přísně tajné, Tajné a důvěrné je umožněn pouze té osobě, která jej nezbytně potřebuje

⁸¹ § 99 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸² Část čtvrtá zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸³ § 117 odst. 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸⁴ § 121 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

k výkonu pracovněprávního nebo obdobného vztahu, je držitelem platného osvědčení fyzické osoby a je řádně poučena.⁸⁵

Poučení fyzické osoby před prvním přístupem k utajované informaci ve stupni utajení Důvěrné a vyšší, je určitou obdobou poučení tak jak jsme si jej probrali u oznámení. Poučení zajistí ten, kdo je vůči fyzické osobě odpovědnou osobou v rámci pracovněprávního či obdobného vztahu. V případě neexistence takovéto odpovědné osoby, je odpovědnou osobou ta osoba, která umožní fyzické osobě přístup k utajované informaci. V případě tohoto poučení se ovšem zhotoví tři kopie, přičemž jedna se předá fyzické osobě, druhá je uložena odpovědnou osobou a třetí se zašle NBÚ. V některých zákonem stanovených případech nemusí být kopie poučení zaslána tomuto úřadu. Jedná se o případy, kdy se poučení týká zpravodajských služeb a Ministerstva vnitra. Poučení ředitele NBÚ a ředitele Bezpečnostní informační služby provádí předseda vlády. Poučení ředitele Úřadu pro zahraniční styky a informace provádí ministr vnitra a poučení ředitele Vojenského zpravodajství provádí ministr obrany.⁸⁶

Jak jsem již napovídal na začátku této části, proces, který vede k přístupu fyzické osoby k utajovaným informacím ve stupni utajení Důvěrné a vyšší je složitější záležitostí. Výčet podmínek, které musí fyzická osoba splňovat s cílem zajistit si osvědčení je rozsáhlejší, než jak tomu bylo u oznámení a dokladu. Fyzická osoba, která je žadatelem o osvědčení tedy musí být, státním občanem České republiky nebo členského státu Evropské unie nebo Organizace Severoatlantické smlouvy. Dále musí být plně svéprávná, bezúhonná a dosáhnout věku minimálně 18 let. Tyto čtyři podmínky netřeba dále rozepisovat, protože první podmínka obsahuje skutečnost, která buď je anebo není naplněna a zbylé tři podmínky jsem již vysvětlil v předchozí části této práce. Mezi další podmínky, které fyzická osoba musí splňovat patří osobnostní způsobilosti a bezpečnostní spolehlivosti. S podmínkou osobnostní způsobilosti jsem se již setkali u dokladu. Ačkoliv se

⁸⁵ § 11 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸⁶ § 11 odst. 2 a 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

jedná o tentýž název podmínky, zákonná úprava věnující se podmínkám osvědčení ji definuje částečně odlišně. Novinkou této problematiky je pro nás podmínka bezpečnostní spolehlivosti, které se budu společně s podmínkou osobnostní způsobilosti věnovat na následujících řádcích.⁸⁷

*„Podmínku osobnostní způsobilosti splňuje fyzická osoba, která netrpí poruchou či obtížemi, které mohou mít vliv na její spolehlivost nebo schopnost utajovat informace.“*⁸⁸ Tato podmínka se ověřuje prohlášením o osobnostní způsobilosti a v některých případech i na základě znaleckého posudku. Fyzické osoby, jejichž náplň práce souvisí nebo bude souviset se zpravodajskými službami, anebo ministerstvem vnitra podstupují i psychologické vyšetření.⁸⁹

Podmínka bezpečnostní spolehlivosti v podstatě stanoví, že u ověřované fyzické osoby nesmí být zjištěno bezpečnostní riziko. Jednotnou definici bezpečnostního rizika v zákoně nenajdeme, místo toho zákon stanoví jednotlivé skutečnosti, které za bezpečnostní riziko můžeme považovat. Obligatorně zákon stanoví tři bezpečnostní rizika, kterými jsou, závažná a případně opakovaná činnost proti zájmům České republiky, podpora nebo přímo činnost spočívající v potlačování základních práv a svobod a skutečnost, že přiznané majetkové poměry zjevně neodpovídají reálné finanční situaci žadatele. Dále zákon stanoví fakultativní, tedy možná bezpečnostní rizika. Mezi tyto rizika patří skutečnost, že žadatel byl v minulosti zařazen do zpravodajské či obdobné složky z dob předchozího komunistického režimu. Ověřování u těchto čtyř bezpečnostních rizik probíhá od věku 15 let žadatele. Dále skutečnost nasvědčující, že žadatel využíval jiné identity. Úmyslné porušování zákona ze strany žadatele vedoucí k poškození zájmu České republiky. Osobnostní vlohy žadatele, které mohou ohrozit schopnost utajovat informace. Styky s osobou, jenž vyvíjela nebo vyvíjí činnost proti zájmu České republiky. V neposlední řadě, neposkytnutí součinnosti při

⁸⁷ § 12 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸⁸ § 13 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁸⁹ § 13 odst. 2 a 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

bezpečnostním řízení podle tohoto zákona a to opakovaně. Tento výčet fakultativních bezpečnostních rizik se ověřuje na základě stupně utajení informace, o které fyzická osoba žádá. V případě Důvěrné informace jde o období 10 let, Tajné informace 15 let, u Přísně tajné informace se tyto rizika ověřují 20 let zpětně anebo za období od 15 let věku v závislosti na tom, které z těchto ověřovaných období je kratší. Posledním možným Fakultativním rizikem jsou skutečnosti spojené s trestněprávní odpovědností žadatele.⁹⁰

Při posuzování, zda jsou možná rizika opravdovými riziky se obdobně jako u dokladu pohlíží na pět kritérií. Prvním je, zda možné fakultativní riziko může ovlivnit schopnost utajovat informace. Dále se jedná o dobu výskytu, rozsahu a charakteru možného rizika. Posledním kritériem je chování osoby v prověřovaném období.⁹¹

Vzhledem k faktu, že držení osvědčení umožňuje přístup k utajovaným informacím ve stupni utajení Důvěrné a vyšší, je logické a potřebné, aby vydání samotného osvědčení předcházelo náležité bezpečnostnímu řízení. V části, věnující se dokladu jsem se již okrajově bezpečnostnímu řízení věnoval. V následujícím textu bude toto řízení, související s osvědčením fyzické osoby rozebráno více do hloubky.

Fyzická osoba, žádající o vydání osvědčení je povinna zaslat NBÚ žádost fyzické osoby.⁹² Pro nalezení vzoru této žádosti znovu zavítáme do vyhlášky č. 363/2011., o personální bezpečnosti a o bezpečnostní způsobilosti a konkrétně do přílohy č. 5. Vzor je rozdělen na dvě části, přičemž první vyžaduje zapojení od fyzické osoby a druhá od odpovědné osoby. v první části tohoto vzoru nalezneme identifikační údaje žadatele, kterými jsou jméno a příjmení, datum narození a místo narození. Dále se v tomto vzoru nachází řádek, který žadatele vybízí, aby zde uvedl, jakého

⁹⁰ § 14 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁹¹ § 14 odst. 6 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁹² § 93 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

stupně utajení si žádá. Žadatel dále musí odůvodnit, jaká nutnost si vyžaduje, aby mu bylo osvědčení vydáno. Uvede místo a den podepsání a podepíše prohlášení, že uvedl pravdivé údaje a seznámil se s podmínkami bezpečnostního řízení. Druhá část tohoto vzoru je potvrzením odpovědné osoby, že vydání osvědčení je pro fyzickou osobu nutné. Zde bychom našli označení odpovědné osoby, označení subjektu a identifikační údaje odpovědné osoby. V dalším řádku nalezneme text hovořící o specifikacích utajovaných informací, které na daném místě vznikaly, nebo budou vznikat. Pod tímto textem je prostor pro odpovědnou osobu, která tyto specifikace uvede. Odpovědná osoba v poslední části tohoto vzoru uvede místo a den podepsání a přidá svůj podpis, případně razítko.

K této žádosti fyzická osoba přiloží vyplněný dotazník fyzické osoby, a to jak v listinné, tak i elektronické podobě. Dotazník k osvědčení tak jak ho chápe bezpečnostní řízení je totožný s dotazníkem, který se přikládá k žádosti o doklad. Již jsem zmiňoval, že vzor tohoto dotazníku nalezneme v příloze č. 6 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ale komplexněji ho nastíním až zde. Obsah dotazníku určitými oblastmi silně zasahuje do soukromí žadatele a je zde tedy patrné, že disponovat možností přístupu k utajovaným informacím je velkým privilegiem, které si na soukromí jedince může vybrat svou daň. Dotazník obsahuje identifikační údaje žadatele a adresy, kde se žadatel ustavičně zdržoval v posledních 10 letech po dobu minimálně 90 dnů a adresu jeho trvalého pobytu. V případě cizince se uvádí údaje o dokladu totožnosti. Název aktuálního zaměstnavatele, označení vykonávané funkce s možností uvést náplň činnosti a názvy předešlých zaměstnavatelů s uvedením data vzniku a skončení. Žadatelův rodinný stav, ustavičný pobyt v zahraničí delší než 90 dnů, nařízené výkony rozhodnutí, informace o trestním řízením vztahujícímu se k osobě žadatele a předešlá bezpečnostní řízení. Kontakty a spojení na současné i minulé bezpečnostní služby cizí moci včetně jejich zpravodajských služeb. Kontakty a spojení na ty státní příslušníky České republiky, kteří žijí v nečlenských zemích Evropské unie nebo Organizace Severoatlantické smlouvy a tytéž kontakty na cizí státní příslušníky žijícími na území mimo tyto organizace. Užívání psychotropních, omamných látek a alkoholu a jejich případné léčby. Nezdravé hráčství a léčby vztahující se k tomuto bodu. Dále se zde nachází, nejvyšší

dosažené vzdělání žadatele, majetkové poměry a žadatelova příslušnost k subjektům vykonávajícím společensky prospěšnou činnost. V neposlední řadě adresa učená pro doručování a identifikační údaje a název zaměstnavatele manželky, partnerky nebo plnoletých osob sdílejících s žadatelem domácnost. V obsahu dotazníku se rovněž nachází životopis a prohlášení vypovídající o hodnověrnosti a úplnosti údajů v dotazníku uvedených.

Dalšími písemnostmi, které fyzická osoba přiloží k žádosti o osvědčení jsou obdobou písemností, které se přikládají k žádosti o doklad. Pro připomenutí, se těmito dokumenty rozumí rodný, křestní či obdobný list a dokumenty dosvědčující příjmy žadatele ze strany zaměstnavatele.⁹³ Dále se přikládá prohlášení osobnostní způsobilosti, písemnost vztahující se k svéprávnosti žadatele a prohlášení o zproštění mlčenlivosti vztahující se k daňovým povinnostem. Součástí je i fotografie viditelně zachycující žadatele. V případě cizince se stanovuje identická příloha jako tomu bylo u dokladu. Fyzická osoba, která má mít přístup k utajovaným informacím i po skončení platnosti je povinna v zákonem stanové lhůtě požádat NBÚ o vydání osvědčení nového. U stupně utajení Důvěrné se jedná o dobu 3 měsíců před uplynutím platnosti osvědčení. U stupně utajení Tajné 7 měsíců a Přísně tajné 10 měsíců.⁹⁴

Proces, který následuje po podání žádosti o osvědčení ze strany žadatele nabývá bezpečnostně ověřovacího charakteru. Osvědčení jako takové se vydává pro jednotlivé stupně utajení, přičemž pokud je osvědčení vydáno ve stupni nejvyšším, umožňuje držiteli přístup k utajovaným informacím ve všech stupních utajení. Pokud tedy chápeme skutečnost, že k utajování informací do jednotlivých stupňů utajení dochází z důvodu, že jednotlivé informace vykazují různou důležitost, pak bychom si mohli dovodit, že procesní řízení s cílem vydat osvědčení se pro jednotlivé stupně utajení liší. Po přijetí žádosti o osvědčení určeného pro stupeň utajení Důvěrné, si NBÚ vyžádá informace potřebné k ověření žadatelem uvedených informací. Tyto informace si vyžádá od subjektů, které s nimi nakládají.

⁹³ § 6 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti.

⁹⁴ § 94 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Pro stupeň utajení Tajné, se ověřují tytéž skutečnosti, ale výše zmíněný úřad navíc provede ověření identity žadatele. K tomuto ověřování může využít zpravodajskou službu nebo policii, která následně informace doplní. Dosud zmiňované úkony se provádí i pro stupeň utajení Přísně tajné, jen s tou změnou, že zpravodajská služba navíc provede šetření k výskytu bezpečnostních rizik v prostředí, ve kterém se žadatel pohybuje.⁹⁵

V případě, že se v průběhu procesu vyskytnou nějaké pochybnosti, které je potřeba objasnit může úřad předvolat svědka, který k tomuto objasnění přispěje. Dále je možné provést pohovor s žadatelem o osvědčení, který rovněž slouží k objasnění pochybností.⁹⁶

NBÚ je v ideálním případě povinen rozhodnout o vydání osvědčení do dvou měsíců u stupně utajení Důvěrné, šesti měsíců u stupně utajení Tajné a devíti měsíců ve stupni utajení Přísně tajné. Lhůta se počítá ode dne zahájení bezpečnostního řízení.⁹⁷ V případě nevydání osvědčení je žadateli doručeno rozhodnutí o nevydání, v opačném případě vydá NBÚ osvědčení, které je následně žadateli doručeno.⁹⁸

Vzor osvědčení fyzické osoby nalezneme v příloze č. 7 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti. Vzor obsahuje identifikační údaje žadatele, stupeň utajení, datum vydání a uvedení počátku a zániku platnosti osvědčení. Dále je zde uveden podpis oprávněného zástupce a otisk úředního razítka.

⁹⁵ § 107 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁹⁶ § 104 a § 105 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁹⁷ § 117 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

⁹⁸ § 121 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

3.2.2 Průmyslová bezpečnost

Problematiku průmyslové bezpečnosti nalezneme v části druhé a hlavně třetí zákona č. 412/2005 Sb. Tento druh bezpečnosti utajovaných informací je jistou obdobou bezpečnosti personální, které byla věnována předchozí kapitola. Na rozdíl od předchozí části ovšem upravuje bezpečnost podnikatele, nikoliv fyzické osoby. *„Průmyslová bezpečnost zajišťuje ochranu utajovaných informací prostřednictvím omezení přístupu k utajovaným informacím pouze na podnikatele spolehlivé, jak co do schopnosti zajistit utajovanou informaci, tak i co do důvěryhodnosti jejího jednání.“*⁹⁹

Podnikateli je ze zákona umožněn přístup k utajovaným informacím ve stupni utajení Vyhrazené jen za předpokladu, že písemně doloží své prohlášení svědčící o schopnosti zabezpečit ochranu utajovaných informací. Druhou možností jeho přístupu k těmto informacím je skutečnost, že je držitelem platného osvědčení podnikatele.¹⁰⁰

Aby mohl podnikatel prohlášení učinit, musí splnit dvě zákonné podmínky. První podmínka podnikatele zavazuje k vytvoření adekvátních podmínek odpovídajících formě přístupu k této informaci a náležející druh zajišťující její ochranu. Druhou podmínkou je skutečnost, že odpovědná osoba musí být držitelem oznámení, osvědčení fyzické osoby anebo dokladu. Toto prohlášení je podnikatel povinen předložit osobě, která mu informaci poskytla. Poskytovatel této informace je zároveň oprávněn požadovat od podnikatele bezpečnostní dokumentaci, kterou nalezneme v části čtvrté a § 98 zákona č. 412/2005 Sb. Ze zákona musí poskytovat jednu kopii prohlášení podnikatele zaslat NBÚ. Pokud u podnikatele utajovaná informace ve stupni utajení Vyhrazené vzniká, musí podnikatel neprodleně zaslat své prohlášení výše zmíněnému úřadu. Platnost tohoto prohlášení je pět let, ale může zaniknout i jiným způsobem. Těmito způsoby jsou například změny údajů uvedených v prohlášení, dále dnem, kdy je podnikateli

⁹⁹ DVORÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 91.

¹⁰⁰ § 15 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

doručeno osvědčení podnikatele anebo v případě, že podnikatel přestal splňovat některou z výše uvedených podmínek umožňujících mu prohlášení učinit.¹⁰¹

Podnikatelův přístup k utajovaným informacím ve stupni utajení Důvěrné a vyšší je podmíněn držením platného osvědčení podnikatele.¹⁰² Na rozdíl od prohlášení předchází zisku osvědčení podnikatele bezpečnostní řízení. Jakým způsobem bezpečnostní řízení probíhá jsem nastínil v části věnující se personální bezpečnosti. Pro potřeby této části práce, zde tedy uvedu jen výčet informací, nezbytných k pochopení této problematiky.

Podnikatel, který má zájem na zisku osvědčení musí splňovat zákonem stanové podmínky, přičemž tyto podmínky s výjimkou poslední musí splňovat po celou dobu platnosti osvědčení. První podmínkou je skutečnost, že podnikatel musí být ekonomicky stabilní. Mezi další podmínky patří bezpečnostní spolehlivost, schopnost náležitě zabezpečit ochranu utajovaných informací a skutečnost, že odpovědná osoba musí být držitelem platného osvědčení fyzické osoby, a to minimálně pro takový stupeň utajované informace pro který si podnikatel žádá. Poslední zákonem stanovenou podmínkou je nutnost uhradit správní poplatek při podání žádosti o osvědčení.¹⁰³

Ekonomickou stabilitu zákon upravuje z pohledu kritérií, která nesmějí být ze strany podnikatele naplněna. Jednotlivá kritéria jsou rozdělena na obligatorní, tedy závazné a fakultativní, tedy možné. Obligatorním kritériem je například skutečnost, že pokud je podnikateli vyhlášeno moratorium, pak nesplňuje podmínku ekonomické stability. Mezi fakultativní riziko zákon například řadí skutečnost, že podnikatele, na kterého je vázaná exekuce lze považovat za ekonomicky nestabilního.¹⁰⁴

¹⁰¹ § 15a zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁰² § 15 písm. b) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁰³ § 16 odst. 1 a 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁰⁴ § 17 odst. 1 a 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

„Podmínku bezpečnostní spolehlivosti nesplňuje podnikatel, u něhož bylo zjištěno bezpečnostní riziko.“¹⁰⁵ Obecnou definici bezpečnostního rizika v této zákonné úpravě nenajdeme, ale rovněž jako u předchozí podmínky zákon vymezuje obligatorní a fakultativní znaky které jsou anebo můžou být považovány za bezpečnostní riziko. Obligatorním rizikem je například činnost statutárního orgánu proti zájmu České republiky. Za možné, a tedy fakultativní riziko zákon považuje například porušení povinnosti vztahující se k ochraně utajovaných informací.¹⁰⁶

„Podmínku způsobilosti zabezpečit ochranu utajovaných informací nesplňuje podnikatel, který není schopen zajistit a dodržovat jednotlivé druhy zajištění ochrany utajovaných informací podle tohoto zákona v závislosti na příslušném stupni utajení a formě přístupu k utajované informaci.“¹⁰⁷

Písemné náležitosti, které podnikatel žádající o osvědčení musí NBÚ úřadu doložit nalezneme ve vyhlášce č. 405/2011 Sb., o průmyslové bezpečnosti. Mezi tyto náležitosti patří žádost podnikatele, kdy vzor této písemnosti nalezneme v příloze č. 1 výše zmíněné vyhlášky. Mezi další přílohy patří například bezpečnostní dokumentace podnikatele, smlouvy o nájmu prostor, smlouva o tichém společenství a účetní závěrky za posledních pět let.¹⁰⁸

V ideálním případě NBÚ ze zákona vydá osvědčení podnikatele do šesti měsíců pro stupeň utajení Důvěrné, osmi měsíců pro stupeň utajení Tajné a deseti měsíců pro stupeň utajení přísně Tajné.¹⁰⁹

¹⁰⁵ § 18 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁰⁶ § 18 odst. 2 a 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁰⁷ § 19 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁰⁸ § 96 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁰⁹ § 117 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Formální vzor vydaného osvědčení nalezneme rovněž ve vyhlášce č. 405/2011 Sb., o průmyslové bezpečnosti, a to konkrétně v příloze č. 2.

3.2.3 Administrativní bezpečnost

Zákon č. 412/2005 Sb. tuto problematiku upravuje v části druhé a hlavě čtvrté. Nutno podotknout, že rozsáhlejší úpravu administrativní bezpečnosti nám v tomto případě poskytne prováděcí předpis, kterým je vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Zákon v oblasti administrativní bezpečnosti uvádí jednotlivá pravidla při označování nosičů utajovaných informací, evidenci a obecně manipulaci s utajovanými informacemi.¹¹⁰

Aby bylo vůbec možné informaci považovat za utajovanou, musí za prvé naplňovat znaky utajované informace tak jak je stanovuje zákon a za druhé musí být za utajovanou informaci označena.¹¹¹

Povinnost označit informaci za utajovanou ukládá zákon původci této informace. Podle § 2 a písmene f) tohoto zákona se za původce považuje orgán státu, právnická nebo fyzická osoba podnikající. Úplné zákonné označení obnáší, uvedení názvu původce, stupeň utajení, evidenční označení a datum vzniku.¹¹²

Původci utajované informace zákon přikládá právo rozhodnout, zda a jestli vůbec stupeň utajení změnit nebo i zrušit. Obecně řečeno je utajovaná informace považovaná za utajovanou na dobu neurčitou, s tím dodatkem, že původce je povinen nejméně každých pět let kontrolovat, zda důvod k utajení nadále trvá. Pokud to vyžaduje charakter utajované informace, může být tato informace utajena na dobu určitou, a i v tomto případě vzniká původci povinnost tuto dobu určit. V případě změny nebo zrušení stupně utajení je původce povinen oznámit

¹¹⁰ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 104.

¹¹¹ § 2 písm. a) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹¹² § 21 odst. 1. zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

tuto skutečnost adresátům utajované informace, kteří oznámí to samé všem dalším adresátům. V případě, že by měl adresát zájem na překladu či okopírování utajované informace ve stupni utajení Přísně tajné, může tak učinit pouze na základě písemného souhlasu původce dané informace. V obdobných případech, vztahujících se k utajovaným informacím ve stupni utajení Tajné a Důvěrné musí adresát získat písemný souhlas nadřízené osoby.¹¹³

Utajovaná informace se eviduje pomocí administrativních pomůcek. Seznam těchto pomůcek nalezneme ve výše zmiňované vyhlášce č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Mezi tyto pomůcky například patří jednací a pomocný jednací protokol, manipulační kniha, kontrolní kniha a doručovací kniha.¹¹⁴

Přeprava utajovaných informací se dělí v závislosti na stupni utajení dané informace. Obecným předpokladem přepravy je skutečnost, že musí být provedena skrze kurýrní služby nebo subjekty, které jsou držiteli poštovní licence. Poštovní službou je možné přepravovat pouze utajované informace do stupně utajení Důvěrné. U stupně utajení Přísně tajné a Tajné je přeprava provedena skrze kurýra, který musí být v doprovodu nejméně jedné další osoby a s výjimkou letecké a námořní dopravy nesmí dojít k této přepravě skrze veřejné dopravní prostředky. Přenos Vyhrazené utajované informace probíhá za využití obálky, pevného obalu nebo přenosné schránky. Obálka a obal musí splňovat takovou kvalitu, že údaje uvedené v jejím obsahu nesmí být čitelné.¹¹⁵

Utajovaný dokument se předává adresátům vždy proti podpisu, pokud původce nebo zákon nestanoví jinak.¹¹⁶

¹¹³ § 21 a § 22 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹¹⁴ § 3 vyhlášky č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

¹¹⁵ § 23 a § 24 vyhlášky č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

¹¹⁶ § 21 odst. 8 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

3.2.4 Fyzická bezpečnost

Tato ochrana je k nalezení v části druhé a hlavně páté zákona č. 412/2005 Sb. Předpis upřesňující tuto problematiku je vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. Primárně je fyzická bezpečnost koncipována za tím účelem, že musí snížit nebo přímo zabránit neoprávněné osobě k přístupu k utajovaným informacím a manipulaci s nimi. Toto zabezpečení je provedeno skrze opatření, která nabývají různých podob a kterými jsou například technická zařízení, režimová opatření anebo i ostraha.¹¹⁷

Zákonná úprava této bezpečnosti ve své podstatě stanovuje a užívá tři základní pojmy, od kterých se následně vše odvíjí. Těmito třemi pojmy jsou objekt, zabezpečená oblast a jednacích oblast.¹¹⁸

Objektem se rozumí ohraničený prostor, ve kterém většinou najdeme zabezpečenou nebo jednacích oblast. Hranice tohoto objektu je stanovena viditelně vymezenou hranicí, kterou může být například oplocení nebo i plášť budovy. Zákon dále objekt kategorizuje na základě stupně utajení utajované informace, která se v objektu zpracovává. V případě uložení Vyhrazené informace je objekt kategorizován jako Vyhrazený. Stejný postup následuje u zbylých tří stupňů utajení, ze kterých vyplývá, že dalšími kategoriemi jsou Důvěrné, Tajné a Přísně tajné objekty. Stanovit, do jaké kategorie patří, je povinností odpovědné nebo odpovědnou osobou pověřené osoby. Objekt dle zákona slouží ke zpracování utajovaných informací a podléhá proto náležitému zabezpečení. Způsob, jakým se objekt zabezpečí záleží na kategorii objektu, jeho hranici a na vyhodnocení rizik tohoto objektu. Vyhrazený objekt je zabezpečen mechanickými zábrannými prostředky, objekt spadající do kategorie Důvěrné a Tajné je zabezpečen jak mechanicky zábrannými prostředky, tak zařízením elektrické zabezpečovací signalizace. V případě objektu kategorizovaného jako Přísně tajný jsou použity všechny doposud zmíněné bezpečnostní prvky a speciální televizní systémy.¹¹⁹

¹¹⁷ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 114.

¹¹⁸ tamtéž

¹¹⁹ § 2 a § 3 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Zabezpečená oblast je ohraničeným prostorem v objektu, který slouží k ukládání utajovaných informací. Hranice této oblasti je stavebně nebo jinak viditelně ohraničena. Zabezpečenou oblast zákon kategorizuje dvěma způsoby. První způsob je obdobou kategorií, tak, jako tomu bylo u objektu. Pro připomenutí tedy zařazujeme tyto oblasti do Přísně tajných, Tajných, Důvěrných a Vyhrazených kategorií. Druhá klasifikace se provádí na základě možností přístupu k utajovaným informacím. Tato klasifikace dělí zabezpečenou oblast do dvou tříd. V případě, že se v této oblasti seznamuje s utajovanou informací pak jí náleží označení I. třídy. II. třída je oblast, ve které k seznámení s utajovanou informací nedochází. K zabezpečení této oblasti dochází v závislosti na její kategorii, třídě a na vyhodnocení rizik. Zabezpečení Vyhrazené a Důvěrné oblasti odpovídá zabezpečení tak, jako tomu bylo u objektu stejné kategorie. Zabezpečená oblast spadající do kategorie Tajné a Přísně tajné podléhá jak výše zmiňovanému zabezpečení, tak i systémy pro kontrolu vstupů, speciálními televizními systémy a zařízeními elektrické požární signalizace.¹²⁰

Jednací oblast je ohraničeným prostorem v objektu, který je jediným prostorem, kde lze pravidelně projednávat utajované informace stupně utajení Tajné a Přísně tajné. S jednací oblastí jsou spojeny povinnosti odpovědné osoby, která určuje hranice jednací oblasti. Odpovědná osoba je dále povinna zajistit takové podmínky v jednací oblasti, aby zde nedocházelo k ohrožení nebo úniku projednávané utajované informace. Zajištění těchto podmínek probíhá za součinnosti NBÚ, který v jednací oblasti provede kontrolu.¹²¹ V závislosti na stupni utajované informace, která se v dané oblasti projednává a na vyhodnocení rizik se určuje rozsah zabezpečení jednací místnosti. V případě, že se v této oblasti projednávají Tajné a Přísně tajné informace dochází k zabezpečení za pomoci zařízení proti odposlechu a všech výše zmíněných zabezpečovacích prvků.¹²²

¹²⁰ tamtéž

¹²¹ § 24 a § 26 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹²² § 4 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

U těchto tří pojmů jsme se setkali s jednotlivými technickými prostředky, které slouží k jejich zabezpečení. Zákon všechny tyto jednotlivé prvky považuje za opatření fyzické bezpečnosti a k tomu tyto opatření dělí na ostrahu, režimová opatření a výše zmíněné technické prostředky.¹²³

Ostraha musí být přítomna u objektu, ve kterém se nachází zabezpečená oblast kategorie Přísně tajné, a to minimálně dvěma osobami. Kategorie Tajná vyžaduje přítomnost minimálně jedné osoby a jedné další osoby, které musí být při poplachovém hlášení umožněn rychlý zásah. Přímá přítomnost ostrahy nemusí být zajištěna u kategorie Důvěrné, ale obdobně jako v předchozí kategorii zde musí být v případě poplachu osoba v „záloze“. V ostatních případech je ostraha zajištěna odpovědnou osobou. Ostraha musí být dle zákona zajištěna u objektu s jednacích oblastí, ve které se projednávají Tajné a Přísně tajné utajované informace.¹²⁴

Režimová opatření upravují podmínky pohybu do a z objektů, zabezpečených oblastí a jednacích oblastí. Dále upravují kontroly těchto vstupů, manipulace s klíči, identifikačními prostředky a manipulace s technickými prostředky a jejich používání.¹²⁵

Technické prostředky nemají v zákoně jednotnou definici. Zákon místo toho uvádí výčet některých technických prostředků. Za technické prostředky se tedy dle zákona například považují mechanické zábranné prostředky, elektrická zámková zařízení, tísňové systémy, zařízení fyzického ničení nosičů informací a prostředky, které jsem zmínil v souvislosti se zabezpečením objektu, zabezpečených oblastí a jednacích oblastí.¹²⁶ Pokud bychom chtěli najít definici technického prostředku pak musíme zavítat do vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a

¹²³ § 27 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹²⁴ § 28 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹²⁵ § 29 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹²⁶ § 30 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

certifikaci technických prostředků. Technickým prostředkem se dle vyhlášky rozumí „*bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje, oznamuje nebo zaznamenává narušení zabezpečení ochrany objektu, zabezpečené oblasti nebo jednacích oblastí, a dále ničí utajované informace.*“¹²⁷ Použité technické prostředky musí buď projít certifikací, která je provedena NBÚ nebo Národním úřadem pro kybernetickou a informační bezpečnost anebo být schváleny odpovědnou nebo jí určenou osobou.¹²⁸

Specifikace jednotlivých zabezpečovacích prostředků, včetně jejich bodového hodnocení je stanovena v přílohách vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

3.2.5 Bezpečnost informačních a komunikačních systémů

Tyto bezpečnostní oblasti nalezneme v části druhé a hlavě šesté zákona č. 412/2005 Sb. Bezpečnost informačních a komunikačních systému je primárně v kompetenci Národního úřadu pro kybernetickou a informační bezpečnost, který byl zřízen zákonem č. 181/2014 Sb., o kybernetické bezpečnosti. Přičemž tento zákon stanoví, že bezpečnost informace je obecně zajištěna za pomoci důvěrnosti, integrity a dostupnosti informací a dat.¹²⁹ K vysvětlení těchto tří pojmů musíme zavítat do vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. Důvěrnost je vlastností utajované informace, která znemožňuje odhalení utajované informace neoprávněnému subjektu. Integritou se rozumí vlastnost, která umožňuje změny například v softwaru pouze určeným způsobem a jen oprávněným subjektem. Dostupnost

¹²⁷ § 2 písm. i) vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

¹²⁸ § 46 a § 30 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹²⁹ § 21 odst. 1 a § 2 písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

je naplněna v případě, že je utajovaná informace přístupná na stanoveném místě, v požadované formě a v určeném časovém horizontu.¹³⁰

3.2.5.1 Informační systém

Informační systém slouží k nakládání s utajovanými informacemi, a to pouze v případě, že je tento systém certifikován Národním úřadem pro kybernetickou a bezpečnost a písemně schválen do provozu odpovědnou nebo odpovědnou osobou pověřená osoba. V případě informačního systému podnikatele s přístupem k Vyhrazené utajované informaci, může být tento systém schválen jen v době platného prohlášení podnikatele. Informační systém jako takový je tvořen například programovým vybavením počítače, počítači jako takovými, ale i správou tohoto systému.¹³¹ Rozsáhlejší úpravu této problematiky nalezneme ve výše zmiňované vyhlášce č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. Ta například stanoví, jaké soubory opatření jsou zapotřebí k provedení bezpečnosti informačních systémů. Mezi tyto opatření patří různé počítačové a komunikační bezpečnosti, kryptografická ochrana, ochrana proti úniku kompromitujícího vyzařování, ale i mnou probraná administrativní, personální a fyzická bezpečnost.¹³²

3.2.5.2 Komunikační systém

Komunikačním systémem je systém, který umožňuje koncovým uživatelům přenos utajovaných informací, přičemž součástí tohoto systému je i koncové komunikační zařízení. Dále je součástí komunikačního systému přenosové prostředí, různé kryptografické prostředky a obsluha tohoto systému, včetně podmínek a postupů, které se vážou na činnost obsluhy. Obdobně jako u informačního systému, i zde musí dojít k certifikaci skrze Národní úřad pro kybernetickou a informační bezpečnost. Podmínkou nakládání s utajovanou informací je v komunikačním

¹³⁰ § 2 písm. i) a k) a § 10 odst. 1 vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

¹³¹ § 34 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹³² § 3 vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

systému předchozí schválení projektu bezpečnosti tímto úřadem. U komunikačního systému podnikatele s přístupem k utajovaným informacím ve stupni utajení Vyhrazené jsou podmínky provozu identické jako tomu bylo u informačního systému.¹³³ Legislativní úprava, která nám poskytuje vhled do projektu bezpečnosti komunikačního systému je znovu k nalezení ve vyhlášce č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

Tato vyhláška například stanoví náležitosti vztahující se k projektu bezpečnosti komunikačního systému. Mezi tyto náležitosti patří bezpečnostní politika, organizační a provozní postupy při provozování, provozní směrnice pro bezpečnostní správu a provozní směrnice uživatele komunikačního systému.¹³⁴

S bezpečnostní politikou jsou spojeny pojmy, které jsem probral na začátku této podkapitoly. Těmi jsou důvěrnost, integrita a dostupnost. Bezpečnostní politika v tomto případě vymezuje způsoby, jakými budou tyto pojmy zajištěny a dále vymezuje zajištění odpovědnosti uživatele komunikačního systému. Obsahem bezpečnostní politiky je souhrn a požadavky z různých oblastí ochrany utajovaných informací v závislosti na stupni utajované informace, která je v komunikačním systému přenášena.¹³⁵

Obsahem organizačních a provozních postupů jsou způsoby jakými bude zajištěn výkon předem certifikovaných kryptografických ochran. Dále obsahuje požadovanou strukturu správy komunikačního systému a zásady a opatření při provozování komunikačního systému.¹³⁶

¹³³ § 35 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹³⁴ § 27 odst. 1 vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

¹³⁵ § 27 odst. 2 a 3 vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

¹³⁶ § 27 odst. 4 vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

Vyhláška č. 523/2005 Sb. provádí rozsáhlejší úpravu informačních a komunikačních systémů, kompromitujícího vyzařování, náležitosti žádostí ke smlouvě o zajištění činnosti a podmínky bezpečného provozování určených zařízení.

3.2.6 Kryptografická ochrana

Obdobně jako u předchozí části, i zde je z pravidla vykonávána státní správa Národním úřadem pro kybernetickou a informační bezpečnost. Slovo kryptografie je synonymem ke slovesu šifrování a s touto znalostí, tedy můžeme považovat kryptografickou ochranu jako ochranu utajovaných informací za pomoci šifrování.¹³⁷

Zákon 412/2005 Sb. tuto ochranu uvádí v části druhé a hlavně osmé. Prováděcími předpisy k tomuto druhu ochrany jsou vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací a vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

Kryptografický prostředek, materiál k zajištění jeho funkce a kryptografický dokument jsou podle zákona považovány za kryptografický materiál. Výroba, ukládání, distribuce, evidence a různé druhy testování kryptografického materiálu a kryptografického prostředku probíhají na kryptografických pracovištích. Role Národního úřadu pro kybernetickou a informační bezpečnost se projevuje například při certifikacích kryptografických prostředků a při certifikaci kryptografického pracoviště.¹³⁸ Rozsáhlejší úpravu v oblasti certifikací nám poskytuje výše zmíněná vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

¹³⁷ DVOŘÁK, Jan a Jiří CHROBÁK. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018, 480 s. ISBN 978-80-7598-016-8. str. 144.

¹³⁸ § 37 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Za výkon kryptografické ochrany je považována bezpečnostní správa, speciální obsluha kryptografického prostředku anebo výroba a servis kryptografického prostředku a materiálu, který zajišťuje jeho funkci. Vykonávat kryptografickou ochranu může pouze ten pracovník, který byl k výkonu pověřen odpovědnou osobou nebo jí pověřenou osobou, dále pracovník, který je držitelem platného osvědčení fyzické osoby, anebo je držitelem osvědčení o zvláštní odborné způsobilosti.¹³⁹

Zisku zvláštní odborné způsobilosti předchází odborná zkouška, která k úspěšnému zvládnutí vyžaduje znalosti vztahující se k problematice kryptografické ochrany. Odborná zkouška je zajišťována Národním úřadem pro kybernetickou a informační bezpečnost.¹⁴⁰

3.2.7 Přestupky podle tohoto zákona

Přestupky, které tento zákon upravuje jsou co do rozsahu obsáhlou záležitostí, ale v případě, kdy se jedná o porušení povinností vztahujících se k utajovaným informacím je tato obsáhlost pochopitelná a potřebná. Samotnou právní úpravu přestupků nalezneme v části osmé tohoto zákona. Definici přestupku nalezneme v zákoně č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. Tento zákon ve svém 5. § stanoví, že *„Přestupkem je společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje stanovené zákonem, nejde-li o trestní čin.“*

Důvodem, proč jsem přestupky zařadil do způsobů ochrany utajovaných informací je skutečnost, že samotná existence přestupků může působit jako preventivní ochrana utajovaných informací. Zákon 412/2005 Sb. nejdříve řeší problematiku

¹³⁹ § 38 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁴⁰ § 39 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

přestupků fyzických osob, následně řeší přestupky osob právnických, fyzických osob podnikajících, státu a v poslední řadě přestupky podnikatelů.

Fyzická osoba se dopouští přestupku podle § 148 v případě, že:

- a.) neoznámí při bezpečnostním řízení změnu údajů u některé z písemností, vázajících se na osvědčení fyzické osoby anebo dokladu,
- b.) neodevzdá nalezenou utajovanou informaci anebo písemnosti opravňující k přístupu k utajované informaci,
- c.) poruší svou povinnost mlčenlivosti vztahující se k utajované informaci,
- d.) neoprávněné osobě umožní přístup k utajované informaci,
- e.) vykonává paralelně funkci bezpečnostního ředitele u více státních orgánů nebo podnikatelů,
- f.) bez zákonného oprávnění provádí kryptografickou ochranu,
- g.) bez zákonného oprávnění provádí provozní obsluhu kryptografického prostředku,
- h.) bez zákonného oprávnění přepravuje kryptografický materiál,
- i.) bez splnění zákonných podmínek si obstará přístup k utajovaným informacím,
- j.) bez povolení Národního úřadu pro kybernetickou a informační bezpečnost vyveze z území České republiky certifikovaný kryptografický prostředek.

Za trestný, se považuje pouhý pokus u přestupků d.), i.) a j.). Přestupku b.) a c.) se dopouští i návodce nebo pomocník.

Za přestupek a.) lze uložit pokutu až do výše 50 000 Kč, přestupky vedené pod písmeny b.) a e.) se mohou potrestat pokutou do výše 100 000 Kč, do 500 000 Kč se mohou potrestat přestupky f.), g.) nebo h.). Za přestupky písmena i.) se pokuta může vyšplhat až do 1 000 000 Kč a v případě zbylých písmen c.), d.) a j.) se jedná o pokuty do maximální výše 5 000 000 Kč.¹⁴¹

¹⁴¹ § 148 odst. 1, 2, 3 a 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Přestupku se podle § 149 dopustí fyzická osoba, které je umožněn přístup k utajovaným informacím tím, že:

- a.) náležitě neeviduje utajovanou informaci v příslušných administrativních pomůckách,
- b.) vytvoří kopii, opis nebo zajistí překlad utajované informace bez souhlasu původce nebo nadřízené osoby,
- c.) předá utajovanou informaci bez zákonného potvrzení ze strany příjemce,
- d.) nedodržuje zákonná opatření při zapůjčení, přenesení a přepravy utajované informace,
- e.) bez souhlasu původce nebo cizí moci změní, nebo přímo zruší stupeň utajení utajované informace,
- f.) při zpracování a ukládání utajované informace nedbá zákonem stanovených kritérií, umožňujících tyto činnosti vykonat,
- g.) nakládá s utajovanou informací v neadekvátně certifikovaném informačním systému, nebo systému, který nebyl zákonem stanovou osobou schválen,
- h.) nakládá s utajovanou informací v necertifikovaném, nebo neadekvátním komunikačním systému,
- i.) v rozporu s bezpečnostní směrnicí zpracovává utajovanou informaci,
- j.) nezaznamenává kryptografický materiál v zákonem stanovených pomůckách,
- k.) manipuluje s kryptografickým materiálem v rozporu se zákonnými pravidly,

U písmena a.), b.), e.), g.) a h.) se přestupku dopouští jak samotná fyzická osoba, tak organizátor, návodce, ale i pomocník.

Přestupky písmena a.), b.), c.), d.), e.), f.), g.), h.) mohou být pokutovány částkou do maximální výše 500 000 Kč a za přestupky písmena i.), j.) a k.) lze uložit pokutu do 1 000 000 Kč.¹⁴²

¹⁴² § 149 odst. 1, 2, a 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Přestupky u držitelů osvědčení fyzických osob mohou být pokutovány maximální částkou do 50 000 Kč. Mezi tyto přestupky zákon například řadí neoznámení ztráty, odcizení nebo i změny údajů osvědčení.¹⁴³

Do 30 000 Kč mohou být v případě přestupku pokutováni držitelé oznámení fyzických osob. Za přestupky na úrovni držitelů oznámení zákon považuje například neodevzdání neplatného oznámení.¹⁴⁴

Fyzické osoby, které jsou držiteli dokladů mohou být pokutovány do 50 000 Kč. Obdobně jako u oznámení, i zde je za přestupek považováno například neodevzdání neplatného dokladu.¹⁴⁵

Přestupky u **právnických, fyzických osob podnikajících a státu** se podle § 153 posuzují podle škodlivosti dopadu daného přestupku a pokutují částkami do 300 000 Kč, 500 000 Kč anebo do 1 000 000 Kč.

Za přestupky výše zmíněných subjektů, které mohou být pokutované částkou do 300 000 Kč patří například:

- a.) nezajištění ostrahy u objektu, ve kterém se nachází Vyhrazená utajovaná informace,
- b.) nevyznačení zákonem stanovených náležitostí na utajované informace,
- c.) nevytvoření nebo neobsazení funkce bezpečnostního ředitele.¹⁴⁶

Do přestupků pokutovaných částkou do 500 000 Kč patří například:

- a.) neoznámení změny nebo stupně utajení, pokud je výše zmíněný subjekt původcem utajované informace,

¹⁴³ § 150 odst. 1 a 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁴⁴ § 151 odst. 1 a 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁴⁵ § 152 odst. 1 a 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁴⁶ § 153 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

- b.) skutečnost, že při ochraně utajovaných informací nedojde k nahlášení porušení povinnosti,
- c.) u objektů s existencí zabezpečené oblasti a jednacích oblastí nedojde k zákonnému zajištění ostrahy.¹⁴⁷

Za přestupky pokutované do částky 1 000 000 Kč jsou považovány například:

- a.) umožnění vykonávání citlivé činnosti osobě, která není držitelem oprávnění k této činnosti,
- b.) odeslání utajované informace Důvěrné a vyšší v rozporu se zákonem.¹⁴⁸

Přestupky na úrovni podnikatele, který má přístup k utajovaným informacím jsou podle § 154 pokutovány částkou do 1 000 000 Kč, 2 000 000 Kč a 5 000 000 Kč.

Mezi přestupky, které se pokutují částkou do 1 000 000 Kč například patří:

- a.) neodevzdání utajované informace podle zákona,
- b.) poskytnutí Vyhrazené utajované informace zahraničnímu partnerovi v rozporu se zákonem.¹⁴⁹

Do přestupků pokutovaných částkou do 2 000 000 Kč patří:

- a.) nezaslání kopie prohlášení nebo prohlášení podnikatele samotnému NBÚ,
- b.) neoznámení zániku prohlášení podnikatele subjektům stanovených zákonem.¹⁵⁰

Přestupky pokutovány částkou do 5 000 000 Kč jsou:

- a.) poskytnutí utajované informace stupně utajení Důvěrné a vyšší zahraničnímu partnerovi, a to v rozporu se zákonem,
- b.) vývoz certifikovaného kryptografického prostředku, a to bez předchozího povolení Národního úřadu pro kybernetickou a informační společnost.¹⁵¹

¹⁴⁷ tamtéž

¹⁴⁸ tamtéž

¹⁴⁹ § 154 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁵⁰ tamtéž

¹⁵¹ tamtéž

Dále se přestupky podle tohoto zákona týkají držitelů osvědčení podnikatelů, kteří například mohou být v případě přestupku pokutováni částkou do 50 000 Kč, pokud neohlásí ztrátu, případně odcizení svého osvědčení. Částkou do 100 000 Kč mohou být pokutováni ti podnikatelé, kteří i přes zánik platnosti osvědčení nezajistí zákonné zabezpečení ochrany utajované informace.¹⁵²

3.3 Ochrana podle zákona č. 40/2009 Sb., trestní zákoník

Trestné činy, podobně jako přestupky tvoří jistý druh ochrany utajovaných informací, neboť mohou působit „odstrašujícím“ způsobem a nemusí být tedy chápány pouze jako sankce, ale i jako prevence v ochraně. Trestný čin jako takový musí mít charakter protiprávního činu, musí být zákonem označen za trestný a musí vykazovat znaky uvedené v trestním zákoníku.¹⁵³ Pro potřeby této práce využijeme část druhou a hlavu devátou tohoto zákona, která nese název „*trestné činy proti České republice, cizímu státu a mezinárodní organizaci*.“ Tato hlava je následně členěna do tří dílů, přičemž relevantním dílem zastřešujícím problematiku utajovaných informací je díl druhý. Tento díl upravuje trestné činy zaměřené proti bezpečnosti České republiky, cizího státu a mezinárodních organizací. Obsah druhého dílu je tvořen § 316, který nese název **vyzvědačství**, § 317, nesoucím název **ohrožení utajované informace** a § 318, nesoucím název **ohrožení utajované informace z nedbalosti**.

3.3.1 Vyzvědačství

Zjednodušeně řečeno jde o úmyslný akt výzvědné činnosti utajovaných informací s cílem vyrazit získané informace cizí moci. Přičemž aktem není v tomto případě myšlena pouze činnost samotného vyzvědačství, ale i činnost, která pachateli umožní, nebo usnadní vyzvídat tyto informace, a to i včetně přípravy. V části věnující se pojmům souvisejícím s utajovanými informacemi jsem uvedl, že k

¹⁵² § 155 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

¹⁵³ § 13 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

utajování některých informací dochází z toho důvodu, že jejich obsah může hypoteticky způsobit újmu zájmu České republiky. V případě vyzvědačství, zákon svým obsahem a volbou slov počítá, že cílem výzvědné činnosti je utajovaná informace ve stupni utajení minimálně Tajném. Trestní zákoník stanoví, že zneužití této informace může vážným způsobem poškodit zájmy v oblasti vnější bezpečnosti České republiky, kterými je například svrchovanost nebo územní celistvost a dále obranu a bezpečnost mezinárodních organizací.¹⁵⁴

Základní trestní sazbou u tohoto trestného činu je odnětí svobody v délce od dvou do osmi let. K vyšší trestní sazbě odnětí svobody v délce od osmi do patnácti let se přiklání v případě, že byl tento trestný čin spáchán členem organizace, která má za cíl tyto informace vyzvídat. Vyšší trestní sazba se uplatní i v případě, že pachatel se tohoto trestného činu dopustí i přes skutečnost, že mu byla ochrana utajovaných informací zákonem zvlášť uložena. Dále v případech, kdy spácháním tohoto trestného činu získá pachatel nebo jiná osoba značný prospěch, nebo je-li tento trestný čin spáchán ve velkém rozsahu. K poslední aplikaci vyšší trestní sazby dochází v případě, že se trestný čin vyzvědačství týká utajované informace ve stupni utajení Přísně tajné. Dvanácti až patnácti lety odnětí svobody nebo mimořádným trestem je potrestán ten pachatel, který se tohoto trestného činu dopustil za stavu ohrožení státu nebo válečného stavu.¹⁵⁵

3.3.2 Ohrožení utajované informace

V tomto případě jde o úmyslné vyzvídání informace, sbírání údajů, které obsahují informaci, nebo vyrazení informace s cílem vyzradit získané poznatky nepovolané osobě. Tento trestný čin se vztahuje na utajované informace v jakémkoliv stupni utajení a za trestný čin je považována i samotná příprava.¹⁵⁶

Trestem pro pachatele, který se dopustil tohoto trestného činu je odnětí svobody v délce až tří let, nebo zákaz činnosti. Vyšší trestní sazba odnětí svobody je

¹⁵⁴ § 316 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

¹⁵⁵ *tamtéž*

¹⁵⁶ § 317 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

stanovena na dvě až osm let. K této trestní sazbě dochází v případě, že pachatel vyzradí utajovanou informaci ve stupni utajení Tajné a Přísně tajné, nebo dopustil-li se tohoto trestného činu i přes skutečnost, že mu byla ochrana utajovaných informací dána zvlášť zákonem. V poslední řadě se vyšší trestní sazba aplikuje na pachatele, kteří spácháním tohoto trestného činu získali pro sebe nebo pro jinou osobu značný prospěch, nebo způsobili značnou škodu anebo jiný zvlášť závažný následek.¹⁵⁷

3.3.3 Ohrožení utajované informace z nedbalosti

Tento trestný čin je vázán pouze na informace ve stupni utajení Tajné a Přísně tajné. K naplnění tohoto trestného činu dochází nedbalostním vyzrazením utajované informace. K potrestání pachatele dochází buď za pomoci odnětí svobody v délce až tří let anebo zákazem činnosti.¹⁵⁸

¹⁵⁷ tamtéž

¹⁵⁸ § 318 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

ZÁVĚR

Mnou vytyčeným cílem bylo seznámit a čtenáři této práce vysvětlit problematiku ochrany utajovaných informací v právním řádu České republiky. Uchopení této problematiky vyžaduje komplexní znalost nejen z oblastí ochrany utajovaných informací, ale i z oblastí s touto problematikou souvisejících. Při strukturování této práce jsem měl tuto skutečnost na paměti a postupoval jsem tak, aby byl čtenář seznámen s touto problematikou pozvolna, ale úplně.

První část této práce byla obecným úvodem do této problematiky. V první podkapitole jsem se snažil čtenáře seznámit s informací jako takovou a poukázat na její mnohovýznamové definice. Ve druhé podkapitole jsem se pomalými krůčky přibližoval k samotnému jádru této práce a nastínil jsem pojem utajované informace v právním řádu České republiky. Třetí a poslední podkapitola první části čtenáři poskytla historický exkurz do legislativní historie utajovaných informací v právním řádu České republiky. V této podkapitole jsem zároveň uvedl srovnávací tabulku, která, jak doufám, čtenáři narovná znalosti pojmů, které jsou v dnešní době leč hojně, tak chybně používány.

Druhá část byla zaměřená na platné legislativní zakotvení utajovaných informací v právním řádu České republiky. První podkapitola věnující se zákonným právním předpisům čtenáře seznámila se zákonem č. 412/2005 Sb. a jeho systematikou. Dále zde byl uveden zákon, který s výše uvedeným souvisí a v poslední části jsem poukázal na fakt, že s problematikou utajovaných informací se setkáme i v jiných zákonných právních předpisech. Druhá podkapitola této části byla věnována vybraným vyhláškám NBÚ a důležitému nařízení vlády, kterým se stanoví seznam utajovaných informací.

V nejpodstatnější třetí části mé bakalářské práce jsem upravil samotnou ochranu utajovaných informací v právním řádu České republiky. První podkapitolu jsem věnoval pojmům, jejichž pochopení předchází samotnému pochopení problematiky celé bakalářské práce.

Druhá podkapitola provedla čtenářem ochranou utajovaných informací podle zákona č. 412/2005 Sb. a vyhlášek NBÚ. Byl zde krátce uveden institut povinnosti mlčenlivosti a dále jsem se v této části věnoval jednotlivým druhům ochran podle tohoto zákona. Nejvíce prostoru dostala bezpečnost personální, která si dle mého názoru tento prostor zasloužila. Na konci této podkapitoly jsem zmínil i přestupky na úrovni tohoto zákona, které rovněž slouží jako ochrana utajovaných informací. V poslední podkapitole jsem upravil ochranu utajovaných informací podle zákona č. 40/2009 Sb., trestní zákoník. Tento obsáhlý právní předpis jsem zúžil pouze na ty oblasti, které se týkají utajovaných informací.

V úvodu této bakalářské práce jsem si stanovil strukturu, které jsem se po celou dobu psaní držel. Dovolím si tvrdit, že jsem rovněž splnil svůj předsevzatý cíl, který měl za úkol seznámit a čtenáři vysvětlit problematiku utajovaných informací v právním řádu České republiky.

SEZNAM POUŽITÉ LITERATURY

Literatura

- (1) DVOŘÁK, Jan. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8
- (2) REJZEK, Jiří. *Český etymologický slovník*. Voznice: Leda, 2001. ISBN 80-85927-85-3

Právní předpisy

- (3) Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod
- (4) Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
- (5) Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti
- (6) Zákon č. 40/2009 Sb., trestní zákoník
- (7) Zákon č. 90/2012 Sb., o obchodních korporacích
- (8) Zákon č. 141/1961 Sb., trestní řád
- (9) Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- (10) Zákon č. 123/1998 Sb., o právu na životním prostředí
- (11) Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností

- (12) Zákon č. 102/1971 Sb., o ochraně státního tajemství
- (13) Zákon č. 383/1990 Sb., kterým se mění a doplňuje zákon č. 102/1971 Sb., o ochraně státního tajemství, a zákon o civilním letectví, ve znění zákona 43/1976 Sb.
- (14) Zákon č. 558/1991 Sb., kterým se mění a doplňuje trestní řád a zákon o ochraně státního tajemství
- (15) Zákon č. 49/1997 Sb., o civilním letectví
- (16) Zákon č. 263/2016 Sb., atomový zákon
- (17) Zákon č. 312/2006 Sb., o insolvenčních správcích
- (18) Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- (19) Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich
- (20) Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací
- (21) Nařízení vlády č. 149/1971 Sb., o základních skutečnostech tvořících předmět státního tajemství
- (22) Nařízení vlády č. 419/1990 Sb., o základních skutečnostech tvořících předmět státního tajemství
- (23) Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti
- (24) Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti

- (25) Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků
- (26) Vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací
- (27) Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor
- (28) Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací
- (29) Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací
- (30) Rozhodnutí NSS sp. zn. 1 AS 17/2008-67 ze dne 7. 5. 2008
- (31) Rozhodnutí Městského soudu v Praze čj. 9A 117/2013-34 ze dne 27. 9. 2016
- (32) Směrnice Evropského parlamentu a Rady 2003/98/ES ze dne 17. 11. 2003 o opakovaném použití informací veřejného sektoru
- (33) Důvodová zpráva k zákonu č. 412/2005 Sb.

Internetové zdroje

- (34) IT-slovník.cz: Co je to informace [online]. [cit. 2023-01-27]. Dostupné z: <https://it-slovník.cz/pojem/informace>.

- (35) Národní bezpečnostní úřad. Prováděcí právní předpisy [online]. [cit. 2023-02-09]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/>.
- (36) *Národní bezpečnostní úřad: O NBÚ* [online]. [cit. 2023-02-05]. Dostupné z: <https://www.nbu.cz/cs/o-nas/>.
- (37) MADDEN, A.D. *A definition of information* [online]. Aslib Proceedings. 2000, vol. 52, no. 9, pp. 343-349 [cit. 2023-01-27]. Dostupné z: doi: <https://doi.org/10.1108/EUM0000000007207>.