Ivan Pavelka

Základní instituty ochrany utajovaných informací v ČR

1. Slovo úvodem

Ochrana utajovaných informací je významným pilířem národní, evropské a mezinárodní bezpečnosti. Na tom, zda bude náš boj proti současným vnějším a vnitřním bezpečnostním hrozbám souvisejícím s rostoucím extremismem, migrační krizí, hrozbou teroristických útoků (včetně kyberterorismu) a s činností některých zahraničních zpravodajských služeb proti zájmům ČR, EU a NATO nadále úspěšný, se bude velkou měrou podílet nepochybně také včasná a správná znalost rozhodujících informací týkajících se bezpečnosti. To, zda budou mít příslušné bezpečnostní složky dostatečnou informační převahu nad těmi, kteří jsou potenciální či reálnou bezpečnostní hrozbou, bude kromě jiného do značné míry závislé také na důsledné ochraně utajovaných informací. Základem účinné ochrany utajovaných informací je pak nepochybně kvalitní právní úprava v této oblasti.

Ačkoliv je problematika ochrany utajovaných informací nezastupitelnou součástí naší národní bezpečnosti, není tato skutečnost v současné době dostatečně reflektována v odborné literatuře. Nejenže od přijetí zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále také „zákon o ochraně utajovaných informací“) nebyla vydána žádná monografie zabývající se uceleně dotčenou problematikou, ale není zde ani dostatek odborných článků či studií zabývajících základními instituty ochrany utajovaných informací. Kromě textů příslušných právních předpisů na úseku ochrany utajovaných informací a důvodových zpráv či odůvodnění je provázejících tak jsou zdrojem informací v této oblasti v zásadě již pouze věstníky a výroční zprávy vydávané periodicky Národním bezpečnostním úřadem (dále jen „NBÚ“). Při vědomí těchto skutečností má předkládaný článek za cíl především uvést čtenáře do problematiky ochrany utajovaných informací a seznámit je se základními instituty právní úpravy v této oblasti.

2. Prameny právní úpravy

Problematika *ochrany utajovaných informací* je v právním řádu ČR poměrně komplexně upravena. Na zákonné úrovni zde máme především zákon o ochraně utajovaných informací. Na úseku ochrany utajovaných informací upravuje tento zákon zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k utajovaným informacím, požadavky na ochranu utajovaných

informací a s tím spojený výkon státní správy.[1)] K zákonu o ochraně utajovaných informací bylo dosud vydáno několik prováděcích právních předpisů upravujících jednotlivé druhy zajištění ochrany utajovaných informací. Jedná se o vyhlášku č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, vyhlášku č. 405/2011 Sb., o průmyslové bezpečnosti, vyhlášku č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, vyhlášku č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, vyhlášku č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, vyhlášku č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků a vyhlášku č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Velký význam má také nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací (dále také „nařízení vlády stanovící seznam utajovaných informací"). Pramenem právní úpravy ochrany utajovaných informací je také zákon č. 40/2009 Sb., trestní zákoník (dále jen „trestní zákoník"), upravující skutkové podstaty trestných činů přímo spojených s ochranou utajovaných informací. Jedná se o úmyslný trestný čin *vyzvědačství*, úmyslný trestný čin *ohrožení utajované informace* a nedbalostní trestný čin *ohrožení utajované informace z nedbalosti*. Za pramen právní úpravy ochrany utajovaných informací je třeba považovat také jednotlivé procesní předpisy upravující řízení před správními a soudními orgány, neboť tyto předpisy upravují v různém rozsahu specifika některých institutů ve vztahu k ochraně utajovaných informací. Zvláštní pravidla v zákoně č. 99/1963 Sb., občanský soudní řád, zákoně č. 141/1961 Sb., o trestním řízení soudním (trestní řád), zákoně č. 500/2004 Sb., správní řád a zákoně č. 150/2002 Sb., soudní řád správní, se týkají zejména účasti v řízení, právního zastoupení, vedení spisu, nahlížení do spisu, ústního jednání, zajištění osob a věcí a dokazování.

Oblast ochrany utajovaných informací je dotčena také právními předpisy Evropské unie (dále jen „EU") upravujícími problematiku ochrany utajovaných informací EU, tj. utajovaných informací, jejichž neoprávněné vyzrazení by mohlo různou měrou poškodit zájmy EU nebo jednoho či více členských států EU. Jedná se zejména o rozhodnutí Rady 2013/488/EU ze dne 23. září 2013, o bezpečnostních pravidlech na ochranu utajovaných informací EU, Rozhodnutí Komise 2001/844/ES, ESUO, Euratom ze dne 29. listopadu 2001, kterým se mění její jednací řád, Nařízení Rady č. 3, kterým se provádí článek 24 Smlouvy o založení Evropského společenství pro atomovou energii.

V oblasti mezinárodního práva jsou pro ČR závazné zejména předpisy Severoatlantické aliance (dále jen „NATO") vztahující se k ochraně utajovaných informací[2)] a významnou roli pochopitelně hrají také bilaterální mezinárodní smlouvy upravující režim poskytování utajovaných informací mezi ČR a druhou

---

[1)] Srov. § 1 zákona o ochraně utajovaných informací.

[2)] Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/. [cit. 2017-6-7].

smluvní stranou, ochranu předaných utajovaných informací a spolupráci příslušných národních orgánů a orgánů cizí moci odpovědných za ochranu utajovaných informací.[3)]

3. Utajovaná informace, stupně utajení a zvláštní režim nakládání

Zákon o ochraně utajovaných informací definuje *utajovanou informaci* jako informaci v jakékoliv podobě zaznamenanou na jakémkoliv nosiči označenou v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu ČR nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací.[4)] Zpracovatelem seznamu utajovaných informací vydávaného ve formě nařízení vlády je NBÚ. Zákon o ochraně utajovaných informací stanoví, že zájmem ČR je zachování ústavnosti, svrchovanosti a územní celistvosti ČR, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany ČR, ochrana ekonomiky ČR a ochrana života a zdraví fyzických osob.[5)] Zákonná definice utajované informace je kombinací materiálního znaku a znaků formálních. *Materiální znak* spočívá ve způsobilosti utajované informace přivodit v případě jejího vyzrazení nebo zneužití újmu zájmu ČR nebo nevýhodnost pro zájem ČR. *Formální znaky* utajované informace spočívají v podřaditelnosti dané informace pod konkrétní bod některé z příloh v seznamu utajovaných informací, zaznamenání informace na nějakém nosiči a označení informace na jejím nosiči v souladu se zákonem o ochraně utajovaných informací.

V ČR rozlišujeme podle významu případné újmy v důsledku vyzrazení utajované informace čtyři stupně utajení, které se od nejvyšší po nejnižší míru ochrany, které požívají, dělí na *Přísně tajné, Tajné, Důvěrné a Vyhrazené.*

Na informaci, která naplňuje materiální znak a z formálních znaků podřaditelnost pod konkrétní bod některé z příloh v seznamu utajovaných informací a zaznamenání na nějakém nosiči, je její původce (viz níže) povinen při jejím vzniku vyznačit svůj název, stupeň utajení, evidenční označení a datum vzniku utajované informace. Jestliže se jedná o utajovanou informaci poskytnutou ČR cizí mocí (viz níže), může nést utajovaná informace kromě označení příslušným stupněm utajení ještě příslušnou zkratku vyplývající z mezinárodní smlouvy nebo předpisu EU.[6)] Vyznačení stupně utajení na utajované informaci musí být zachováno po celou dobu trvání důvodů utajení.

V souvislosti s uvedenými náležitostmi označení utajované informace není podle autora tohoto článku zřejmé, proč zákonodárce zvolil koncepci uvedení data vzniku utajované informace a nikoli okamžiku vzniku utajované informace s přesností např. na hodiny a minuty.

[3)] Dostupné z: https://www.nbu.cz/cs/mezinarodni-vztahy/941-mezinarodni-smlouvy-o-vymene-a-vzajemne-ochrane-utajovanych-informaci/. [cit. 2017-6-7].
[4)] Srov. § 2 písm. a) zákona o ochraně utajovaných informací.
[5)] Srov. § 2 písm. b) zákona o ochraně utajovaných informací.
[6)] Např. „EU“, „EURA“, „NATO“.

Ze shora uvedené zákonné definice a pojmových znaků utajované informace je zřejmé, že informace, u které absentuje byť i jen některý ze znaků, jehož přítomnost zákon o ochraně utajovaných informací u utajované informace vyžaduje, není utajovanou informací. To se týká jak materiálního znaku, tak i znaků formálních. Pokud jde o formální znak utajované informace v podobě označení informace v souladu se zákonem o ochraně utajovaných informací (např. příslušným stupněm utajení), je třeba podle autora tohoto článku uvedené chápat v tom smyslu, že se v případě absence takového označení na nosiči utajované informace o utajovanou informaci nejedná pouze tehdy, nebyla-li takto informace označena proto, že nesplňuje buď materiální znak utajované informace, nebo ji nelze podřadit pod konkrétní bod některé z příloh v seznamu utajovaných informací.

Zákon o ochraně utajovaných informací rozlišuje mezi *utajovanou informací a nosičem utajované informace*. Není-li informace zaznamenána na nějakém nosiči, nemůže se jednat o utajovanou informaci. Tato konstrukce vylučuje z množiny utajovaných informací takové informace, které by byly mezi osobami sděleny, aniž by předtím byly zaznamenány na nějaký nosič. Uvedená konstrukce neznamená, že utajovaná informace přestává být utajovanou, je-li následně šířena sdělením mezi osobami, a je-li tak *de facto* oddělena od svého nosiče. Uvedené pravidlo, spočívající v tom, že šíření utajované informace osobou, která neví o tom, že se jedná o utajovanou informaci, nečiní z takové informace neutajovanou informaci, se však podle autora článku neuplatní bezvýjimečně. Autor tohoto článku zastává názor, že v některých extrémních případech, zejména při rozšíření utajované informace v hromadných sdělovacích prostředcích, by již objektivně nebylo možné považovat danou informaci za utajovanou. Podle názoru autora článku by osoba, která by sdělila neoprávněné osobě[7)] informaci, o níž by sdělující osoba věděla, že se jedná o utajovanou informaci, nesla odpovědnost za takové jednání podle zákona o ochraně utajovaných informací, případně podle trestního zákoníku, i v případě, kdy by v důsledku následného rozšíření utajované informace došlo případně k tomu, že by již danou informaci nebylo možné považovat za utajovanou. Podle autora článku nelze za určitých okolností vyloučit ani právní odpovědnost osoby, které by utajovanou informaci sdělila neoprávněné osobě, aniž by tato osoba věděla, že sděluje informaci utajovanou.

Kromě národních utajovaných informací rozlišuje zákon o ochraně utajovaných informací také utajované informace cizí moci. Cizí mocí se rozumí cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán.[8)] NBÚ vyhlašuje v souladu s obsahem příslušných mezinárodních smluv, kterými je ČR vázána, *převodní tabulky stupňů utajení utajovaných informací cizích států* sdělením ve Sbírce zákonů.[9)]

[7)] Neoprávněnou osobou se podle zákona o ochraně utajovaných informací rozumí fyzická nebo právnická osoba, která nesplňuje zákonné podmínky přístupu k utajované informaci.
[8)] Srov. § 2 písm. g) zákona o ochraně utajovaných informací.
[9)] Srov. § 23 odst. 4 zákona o ochraně utajovaných informací.

Některé utajované informace v oblastech stanovených mezinárodní smlouvou, předpisy mezinárodních organizací apod. vyžadují dodržování zpřísněných podmínek při zajišťování jednotlivých druhů ochrany utajovaných informací. Zákon o ochraně utajovaných informací v této souvislosti používá termín *zvláštní režim nakládání*[10]. Taková utajovaná informace nese kromě označení příslušným stupněm utajení ještě příslušné doplňující označení vyplývající z mezinárodní smlouvy.[11] Zákon o ochraně utajovaných informací upravuje ještě *taktickou informaci*, kterou se rozumí utajovaná informace s krátkou dobou trvání důvodu utajení.[12]

4. Utajovaný dokument

Zatímco zákon o ochraně utajovaných informací operuje důsledně s pojmem *utajovaná informace*, některé z vyhlášek na úseku ochrany utajovaných informací používají také pojem *utajovaný dokument*. Ačkoliv používání pojmu utajovaný dokument v prováděcích předpisech k zákonu o ochraně utajovaných informací nevychází explicitně a přímo ze žádného ze zákonných zmocnění k vydání dotčených podzákonných předpisů, nejedná se podle autora tohoto článku o nepřijatelné překročení zákonného zmocnění k vydání prováděcího právního předpisu ani o zřejmý rozpor prováděcího právního předpisu se zákonem o ochraně utajovaných informací. Zatímco pojem utajovaná informace je obecně užíván napříč celým zákonem o ochraně utajovaných informací, termín utajovaný dokument je užíván především v podzákonné právní úpravě v rámci stanovení pravidel administrativní bezpečnosti utajovaných informací. Utajovaná informace a utajovaný dokument nejsou pojmy významově totožné. Utajovaný dokument může obsahovat různý počet utajovaných informací a může obsahovat i neutajované části. Pokud není na utajovaném dokumentu vyznačeno, že nějaká jeho část je neutajovaná, musí se k takovému dokumentu přistupovat, jako by byl utajovaný veškerý jeho obsah. V tomto kontextu lze utajovaný dokument chápat jako určitý souhrn informací, z nichž jsou buď všechny, nebo pouze některé utajované. Utajovaná informace je vždy utajována jako celek. Navzdory uvedenému někdy dochází k užívání pojmů utajovaná informace a utajovaný dokument *promiscue*. Pojem utajovaná informace je obecnější než pojem utajovaný dokument, neboť všechny utajované dokumenty jsou zároveň utajovanými informacemi či souhrny utajovaných informací, kdežto všechny utajované informace nejsou utajovanými dokumenty. Ze zákonné definice utajované informace kromě jiného vyplývá, že se jedná pouze o takovou informaci, která je zaznamenána na nějakém nosiči. Tímto nosičem je nejčastěji papír, jiný obdobný materiál nebo paměťový disk. Je-li nosičem utajované informace papír nebo jiný obdobný materiál, můžeme hovořit o listinném utajovaném doku-

---

[10] Srov. § 21 odst. 3 zákona o ochraně utajovaných informací.

[11] Jedná se o označení „KRYPTO“, jde-li o utajovanou informaci z oblasti kryptografické ochrany, a označení „ATOMAL“, jde-li o utajovanou informaci z oblasti zbraní hromadného ničení.

[12] Srov. § 35a odst. 1 zákona o ochraně utajovaných informací.

mentu. V případě, že nosičem utajované informace je paměťový disk, jedná se o nelistinný utajovaný dokument. V tomto kontextu lze *de facto* položit rovnítko mezi pojem *utajovaný dokument* a pojem nosič *utajované informace*. Je-li však paměťový disk relativně pevnou součástí informačního systému, nelze jej označovat jako utajovaný dokument. Utajovanými dokumenty nejsou ani utajované informace, které se na takovém paměťovém disku nacházejí. Je tomu tak proto, že na nakládání s utajovanými informacemi v informačních systémech se nevztahují pravidla administrativní bezpečnosti. Utajované informace nemusí při jejich zpracování a přenosu v informačních systémech dokonce ani nést označení stupněm utajení a další označení identifikující tyto informace jako utajované.[13)] Utajovaným dokumentem je až případný výtisk utajované informace nacházející se na takovém paměťovém disku.[14)] Ten již musí být označen v souladu se zákonem o ochraně utajovaných informací.

5. Přístup k utajované informaci

Přístup k utajované informaci lze umožnit fyzické osobě nebo podnikateli (podnikající fyzické osobě nebo právnické osobě), splňují-li pro to tyto osoby zákonné předpoklady. Podmínky přístupu fyzické osoby i právnické osoby k utajované informaci jsou dvojího druhu. Podmínkou umožnění přístupu osoby k utajované informaci je skutečnost, že jej tato osoba nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti. Jedná se o *potřebu vědět (need to know)*. Další podmínkou umožnění přístupu k utajované informaci je držení příslušného dokladu opravňujícího danou osobu k přístupu k utajované informaci daného nebo nižšího stupně utajení. Těmito doklady jsou u fyzické osoby *oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, osvědčení fyzické osoby či doklad o bezpečnostní způsobilosti fyzické osoby (viz níže), a u podnikatele osvědčení podnikatele*. K přístupu podnikatele k utajované informaci stupně utajení Vyhrazené postačuje i *prohlášení podnikatele* dokládající schopnost daného podnikatele zabezpečit ochranu utajované informace.

O žádosti o vydání osvědčení fyzické osoby a o žádosti o vydání osvědčení podnikatele se rozhoduje v *bezpečnostním řízení*. Bezpečnostní řízení je principiálně *správním řízením sui generis*, které však neprobíhá podle obecné úpravy správního řízení[15)], nýbrž podle zákona o ochraně utajovaných informací.

6. Neutajované dokumenty EU a NATO s omezeným přístupem

Kromě utajovaných informací se lze setkat také s neutajovanými dokumenty EU označenými nikoli stupněm utajení, nýbrž nesoucími označení „LIMITE“. Přístup k těmto dokumentům je většinou omezen na okruh osob majících po-

---

[13)] Srov. § 23 odst. 3 zákona o ochraně utajovaných informací.
[14)] Srov. § 2 písm. e) vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.
[15)] Zákon č. 500/2004 Sb., správní řád.

třebu vědět, přičemž po určité době se tyto informace mohou stát obecně přístupnými. Zvláštní režim platí u neutajovaných dokumentů NATO označených jako „NATO UNCLASSIFIED“. Potřebuje-li konkrétní osoba znát obsah některého z takto označených předpisů NATO, může se obrátit na NBÚ s žádostí o poskytnutí takového dokumentu. V žádosti musí taková osoba zdůvodnit, jak požadované informace souvisejí s předmětem její činnosti. NBÚ zváží oprávněnost takové žádosti a shledá-li ji oprávněnou, požadovaný předpis žadateli poskytne.[16)] NBÚ zde de facto zvažuje potřebu vědět dotyčné osoby ve vztahu k požadovanému dokumentu NATO.

7. Citlivé činnosti

Od utajovaných informací je třeba odlišovat *citlivé činnosti*. Citlivou činností se rozumí některé činnosti vykonávané pro potřeby zpravodajských služeb stanovené zákonem o ochraně utajovaných informací[17)] a další citlivé činnosti stanovené jinými právními předpisy[18)]. Společným znakem všech citlivých činností je skutečnost, že zneužitím citlivé činnosti může dojít k ohrožení zájmu ČR. Zatímco jiné právní předpisy výslovně popisují, co se považuje za citlivou činnost,[19)] výkon citlivé činnosti pro zpravodajské služby zákon o ochraně utajovaných informací s ohledem na působnost zpravodajských služeb a charakter plnění jejich úkolů explicitně nepopisuje, ale omezuje se pouze na to, že se jedná o úkony třetích osob prováděné pro zpravodajskou službu na základě dohody v souvislosti s výkonem státní správy nebo z jiného důvodu. Poměrně strohé zákonné ustanovení je ve zvláštní části důvodové zprávy k zákonu o ochraně utajovaných informací dále rozvedeno v tom smyslu, že v případě zpravodajských služeb lze zneužít k ohrožení zájmu ČR většinu činností, které provádějí pro zpravodajské služby třetí osoby, aniž se seznamují s utajovanými informacemi. Jako příklad se zde pak uvádí provádění prací pro zpravodajské služby, dodávky zboží, seznámení se s objekty zpravodajské služby či seznámení se s vybavením objektů zpravodajské služby.[20)]

Souhrn podmínek, jejichž splnění je nezbytné pro to, aby daná osoba mohla vykonávat citlivou činnost, se označuje jako *bezpečnostní způsobilost*. Splňuje-li

---

16) Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/. [cit. 2017-6-7].

17) Srov. § 138 odst. 1 písm. l) a § 88 zákona o ochraně utajovaných informací.

18) Konkrétní obsah citlivé činnosti pak stanoví jiné zákony jako např. zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., trestní zákon, zákon č. 263/2016 Sb., atomový zákon, zákon č. 134/2016 Sb., o zadávání veřejných zakázek, zákon č. 312/2006 Sb., o insolvenčních správcích či zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě.

19) Např. podle 220 odst. 1 zákona č. 134/2016 Sb. o zadávání veřejných zakázek se za citlivou činnost podle zákona o ochraně utajovaných informací při zadávání veřejné zakázky veřejným zadavatelem podle § 4 odst. 1 písm. a) nebo c) považuje schválení zadávací dokumentace nebo zadání veřejné zakázky u veřejné zakázky, jejíž předpokládaná hodnota přesáhne 300 000 000 Kč.

20) Srov. Důvodovou zprávu k zákonu o ochraně utajovaných informací, s. 13 a 14.

osoba podmínky pro výkon citlivé činnosti, může jí NBÚ vydat *doklad o bezpečnostní způsobilosti fyzické osoby*. Problematika ochrany utajovaných informací je s problematikou citlivých činností do určité míry propojena. Ekvivalentem držení dokladu o bezpečnostní způsobilosti fyzické osoby je pro účely výkonu citlivé činnosti držení platného osvědčení fyzické osoby. Ekvivalentem držení oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené pro účely přístupu k utajované informaci stupně utajení Vyhrazené je na druhou stranu držení dokladu o bezpečnostní způsobilosti fyzické osoby. Podmínky pro výkon citlivé činnosti se tedy částečně překrývají s podmínkami pro přístup k utajované informaci.[21)] Dalším společným prvkem oblasti ochrany utajovaných informací a oblasti citlivých činností je skutečnost, že gestorem obou oblastí je NBÚ.

8. Jednotlivé druhy zajištění ochrany utajovaných informací

V souladu s tím, jaká existují při nakládání s utajovanými informacemi rizika s možným důsledkem v podobě vyzrazení utajované informace, rozlišuje zákon *jednotlivé druhy zajištění ochrany utajovaných informací*. Ochrana utajovaných informací je zajišťována především prostřednictvím *personální bezpečnosti*, zahrnující výběr, výchovu a ochranu fyzických osob, které mají mít přístup k utajované informaci, včetně ověřování podmínek pro přístup fyzických osob k utajované informaci.[22)] Dalším druhem zajištění ochrany utajovaných informací je *průmyslová bezpečnost*, zahrnující systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajované informaci a k zajištění nakládání s utajovanou informací u podnikatele v souladu se zákonem o ochraně utajovaných informací.[23)] *Administrativní bezpečnost* zahrnuje systém bezpečnostních opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, popř. jiném nakládání s utajovanou informací.[24)] Ochrana utajovaných informací je zajišťována také prostřednictvím *fyzické bezpečnosti*, která zahrnuje systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajované informaci, popř. přístup nebo pokus o něj zaznamenat.[25)] Dalším z druhů zajištění ochrany utajovaných informací je *bezpečnost informačních nebo komunikačních systémů*, která zahrnuje systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž nakládají informační nebo komunikační systémy a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému.[26)] V neposlední řadě je ochrana utajovaných informací zajišťována také prostřednictvím *kryptografické ochrany*, zahrnující systém opatření na ochranu utajovaných informací použitím kryptografických (šifrovacích) metod a krypto-

---

[21)] Srov. § 6 odst. 1 a § 80 zákona o ochraně utajovaných informací.
[22)] Srov. § 5 písm. a) zákona o ochraně utajovaných informací.
[23)] Srov. § 5 písm. b) zákona o ochraně utajovaných informací.
[24)] Srov. § 5 písm. c) zákona o ochraně utajovaných informací.
[25)] Srov. § 5 písm. d) zákona o ochraně utajovaných informací.
[26)] Srov. § 5 písm. e) zákona o ochraně utajovaných informací.

grafických (šifrovacích) materiálů při zpracování, přenosu nebo ukládání utajovaných informací.[27)]

9. Původce utajované informace, odpovědná osoba a bezpečnostní ředitel

Tím, u něhož utajovaná informace vzniká, tedy *původcem utajované informace*, je nejčastěji orgán státu. Původcem utajované informace však může být také právnická osoba nebo podnikající fyzická osoba. Nepodnikající fyzická osoba nemůže být původcem utajované informace, avšak jednání takové osoby může být příčinou ke vzniku utajované informace. Je tomu tak v případě, podá-li fyzická osoba Úřadu průmyslového vlastnictví přihlášku vynálezu, užitného vzoru nebo topografie polovodičového výrobku, jejíž předmět obsahuje utajovanou informaci.

Zákon o ochraně utajovaných informací zavádí institut *odpovědné osoby*, jakožto osoby mající, v rámci subjektů majících přístup k utajované informaci z hlediska ochrany utajovaných informací, nejvýznamnější postavení. Zákon specifikuje, kdo je odpovědnou osobou u jednotlivých kategorií subjektů majících přístup k utajované informaci.[28)] Zákon o ochraně utajovaných informací také v zájmu zajištění funkčnosti systému ochrany utajovaných informací stanoví orgánu státu, právnické osobě a fyzické osobě majícím přístup k utajované informaci povinnost jmenovat *bezpečnostního ředitele*. Funkci bezpečnostního ředitele může vykonávat i samotná odpovědná osoba. Většina nejdůležitějších povinností souvisejících s ochranou utajovaných informací je zákonem o ochraně utajovaných informací svěřena právě odpovědné osobě a bezpečnostnímu řediteli. Vzhledem k tomu, že většinou není v možnostech odpovědné osoby při jejích dalších povinnostech obsáhnout fyzicky všechny povinnosti na úseku ochrany utajovaných informací, může odpovědná osoba přenášet část svých pravomocí při zajišťování ochrany utajovaných informací na bezpečnostního ředitele a může také určovat k plnění těchto povinností jiné osoby.[29)]

10. Obecné povinnosti při ochraně utajovaných informací

Zákon o ochraně utajovaných informací stanoví určité *obecné povinnosti při ochraně utajovaných informací*, které je povinen splnit každý, nastanou-li pro jejich splnění předpoklady. Jedná se o povinnost neprodleně odevzdat NBÚ, policii a v zahraničí zastupitelskému úřadu ČR nalezenou utajovanou informaci nebo utajovanou informaci získanou v rozporu se zákonem anebo nalezené osvědčení pro přístup k utajované informaci. Dále se jedná o povinnost každého, kdo měl nebo má přístup k utajované informaci, zachovávat o ní mlčenlivost

---

[27)] Srov. § 5 písm. f) zákona o ochraně utajovaných informací.

[28)] U většiny orgánů veřejné moci a dalších organizačních složek státu je odpovědnou osobou osoba stojící v čele takového orgánu, resp. organizační složky. U většiny právnických osob je odpovědnou osobou statutární orgán, resp. fyzická osoba v rámci statutárního orgánu, která je touto funkcí pověřena.

[29)] Srov. § 67 a § 71 zákona o ochraně utajovaných informací.

a neumožnit k ní přístup neoprávněné osobě.[30)] Stanovení a plnění uvedených povinností nejenže přispívá k zajištění fungování systému ochrany utajovaných informací jako celku, ale má také preventivní význam.

11. Závěr a úvahy de lege ferenda

Autor tohoto článku je přesvědčen, že základní instituty ochrany utajovaných informací jsou v ČR upraveny v zákonné i podzákonné rovině na poměrně vysoké úrovni. Současně považuje národní právní úpravu ochrany utajovaných informací, včetně úpravy některých jejích základních institutů, za značně složitou. Právě komplikované definice a související úpravy některých institutů ochrany utajovaných informací mohou v aplikační praxi přinášet nemalé obtíže.

Podle autora tohoto článku by mělo být v zákoně o ochraně utajovaných informací explicitně uvedeno, že absentuje-li u informace formální znak v podobě jejího označení v souladu se zákonem o ochraně utajovaných informací (např. příslušným stupněm utajení), nejedná se o utajovanou informaci pouze tehdy, nebyla-li takto informace označena proto, že nesplňuje buď materiální znak utajované informace, nebo ji nelze podřadit pod konkrétní bod některé z příloh v seznamu utajovaných informací.

Jako problematický moment spatřuje autor tohoto článku rozlišování utajované informace na straně jedné a utajovaného dokumentu na straně druhé, a to zejména s ohledem na ne zcela jasné vymezení pojmu utajovaný dokument.

S uvedeným souvisí skutečnost, že na utajované informace nacházející se pouze na paměťovém disku, který je relativně pevnou součástí informačního systému, se aplikují v některých ohledech značně odlišná pravidla než na ostatní utajované informace. Podle autora tohoto článku je takováto dvojí úprava nakládání s utajovanými informacemi v závislosti na tom, zda se jedná o informace, které jsou součástí utajovaného dokumentu, nebo jde o informace nacházející se pouze na paměťovém disku počítače, neodůvodněná a v důsledku nepřispívá ke kvalitní ochraně utajovaných informací.

Autor tohoto článku se dále domnívá, že na nosiči utajované informace by měl být zachycen nikoli pouze datum vzniku utajované informace, ale s přesností na minuty i samotný okamžik vzniku utajované informace. V dnešní době, kterou již lze do značné míry označit jako dobu kybernetickou, bude pravděpodobně stále častěji třeba reagovat na vnější a vnitřní hrozby a nastalé situace bez zbytečného prodlení. Tomu odpovídá daleko spíše možnost zaznamenávání a ověřování přesného okamžiku vzniku konkrétní informace, zvláště pak jedná-li se o informaci utajovanou.

[30)] Srov. § 65 odst. 1 a 2 zákona o ochraně utajovaných informací.

Shrnutí:

Článek se zabývá problematikou základních institutů ochrany utajovaných informací v ČR. Po úvodním slovu se článek věnuje ukotvení ochrany utajovaných informací v právním řádu. Další kapitola pojednává koncept utajované informace. Podrobněji se článek zabývá také obsahovými rozdíly mezi termíny utajovaná informace a utajovaný dokument. Článek krátce pojednává o základních aspektech přístupu k utajované informaci. Stručně se článek zabývá jednotlivými druhy zajištění ochrany utajovaných informací. Článek se zabývá také neutajovanými dokumenty Evropské unie a Severoatlantické aliance s omezeným přístupem. Článek poskytuje obecný vhled také do problematiky citlivých činností a bezpečnostní způsobilosti. V závěru autor prezentuje některé úvahy *de lege ferenda*.

Basic institutes for the protection of classified information – summary:

The article deals with the issue of basic institutes for the protection of classified information in the Czech Republic. After the introductory word, the article focuses on anchoring the protection of classified information in the legal order. Another chapter discusses the concept of classified information. In more detail, the article also deals with semantic differences between the term classified information and the term classified document. The article briefly discusses basic aspects of access to classified information. The article briefly deals with respective forms of securing protection of classified information. The article also deals with unclassified documents of the European Union and the North Atlantic Alliance with limited access. The article provides a general insight into the issues of sensitive activities and security eligibility. In conclusion, the author presents some considerations *de lege ferenda*.