Analýza dostupnosti informací podle zákona č. 106/1999 Sb. včetně navržení variant k ochraně aktivit BS a ZS

Záměry a návrhy na zvýšení ochrany některých bezpečnostně citlivých informací z hlediska zákona o svobodném přístupu k informacím

Ministerstvo vnitra

Bezpečnostní odbor

Zpracoval: ing. Oldřich Kužílek, 2016

Obsah

1. Východisko a typické situace, vyvolávajících nejistotu o ochraně informací

S rozvojem informační společnosti, doprovázeném též snahou o transparentnost veřejné správy a zejména poskytováním a zpřístupňováním rozsáhlých souborů informací (včetně fenoménu „otevřených dat“), vzniká v některých případech nejistota orgánů veřejné moci zejména na poli bezpečnosti, o možnosti ochrany informací významných pro bezpečnost nebo jiné důležité právem chráněné zájmy. Kladou si otázku, zda je možné efektivně ochránit všechny informace, které by mohly být **využity k vytěžení** takových údajů, jejichž veřejná dostupnost **přináší riziko** například při ochraně před kybernetickými hrozbami, terorismem, organizovaným zločinem, či prostě takovým obejitím případně nedokonalé právní úpravy, kdy by se (snad) měly poskytnout informace, jež mají zůstat utajené či důvěrné.

V poslední době se objevuje několik iniciativ, které požadují zvýšit ochranu některých bezpečnostně citlivých informací před možností získat je pomocí žádosti o informace postupem podle zákona o svobodném přístupu k informacím a na základě článku 17 Listiny základních práv a svobod.

Příkladem je projednávaný návrh novely zákona o kybernetické bezpečnosti, zahrnující původně též přímou novelu zákona o svobodném přístupu k informacím (InfZ, Infozákon), který **sleduje cíl kybernetické bezpečnosti a ochrany bezpečnosti sítí a informačních systémů.** Tento návrh však byl později modifikován v doporučeném smyslu, tedy vynětí z obecného zákona a zařazení do speciálního zákona o kybernetické bezpečnosti[1].

Dalším příkladem je, že při projednávání novelizace zákona o registru smluv předkládají někteří poslanci návrhy, které by měly více ochránit přístup k informací, týkající se **nakládání s výbušninami.**

Dále Bezpečnostní odbor Ministerstva vnitra řeší otázky, kdy se údajně může podařit pomocí žádostí o informace a srovnáváním získaných datasetů **extrahovat informace, které jsou v datasetech za normálních okolností skryté**.

Dále se uvádí žádost o poskytnutí **otázek a správných odpovědí pro úřednické zkoušky** v gesci Ministerstva vnitra, kdy údajně nelze najít právní ustanovení, podle kterého by bylo možné tuto žádost odmítnout.

[1] Materiál do jednání vlády, návrh nového § 10 v zákoně o kybernetické bezpečnosti:
§ 10a
Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, anebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, jež kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím neposkytují.

2. Problémy návrhů – typy ohrožených informací a odůvodnění požadovaných změn

a) Absence konkrétního popisu a racionálního odůvodnění návrhu

Kybernetická bezpečnost

Obvyklým problémem zvažovaných návrhů je nedostatečné odůvodnění. Například důvodová zpráva ke změně v souvislosti s novelizací kybernetického zákona ve speciální části uvádí toliko: *„Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona (míněn Infozákon) správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout“*. Toto **tvrzení v důvodové zprávě není nijak doloženo,** neobsahuje ani jeden (třeba i jen modelový) příklad potenciálního problému, ani žádnou charakteristiku situací, v nichž by (snad) nebylo možné chránit informaci, jejíž poskytnutí by ohrozilo bezpečnost komunikačních systémů kritické informační infrastruktury nebo významných informačních systémů. Tvrzení, že povinný subjekt bude povinen informace *o přijatých bezpečnostních opatřeních* poskytovat, je do značné míry nepravdivé. Povinný subjekt by naprostou většinu takových informací legitimně odmítl poskytnout na základě **§ 11 odst. 1 písm. a) InfZ** *(informace se se vztahuje výlučně k vnitřním pokynům)***.** Dosavadní výkladová a judikaturní situace umožňuje chránit prakticky všechny případy, které zamýšlená úprava má nejspíše na mysli (viz dále).

Nicméně z osobního projednání plyne, že problematické by mělo být například poskytování informací o zakoupených prostředcích ochrany kybernetického prostoru a sítí komunikací, zejména typu bezpečnostního software, hardware, případně objednávek dalších služeb souvisejících se zajištěním kybernetické bezpečnosti konkrétních subjektů.

Zároveň však z konzultací s odborníky na bezpečnost IT systémů plyne, že až 80% případů úspěšných útoků na bezpečnost sítí a IT systémů je založeno na selhání jedinců. Velkou část informaci o technickém zabezpečení sítě nebo IT systému si útočníci zjistí přímo v kontaktu se systémem. Podíl získání pro útok potřebných informací z otevřených zdrojů je naopak minimální. Může spočívat zejména v získání přehledu o poskytovaných službách, zejména časovém rozložení dohledu poskytovatele služby, kdy například o víkendu může mít případný útočník nerušený čas pro svou operaci, kdy nehrozí rychlé protiopatření.

Význam ochrany potenciálně rizikových informací, které by se jinak poskytly veřejnosti, je tedy velmi malý, významně menší než jiné formy získání informací potřebných pro útok.

Znovu nutno zdůraznit, že popsané informace by bylo možné odmítnout poskytnout na základě § 11 odst. 1 písm. a) InfZ.

Obecná bezpečnost

Podobně problematické jsou příklady z oblasti obecné bezpečnosti, jako dále uvedené otázky spojené s utajenými registračními značkami vozidel nebo informacemi o infrastruktuře typu přípojných bodů či odběru energií. Nepodařilo se však vyhledat jakýkoliv případ, ať už jako rozhodnutí nadřízeného orgánu anebo rozsudek soudu, který by skutečně způsobil, že povinný

subjekt je povinen poskytnout informace, které by materiálně, nikoli formálně, odpovídaly nutné ochraně ve smyslu čl. 17 odst. 4 Listiny, která umožňuje chránit informace *„jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.“*

Z osobního projednání plyne, že rizikové se jeví například poskytnutí celkových datasetů informací o registračních značkách vozidel, distribuovaných na různých úrovních dopravních úřadů v ČR. Jejich shromažďováním a porovnáním s takovou databází poskytnutou centrálně lze údajně selektovat registrační značky, které byly přiděleny jiným postupem, než běžným uživatelům. Tím údajně dochází k možnosti filtrovat registrační značky určené pro bezpečnostní složky v režimu, kdy by přímé poskytnutí těchto údajů nebylo možné (šlo by o utajovanou informaci).

Podobně lze uvažovat o využití databáze povinného pojištění vozidel, která je veřejně dostupná. Bezpečnostní složky vozidla nepojišťují, tím pádem vzniká možnost určité filtrace údajů, která může vést k přiřazení určitých registračních čísel k bezpečnostním složkám.

Dalším případem mohou být dotazy dle Infozákona na to, zda určité osoby jsou příslušníky Policie (přičemž Nařízení vlády č. 522/2005 Sb. kterým se stanoví seznam utajovaných informací, umožňuje chránit jako utajovanou informaci v bodě 15. *„Příslušnost vybraného policisty k určenému útvaru Policie České republiky* ***nebo k Policii*** *České republiky“*). Toto ustanovení by mělo dostatečně pokrýt veškeré případy, neboť umožňuje odepřít i informaci o tom, zda je určitá osoba vůbec policistou. Otázka, které útvary jsou „určené“ je plně v moci ministerstva vnitra.

Dalším případem by údajně mohly být dotazy typu informací o přípojných bodech určitých budov (kritické infrastruktury) k energetickým a dalším sítím, případě dotazy na spotřebu elektrické energie či jiné dodávky, z nichž by bylo možné dedukovat na utajované činnosti, které samy o sobě oprávněně spadají pod různé stupně utajení podle zákona o utajovaných informacích.

Žádný z předkládaných problematický okruhů informací však nebyl doložen konkrétně a tak, aby bylo možné posoudit, zda rizikové informace nelze chránit jiným způsobem, a to ať právně, anebo organizačním opatřením, kdy poskytnuté informace nevedou k vytěžení rizikových informací.

Otevřená data

Poněkud jiným případem je zveřejnění otevřených dat. Například v systému CRAB (centrální registr administrativních budov, provozuje Úřad pro zastupování státu ve věcech majetkových, ÚZSMV), se zveřejňují údaje o nájmu administrativních budov. Informační systém je podle § 14a zákona č. 219/2000 Sb. o majetku České republiky neveřejný. Ovšem status „neveřejný“ nebrání tomu, aby se z něj vybraná data zveřejňovala formou otevřených dat anebo výpisů zveřejněných na webu. Vedení Ministerstva financí a ÚZSVM rozhodlo některá data zveřejnit, především z hlediska možné kontroly nakládání s veřejnými prostředky. Lze tak například

dohledat prostory obvodních oddělení Policie[2], kde se mj. uvádí hodnota „Skutečný počet zaměstnanců v nájmu“ případně „„Dislokováno zaměstnanců (skutečnost)“. Údajně tak lze zjistit, jaké jsou podstavy na jednotlivých obvodních odděleních, a tím i schopnost zásahu Policie při odčerpání kapacity jinou, například fingovanou událostí. Tato úvaha však vychází jednak z toho, že by byl dostupný též údaj o plné (tabulkové) kapacitě, jednak z toho, že data by byla zcela aktuální. Ani jedno však neplatí. Údaj navíc nemusí vyjadřovat počet policistů, může zahrnovat i civilní zaměstnance, a údaj o dislokaci nemusí odpovídat skutečnému stavu policistů přítomných v určitém okamžiku, již třeba jen s ohledem na rozdělení služeb. Případná snaha koncipovat teroristický útok při využití těchto údajů tedy není prakticky nijak významně usnadněná, vyžadovala by sběr mnoha dalších, nedostupných údajů.

Ani u Hasičského záchranného sboru nejsou veřejně dostupné informace o počtu hasičů na jednotlivých územních odborech. Navíc je otázkou, jakou realitu tyto údaje deklarují a jak jsou v souladu se zásadou uvedenou v § 14a odst. 2 z. č. 219/2000 Sb., hovořící o „úplných a pravdivých údajích“, které organizační složka poskytuje do CRABu.

Případná snaha koncipovat teroristický útok při využití údajů o kapacitách tak není zveřejněním údajů nijak významně usnadněná.

Problematika otevřených dat se tedy jeví tak, že případná citlivá data je nutno chránit organizačně při vstupu a není třeba kvůli nim hledat legislativní nástroj specifické ochrany informací.

Nedostatek těchto konkrétnějších popisů anebo jejich spíše organizační povaha pak zásadně brání tomu, aby se případné legislativní opatření formulovalo ústavně konformně a tak, aby se nedostalo do rozporu s čl. 17 Listiny, což by vyvolávalo riziko zrušení Ústavním soudem.

b) Příliš široké dopady návrhů a jejich paradoxní působení proti vytčenému cíli

Uvedeného cíle ochrany některých informací se často navrhuje dosahovat pomocí legislativního opatření, které zajištění tohoto cíle značně **přesahuje a** jeho formulace neodpovídá záměru**.** Tím pádem jednak směřuje k nepřístupnosti informací, jejichž odepírání nemůže obstát ve světle čl. 17 Listiny, jednak zcela nadbytečně ukládá (namísto aby toliko umožňoval) chránit určité okruhy informací.

V některých případech dokonce překračuje nutnou úroveň ochrany natolik, že způsobuje paradox: povinným subjektům **zakazuje zveřejnit** informaci, jejíž zveřejnění by naopak podpořilo dosažení vytčeného cíle, tedy například zvýšilo bezpečnost sítí (může jít například o informace, působící preventivně proti snahám narušit kybernetickou bezpečnost a bezpečnost sítí). Například pokud se navrhne, aby se nutnost odepření informace týkala všech informací, *„které se týkají zajištění kybernetické bezpečnosti“*, pak taková formulace zahrne i informace, u kterých není důvod ochrany. Z tohoto hlediska je správné použít formulaci, vymezující

[2] Např. Soubor „08a-Porovnani-vydaju-za-najem“ na adrese http://crab.uzsvm.cz/Prehledy-z-registru-415-0-84/Porovnani-vydaju-za-najem--123449/, položka „Skutečný počet zaměstnanců v nájmu“, anebo soubor „Dislokace“ na adrese http://data.mfcr.cz/cs/dataset/centralni-registr-administrativnich-budov, položka „Dislokováno zaměstnanců (skutečnost)“.

informace jako ty, jejichž **poskytnutím může dojít k ohrožení** určitého chráněného zájmu, nikoli které **se tohoto zájmu týkají**.

Uvedený problém vzniká zpravidla také nevhodným zařazením do struktury Infozákona, který rozlišuje obligatorní a fakultativní případy odmítnutí žádostí o informace. Zpravidla zcela nevhodné je zařazení do **druhého odstavce** v § 11 InfZ, který je tzv. „obligatorní", tzn., že jeho **disposice** přímo **ukládá** povinnému subjektu informaci **odepřít** a neumožňuje mu zvážit, zda skutečně existuje zájem na ochraně informace (*„Povinný subjekt informaci neposkytne, pokud…"*). Pro zajištění sledovaných cílů bezpečnosti je ale zpravidla systematicky vhodnější „fakultativní" forma disposice, která je použita **v předchozím prvním odstavci** (*„Povinný subjekt může omezit poskytnutí informace, pokud…"*).

c) Nevhodné legislativně technické řešení – využívání obecného Infozákona, namísto oborových zákonů

Dalším nevhodným aspektem zvoleného legislativně-technického řešení je zařazování speciálních výjimek, zahrnujících pouze určitý obor činnosti některých povinných subjektů, do obecného zákona o přístupu k informacím. Navržení normy **do obecného zákona o přístupu k informacím**, ačkoliv jde zpravidla o úzce vymezenou věcnou oblast v určitém oboru (kybernetická bezpečnost, nakládání s výbušninami), a to za situace, kdy **tato oblast je upravena speciálním zákonem** (zákon o kybernetické bezpečnosti, zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě), přináší následně značné výkladové problémy, destruuje Infozákon a v posledku vede k celkově horší ochraně informací. Obecný zákon nemá obsahovat normy, týkající se jen jedné, úzce specializované oblasti (protiargumentem nemůže být, že se tento princip již v InfZ prolomil a nesprávně obsahuje některé takové úzce specializované normy[3]). Důvodem není jen „estetika" právních norem, ale především **desinterpretace,** která se tak vytváří: Problematika speciálního oboru se totiž přenáší a promítá do intepretace obecné normy i pro jiné věcné oblasti, a to buď přímo, anebo často na základě argumentu *a contrario.*

Například vložením úzce oborově formulované ochrany některých informací do § 11 odst. 2 nebo odst. 4 InfZ se výkladově vylučuje možnost širokého výkladu § 11 odst. 1 písm. a) tak, aby požadovanou ochranu zahrnoval. Zužuje se tím možnost takového výkladu, aby jako *„informace vztahující se výlučně k vnitřním pokynům"* bylo obecně možné chránit informace, jejichž poskytnutí by ohrozilo účinnost některých bezpečnostních opatření. Přitom je samozřejmé, že dopředu nelze odhadnout všechny případy, které praxe přinese, kdy by bylo potřebné pod ochranu v § 11 odst. 1 určité informace zahrnout. A samozřejmě se nepodaří tyto situace vystihnout ani v oněch úzce speciálních ustanoveních (např. o kybernetické bezpečnosti, o informacích o činnosti OČTŘ případně i bezpečnostních sborů ad.). Všechny tyto formulace jsou příliš úzké a například při případech spolupráce se soukromým sektorem může dojít k situacím, které nezahrnou, ačkoliv by bylo třeba některé informace chránit.

[3] Aktuálně v souvislosti s úpravou informací o kybernetické bezpečnosti dojde naopak k vynětí takto nesprávně zařazeného ustanovení

Reálným dopadem tedy je, že zatímco pro jednu resortní oblast se možnost ochrany zvýší (např. jak bylo původně navrženo pro kybernetickou bezpečnost), pro jiné oblasti, které si ochranu také zasluhují, se paradoxně sníží.

Zároveň lze konstatovat, že „poptávka" po obdobných zřetelnějších formách ochrany vzniká i v jiných oblastech veřejné správy, kde se povinné subjekty setkávají se situacemi, kdy mají nejistotu, zda budou moci účinně chránit specifické typy informací, které jsou „na hraně" charakteristiky, kterou InfZ či jiný předpis umožňuje chránit.

Proto je zcela správné, že při aktuální novelizaci InfZ v rámci novelizace zákona o kybernetické bezpečnosti se navrhuje přenesení ochrany informací vedených v evidenci incidentů z dosavadního § 11 odst. 4 písm. f) přímo do nového § 10a zákona o kybernetické bezpečnosti.

Popsaný problém (přílišná speciálnost v určitém oboru) by se tedy také dala řešit nalezením takové formulace, která by byla **obecnější a řešila podobnou nejistotu i v dalších oborech.**

d) Návrh na doplnění § 11 odst. 6 InfZ - polemika

Při přípravě novelizace InfZ ministerstvem vnitra v r. 2016 byla při vypořádání vnitroresortního připomínkového řízení na MV připravena následující změna znění § 11 odst. 6:

*„(6) Povinný subjekt neposkytne informaci**, jejíž poskytnutí by mohlo ohrozit bezpečnost České republiky, nebo informaci** o činnosti orgánů činných v trestním řízení **a bezpečnostních sborů**, včetně informací ze spisů, a to i spisů, v nichž nebylo zahájeno trestní řízení, dokumentů, materiálů a zpráv o postupu při prověřování oznámení, které vznikly činností těchto orgánů **a sborů** při ochraně bezpečnosti osob, majetku a veřejného pořádku, předcházení trestné činnosti a při plnění úkolů podle trestního řádu, pokud by se tím ohrozila práva třetích osob anebo schopnost orgánů činných v trestním řízení **a bezpečnostních sborů** předcházet trestné činnosti, vyhledávat nebo odhalovat trestnou činnost nebo stíhat trestné činy, zajišťovat **veřejný pořádek nebo** bezpečnost České republiky. Ustanovení jiných zákonů o poskytování informací tím nejsou dotčena."*

Problémy tohoto návrhu lze spatřovat zejména v následujících bodech:

1) První část návrhu *„Povinný subjekt neposkytne informaci**, jejíž poskytnutí by mohlo ohrozit bezpečnost České republiky",*** je naprosto všeobecná a je pouhým přepisem odpovídající části čl. 17 Listiny, která *zní „…právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro …bezpečnost státu…"*. Není tedy použitelná pro upřesnění obecné ústavní normy v prováděcím běžném zákonu a neodpovídá tak požadavku čl. 4 odst. 2 Listiny, protože v takto navrženém znění by zákon nic neupřesňoval *(„Meze základních práv a svobod mohou být za podmínek stanovených Listinou základních práv a svobod upraveny pouze zákonem.")*

2) Uvedená formulace *„informace, jejíž poskytnutí by mohlo ohrozit bezpečnost České republiky“* je zcela vágní. Ostatní formulace dosavadního i navrženého znění odstavce 6 se opírají o znak **„ohrožení schopnosti“** příslušných orgánů. Naopak nově navržený znak *„poskytnutí by mohlo ohrozit bezpečnost“* stojí ve formulaci **samostatně**. To vytváří absurdní možnost neomezeného výkladu na jakoukoliv situaci: V informační době lze s jistotu říci, že prakticky každá informace, týkající se tak či onak výkonu veřejné moci v oblasti související s bezpečností státu může při kombinaci s dalšími zdroji informací v nějaké, třeba i zanedbatelné míře, ohrozit bezpečnost České republiky. Informační doba, kybernetické hrozby a terorismus využívají kombinací jakýchkoliv zdrojů informací ke generování informací, které mohou posloužit k jiným než původně zamýšleným účelům. Například informace o tom, kdo je odpovědným pracovníkem určitého úseku vodní elektrárny může za určitých okolností napomoci kybernetickému útoku. Informace o smlouvě města může napomoci přípravě teroristického útoku na základě znalosti konkrétní formy protipovodňového zařízení.

3) Již beztak přebujelá formulace odst. 6 se tímto dalším navrženým rozvinutím stala právně nejednoznačná, protože je logicky neuchopitelná a jazykově nejednoznačná. Není jasné, zda poslední pasáž prvního souvětí, tj. text *„pokud by se tím ohrozila práva třetích osob anebo schopnost orgánů činných v trestním řízení* ***a bezpečnostních sborů*** *předcházet trestné činnosti, vyhledávat nebo odhalovat trestnou činnost nebo stíhat trestné činy,* ***zajišťovat veřejný pořádek nebo bezpečnost České republiky.“*** se vztahuje jako podmínka i k pasáži ***„, jejíž poskytnutí by mohlo ohrozit bezpečnost České republiky,“,*** protože je odděleno spojkou „nebo“.

4) Dále došlo k duplicitě - pasáž *„jejíž poskytnutí by mohlo ohrozit bezpečnost České republiky“* vyjadřuje zcela totéž jako pasáž *„pokud by se tím ohrozila … schopnost orgánů činných v trestním řízení a bezpečnostních sborů … zajišťovat … bezpečnost České republiky.“*

V meziresortním řízení se však nakonec (v listopadu 2016) rozhodlo, že předložený návrh je natolik konfliktní, že se kvůli němu nebude pokračovat v přípravě novelizace Infozákona.

<u>Případné řešení pro futuro</u>

Pokud by podobně koncipovaný návrh na ochranu bezpečnostních informací měl být v budoucnu opět oživen, pak lze předložit konkrétní doporučení, aby se minimalizovaly jeho konfliktní a ústavně problematické aspekty.

Formulace by jednak měla být rozčleněna, jednak by měla být upřesněna tak, aby se neopírala toliko o teoreticky myslitelnou *„možnost ohrozit bezpečnost“*, ale aby byla vázaná na splnění dalších podmínek. Takovou podmínkou může být (jako v dosavadním znění) vazba na ohrožení schopnosti příslušných orgánů plnit své úkoly, anebo na významné snížení účinnosti bezpečnostních opatření. Bezpečnostními opatřeními se

přitom mohou mínit různé formy ochrany zájmů, uvedených v čl. 17 odst. 4 Listiny.

Návrh úpravy při využití výše uvedeného návrhu:

„(6) Povinný subjekt neposkytne informaci,

a) ***jejíž poskytnutí by mohlo významně nebo přímo snížit účinnost bezpečnostního opatření při ochraně bezpečnosti České republiky, stanoveného na základě zvláštního předpisu***[1]

b) ~~***informaci***~~ *o činnosti orgánů činných v trestním řízení* ***a bezpečnostních sborů****, včetně informací ze spisů, a to i spisů, v nichž nebylo zahájeno trestní řízení, dokumentů, materiálů a zpráv o postupu při prověřování oznámení, které vznikly činností těchto orgánů* ***a sborů*** *při ochraně bezpečnosti osob, majetku a veřejného pořádku, předcházení trestné činnosti a při plnění úkolů podle trestního řádu, pokud by se tím ohrozila práva třetích osob anebo schopnost orgánů činných v trestním řízení* ***a bezpečnostních sborů*** *předcházet trestné činnosti, vyhledávat nebo odhalovat trestnou činnost nebo stíhat trestné činy nebo* ***zajišťovat veřejný pořádek****.*

Ustanovení jiných zákonů o poskytování informací tím nejsou dotčena.

---

[1] Např. § 4 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ve znění pozdějších předpisů; § 22 až 26 zákona č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů; § 3 zákona č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením, ve znění pozdějších předpisů; § 5 odst. 1 písm. a) zákona č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů; § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.“

Mnohem lepší by však bylo formulovat tuto problematiku v jiném ustanovení, což se předkládá v závěrečném návrhu (viz dále).

e) Návrh na speciální ochranu nakládání s výbušninami při zveřejňování smluv v Registru smluv

Při projednávání návrhu novelizace zákona o Registru smluv (dále novela ZRS, sněmovní tisk č. 699) někteří poslanci navrhli doplnit zákon o povinném zveřejňování smluv o další výjimku, která by z povinnosti zveřejnit vyjímala smlouvy, jejichž *předmětem je nakládání s výbušninou*[1] *nebo zařízením či objektem určeným k její výrobě nebo skladování* (např. pozměňovací návrh č. 4438).

Takto navržená ochrana některých typů informací ve smlouvách je však již dostatečně zajištěna především pomocí Infozákona, a návazně pomocí zákona o ochraně utajovaných informací a případně též občanského zákoníku (obchodní tajemství). Na ochranu některých prvků smluv, uzavíraných povinnými subjekty v oblasti nakládání s výbušninami, či jiných dokumentů, lze totiž aplikovat ustanovení § 11 odst. 1 písm. a) Infozákona. Údaje o tom, kde je určitá komodita uložena, je informací, výlučně se vztahující k vnitřním pokynům. Podrobněji

k tomu dále v části **f) Nedostatečné využívání nástrojů platného Infozákona – přehled využitelnosti § 11 odst. 1 InfZ k ochraně informací**.

Zároveň lze na většinu předvídaných kritických typů informací o výbušninách v případě smluv či jiných dokumentů obchodních organizací aplikovat ochranu obchodním tajemstvím, a to proto, že právě pro jejich citlivost představují konkurenčně významnou skutečnost (jak primárně, např. kde jsou výbušniny skladovány, tak i sekundárně, tedy zda je tato skutečnost utajována, protože samotná skutečnost utajování má konkurenční význam a podnikatel, který by nebyl schopen dostatečně tyto informace chránit, by byl v konkurenční nevýhodě).

V případě výbušnin navíc lze ochranu alespoň části informací o nakládání s výbušninou nebo zařízením či objektem určeným k její výrobě nebo skladování zajistit označením za utajovanou informaci podle Zákona o ochraně utajovaných informací. Nařízení vlády k zákonu o ochraně utajovaných informací výslovně uvádí jako utajovanou informaci ve stupni Vyhrazené:

Příl.6

Seznam utajovaných informací v oblasti působnosti Ministerstva průmyslu a obchodu

1. Souhrnné informace o výzkumu, vývoji a výrobě výbušnin a o subjektech působících v tomto oboru

Příl.8 - Seznam utajovaných informací v oblasti působnosti Ministerstva vnitra

d) dislokace, kapacita a systém bezpečnostní ochrany muničních skladů, skladů zbraní, výbušnin nebo jiných nebezpečných látek

Zde je samozřejmě otázka, zda povinný subjekt v tomto smyslu s informacemi o dislokaci a přepravě výbušniny nakládá jako s utajovanou informací, ale možné to v zásadě je. Pak jde o část smlouvy, kterou jednoznačně nezveřejnění na základě § 3 odst. 1 zákona o registru smluv v kombinaci s § 7 Infozákona. V případě, že nejde o smlouvu zveřejňovanou v registru smluv, se pak chrání přímo na základě § 7 InfZ.

Dále lze překryvně pro utajení takto rizikových částí smluv či jiných dokumentů uplatnit i samotnou Listinu, která v čl. 17 odst. 4 uvádí ochranu informací v zájmu ochrany práv druhých osob.

Na druhou stranu je nutno si při snaze utajovat související typy informací uvědomit, že například údaj o tom, kdo a kde výbušniny vyrábí, je alespoň rámcově zřejmý z obchodního rejstříku a rovněž z živnostenského rejstříku, totiž z předmětu podnikání, druhu živnosti a provozoven (výroba výbušnin je koncesovanou živností dle přílohy č. 3 zákona č. 455/1991 Sb., živnostenského zákona). Z tohoto hlediska je nadbytečná snaha o neuveřejnění smluv týkajících se zařízení nebo objektů určených k výrobě v registru smluv.

Zákon o registru smluv sám o sobě chrání informace o tom, komu se výbušnina prodává. Taková informace totiž může být vyjmuta z uveřejnění dle § 5 odst. 6 ZRS, neboť jde o informaci o smluvní protistraně. Například Explosia, a.s. může z uveřejnění v registru smluv vyjmout informaci o tom, komu (a za jakou cenu) výbušniny prodává, a to podle § 5 odst. 6

ZRS, pokud by taková informace sama nebo ve svém souhrnu (coby seznam klientů či cenová politika) byla obchodním tajemstvím Explosie, a.s.

f) Nedostatečné využívání nástrojů platného Infozákona – přehled využitelnosti § 11 odst. 1 InfZ k ochraně informací

Další rovina problému spočívá v tom, že již dosavadní znění InfZ umožňuje chránit prakticky všechny případy, které se identifikují jako potenciálně rizikové informace. Judikatura již totiž postupně dovodila k § 11 odst. 1 písm. a) *(informace se se vztahuje výlučně k vnitřním pokynům)* možnost zahrnout pod něj například následující typy informací:

- pokyny k ochraně majetku, např. o ostraze objektů,
- pracovní postupy (rozsudek č.j. 5 As 28/2007 – 89)
- konkretizace úkolů, mohou v nich být stanoveny interní toky informací a konkrétní instrukce – v případě správce daně např. postupy při vkládání dat do automatizovaného daňového systému, způsoby ověřování důvěryhodnosti daňových subjektů, kritéria hodnocení kontrolní činnosti, způsoby výměny informací mezi státními orgány, zásady dohlídkové činnosti (rozsudek č.j. 5 As 28/2007 – 89)
- pokyny, které státní zástupce udílí policejnímu orgánu v rámci přípravného řízení, náleží do skupiny vnitřních pokynů ve smyslu § 11 odst. 1 písm. a) zákona o svobodném přístupu k informacím. (rozsudek č.j. 1 As 105/2010 – 73)
- pravidla interní kontroly zaměstnanců,
- informace např. o telefonních číslech zaměstnanců povinného subjektu,
- o rozmístění v jednotlivých kancelářích,
- výpisy z elektronického systému spisové služby (rozsudek NSS č. j. 4 As 23/2012-20 a rozsudek MS Praha č. j. 11 Ca 337/2008-50)
- informace z dozorových spisů vedených státním zastupitelstvím (nejčastěji se jednalo o snahu získat pokyny policejnímu orgánu) (rozsudky č.j. 2 As 51/2012-24, 2 As 93/2011-79 (2462/2012 Sb.NSS), 1 As 105/2010-73 a Městský soud v Praze v rozsudcích č. j. 6 A 245/2010-41, č. j. 8 Ca 187/2009-58 a č. j. 9 A 84/2011-69),
- evakuační plán úřadu, 1 As 98/2008-148 (1944/2009 Sb.NSS)
- různé interní metodické pomůcky, zápisy ze školení ale i metodické návody s předepsanými postupy při výkonu veřejné správy – jedná-li se pouze o zjednodušeně řečeno učební pomůcky, pak mají povahu výlučně vnitřní informace a lze je podle komentovaného ustanovení chránit (NSS č. j. 8 As 108/2014-54 a 1 As 70/2013-58).
- organizační řád (byť jsou různé výklady), spisový řád, skartační řád, docházkový systém, popř. další předpisy týkající se organizace a chodu „uvnitř“ úřadu. (rozsudek č.j. 5 As 28/2007 – 89)

- pravidla parkování zaměstnanců,
- pravidla čerpání dovolené zaměstnanců nebo prostředků fondu kulturních a sociálních potřeb,
- pravidla evidence docházky nebo pravidla výdeje stravenek
- o používání kopírovacích strojů
- pravidla zvyšování kvalifikace zaměstnanců.
- pokyn o výdeji spotřebního materiálu (rozsudek č.j. 1 As 98/2008-148; 1944/2009 Sb. NSS).

Obecně některé rozsudky charakterizovaly informace, podřaditelné pod § 11 odst. 1 písm. a) takto:

- Pojem vnitřní pokyn je třeba vykládat šířeji, nelze ho omezit pouze na skupinu interních správních aktů (rozsudek č.j. 1 As 105/2010 – 73),
- musí být rozšířena i varieta úkonů náležejících do skupiny vnitřních pokynů, neboť je třeba pamatovat i na vnitřní pokyny povinných subjektů, jež nejsou správními orgány, týkající se jejich činnosti, kterou však není možné označit za výkon veřejné správy. (rozsudek č.j. 1 As 105/2010 – 73).

Z podaného soupisu judikaturně „již uznaných" typů informací, podřaditelných pod ochranu podle § 11 odst. 1 písm. a), je zřejmé, že jde o široce pojatý okruh informací.

Jediná nejistota, týkající se tohoto jednoznačného výkladu, spočívá v podmínce § 11 odst. 1 písm. a) vyjádřené textem „*vztahuje se výlučně k vnitřním pokynům*". Tento pojem se vykládá tak, že neexistuje „působení navenek" [4]. V tom se někdy ze strany odpovědných pracovníků spatřuje riziko, zda lze informace o různých bezpečnostních opatřeních pod uvedené ochranné ustanovení podřadit. Rozsudky uvádějí jako významný parametr, že nelze *„považovat za informace vyloučené z práva na jejich poskytnutí těm, jichž se postupy v nich upravené bezprostředně týkají."*[5]

Výklad je však i zde nutno provést podle smyslu, nikoli formalisticky jen podle jazykového znění. „Působením navenek" nemůže být takové působení, které je fakticky využitelné jen pro případné protiprávní jednání (nějaký druh překonání bezpečnostních opatření), protože takové jednání nepožívá právní ochrany. Například informace o zabezpečovacích kódech, o nastavení ochrany přístupu do sítě a podobně sice působí „navenek" právě svou zabezpečovací funkcí, ovšem tu nelze považovat za „působení navenek" v tom smyslu, jak jej dovodily soudy při definování vztahu k „výlučně vnitřnímu pokynu".

Argumentaci, prokazující možnost uplatnit § 11 odst. 1 písm. a) lze ještě rozvinout tak, že disposice normy neuvádí přímo informace, které „jsou" výlučně vnitřními pokyny, ale které

[4] rozsudek Nejvyššího správního soudu ze dne 17. 1. 2008, čj. 5 As 28/2007-89
[5] rozsudek Nejvyššího správního soudu ze dne 30. dubna 20084 As 20/2007 - 64

„se týkají“ výlučně vnitřních pokynů. Vazba je tedy volnější a pod takový pojem lze zahrnout například informace o tom, jak se určitý (bezpečnostní) pokyn v praxi provádí, čím se naplňuje.

Nejde tedy o samotný „vnitřní pokyn“, ale o informace, které se k němu vztahují. Vztah navenek je však jako definující charakteristika vztažen pouze k vnitřnímu pokynu. Pakliže tedy například určité bezpečnostní opatření má povahu vnitřního pokynu, který se sám o sobě nijak nedotýká osob vně povinného subjektu (například pokyn k zajištění objektové nebo kybernetické bezpečnosti), pak navazující informace, které se ho týkají „výlučně“, se již v nějaké míře mohou projevovat nebo nějak dotýkat osob vně povinného subjektu. Například půjde o informaci, jakými konkrétními bezpečnostními prvky, zařízeními, postupy apod. zajistit objektovou nebo kybernetickou bezpečnost, tedy například o údaje z kupní smlouvy nebo objednávky na určité zařízení. Pro posouzení, zda je možné takové informace odmítnout, tedy již nebude hrát roli, že samy tyto informace se v určité míře mohou týkat i osob mimo povinný subjekt (např. dodavatele, anebo i veřejnosti, jejímž právem je kontrolovat racionální nakládání s veřejnými prostředky), ale půjde jen o posouzení, zda tyto informace jsou opravdu případnému útočníkovi nedostupné a zda jejich získání skutečně může ohrozit legitimní zájem (viz pasáž o „fakultativní“ povaze § 11 odst. 1 v podkapitole **b) Příliš široké dopady návrhů a jejich paradoxní působení proti vytčenému cíli**, kdy je třeba doložit nejen verbální shodu s formulací tohoto ustanovení, ale také legitimní zájem, jenž by byl poskytnutím informace ohrožený). V uvedeném případě by legitimním zájmem byla ochrana bezpečnosti objektu (případně kybernetického prostoru) a ve světle dosavadní judikatury by soud měl vždy tento důvod ochrany akceptovat.

Pokud je mi známo, nebyly předloženy žádné příklady, kdy odepření informace, která by ohrozila některé bezpečnostní opatření či jiný bezpečnostní legitimní zájem, bylo soudem odmítnuto a reálně tak hrozilo, že bude muset být poskytnuta. Nelze tedy než učinit závěr, že **návrhy jsou spíše nadbytečné**, anebo přinejmenším lze tvrdit, že by měla postačovat minimální změna dosavadního § 11 odst. 1 písm. a) tak, aby dopad na zamýšlené typy informací byl formulovaný bezpečněji.

3. Možnosti řešení

Z výše uvedeného rozboru plyne, že řešením by mělo být:

a) zařazení případné úzce specifické normy do zvláštního předpisu, nikoli do obecného zákona o přístupu k informacím, a/nebo
b) taková formulace, aby **obecněji zahrnovala případy, které se obdobně identifkují v dalších oblastech,** a zároveň
c) zařazení normy do správného místa struktury § 11 InfZ, tj. do odst. 1, a zároveň
d) taková formulace, aby v hypotéze vyjadřovala jako podmínku i reálné riziko ohrožení chráněných statků (bezpečnosti, veřejného pořádku).

Pokud by se tedy požadované zvýšení ochrany některých rizikových informací mělo provést v obecném zákonu (zákon č. 106/99 Sb. o svobodném přístupu k informacím), pak by přicházely v úvahu například tyto varianty (liší se jen tím, zda se úprava uvede jako samostatné další písmeno v § 11 odst. 1 anebo se jen připojí k dosavadnímu § 11 odst. 1 písm. a)**:**

Varianta I:

Změna zákona o svobodném přístupu k informacím

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 101/2000 Sb., zákona č. 159/2000 Sb., zákona č. 39/2001 Sb., zákona č. 413/2005 Sb., zákona č. 61/2006 Sb., zákona č. 110/2007 Sb., zákona č. 32/2008 Sb., zákona č. 254/2008 Sb., zákona č. 274/2008 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 123/2010 Sb., zákona č. 227/2009 Sb., zákona č. 375/2011 Sb., zákona č. 167/2012 Sb., zákona č. 181/2014 Sb. a zákona č. 222/2015 Sb., se mění takto:

1. V § 11 odst. 1 se na konci písmene b) slovo „nebo“ zrušuje.
2. V § 11 odst. 1 se na konci písmene c) tečka nahrazuje slovem „, nebo“ a doplňuje se písmeno d), které včetně poznámky pod čarou zní:

„d) její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření, stanoveného na základě zvláštního předpisu[1] pro účel nezbytné ochrany osob, majetku, jakož i veřejného pořádku nebo bezpečnosti České republiky.“.

---

[1] Např. § 4 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ve znění pozdějších předpisů; § 22 až 26 zákona č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů; § 3 zákona č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením, ve znění pozdějších předpisů; § 5 odst. 1 písm. a) zákona č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů; § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Varianta II:

Změna zákona o svobodném přístupu k informacím

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 101/2000 Sb., zákona č. 159/2000 Sb., zákona č. 39/2001 Sb., zákona č. 413/2005 Sb., zákona č. 61/2006 Sb., zákona č. 110/2007 Sb., zákona č. 32/2008 Sb., zákona č. 254/2008 Sb., zákona č. 274/2008 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 123/2010 Sb., zákona č. 227/2009 Sb., zákona č. 375/2011 Sb., zákona č. 167/2012 Sb., zákona č. 181/2014 Sb. a zákona č. 222/2015 Sb., se mění takto:

V § 11 se v odst. 1 písmeno a) na konci doplňuje text včetně poznámky pod čarou:

„anebo její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření, stanoveného na základě zvláštního předpisu[1] pro účel nezbytné ochrany osob, majetku, jakož i veřejného pořádku nebo bezpečnosti České republiky,“.

---

[1] Např. § 4 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ve znění pozdějších předpisů; § 22 až 26 zákona č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů; § 3 zákona č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením, ve znění pozdějších předpisů; § 5 odst. 1 písm. a) zákona č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů; § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Tato varianta vychází z toho, že výklad dosavadního § 11 odst. 1 písm. a) v judikatuře správních soudů prakticky umožňuje chránit zamýšlené typy informací, a pouze jej konkretizuje tak, aby o tomto výkladu nebylo sebemenší pochybnosti.

Úplné znění:

§ 11

Další omezení práva na informace

(1) Povinný subjekt může omezit poskytnutí informace, pokud:

a) se vztahuje výlučně k vnitřním pokynům a personálním předpisům povinného subjektu anebo její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření, stanoveného na základě zvláštního předpisu[1] pro účel nezbytné ochrany osob, majetku, jakož i veřejného pořádku nebo bezpečnosti České republiky,

---

[1] Např. § 4 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ve znění pozdějších předpisů; § 22 až 26 zákona č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů; § 3 zákona č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením, ve znění pozdějších předpisů; § 5 odst. 1 písm. a) zákona č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů; § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

4. Výklad navrženého ustanovení – limity využití navržené ochrany informací

V důvodové zprávě k navržené změně, která se později může stát jedním z pramenů výkladu, je nutno přinejmenším vyjasnit, jaké typy informací se touto změnou mají chránit. To nejlépe plyne z parametrů testu proporcionality, který lze nad jeho formulací provést.

Test proporcionality

Především je nutno uvést, že jak při obligatorním, tak i fakultativním vyjádření normy je vždy nutno zvážit v testu proporcionality **potřebnost omezení** přístupu k informaci (srov. rozsudky NSS č. j. 8 As 108/2014-54, č. j. 1 As 70/2013-58, č. j. 1 As 105/2010-73, č. j. 1 As 44/2008-116, rozsudek MS v Praze č. j. 8 A 167/2010-92). Jinými slovy, Nejvyšší správní soud prakticky nepřipouští jakýkoliv „absolutní“ důvod pro odepření přístupu k informacím.

Splnění formálních znaků, odpovídajících jazykové formulaci normy, nemůže být samo o sobě dostatečným důvodem pro odepření informace. Posouzení bude vždy „dvoufázové“: nejdříve je nutné informaci (dokument) vyhodnotit jako informaci, jazykově podřaditelnou pod navržené ustanovení, a splňuje-li příslušné znaky, je nutné dále odůvodnit nezbytnost omezení práva na informace. Pokud poskytnutí takové formálně odpovídající informace reálně nevyvolá riziko ohrožení některého chráněného statku (bezpečnosti, veřejného pořádku, majetku atd.), pak nebude možno toto ustanovení uplatnit a informaci odepřít. Vždy bude nutno zaměřit se na obsahový znak poskytované informace v dané situaci, tedy to, zda její poskytnutí opravdu nějaký chráněný zájem (např. bezpečnost opatření) ohrozí.

Test proporcionality, jak je judikaturou Ústavního soudu tradičně aplikován při kolizi dvou základních práv (případně základního práva a veřejného statku), se skládá ze tří kroků. V prvním kroku je zvažováno 1) kritérium **vhodnosti** (zkoumá se, zda institut omezující určité základní právo umožňuje dosáhnout stanovený cíl), ve druhém kroku 2) kritérium **potřebnosti** (zkoumá se, zda by stanoveného cíle nemohlo být dosaženo jinými opatřeními nedotýkajícími se základních práv a svobod), konečně ve třetím kroku 3) kritérium **závažnosti** (někdy též kritérium proporcionality v užším smyslu nebo přiměřenosti, porovnává se závažnost obou v kolizi stojících základních práv, což spočívá ve zvažování empirických, systémových, kontextových i hodnotových argumentů).

Kritérium vhodnosti

Toto kritérium bude v některých případech splněno – odepřením informace by bylo cíle dosaženo – žadatel by se s informací nemohl seznámit.

Bude však nepochybně existovat velký okruh informací tak či onak vypovídající o bezpečnostním riziku, **u kterých se odepřením informací sledovaného cíle nedosáhne**, a to prostě proto, že potenciální útočník si při běžně předpokládatelné kvalifikaci tyto informace obstará bez velkého úsilí jinak – například v oblasti kybernetické bezpečnosti přímým testováním systému po síti. Není tedy přípustné odepírat například informaci o typu použitého softwaru, pokud typický potenciální útočník tuto informaci snadno zjistí dálkovým přístupem a testováním. V takovém případě převáží právo na přístup k informaci, například proto, aby žadatel mohl posoudit, zda se finanční prostředky na určitý software využily efektivně.

Podobně bude třeba hodnotit situace, kdy určitá informace není pro potenciální útok proti bezpečnostnímu zájmu v daném případě významná a potenciální útočník může postupovat i bez její znalosti.

Kritérium potřebnosti

V případě navržené normy však bude třeba především posuzovat kritérium **vhodnosti,** zda ochrany informace nelze dosáhnout například **pouze organizačním opatřením**. K tomu může docházet především tehdy, kdy hrozí „vytěžení“ chráněné informace z porovnávaní (zejména strojového) sestav informací, které se jinak jeví jako bezproblémově poskytnutelné. Často totiž pouze v rámci dosavadní praxe povinnému subjektu uniklo, že rastrováním a postupným separováním volně dostupných informací lze vytěžit také informaci, kterou je nutno z bezpečnostních důvodů chránit (může k tomu docházet z různých hledisek například při utajení identity osob, vozidel, účelu budov, některých zařízení, taktických postupů apod.). Nelze však připustit, že nesprávnou organizací takových opatření by bylo možné bezbřeze expandovat rozsah nepřístupných informací. Na druhé straně je nutno respektovat reálný sta a pokud již určité informace (byť nevhodně) jsou veřejně dostupné, vycházet z toho jako z dané skutečnosti.

Test proporcionality pak má vést k tomu, že se pro ochranu informace přednostně uplatní organizační opatření tak, aby se taková cílená separace informací rastrováním neumožňovala.

Kritérium závažnosti:

Pokud by byla předchozí kritéria při odepření určité informace splněna, bude nutno posoudit, zda přínos jejího odepření ke zvýšení bezpečnosti je vyšší, než veřejný zájem na znalosti informace. Jde tu tedy o takový obsahový znak informace, který vypovídá o míře jejího významu. Neposuzuje se tedy význam samotné „bezpečnosti“ (ten je jistě vždy vysoký), ale toliko přínos konkrétní informace k jejímu zajištění.

Účinnost každého bezpečnostního opatření je kolísavý parametr, závislý na mnoha vnějších i vnitřních okolnostech. Teoreticky si lze představit, že **jakákoliv informace** (i banální) z prostředí povinného subjektu, který uplatňuje některé bezpečnostní opatření, může tak či onak napomoci potenciálnímu útočníkovi a **snížit účinnost opatření.** Na tom je v zásadě založena každá špionáž či sofistikovaná příprava trestného činu, která sbírá libovolné „střípky“ a snaží se sestavit pro své účely použitelný obraz. (Například z oblasti personálních informací by znalost, kterou vysokou školu absolvoval programátor, může za výjimečných okolností pomoci prolomit heslo, které používá.) Těmto přirozeným a trvale přítomným rizikům však nelze čelit blokací veškerých informací. **Tím by se zlikvidovala demokratická povaha právního státu.** Je tedy třeba definovat a používat pro ochranu informací až určité **vyšší, kvalifikované stupně hrozícího ohrožení účinnosti bezpečnostních opatření**.

Povinné subjekty musejí být motivovány zajišťovat účinnost bezpečnostních opatření primárně jejich organizačními a taktickými parametry, nikoliv utajováním širokého okruhu informací, které se jich mohou i vzdáleně týkat.

Ohrožení poskytnutím informace se tedy musí charakterizovat až od určitého stupně závažnosti, například jako významné nebo přímé.

Významné ohrožení účinnosti by mělo být takové, které by samo o sobě vedlo k nemožnosti zajistit chráněný účel. Například při ostraze budov by znamenalo úplnou nejistotu o tom, zda se do budovy dostane či dostala neoprávněná osoba, tedy například výpadek části senzorů, monitoringu apod., způsobený tím, že by se útočník dozvěděl údaje, které to umožní.

Přímé ohrožení účinnosti by mělo být takové, které k ohrožení účinnosti bezpečnostního opatření vede přímo, tzn. nevyžaduje řady dalších informací a zjištění, náročné analýzy, filtrace a separace údajů apod.

V kritériu závažnosti by tedy měly získat ochranu jen ty informace, u kterých lze prokázat kombinaci uvedených rysů – poskytnutí by významně a přímo ohrozilo účinnost bezpečnostního opatření, například v případě kybernetické bezpečnosti kybernetickou bezpečnost a bezpečnost sítí a informačních systémů.

Zároveň si lze představit, že veřejný zájem na informaci může za určitých okolností převýšit i takto kvalifikované důvody ochrany, například v případě závažného podezření na korupci při zakázce na určitý segment hardwaru, softwaru nebo služeb, potřebných k zajištění určitého bezpečnostního opatření. Toto hledisko však není třeba zvažovat jako systematicky přítomný prvek, jde o naprostou výjimku.

Účel nezbytné ochrany

Jelikož se navrhuje zavést do zákona výjimku z přístupu k informacím s širokým a obecným dopadem na všechny povinné subjekty (oproti ochraně utajovaných informací, která je zaměřena na poměrně úzký okruh původců utajovaných informací - viz Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací), je nutné jeho šíři jasně vymezit. Z hlediska závažnosti chráněného zájmu je nutno ještě zvážit jeden aspekt ochrany bezpečnostních zájmů: zda jde **o nezbytné opatření**. Nebylo by totiž přiměřené, pokud by se umožnilo rozsáhlé a neobvyklé utajování informací jen proto, že si některý povinný subjekt vytvořil natolik mimořádné, komplikované či sofistikované řešení ochrany, které již není nezbytné, ale jehož funkce je na mimořádném rozsahu utajování závislá. Vždy totiž existuje určitá úměrnost mezi účinností bezpečnostního opatření a tím, do jaké míry jsou o něm dostupné informace – čím méně dostupných informací, tím vyšší účinnost. Tak lze teoreticky eskalovat potřebu utajování do nekonečna. Takové opatření nemůže požívat ústavní ochranu a nemůže být oprávněným důvodem pro rozsáhlé utajování a omezení přístupu k informacím. Chránit lze toliko **nezbytná** opatření, což mj. plyne z ústavní kautely v čl. 17 odst. 4 Listiny, kde se přístup k informacím umožňuje omezit jen potud, pokud *„jde o opatření v demokratické společnosti nezbytná“*.

Zde však nutno upřesnit, že případná významná bezpečnostní patření a informace s nimi související, přesahující „účel nezbytné ochrany“ je samozřejmě možné chránit jako utajované informace podle § 7 InfZ a návazně podle zákona o ochraně utajovaných informací, jehož logika spočívá v taxativním vyjmenování stanovených okruhů zvlášť významných informací (formální znak utajované informace).

5. Možnost legislativní úpravy označování bezpečnostně rizikových informací pro využití formou otevřených dat

V souvislosti s fenoménem otevřených dat a poskytování datasetů informací na základě tzv. opakovaného použití informací veřejného sektoru (REUSE, na základě Směrnice Evropského parlamentu a Rady 2003/98/ES o opakovaném použití informací veřejného sektoru ve znění Směrnice 2013/37/EU) se objevuje jako nově vznikající otázka to, zda je potřebné označovat některé druhy informací zvláštním příznakem, který by měl vést **ke zvýšené pozornosti** při případném aktivním zveřejnění anebo pasivním poskytnutí na žádost.

Konkrétní příklady potenciálně rizikových situací jsou uvedeny v kapitole **0**

Problémy návrhů – typy ohrožených informací a odůvodnění požadovaných změn, v bodu **a) Absence konkrétního popisu a racionálního odůvodnění návrhu**.

Uvedený příznak by měl pracovníkům ve veřejné správě, kteří mohou řešit situaci zveřejnění anebo poskytnutí na žádost takových informací, vyvolat zvýšenou pozornost, protože z běžného nakládání s takovou informací jim nemusí být bez specifických znalostí kontextu zřejmé, že jde o potenciálně rizikovou informaci.

Takový přístup by nejvíce odpovídal k postupu při ochraně utajovaných informací v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, kde se stanoví povinnosti „původce informace“. Podle jeho § 21 odst. 1 *„Na informaci, která naplňuje znaky § 4 a je uvedena v seznamu utajovaných informací, je původce povinen vyznačit svůj název, stupeň jejího utajení, její evidenční označení a datum jejího vzniku, není-li dále stanoveno jinak.“*

Podobně se v archivním zákonu v rámci HLAVY III, SPISOVÁ SLUŽBA, v § 64a upravuje označování vzniklých dokumentů, a specificky se upravuje nakládání s dokumenty poskytnutými Organizací Severoatlantické smlouvy nebo Evropskou unií a označenými „NATO UNCLASSIFIED“ nebo „LIMITE“. Ukládá se též specifický druh ochrany těchto informací, spočívající pouze v uložení povinnosti s dokumentem nakládat tak, *„aby se s ním neseznámila neoprávněná osoba“*. Samotnou ochranu informace zároveň upravuje InfZ v § 11 odst. 1 písm. c), kdy při případném odmítnutí žádosti o takovou informaci nutno vzít v potaz i materiální povahu informace, tedy zda z jejího poskytnutí skutečně plyne ohrožení nějakého chráněného zájmu. Tím se konkretizuje, co chápat pod pojmem „neoprávněná osoba“ uvedená v § 64a archivního zákona.

Naopak v rámci obecného přístupu k informacím podle Infozákona se žádná srovnatelná povinnost původce informace vyznačovat na ní nějakou její specifickou vlastnost nestanoví.

Z těchto typů postupů se jeví jako případně vhodné k úvaze takový, kdy by se v archivním zákonu v rámci HLAVY III, SPISOVÁ SLUŽBA v kombinaci s doplněním zákona č. 106/1999 Sb. o svobodném přístupu k informacím upravil specifický postup, spočívajíc v následujících tezích:

Původce informace posoudí, zda existuje potenciální riziko, kdy by informace v určitém kontextu, zejména v kombinaci s dalšími informacemi, zejména volně dostupnými databázemi (např. otevřenými daty), významně anebo přímo mohla ohrozit účinnost bezpečnostního opatření, stanoveného na základě zvláštního předpisu pro účel nezbytné nezbytné ochrany osob, majetku, jakož i veřejného pořádku nebo bezpečnosti České republiky. Tento materiální znak by tedy byl formulovaný stejně, jako případný zvláštní důvod odmítnutí žádosti, uvedený výše v kapitole **0**

1. **Možnosti řešení**.
2. Pokud takové riziko vyhodnotí, vyznačí to na informaci (obdobně jako se vyznačuje stupeň utajení podle § 21 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací).
3. V zákoně č. 106/1999 Sb. o svobodném přístupu k informacím by se zakotvila zvláštní povinnost povinného subjektu, který hodlá takovou informaci poskytnout, posoudit riziko, které tak případně vzniká. Měl by též zvážit, zda je třeba situaci konzultovat s původcem informace.

Částečně srovnatelný postup se používá při vyhodnocení vhodnosti zveřejnění informací povinně zveřejňovaných jako otevřená data (datasetů otevřených dat) podle Nařízení vlády vydaného na základě § 21 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 298/2016 Sb., v rámci hodnocení dopadů regulace (RIA).

V případě zveřejnění prvních datasetů se vyhodnocovala tato rizika:

R1. Zveřejnění dat v rozporu se zákonem;
R2. Porušení ochrany obchodního tajemství;
R3. Porušení ochrany osobních údajů;
R4. Zveřejnění nevhodných dat či informací;
R5. Dezinterpretace dat;
R6. Absence konzumentů dat;
R7. Překrývání dat;
R8. Ohrožení bezpečnosti státu /majetku /osob.

Pro účel této analýzy, zaměřené toliko na otázky rizik z hlediska bezpečnosti, by připadalo v úvahu riziko R8.

a) Obtíže návrhu

Taková právní úprava má však zásadní nevýhodu. Sama o sobě by totiž nepředstavovala specifický důvod odepření informace, pouze by ukládala **„zvláštní opatrnost“ při posouzení,** zda poskytovanou informaci anebo její část nepodřadit pod některý hmotně-právní důvod ochrany informací. V dané souvislosti by pravděpodobně jediným takovým důvodem byl § 11 odst. 1 písm. a) *(informace se se vztahuje výlučně k vnitřním pokynům)*. Ve výsledku by tedy navržené ustanovení bylo pouze zvláštním upozorněním, aby se u určité informace důkladněji prověřily souvislosti. Takové právní ustanovení se však jeví jako zcela nadbytečné a potenciálně rizikové, protože by tak vznikly dvě kategorie chráněných informací – jedna se zvýšenou povinností povinného subjektu zvážit souvislosti její ochrany, a druhá (např. včetně utajovaných informací či osobních údajů), kde by paradoxně taková povinnost nebyla zdůrazněna. Odpovědnost za případné selhání při správném určení, zda informaci poskytnout či nikoliv, by byla nejasná.

Dalším negativem by bylo předpokládatelné nadužívání a s ním spojená administrativní náročnost, protože preventivně by u každé informace, u níž by nebylo možné vyloučit jakékoliv riziko (což skoro nikdy nelze), původci vyznačovali uvedené upozornění, aby se tak zbavili případné zodpovědnosti.

Proto výše popsané případné ustanovení, označující zvýšené riziko při poskytnutí informace, **nelze doporučit**.

Oldřich Kužílek

poradce pro otevřenost veřejné správy

Praha, prosinec 2016