Ochrana informačných zdrojov spravodajských služieb

Asociácia bývalých spravodajských dôstojníkov spolu s Fakultou práva Paneurópskej vysokej školy v Bratislave usporiadali 3. 12. 2014 už 8. medzinárodné sympózium na tému „Ochrana informačných zdrojov spravodajských služieb". Uverejňujeme referáty, ktoré budú koncom februára 2014 vydané v printovej verzii zborníka.

Obsah

Predslov

Na úvod zborníka príspevkov z ôsmeho medzinárodného sympózia o ochrane informačných zdrojov spravodajských služieb sa žiada stručný exkurz do minulosti týchto podujatí, ktorých začiatok sa datuje 4. decembrom 2007. Vtedy sme sa zišli na akademickej pôde Fakulty práva Paneurópskej vysokej školy po prvýkrát: bývalí šéfovia spravodajských služieb, bezpečnostní experti, politici, politológovia, právnici, publicisti i študenti. Možno nie všetci účastníci tohto medzinárodného podujatia boli presvedčení o tom, že sa nám podarí vytvoriť pravidelné diskusné fórum o problémoch spravodajskej komunity, ktoré sa zíde každý rok a nastolí témy, inšpirujúce k premýšľaniu nielen odborníkov, ale tiež širší okruh zainteresovanej verejnosti. Začínali sme v období, keď sa oficiálne štruktúry pozerali na našu aktivitu s nedôverou a podozrením. Napriek tomu sme pokračovali v úsilí, aby sme prostredníctvom našich medzinárodných sympózií inšpirovali kritické premýšľanie o defektoch, ktoré brzdia objektívnu reflexiu spravodajskej komunity na Slovensku.

Možno niektorým sa to zdá nenáležité, ale napriek tomu treba uviesť sympózium do širších spoločenských súvislostí. Pred nedávnom sme si pripomínali 25. výročie pádu komunistického režimu v Česko-Slovensku. Nebyť tejto historickej udalosti by sme si nemohli teraz dovoliť takto verejne – ba dokonca niekedy kriticky – diskutovať o spravodajských službách, ich defektoch a problémoch. Verejne diskutovať o spravodajských štruktúrach komunistickej Štátnej bezpečnosti bolo tabu; azda iba v rámci propagandy objavila sa napríklad v médiách zmienka o ŠtB. Prepáčte mi, toto odbočenie, ale považoval som za potrebné mladšej generácii pripomenúť, že pred 17. novembrom 1989 bola problematika spravodajských služieb jedným z najstráženejších štátnych tajomstiev.

Je nepopierateľné, že utajovanie funguje aj v demokratickej spoločnosti. Osobitný význam má štátne utajovanie v spravodajských službách, ktoré majú nezastupiteľné postavenie v systéme ochrany národnej bezpečnosti. V tomto kontexte je mimoriadne dôležitá ochrana informačných zdrojov spravodajských služieb, a preto sme sa rozhodli venovať tejto téme tohtoročné sympózium. Uvedenú tému možno reflektovať z viacerých hľadísk. Samozrejme, že pre spravodajských expertov je primárny záujem, aby informačné zdroje služieb zostali najtajnejším z tajomstiev spravodajských služieb. Legitimita ochrany informačných zdrojov spravodajských služieb je základom regulačného rámca ochrany štátnych tajomstiev.

Hoci avizovaná téma 8. medzinárodného sympózia „Ochrana informačných zdrojov spravodajských služieb“ má do značnej miery predovšetkým profesionálny charakter, dotýka sa tiež morálnych i politických štandardov modernej demokratickej spoločnosti. Úvahy o tom, ako spravodajské služby zaštíťujú svoje informačné zdroje pred odhalením, nastoľujú totiž aj otázku, či takýto postup služieb výlučne slúži na ochranu nástrojov národnej bezpečnosti alebo tiež aj na zakrytie zneužívania štátnej moci. Úniky z poznatkových fondov spravodajských služieb už verejnosť nepovažuje za sabotáž spravodajských programov, ale za morálne oprávnený nástroj proti zneužívaniu štátnej moci. Napriek tomu kategorickým imperatívom spravodajských služieb je zdokonaľovať systém ochrany informačných zdrojov tak, aby nedošlo k ich prezradeniu.

Diskusia účastníkov sympózia k jednotlivým príspevkom potvrdila zámer a očakávania organizátorov podujatia priblížiť sa viac k praktickým otázkam, ktoré sa týkajú efektívnejšieho fungovania spravodajských služieb v súčasných podmienkach. Prezentovali sa nielen názory odborníkov na špecifickú spravodajskú problematiku, ale tiež právne limity ochrany spravodajských zdrojov i využitie spravodajských informácií v trestnom konaní. Ako osobitne významný možno vyzdvihnúť jeden zo záverov sympózia, že legitimita ochrany informačných zdrojov spravodajských služieb je základom regulačného rámca ochrany štátnych tajomstiev.

PhDr. Igor Cibula,
predseda Asociácie bývalých spravodajských dôstojníkov

Príhovor

Vážený pán dekan, vážené dámy, vážení páni !

Už po tretí krát som dostal príležitosť prehovoriť na tomto významnom fóre, ktoré sa schádza pravidelne už osem rokov a poskytuje priestor výmene aktuálnych názorov na problémy, ktorými žije medzinárodná spravodajská komunita. Ďakujem Asociácii bývalých spravodajských dôstojníkov a Fakulte práva Paneurópskej vysokej školy za to, že organizujú tieto podujatia a - obrazne povedané – širšej verejnosti otvárajú dvere do komnaty tajných služieb. Oceňujem Vaše úsilie prekonať izoláciu spravodajskej komunity od demokratickej spoločnosti a vytvárať tak podmienky pre permanentnú diskusiu k témam, donedávna považovaným za tabu. Dovoľujem si zdôrazniť, že vďaka Paneurópskej vysokej škole a hlavne bývalým spravodajským dôstojníkom sa podarilo zakotviť užitočnú tradíciu, ktorá slúži národnej bezpečnosti Slovenskej republiky.

Na tohtoročnom v poradí už 8. medzinárodnom sympóziu sa bude hovoriť o ochrane informačných zdrojov spravodajských služieb, čo možno v súčasnosti považovať za mimoriadne aktuálnu tému. Jej význam zvýrazňuje prípad bývalého špecialistu CIA Edwarda Snowdena, ktorý v júni minulého roku rozpútal mediálny rozruch svojimi odhaleniami z americkej „spravodajskej kuchyne“. Začala sa nekončiaca verejná debata o štátnom tajomstve a únikoch, ktorá ďalej pokračuje po sérií nasledujúcich odhalení. Podľa mienky časti verejnosti v samotnej podstate prezradených tajomstiev alebo ich únikov nie je nič škandalózne. Ale ako prípad Snowdena ukazuje, týkajú sa vážnych otázok národnej bezpečnosti a môžu ohroziť dôležité záujmy štátu. Predsa žiadna vláda nemôže spoľahlivo plniť svoje funkcie, ak unikajú tajomstvá spravodajských služieb, ktoré mali navždy zostať „zamknuté na sedem zámkov“.

Základnou úlohou vášho tohtoročného sympózia by mala byť odpoveď na otázku, ako možno realizovať plnohodnotnú spravodajskú činnosť tak, aby nedošlo k odkrývaniu informačných zdrojov, ktoré sú považované za najcennejší klenot každej spravodajskej služby. V aktuálnej atmosfére rozličných odhalení, ktoré nám v poslednej dobe servírovali médiá, je potrebné koncentrovať sa na to, aby problémy úniku informácií z prostredia spravodajských služieb nepôsobili odradzujúco a demotivačne na osoby, ochotné spolupracovať so spravodajskými službami. Nejde iba o operatívnu ochranu identity a bezpečnosti ľudských zdrojov informácií, ale aj o zodpovedné zaobchádzanie so spravodajskými výstupmi na strane adresátov. Zaiste sotva niekto pochybuje o tom, že je naliehavo potrebné zdokonaľovať regulačný rámec ochrany informačných zdrojov, aby spoľahlivo fungovala ochrana bezpečnosti štátu.

Program 8. medzinárodného sympózia potvrdzuje programové predsavzatie ABSD orientovať pozornosť verejnosti – politikov nevynímajúc – v aktuálnej problematike, ktorej sa venuje v súčasnosti spravodajská komunita. Účasť bezpečnostných a spravodajských expertov z Českej republiky na tomto podujatí je užitočným príspevkom do diskusie; zaiste obohatí výmenu názorov, ktoré budú na sympóziu prezentovať ich slovenskí kolegovia. Žiada sa tiež vyzdvihnúť prítomnosť odborníkov z akademického prostredia, pretože svojimi referátmi umocnia komplexnosť prezentácie témy ochrany spravodajských zdrojov.

Vážené dámy, vážení páni !

Dovoľte mi - prosím - aby som osobitne pri tejto príležitosti spomenul aj to, aký priestor venuje Fakulta práva Paneurópskej vysokej školy odbornému a vedeckému skúmaniu fenoménu spravodajských služieb. Popri týchto sympóziách škola umožňuje už osem rokov poslucháčom magisterského študijného programu absolvovať výberový predmet spravodajské služby. Pamätám si, že minuloročné sympózium moderovala po prvýkrát absolventka fakulty Mgr. Alexandra Macúchová; je chvályhodné, že absolventi fakulty sa aj takto aktívne zapájajú do organizácie týchto medzinárodných podujatí. A treba ešte dodať, že fakulta participovala aj na pripomienkovom konaní k návrhu pripravovaného zákona o spravodajských službách, ktorý by mal nahradiť existujúcu právnu úpravu činnosti SIS a Vojenského spravodajstva.

Na záver by som chcel opakovane vyzdvihnúť, že na základe iniciatívy a určite obetavého úsilia Asociácie bývalých spravodajských dôstojníkov sa zrodila veľmi prospešná tradícia. Fakulta práva Paneurópskej vysokej školy ochotne poskytla akademickú pôdu pre organizovanie medzinárodných sympózií a aj organizačne pomohla tomu, aby tieto podujatia boli úspešné. Kvôli úplnosti pozitívnej bilancie osemročnej histórie sympózií je potrebné spomenúť tiež fakt, že nezanedbateľnou mierou sa na kvalite obsahu sympózií podieľali aj bezpečnostní a spravodajskí experti z Českej republiky. Bez zveličenia možno konštatovať, že na sympóziách sa doteraz vystriedali temer kompletné spravodajské elity pôvodného Česko-Slovenska.

V takomto kontexte si dovolím vyjadriť želanie, aby toto fórum naďalej prispievalo k zdokonaľovaniu a rozvíjaniu efektívne fungujúceho a zákonného spravodajského systému Slovenskej republiky – ako som to deklaroval už pred

rokom. Zaslúžite si uznanie, že ste sa dokázali vymaniť z profesionálnej ulity a poskytujete priestor na kompetentnú diskusiu o témach, ktorými nežije iba spravodajská komunita.

Úprimne vám želám plodnú výmenu názorov!

Ing. Pavol Abrhan,
predseda Osobitného kontrolného výboru
Národnej rady Slovenskej republiky
na kontrolu činnosti Slovenskej informačnej služby

L. Pokorný: Právní režim ochrany zpravodajských zdrojů

Doc. JUDr. Ladislav Pokorný, Ph.D. *(1957) - Absolvoval studia práva na Právnické fakultě Univerzity J. E. Purkyně v Brně. Dlouhodobě se věnuje problematice trestního práva ve srovnávací perspektivě, problematice práva v oblasti bezpečnosti a právním aspektům činnosti zpravodajských služeb. Ve zpravodajské komunitě pracuje od roku 1991. Intenzivně se věnuje pedagogické činnosti, vyučuje na Právnické fakultě a na Fakultě sociálních studií Masarykovy Univerzity v Brně a na Policejní akademii České republiky v Praze. Je autorem řady odborných publikací, mj. monografie „Zpravodajské služby" (Auditorium, Praha 2012).*

Úvodem

Zpravodajské služby jsou státní orgány, které jsou zřízeny za účelem získávání, shromažďování a vyhodnocování informací z bezpečnostní oblasti vymezené působností stanovenou příslušnou legislativou a jejich poskytování oprávněným adresátům – příslušným ústavním činitelům (politickým představitelům), případně dalším státním orgánům, které jim mají napomáhat k co možná nejlepšímu rozhodování. Jsou tedy státními orgány, které jednak naplňují standardní charakter státního orgánu (jsou zřízeny a financovány státem, mají vymezenu působnost a pravomoc atp.), jednak jsou však státními orgány sui generis – jsou specifické svým předmětem činnosti, kterým jsou informace, nikoli rozhodovací činnost, specifické svým oborem působnosti /národní bezpečnost/, a specifické jim svěřenými oprávněními /specifické prostředky získávání informací/.

Obecně tedy i na zpravodajské služby dopadají všeobecné principy vztahující se na postavení a činnost státních orgánů, mezi nimiž též principy transparentnosti a otevřenosti. V jejich činnosti se ovšem uplatňuje paradox spočívající v obraně otevřené společnosti utajovanými prostředky. Zpravodajské služby jsou totiž z povahy své činnosti založeny na principu utajenosti, který může zakrýt jejich činnost před veřejností – působí v utajení a charakter jejich činnosti (úkolů) vyžaduje

vykonávat jejich povinnosti utajeně, což je v rozporu s principy otevřené společnosti.[1] Požadavek transparentnosti tedy musí být s ohledem na jejich charakter přiměřeně modifikován.

Princip utajenosti v činnosti zpravodajských služeb

Zpravodajství je možno obecně definovat jako „..záměrnou lidskou činnost, která spočívá v *utajovaném* získávání a zpracování *utajených* (tj. nejen formálně utajených, ale všech informací záměrně nezveřejňovaných nebo dokonce popíraných) či latentních informací protihráče – chceme-li - protivníka a dále v jejich následném využití oprávněným příjemcem.“[2]

Zpravodajské služby jsou „tajné“[3] právě proto, že základním principem jejich činnosti je utajování konkrétních úkolů, osob, které je plní, a způsobů a prostředků, jimiž splnění svých úkolů dosahují. Zpravodajské služby musí zásadu utajení těchto záležitostí dodržet. Zabývají se totiž oblastmi, v nichž otevřená a neutajená činnost nemůže přinést kýžený výsledek. V oboru své působnosti musí být schopny garantovat ochranu identity zdrojů, jakož i ochranu důvěrně poskytnutých informací. Je to nezbytné nejen kvůli samotným službám a jejich personálu, ale také kvůli lidem „z vnějšího světa“, kteří s nimi spolupracují. Utajení je nezbytné, jelikož je to jediná cesta, jak ujistit lidské zdroje (a to i potenciální) o jejich vlastní bezpečnosti. Nikdo se dobrovolně nepřihlásí ke spolupráci zpravodajské službě, která nedokáže předejít zveřejnění svých zdrojů.[4]

Otázkou důvodů zachovávání utajení ve zpravodajských službách se zabývá např. Laurie Nathan.[5] Především označuje utajení jako podstatný a nezbytný rys zpravodajských služeb, vyplývající z podstaty jejich mandátu a funkcí. Zpravodajské služby se zabývají konvenčními i nekonvenčními hrozbami pro národní bezpečnost, a utajení jim přináší kompetitivní výhodu při dosahování cílů týkajících se ochrany národní bezpečnosti. Extrémní transparentnost by jim způsobila značnou a nebezpečnou nevýhodu. Konkrétně je utajení nezbytné z těchto důvodů:

- zabránit tomu, aby si cíle zpravodajských operací byly vědomy toho, že jsou předmětem zájmu zpravodajských služeb,
- předejít tomu, aby si protivníci mohli osvojit informace o metodách používaných zpravodajskými službami,
- ochránit životy zpravodajských důstojníků a zdrojů jejich informací,
- ochránit bezpečnost VIP, které jsou pod ochranou zpravodajských služeb,
- ochránit důvěrnost (utajení) informací získaných zahraničními zpravodajskými službami,

---

[1] Born, H., Leigh, I. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies.* Oslo: Publishing House of the Parliament of Norway, 2005, s. 16.

[2] Viz Zeman, P. *České zpravodajské služby po roce 1989*. In Balabán, M., Stejskal, L. a kol. *Kapitoly o bezpečnosti.* Karolinum, Praha 2010, s. 234.

[3] Je třeba nicméně poznamenat, že označování a chápání zpravodajských služeb jako „tajných“ je vyjádřením zvláštního přístupu k nim, které je specifické v určitých zemích, a nelze je bez zjednodušení užívat k označení zpravodajských služeb obecně.

[4] Viz Zeman, op. cit. v pozn 2, s. 235.

[5] Laurie Nathan. *Intelligence Transparency, Secrecy and Oversight in a Democracy.* In Overseeing Intelligence Services: A Toolkit. Edited by Hans Born and Aidan Wills. Tool 3, p.49-65. DCAF, 2012, www.dcaf.ch.

- vyhnout se různým způsobům kompromitace ze strany rivalských zpravodajských služeb.[6]

Utajení ve vztahu ke zpravodajské komunitě se týká (musí týkat) oblastí, ve kterých by zveřejnění (odtajnění) informací způsobilo zjevnou újmu - ohrožení života jednotlivců, zájmů zpravodajských služeb, státu nebo země jako celku. Těmito oblastmi se rozumí:

- identita zpravodajských důstojníků (s výjimkou šéfů zpravodajských služeb),
- identita zdrojů zpravodajských informací,
- technické detaily a operativní metody,
- podrobnosti ochrany VIP,
- probíhající operace a šetření,
- identita a osobní data jednotlivců, kteří jsou předmětem zájmu zpravodajské služby.[7]

Princip vlastní bezpečnosti a *utajení* je tedy jedním ze základních principů uplatňovaných ve zpravodajství. Dalšími principy vedle primárního principu *podřízenosti ústavě a zákonům*, jsou pak dále zejména tyto:[8]

- princip nezbytné znalosti (*need to know*);
- princip efektivity;
- princip nezbytnosti a proporcionality;
- princip předběžné opatrnosti (přednostně se zvažují nejhorší možné dopady situace a zvolených prostředků; jedním z produktů zpravodajských služeb jsou varovné prognózy);
- princip ochrany dat.

V rámci spolupráce se zpravodajskými službami cizí moci má dále mimořádný význam především tzv. *pravidlo třetí strany*. Toto pravidlo v podstatě stanoví, že zpravodajská služba může informaci, kterou získala výměnou od jiné služby (ale i fakt projeveného zájmu o určitou informaci), poskytnout třetí straně pouze se souhlasem poskytovatele.[9] Tento princip stanoví pravidla ochrany informací a jejich zdrojů v oblasti mezinárodní spolupráce, v níž je tato ochrana považována za mimořádně významnou a v zásadě i limitující samotnou existenci výměny informací a budoucí spolupráce. Absence či porušení této ochrany má zásadní význam pro pokračování vzájemné zpravodajské spolupráce.

V činnosti zpravodajských služeb jsou tedy utajeny zejména tři oblasti:[10]

1. Informace o operacích, zdrojích, metodách, procedurách a prostředcích.
2. Anonymita personálu služeb a ochrana jejich znalostí.
3. Původ a detaily zpravodajských poznatků a informací poskytnutých zahraničními vládami nebo zahraničními zpravodajskými službami.[11]

---

[6] Tamtéž, s. 51.
[7] Tamtéž, s. 53.
[8] Viz Zeman, op. cit. v pozn 2, s. 234.
[9] Podrobněji k tomuto viz Zeman, P. *Spolupráce zpravodajských služeb v EU a její limity*. In: Závěšický, J. (ed.): Evropská unie a její bezpečnost. Vybrané problémy evropské bezpečnosti. Mezinárodní politologický ústav MU, Brno 2006, s. 87.
[10] Viz Zeman, P. *České zpravodajské služby po roce 1989*. In Balabán, M., Stejskal, L. a kol. *Kapitoly o bezpečnosti.* Karolinum, Praha 2010, s. 235.

Ochrana uvedených prvků zpravodajské činnosti je vykonávána prostřednictvím opatření různé povahy, ať už legislativních, organizačně technických, personálních aj. Těmto požadavkům na řádnou a efektivní činnost zpravodajských služeb pak musí odpovídat příslušná právní úprava ochrany utajovaných informací,[12] ale i dalších informací, bez nichž zpravodajské služby nemohou standardně a efektivně fungovat. Úlohou legislativy je především stanovit pravidla ochrany a přístupu ke státem drženým (chráněným) informacím, především s cílem stanovit:

- principy a kritéria klasifikace (utajení) a odtajnění informací,
- oprávněné orgány a postupy při utajení a odtajnění informací,
- soudní či jinou úroveň přezkumu utajení,
- práva jednotlivců a skupin veřejného zájmu na přístup ke státem drženým informacím,
- proceduru vyžadování přístupu k těmto informacím a právo na přezkum v případě odmítnutí přístupu,
- roli soudů v posuzování sporů týkajících se utajení a přístupu k utajovaným informacím,
- postih za neoprávněné odtajnění informace.[13]

Transparentnost státních orgánů

V souvislosti s kontrolou bezpečnostního sektoru obecně se v roce 2005 zabývalo Parlamentní shromáždění Rady Evropy otázkou kontroly zpravodajských služeb, a přijalo Doporučení č. 1713 (2005), týkající se demokratické kontroly bezpečnostního sektoru v členských zemích Rady Evropy.[14] Ve vztahu ke zpravodajským službám zformulovalo mj. princip „odložené transparentnosti“, který zohledňuje specifičnost zpravodajských služeb právě v ohledu na potřebu utajování informací. Tímto doporučilo Výboru ministrů zpracovat a schválit ve vztahu k vládám řídící zásady, které by měly ve vztahu ke zpravodajským službám znamenat tyto principy:

- činnost zpravodajských služeb musí být založena na jasné a přiměřené legislativě, podléhající soudní kontrole

---

[11] Obdobně tyto oblasti vymezuje Stieranka (viz Michálek, L., Pokorný, L., Stieranka, J., Marko, M. *Zpravodajství a zpravodajské služby.* Plzeň: Aleš Čeněk, 2013, s. 53), který hovoří o zásadě utajení, konspirativnosti a zdůrazňuje, že dodržování zásad utajení se netýká jen informací, ale také jiných prvků zpravodajství – zejm. jde o ochranu: informačních zdrojů (zejm. specifických, např. informátorů), taktiky a metodiky zpravodajství, metod, forem a prostředků zpravodajství, identity pracovníků zpravodajského pracoviště nebo útvaru vykonávajícího zpravodajství.

[12] Samotné druhy ochrany utajovaných informací lze pak dělit na kategorie, označované jako personální bezpečnost, průmyslová bezpečnost, administrativní bezpečnost, fyzická bezpečnost, bezpečnost informačních a komunikačních systémů, ochrana utajovaných informací při zpracování v elektronické podobě v zařízení, které není součástí informačního nebo komunikačního systému a kryptografická ochrana (viz zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti).

[13] Srov. Laurie Nathan. *Intelligence Transparency, Secrecy and Oversight in a Democracy.* In Overseeing Intelligence Services: A Toolkit. Edited by Hans Born and Aidan Wills. Tool 3. DCAF, 2012, www.dcaf.ch., p. 54.

[14] Dostupné z: www.assembly.coe.int/documents/adoptedtext/ta05/EREC1713.htm

- každý parlament by měl disponovat řádně fungující specializovanou komisí, jejíž minimální podmínkou by byla kontrola „mandátu“ a rozpočtu zpravodajských služeb
- mimořádné postupy (prostředky) zpravodajských služeb musí být definovány zákonem a časově přesně limitovány
- zpravodajské služby nesmějí být v žádném případě politizovány, zprávy pro politickou reprezentaci musejí zpracovávat objektivně, nestranně a profesionálně. Omezení občanských a politických práv pracovníky zpravodajských služeb musejí být určeny zákonem
- Výbor ministrů Rady Evropy je povolán přijmout evropský etický kodex zpravodajských služeb (obdobný modelu téhož u policie)
- parlament musí být periodicky informován o změnách, které se mohou dotknout obecné politiky v oblasti zpravodajských služeb (zpravodajství).

Ve vztahu k utajení zmíněné Doporučení postuluje princip odložené transparentnosti, jehož obsah formuluje takto: „citlivá rovnováha mezi utajením a závazkem skládat účty může být v určitém rozsahu zajištěna cestou *principu odložené transparentnosti* – tedy odtajněním utajovaného materiálu po uplynutí lhůty stanovené zákonodárcem“.

V podmínkách právního řádu České republiky je princip transparentnosti obecně zakotven v ustanovení čl. 17 odst. 5 Listiny základních práv a svobod, které ukládá státním orgánům povinnost přiměřeným způsobem poskytovat informace o své činnosti. Obdobně je tento princip zakotven v dokumentech Rady Evropy, např. v Doporučení Rady ministrů (2002)2[15] a v Úmluvě Rady Evropy o přístupu k úředním dokumentům (Tromso, 18. 6. 2009).

Zdroje informací podléhající ochraně a utajení

K zajištění plnění úkolů vyplývajících z jejich působnosti jsou zpravodajské služby vybaveny možností využívat oprávnění, směřujících především k zajištění možností získávat informace. Zdroje zpravodajských informací je možno obecně rozlišit na a) *zdroje otevřené* (tzv. Open-Source Intelligence /OSINT/), b) *zdroje s omezeným přístupem* a c) *specifické zdroje* (označované jako „specifické zdroje informací“, „speciální pravomoci“ (*special powers*) nebo „zpravodajské prostředky“ či „specifické prostředky získávání informací“). Právě používání posléze jmenovaných zdrojů je specifické pro zpravodajské služby (byť samozřejmě nikoli výlučné), a je jim, s ohledem na možnost zasáhnout použitím těchto prostředků do práv a svobod jednotlivců, věnována v příslušné právní úpravě zvláštní pozornost i z pohledu utajení. Ochrana je nicméně poskytována všem druhům zdrojů, není limitována pouze klasifikovaným (utajeným) charakterem, chráněn je například i samotný zájem o určitou informaci, byť nikoli formálně klasifikované podle příslušné legislativy.

Zvláštní význam s ohledem na utajení zdrojů informací mají osoby jednající ve prospěch zpravodajské služby (HUMINT v užším slova smyslu), zpravodajské prostředky (zpravodajská technika, krycí doklady a krycí prostředky a sledování), informace získané v rámci mezinárodní spolupráce zpravodajských služeb (LIAISON)

[15] Recommendation Rec (2002)2 of the Committee of Ministers to member states on Access to official documents (Adopted by the Committee of Ministers on 21 February 2002).

a samozřejmě také evidence obsahujících osobní údaje, které zpravodajské služby vedou, aniž tuto skutečnost těmto osobám sdělují, a informace mohou sdružovat a získávat je pod krytím jiným účelem nebo jinou činností.[16]

Mandát zpravodajských služeb – použitelnost informací z nich pocházejících

K posouzení charakteru režimu ochrany a následného použití informací pocházejících ze zpravodajských služeb je rozhodující vymezení mandátu zpravodajských služeb.

Základním úkolem zpravodajských služeb je *získávat, shromažďovat a vyhodnocovat* (tzv. „zabezpečovat“) *zpravodajské informace* v oblastech vymezených věcnou působností, a tyto poskytovat výkonné moci, v předstihu upozorňovat na existující hrozby, a tak umožnit přijetí opatření, která by je v souladu se zájmem státu eliminovala.[17] *Role zpravodajských služeb* se projevuje ve dvojí podobě: jednak jako důležitého *zdroje kvalifikovaných podkladů pro tvorbu bezpečnostní politiky státu,* jednak jako nezastupitelného *zdroje informací při průběžném zvládání bezpečnostní situace v zemi.*[18]

Z hlediska obsahového je mandátem zpravodajských služeb podpora životně důležitých funkcí státu, zajišťujících trvání ústavních hodnot, obranu proti násilnému napadení a zabezpečení proti hrozbám politického, ekonomického či anticivilizačního charakteru.[19]

Z hlediska formy je to pak jednak informační podpora rozhodovací činnosti příslušných oprávněných adresátů – ústavních orgánů (policymakers), tedy jako zdroj kvalifikovaných podkladů pro tvorbu bezpečnostní politiky státu, jednak informace pro jiné státní a policejní orgány v oboru jejich působnosti, jako zdroj informací při průběžném zvládání bezpečnostní situace v zemi.

První aspekt mandátu – *zdroj kvalifikovaných podkladů pro tvorbu bezpečnostní politiky státu* - nalezl své vyjádření v platné české právní úpravě v ustanovení § 8 odst. 1 a odst. 2 zákona č. 153/1994 Sb., o zpravodajských službách ČR, podle kterých zpravodajské služby předávají zprávy o své činnosti prezidentu republiky a vládě jednou za rok a kdykoli o to požádají, a prezidentu republiky, předsedovi vlády a příslušným členům vlády v případech zjištění, která nesnesou odkladu, informace bezprostředně.

Druhý aspekt – *zdroj informací při průběžném zvládání bezpečnostní situace v zemi* - pak v české právní úpravě nalezl tento odraz v ust. § 8 odst. 3 téhož zákona, podle kterého zpravodajské služby předávají státním orgánům a policejním orgánům informace o zjištěních, která náleží do oboru jejich působnosti; to neplatí, jestliže by

[16] Srov. např. § 16 zákona č. 154/1994 Sb., o Bezpečnostní informační službě.

[17] Lowenthal (Lowenthal, M., M.: *Intelligence. From Secrets to Policy*. CQPress, Washington DC, Fourth Edition, 2009, s. 2-4.) například uvádí čtyři důvody existence zpravodajských služeb, jimiž jsou: vyhnout se strategickému překvapení, poskytovat dlouhodobější expertizu, podporovat proces formování politiky a udržovat utajení informací, potřeb, zdrojů a metod.

[18] Srov. Duchek, J.: *Zpravodajské služby při tvorbě a realizaci bezpečnostní politiky*. Vojenské rozhledy. Teoretický časopis armády České republiky, 2005, číslo 1, s. 55.

[19] Viz Důvodová zpráva k § 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.

poskytnutí ohrozilo důležitý zájem sledovaný příslušnou zpravodajskou službou. V tomto případě konkretizujme mezi státními a policejními orgány činné v trestním řízení, a informace o zjištěních, která náleží do oboru jejich působnosti, jako ty, které jsou relevantní pro zahájení či postup již zahájeného trestního řízení. Tímto způsobem se zpravodajské služby, ač nejsou orgány činnými v trestním řízení, podílejí na informační podpoře činnosti těchto orgánů a na průběžném zvládání bezpečnostní situace v zemi včetně stíhání trestných činů. V tomto aspektu jejich mandátu pak lze diskutovat roli, možnosti a formy jeho naplňování operativními informacemi, či dokonce případným přiznáním důkazní použitelnosti informacím pořízeným zpravodajskými službami mimo trestní řízení.

V případech obou podob naplňování mandátu zpravodajských služeb existuje tlak na odhalení zdroje zpravodajských informací, který hrozí ze strany vnějších kontrolních mechanismů, ve druhém pak v souvislosti s aplikací pravidel dokazování, měly-li by zpravodajské informace být použity jako důkazy v řízení, především v trestních věcech. V případě extrémního nastavení oprávnění kontrolních orgánů či nechráněného použití zpravodajských informací jako důkazu v soudním řízení[20] hrozí odhalení identity zdrojů informací, jejichž ochranu jsou zpravodajské služby ze zákona povinny zajistit, ale například i omezení mezinárodní spolupráce v případě neautorizovaného poskytnutí informace třetí straně.

V případě důkazního použití zpravodajské informace zároveň tkví ono riziko i v samotném charakteru a podstatě zpravodajské činnosti, které se v tomto ohledu liší od charakteru a povahy činnosti orgánů typu law enforcement. K tomuto rozlišení podstaty (povahy) zpravodajství (*Intelligence*) a *law enforcement* lze využít shrnující specifikaci, kterou provedl Gregory F. Treverton[21] takto[22]:

- Law Enforcement řeší případy s cílem shromáždit dostatečné důkazy k prokázání viny před soudem, kdežto Intelligence shromažďuje informace s cílem podat tvůrcům politiky (policymakers) informace, které jim pomáhají snižovat nejistotu a přijímat lepší rozhodnutí;
- Charakter law enforcement je reaktivní – shromažďují informace poté, co byl trestný čin spáchán, kdežto intelligence proaktivní (preventivní) – shromažďuje informace před skutkem, za účelem pomoci tvořit politiku, navrhovat (tvořit) strategii a/nebo předcházet nežádoucím jevům (např. teroristickým útokům);
- Standardem sběru informací jsou v případě law enforcement pravidla dokazování – získat informace a důkazy v přísném souladu s ústavou a všemi aplikovatelnými pravidly dokazování (rule of evidence), v případě intelligence jde o princip dostatečnosti (Good Enough), tedy získat a využít každou informaci, pokud je její věrohodnost (credibility) dostatečná;
- Cílem u law enforcement je předložit soudu důkazy způsobilé prokázat, že obviněný je vinen, tedy, jak zdroj důkazu, tak i metoda, kterou byl získán, musí být podle zákona identifikován (vyjeven), *v případě intelligence je cílem ochrana zdrojů – ochránit zdroje a metody za každou cenu. Konečný cíl je zajistit, že zůstanou neznámé a schopné přinášet užitečné věrohodné informace tak dlouho, jak jen to bude možné.*

---

[20] Srov. např. důvody pro přijetí Justice and Security Act 2013 ve Velké Británii – viz Exkurz.
[21] Analytik a ředitel RAND Center for Global Risk and Security (RAND Corporation), www.rand.org.
[22] Viz Jensen, Carl J., McElreath, David H., Graves, Melissa. *Introduction to Intelligence Studies*. Boca Raton, CRC Press, 2013, ISBN 978-1-4665-0003-7, s. 276.

Způsoby ochrany zpravodajských zdrojů – příklad České republiky

Zákony o zpravodajských službách

Zákony upravující postavení a činnost zpravodajských služeb České republiky obsahují řadu dílčích ustanovení zajišťujících ochranu zpravodajských zdrojů, zejména tyto:

- výhradu důležitého zájmu sledovaného zpravodajskou službou
- úpravu vedení evidencí
- evidenční ochranu údajů vedených v registrech
- zvláštní způsob vykazování údajů
- ochranu specifických prostředků získávání informací
- parlamentní kontrolu Bezpečnostní informační služby a Vojenského zpravodajství.

- Už při vymezení okruhu adresátů informací ze zpravodajských služeb a předávání informací je ochrana zajištěna zakotvením tzv. *výhrady důležitého zájmu sledovaného zpravodajskou službou.* Tato výhrada podmiňuje předávání informací za strany zpravodajských služeb státním a policejním orgánům absencí důležitého zájmu sledovaného zpravodajskou službou, který by mohl být tímto ohrožen.[23] Takovým důležitým zájmem může být např. probíhající akce, metody a formy činnosti zpravodajských služeb, ochrana osoby jednající ve prospěch zpravodajské služby, ochrana pravidla třetí strany.

- *Vedení evidencí, ochrana osobních údajů*

Vedení evidencí a ochranu údajů v nich obsažených upravuje § 16 zákona o BIS takto:
„(1) Bezpečnostní informační služba je oprávněna ukládat, uchovávat a využívat údaje o fyzických a právnických osobách, jestliže je to nutné k plnění úkolů v její působnosti.
(2) Bezpečnostní informační služba je povinna zabezpečit ochranu údajů obsažených v evidencích před vyzrazením, zneužitím, poškozením, ztrátou a odcizením.
(3) Bezpečnostní informační služba skutečnost o vedení evidence o fyzických a právnických osobách ani její obsah těmto osobám nesděluje.
(4) Bezpečnostní informační služba může informace a informační systémy sdružovat a získávat informace pod krytím jiným účelem nebo jinou činností.
(5) Bezpečnostní informační služba zřizuje bezpečnostní archiv k trvalému zachování informací.“

- Dalším nástrojem je tzv. *evidenční ochrana údajů vedených v registrech*:

§ 11 zákona č. 153/1994 Sb., o zpravodajských službách ČR, upravuje poskytování informací zpravodajským službám a také jejich evidenční ochranu: „(1) V rámci své působnosti mohou zpravodajské služby žádat od orgánů veřejné správy nezbytnou pomoc a informace uchovávané těmito orgány v souvislosti s plněním

[23] V ČR viz ust. § 8 odst. 3 zákona č. 153/1994 Sb., o zpravodajských službách ČR: „Zpravodajské služby předávají státním orgánům a policejním orgánům informace o zjištěních, která náleží do oboru jejich působnosti; *to neplatí, jestliže by poskytnutí ohrozilo důležitý zájem sledovaný příslušnou zpravodajskou službou*.“

úkolů státní správy. ….(4) Poskytnutí údajů je zpravodajská služba oprávněna požadovat v rozsahu potřebném pro plnění konkrétního úkolu ve své působnosti nebo pro *provádění opatření k evidenční ochraně údajů vedených v registrech, informačních systémech a evidencích* uvedených v odstavcích 2 a 3.“

- Jestliže je to nutné k utajení jejich činnosti, mohou zpravodajské služby a jejich příslušníci podle § 20 zákona o zpravodajských službách ČR, používat *zvláštní způsoby vykazování údajů* při hospodaření s prostředky státního rozpočtu, včetně devizového hospodaření a vykazování údajů pro účely státní sociální podpory. Tento zvláštní způsob vykazování údajů stanoví vláda.

- *Ochrana specifických prostředků získávání informací*

Zvláštní ochranu požívají specifické prostředky získávání informací, kterými se pro účely tohoto zákona č. 154/1994 Sb., o BIS, rozumějí zpravodajské prostředky (zpravodajská technika, krycí prostředky a krycí doklady, sledování) a využívání služeb osob jednajících ve prospěch Bezpečnostní informační služby. *Bezpečnostní informační služba je pak ze zákona povinna zabezpečit ochranu zpravodajských prostředků před vyzrazením, zneužitím, poškozením, zničením, ztrátou a odcizením.*

Speciální účel pak mezi zpravodajskými prostředky plní krycí prostředky a krycí doklady, které mají ex lege stanoven jako účel vydání a použití „*utajení skutečné totožnosti příslušníka nebo jeho příslušnosti k Bezpečnostní informační službě nebo k utajení skutečných zájmů nebo objektů Bezpečnostní informační služby, je-li toto utajení nutné pro plnění úkolů Bezpečnostní informační služby.“*

„Je-li to vzhledem k povaze krycího dokladu nutné, je Bezpečnostní informační služba oprávněna v nezbytné míře zajistit v informačních systémech vedených podle zvláštních právních předpisů vložení, změnu nebo vyjmutí (fyzické vymazání) údajů souvisejících s krycím dokladem, popřípadě blokování těchto údajů. Orgán veřejné správy příslušný k vedení informačního systému je povinen poskytnout k provedení těchto úkonů potřebnou součinnost.“

V případě využívání služeb osob jednajících ve prospěch Bezpečnostní informační služby je jejich zákonným pojmovým znakem mj. právě *utajený způsob poskytování služeb*.[24] Bezpečnostní informační službě je pak stanovena povinnost „*ochraňovat osobu jednající ve prospěch Bezpečnostní informační služby před vyzrazením a způsobením újmy na cti, životě, zdraví nebo majetku, která by jí mohla vzniknout pro poskytování těchto služeb nebo v souvislosti s ním.“*

- *Parlamentní kontrola Bezpečnostní informační služby a Vojenského zpravodajství*

Členům parlamentního kontrolního orgánu pro kontrolu činnosti BIS (obdobně VZ) je zákonem (§§ 18- 21 zákona o BIS, resp. §§ 21-24 zákona o VZ) vymezen okruh oprávnění, přičemž kontrolní orgán není oprávněn zasahovat do personálních pravomocí vedoucích pracovníků Bezpečnostní informační služby (resp. VZ) a nahrazovat jejich řídící činnost. Ředitel BIS předkládá kontrolnímu orgánu zákonem vymezené podklady (statut Bezpečnostní informační služby, návrh rozpočtu

[24] „Osobou jednající ve prospěch Bezpečnostní informační služby se pro účely tohoto zákona rozumí fyzická osoba starší 18 let, která dobrovolně a *utajeným způsobem* poskytuje služby Bezpečnostní informační službě při plnění jejích úkolů.“

Bezpečnostní informační služby, písemná zadání úkolů uložených vládou nebo prezidentem republiky, podklady potřebné ke kontrole plnění rozpočtu Bezpečnostní informační služby, vnitřní předpisy, vydávané podle § 148 odst. 2), na jeho požádání pak zprávu o činnosti Bezpečnostní informační služby, zprávu o použití zpravodajských prostředků, a to pouze *ve věcech a případech, ve kterých Bezpečnostní informační služba svou činnost již ukončila*, *počet případů použití zpravodajské techniky*, ve kterých je Bezpečnostní informační služba činná, s uvedením jednotlivých oblastí působnosti Bezpečnostní informační služby a druhu zpravodajské techniky, *souhrnnou informaci* obsahující zaměření a počet případů a věcí, v nichž je Bezpečnostní informační služba činná; v informaci odliší případy a věci podle zvláštního zákona, *počet případů*, ve kterých byla podána žádost o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství, ve kterých je Bezpečnostní informační služba činná s uvedením jednotlivých oblastí působnosti bezpečnostní informační služby, zprávu o využívání žádostí o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství, a to *pouze ve věcech a případech, ve kterých Bezpečnostní informační služba svou činnost již ukončila*. Každé porušení zákona příslušníky, které kontrolní orgán zjistí při své činnosti, je povinen oznámit řediteli a nejvyššímu státnímu zástupci.

Povinnost zachovávat mlčenlivost uložená členům kontrolního orgánu podle zákona se nevztahuje na případy, kdy kontrolní orgán podává oznámení podle § 20 odst. 2. Skutečnosti, o nichž se členové kontrolního orgánu dovědí při výkonu své funkce, oznamují v míře nezbytné pro dosažení účelu kontroly podle tohoto zákona.

Ochrana utajovaných informací, povinnost mlčenlivosti

V této oblasti jde především o ochranu klasifikovaných informací dle zákona č. 412/2005 Sb., a jeho prováděcích předpisů,[25] ale i stanovení povinnosti

[25] Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, určuje v Příloze 18 Seznam utajovaných informací v oblasti působnosti zpravodajských služeb České republiky takto:

Pořadové číslo	*Informace*	*Stupeň utajení*
1.	*Formy, metody, zásady a směrnice pro zpravodajskou činnost*	*V - PT*
2.	*Administrativní pomůcky k evidenci utajovaných informací*	*V - T*
3.	*Plány zpravodajské činnosti*	*V - PT*
4.	*Vyhodnocení a výstupy zpravodajské činnosti*	*V - PT*
5.	*Bezpečnostní rozbory a bezpečnostní opatření k ochraně důležitých zájmů České republiky*	*V - PT*
6.	*Finanční zabezpečení, evidence a doklady, rozbory hospodaření*	*V - T*
7.	*Organizační struktura*	*V - T*
8.	*Stanovené údaje o formách, metodách, prostředcích a výsledcích činnosti, včetně příslušné dokumentace, vzniklé do 31.12.1992 z činnosti zpravodajských služeb, popř. jiných bezpečnostních orgánů státu*	*V - D*
9.	*Dislokace a ochrana stanovených organizačních částí zpravodajské služby*	*V - PT*
10.	*Plány přípravy a příprava příslušníků zpravodajské služby a osob tvořících zpravodajské struktury*	*V - T*
11.	*Zpravodajské a specifické prostředky, včetně jejich ochrany*	*V - PT*
12.	*Údaje o stanovených informačních zdrojích*	*V - PT*
13.	*Plány realizace, průběh a výsledky stanovených zpravodajských činností*	*V - PT*

mlčenlivosti uloženou příslušníkům zpravodajských služeb ohledně jiných než klasifikovaných informací souvisejících s činností zpravodajských služeb podle zákona č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů. Ustanovení § 45 odst. 1, písm. c) zákona č. 361/2003 Sb., ukládá příslušníkům civilních zpravodajských služeb jako základní povinnost zachovávat *mlčenlivost o skutečnostech, o kterých se dověděli při výkonu služby.*

Svobodný přístup k informacím

Obecně široká míra dostupnosti informací v rámci svobodného přístupu k nim s evidentní tendencí k jejímu rozšiřování,[26] je zákonem limitována ve vztahu k zdrojům a informacím pocházejícím či souvisejícím s činností zpravodajských služeb. Zpravodajské služby nicméně obecně nejsou vyloučeny z okruhu povinných subjektů podle ust. § 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a jsou tedy, jako státní orgány, povinny poskytovat informace vztahující se k jejich působnosti.[27] Z toho platí dva speciální explicite zákonem vyjádřené důvody, pro které zpravodajská služba jako povinný subjekt informace neposkytne. Za prvé jde o případ, kdy je požadována informace, která je v souladu s právními předpisy označena za utajovanou informaci, k níž žadatel nemá oprávněný přístup,[28] a za druhé, kdy jde o informaci o plnění úkolů zpravodajských služeb.[29]

Trestní zákoník

Trestněprávní ochrana zpravodajských zdrojů je poskytována ustanoveními trestního zákoníku, která upravují trestní postih jednání ohrožujících utajované informace ve prospěch cizí moci nebo nepovolané osoby (trestné činy proti bezpečnosti České republiky, cizího státu a mezinárodní organizace – vyzvědačství, ohrožení utajované informace).

Důkazní použití v trestním řízení /použitelnost odposlechu, utajený svědek/

---

14. Organizace spojení, informační systémy *V - PT*
15. Evidence vedené za účelem plnění úkolů v působnosti zpravodajské služby *V - PT*
16. Spolupráce se zpravodajskými službami cizí moci *V - PT*
17. Příslušnost stanovených osob ke zpravodajské službě *V - PT*
18. Personální a bezpečnostní evidence zpravodajské služby *V- PT*
19. Materiálně technické zabezpečení, evidence a doklady, výzkum a vývoj *V - T*

[26] Srov. např. rozhodovací činnost Evropského soudu pro lidská práva – viz *Youth Initiative for Human Rights c. Serbie – 48135/06 z 25.6.2013 (*Odmítnutí zpravodajské služby poskytnout informace nevládní organizaci). Dostupné z: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-120955.

[27] „ Povinnými subjekty, které mají podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti, jsou *státní orgány*, územní samosprávné celky a jejich orgány a veřejné instituce."

[28] § 7 zákona č. 106/1999 Sb., o svobodném přístupu k informacím: „Je-li požadovaná informace v souladu s právními předpisy *označena za utajovanou informaci,* k níž žadatel nemá oprávněný přístup, povinný subjekt ji neposkytne." Dále by mohlo jít o ust. § 11 odst. 1, písm. c): „jde o informaci poskytnutou Organizací Severoatlantické smlouvy nebo Evropskou unií, která je *v zájmu bezpečnosti státu, veřejné bezpečnosti nebo ochrany práv třetích osob chráněna uvedenými původci označením „NATO UNCLASSIFIED" nebo „LIMITE"* a v České republice je toto označení respektováno z důvodů plnění povinností vyplývajících pro Českou republiku z jejího členství v Organizaci Severoatlantické smlouvy nebo Evropské unii, pokud původce nedal k poskytnutí souhlas."

[29] § 11 odst. 4, písm. c) zákona č. 106/1999 Sb., o svobodném přístupu k informacím: „Povinné subjekty dále neposkytnou informace o …, *c) plnění úkolů zpravodajských služeb,".*

Samostatným a komplikovaným tématem pak je otázka využití informací ze zpravodajských služeb v trestním řízení.

Zpravodajské služby nejsou orgánem činným v trestním řízení,[30] nemají zpravidla žádné výkonné pravomoci, a informace jimi získané také zpravidla nejsou použitelné jako důkaz v trestním řízení.[31] Jejich povaha je pouze operativní, umožňující orgánům činným v trestním řízení případně pouze zaměřit další procesní postup a relevantní informace převést do procesně využitelné podoby jejich provedením - zprocesněním postupem podle trestního řádu. Možnost využití jednotlivých důkazních prostředků vyplývá z vnitrostátní právní úpravy trestního řízení v té které zemi. Ve většině zemí však informace - „důkazy" opatřené zpravodajskými službami mají v trestním řízení pouze podpůrnou úlohu. Důvody tohoto jsou jednak formální, resp. formálně právní – tedy právní úprava jednotlivých prostředků mimo trestní řád, jednak věcné – především právě ochrana zdroje informace.[32] Proto je také velmi významné zakotvení tzv. výhrady důležitého zájmu sledovaného zpravodajskou službou v příslušné zákonné úpravě předávání informací zpravodajskými službami jiným subjektům.

Na zvláštní povahu práce zpravodajských služeb v této souvislosti poukazuje např. Zeman[33] - upozorňuje na to, že po zpravodajských službách se žádá práce v předstihu, tedy práce ve vztahu ke skutkům, které ještě nenastaly; z hlediska trestněprávního, resp. trestně-procesního je to činnost *extra legem*, přestože tato činnost je upravena zákonem a sleduje zákonem dané cíle, což vyvolává velké potíže s následným zprocesněním získaných informací v trestním řízení. Mezi cíle zpravodajských služeb však pohnání pachatele trestného činu před soud nepatří. Výsledky činnosti zpravodajských služeb tak nejsou z procesního hlediska využitelné jako důkaz v trestním řízení. V případě získání informací vedoucích k důvodnému podezření z naplnění skutkové podstaty trestného činu pak, mají-li být trestněprávně využitelné, musí v těchto případech následovat předání těchto informací příslušným orgánům, tedy orgánům činným v trestním řízení, v jejichž působnosti je vedení trestního řízení. K závěru o nepoužitelnosti záznamu odposlechu pořízeného zpravodajskou službou se vyslovil Ústavní soud České republiky,[34] a to s argumentem institucionální teleologií zpravodajských služeb, tedy účelem pořízení

---

[30] Jedinou výjimkou jsou pověřené orgány zabývající se trestnou činností vlastních příslušníků, které mají procesní postavení policejních orgánů podle § 12 odst. 2 trestního řádu.

[31] Policejní informace a zpravodajské poznatky se liší v řadě aspektů, kromě rozdílných subjektů jejich získávání, je lze spatřovat zejména v cíli (účelu) jejich využití, v jejich objektovém zaměření, způsobu získávání, způsobu využití, a v jejich právním zakotvení. (Srov. např. Pikna, B. *Mezinárodní terorismus a bezpečnost Evropské unie (právní náhled).* Linde, Praha 2006, s. 203,204.) K důkaznímu využití odposlechu provedeného zpravodajskou službou viz Nález ÚS ČR sp. zn. I ÚS 3038/07.

[32] Např. ředitelka britské vnitřní služby Manningham-Bullerová se k této otázce vyjádřila tak, že „.. ke sdílení zpravodajských poznatků nesmíme být nuceni, a proto při využití těchto poznatků v trestním procesu je třeba s nimi zacházet obezřele." Viz Manningham-Buller, E. (2005) *The International Terrorist Threat and the Dilemmas in Countering It.* Speech by the Director General of the Security Service, Dame Eliza Manningham-Buller, At the Ridderzaal, Binnenhof, The Hague, Netherlands, 1 September 2005, on line verze (http://www.mi5.gov.uk/output/Page387.html). Cit dle Zeman, P. *Spolupráce zpravodajských služeb v EU a její limity*. In: Závěšický, J. (ed.): *Evropská unie a její bezpečnost. Vybrané problémy evropské bezpečnosti.* Mezinárodní politologický ústav MU, Brno 2006. s. 91.

[33] Zeman, P.: *Spolupráce zpravodajských služeb v EU a její limity*, op. cit., s. 90.

[34] viz zmíněný Nález ÚS ČR sp. zn. I ÚS 3038/07.

tohoto záznamu pro jiné než důkazní použití a pro jeho pořízení na základě jiného zákona než trestního řádu.

V poslední době se však vede diskuse o případné použitelnosti těchto informací jako důkazu v trestním řízení a důvody jsou shledávány v onom druhém aspektu mandátu zpravodajských služeb, legitimitě použití legálně získaných informací státním orgánem při postihu závažné kriminality, srovnatelné úrovni standardu garance práv dotčených osob stanovených relevantní právní úpravou, inspiraci zahraničními právními úpravami, posunu v nových bezpečnostních hrozbách, i v doktrinálních názorech.

Pokud jde o konkrétní možnosti utajení zdroje informací v trestním řízení, je možné zmínit pouze institut utajeného svědka. Ten je upraven v ustanovení § 55 odst. 2 trestního řádu jako výjimečný: „Nasvědčují-li zjištěné okolnosti tomu, že svědku nebo osobě jemu blízké v souvislosti s podáním svědectví zřejmě hrozí újma na zdraví nebo jiné vážné nebezpečí porušení jejich základních práv, a nelze-li ochranu svědka spolehlivě zajistit jiným způsobem, orgán činný v trestním řízení učiní *opatření k utajení totožnosti i podoby svědka; jméno a příjmení a jeho další osobní údaje se do protokolu nezapisují, ale vedou se odděleně od trestního spisu a mohou se s nimi seznamovat jen orgány činné v trestním řízení v dané věci*. Svědek se poučí o právu požádat o utajení své podoby a podepsat protokol smyšleným jménem a příjmením, pod kterým je pak veden. Je-li třeba zajistit ochranu těchto osob, orgán činný v trestním řízení činí bezodkladně všechna potřebná opatření. Zvláštní způsob ochrany svědků a osob jim blízkých stanoví zvláštní zákon. Pominou-li důvody pro utajení podoby svědka a oddělené vedení osobních údajů svědka, orgán, který v té době vede trestní řízení, zruší stupeň utajení těchto informací, připojí uvedené údaje k trestnímu spisu a podoba svědka ani údaje o jeho totožnosti se nadále neutajují; to neplatí, je-li utajována totožnost a podoba osob uvedených v § 102a.“

Exkurz: Justice and Security Act 2013

S ohledem na ochranu zpravodajských zdrojů zasluhuje zvláštní zmínku nepochybně britský *Justice and Security Act 2013*.[35] Tento zákon, kromě posílení role parlamentního výboru pro bezpečnost a zpravodajské služby (*The Intelligence and Security Committee of Parliament),* umožňuje utajení občanských (civilních) soudních procesů, při kterých by veřejným jednáním mohlo dojít k úniku citlivých informací či kompromitaci zpravodajských služeb. Soudci mají podle tohoto zákona pravomoc rozhodnout o vyloučení neprověřených účastníků řízení tam, kde soud pracuje s klasifikovanými důkazními materiály či, kde vystupují příslušníci zpravodajských služeb. Zákon tak dává možnost soudcům civilních soudů vést jednání v utajení (*tzv. closed material procedure)*, což bylo dosud možné pouze v případě imigračních a deportačních soudů. Rozšířil tak okruh případů, kdy může soudce rozhodnout o vyloučení neprověřených osob, včetně žalobců a odpůrců, ze soudních přelíčení, pokud by hrozilo vyzrazení utajovaných informací. Přítomni jednání mohou v takových případech být pouze právníci s bezpečnostní prověrkou. Tento zákon, jehož návrh byl od počátku kontroverzní, byl odůvodňován jako nezbytný pro národní bezpečnost (zejména s argumentem, že *zahraniční*

[35] Justice and Security Act 2013 Chapter 18. Dostupný z http://legislation.gov.uk/ukpga/2013/18/pdfs/ukpga_20130018_en.pdf

zpravodajské služby nejsou ochotny sdílet s Brity informace z obavy, že se u britských soudů dostanou jejich data či identita agentů na veřejnost). Ochráněni ale mají především být příslušníci domácích zpravodajských služeb, kteří se budou moci hájit u soudů bez rizika vyzrazení identity.

Souhrn

Zpravodajské služby v sobě slučují standardní charakter státních orgánů, na které dopadá princip transparentnosti, a specifický charakter státního orgánu sui genesis, spočívající v požadavku utajenosti jejich činnosti. Toto má pak svůj dopad v nezbytné potřebě modifikace principu transparentnosti na činnost zpravodajských služeb a také na zajištění ochrany zpravodajských zdrojů. Tato potřeba se pak promítá do opatření různého charakteru, která tuto potřebu zajišťují. Zásadní význam má v tomto směru legislativa – právní úprava, která zajistí ochranu zpravodajských zdrojů před vyzrazením, ohrožením, způsobením újmy na cti, životě, zdraví nebo majetku, a tím i funkčnost, efektivitu a akceschopnost činnosti zpravodajských služeb. Rizika a limity pro tuto ochranu však vytváří řada vlivů, aspektů a okolností, mj. i takové, které jsou obecně žádoucí a standardní, nicméně při neadekvátním nastavení či aplikaci (kontrolní mechanismy), nebo z povahy věci (důkazní použití) mohou přinést ohrožení zpravodajských zdrojů. I extrémně nastavená oprávnění vnějších kontrolních mechanismů mohou limitovat činnost zpravodajských služeb např. v podobě omezení mezinárodní spolupráce v případě omezení schopnosti zachovávat v rámci mezinárodní spolupráce pravidlo třetí strany ve vztahu k partnerským zahraničním službám, a obdobně možnosti a podmínky externího využití informací ze zpravodajských služeb např. v soudním řízení v podobě důkazů, na něž se vztahují přísná pravidla dokazování.

Současnou právní úpravu v České republice, která je v předloženém příspěvku v základní podobě shrnuta, očekává v blízké budoucnosti změna spočívající v připravovaném zákoně o kontrole zpravodajských služeb České republiky,[36] jímž budou mj. otázky limitů ochrany zpravodajských zdrojů nepochybně nově legislativně upraveny.

[36] Viz Programové prohlášení vlády ČR z února 2014, které jako jednu z hlavních priorit stanoví: „Posílení parlamentní kontroly zpravodajských služeb České republiky. Vláda předloží návrh zákona, který stanoví rozsah a způsob kontroly zpravodajských služeb Parlamentem ČR. Zákon bude vycházet ze zásady, že parlamentní kontrole musí podléhat všechny zpravodajské služby České republiky. Zákon zavede dvoustupňový systém kontroly, proto bude kromě zřízení kontrolních orgánů v Poslanecké sněmovně ČR zřízen i od Parlamentu ČR odvozený expertní kontrolní orgán složený z důvěryhodných, bezpečnostně prověřených a veřejností respektovaných občanů.“ Dostupné z www.vlada.cz/cz/media-centrum/dulezite-dokumenty/programove_prohlaseni_unor_2014.pdf

T. Rulíšek: K limitom právnej ochrany spravodajských zdrojov

JUDr. Tomáš Rulíšek, PhD. *(1977) - Absolvoval Právnickú fakultu Univerzity Komenského v Bratislave. Doktorandské štúdium v odbore trestné právo ukončil na Právnickej fakulte Trnavskej univerzity s témou dizertačnej práce „Trestné činy proti republike a spravodajské služby“. Od roku 2003 pôsobí v rôznych funkciách v Slovenskej informačnej službe.*

Právo štátu mlčať

Na prvý pohľad je myšlienka spočívajúca v práve štátu zamlčať informácie, ktorými disponuje jeho vlastný inštitucionálny aparát a ktoré sú navyše potrebné na ochranu a presadzovanie práva, absurdná a v podmienkach právneho štátu neakceptovateľná. V podmienkach slobodnej spoločnosti, presadzujúcej právo na informácie a konštitučnými mechanizmami zabezpečeného práva na šírenie a vyhľadávanie informácií sa súčasne ustálila nekriticky prijímaná, avšak popularizovaná téza o tom, že požiadavka transparentnej vlády v sebe imanentne nesie povinnosť štátnej moci informovať verejnosť o všetkom - a to často bez zváženia legitímnych dôsledkov takéhoto extrémistického prístupu.

Avšak napriek tomu, že v žiadnom formálnom prameni pozitívneho práva v podmienkach slovenského právneho poriadku nenájdeme explicitné vyjadrenie niečoho, ako „právo štátu mlčať“, pri hlbšom rozbore zistíme, že takéto právo existuje a že jeho realizácia môže byť dokonca rozhodujúca pre zachovanie - keď nie vždy existenčných, tak prinajmenšom dôležitých záujmov štátu, ktorého politicko-hodnotová orientácia spĺňa kritériá postulované pre demokratický a právny štát.

Uznávaný francúzsky štátnik a jeden zo zakladateľov modernej podoby národných štátov formovaných na európskom kontinente a fungujúcich v komplikovaných vzájomných vzťahoch medzinárodnej politiky, kardinál Armand Jean du Plessis de Richelieu, vo svojom diele *Testament Politique (1641)* zdôraznil dôležitosť legitímneho a legálneho utajovania pre správne politické spravovanie štátu. Vzájomné puto medzi efektívnym štátom a utajovanou časťou činnosti štátnej moci možno v rámci historického exkurzu vystopovať napríklad do obdobia alžbetínskeho Anglicka, kedy Sir Francis Walsingham konštituoval ideové a inštitucionálne základy fungovania moderného spravodajského aparátu štátu, ktoré pretrvávajú v britskom bezpečnostnom systéme dodnes.

Utajovať nie je zatajovať

Zo sémantického hľadiska možno obe titulné slová považovať za synonymické. Významová rozdielnosť toho, čo vyjadrujú v slovenskom jazyku, je však napriek tomu zreteľná práve v súvislosti s výkladom tých skutočností, ktorých utajenie je štátom uznaným a právom formalizovaným spôsobom ochrany pred nežiaducim zásahom v podobe vyzradenia či odhalenia obsahu takýchto skutočností. Prostredníctvom utajovania vláda realizuje právo štátu mlčať o skutočnostiach, ktoré sú zásadné pre jeho politické, ekonomické, obranné a bezpečnostné záujmy, prípadne iné verejné záujmy, na ktorých ochranu sa zaviazal. Samozrejme, tým nepopierateľne prelamuje či prinajmenšom relativizuje transparentnosť, ako princíp dobrého vládnutia.

Legitimita dôvodov utajenia, hoc akokoľvek môže byť predmetom polemiky, je rozhodujúcim diferenciačným kritériom na objasnenie rozdielneho významu oboch slov. Kedy má teda štát legitímne právo mlčať, ak funguje v podmienkach štátu na princípe „rule of law"?

Takto formulovaný otáznik zahŕňa však nielen oblasť právnych nástrojov garantujúcich zachovanie utajenia zdrojov spravodajských služieb, ale celý generálny právny režim ochrany skutočností a informácií, ktorým sa štát rozhodol priznať povahu tajomstva zachovávaného v jeho záujme. K predmetu tohto tajomstva sa štát zároveň rozhodol obmedziť prístup prostredníctvom právne regulovaných administratívnych, personálnych, objektových a ďalších opatrení. V podmienkach fungovania právneho štátu rešpektujúceho právo na slobodné šírenie a vyhľadávanie informácií však ustanovenie akýchkoľvek medzí pre jeho realizáciu sa musí v súlade s ústavnými požiadavkami na obmedzovanie základných práv a slobôd diať výlučne zákonom. V právnom poriadku Slovenskej republiky je na tento účel v účinnosti zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. Ide o generálnu administratívno-právnu úpravu, z ktorej je však potrebné vyvodzovať *inter alia* aj základný prameň právnej ochrany spravodajských zdrojov. Blanketová norma v tomto zákone[1] zároveň splnomocnila vládu Slovenskej republiky ustanoviť svojím nariadením oblasti, v ktorých môže vznikať právne dovoleným spôsobom utajovaná skutočnosť. Normatívne znenie blankety zároveň vylúčilo možnosť vzniku právnej ochrany v podobe zákonného utajenia pre informácie alebo veci vzniknuté v iných, než vládou ustanovených oblastiach. Do škály predmetov s takouto ochrannou exkluzivitou boli zahrnuté medzi iným aj formy, metódy a výsledky činnosti spravodajských služieb. Osobitne podzákonná právna úprava priznáva prostredníctvom legálneho utajovania protekčnú výlučnosť aj prostriedkom utajenia metód, foriem a výsledkov činnosti spravodajských služieb a zároveň používaniu informačno-technických prostriedkov a informačno-operatívnych prostriedkov. Zakotvenie zákonnej definície utajovanej skutočnosti priamo v zákone tu nie je len garanciou právnej ochrany s dostatočným stupňom právnej sily, ale tiež obmedzením pre vládu, ktorá reprezentujúc výkonnú moc, musí pri určení oblastí, v ktorých môže utajovaná skutočnosť vzniknúť - rešpektovať zákonom fixované obsahové obmedzenie. Ide o významný nástroj regulácie diskrečnej právomoci vlády a prostriedok na zabránenie jej arbitrárnemu rozhodovaniu. Samozrejme, priznanie právnej ochrany spravodajským zdrojom prostredníctvom režimu legálneho utajovania *per se* nepostačuje na dosiahnutie potrebnej prevencie pred ich vyzradením, tvorí však základ pre ďalšie prostriedky a inštitúty právnej ochrany, najmä osobitnej administratívno-právnej a tiež trestnoprávnej povahy.

Z perspektívy práva ako nástroja slúžiaceho ochrane spravodajských zdrojov je teda hľadanie optimálneho modelu vždy spojené so schopnosťou vlády poskytnúť spravodajskej službe dostatočne účinné možnosti ich legálneho utajovania. Táto schopnosť je vystavená skúške najmä tam, kde je silnejúci tlak na interakciu medzi činnosťou spravodajskej služby a jej výsledkami na jednej strane a požiadavkami recipientov spravodajskej produkcie na strane druhej. Žiadosť oprávneného recipienta o odpoveď na otázku „Čo viete ?" je prirodzenou a v zásade legitímnou - a to bez ohľadu nato, či účelom poskytnutia odpovede je tajná informačná podpora

[1]) § 2 písm. a) zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

rozhodovania najvyšších štátnych orgánov zodpovedných za realizáciu štátnych záujmov na jednotlivých úsekoch politiky vlády, alebo ide o súčinnosť spravodajskej služby v oblasti ochrany práva. To, čo však vždy vyvoláva zimomriavky na tele každého spravodajského dôstojníka je otázka dopytujúca sa po spôsobe ako spravodajská služba určitú informáciu získala. Obe otázky však spolu samozrejme súvisia a riziko, že s tou prvou bude spravodajská služba konfrontovaná aj s tou druhou je zvlášť vysoké vtedy, keď spôsob získania informácie podmieňuje jej právne súladnú alebo i právne nedovolenú využiteľnosť na dosiahnutie recipientom zamýšľaného účelu. Na exemplifikáciu prípadu, v ktorom môže vzniknúť takéto riziko, je neúmerne extenzívny rozsah oprávnení orgánu povereného vonkajším dohľadom nad činnosťou spravodajskej služby, či už v rámci moci výkonnej alebo zákonodarnej. Umožniť oprávnenie na prístup k identite ľudského zdroja či odhaleniu iného druhu spravodajského zdroja spojené s právne ustanovenou povinnosťou spravodajskej služby takýto prístup v rozsahu účelu externej kontroly možno rozumne odôvodniť výlučne *in extremis.* Môže tomu byť napr. vtedy, ak by vznikli dôvodné pochybnosti o súlade postupu spravodajskej služby pri evidovaní či použití spravodajského zdroja so zákonom. Aj v tomto prípade by však museli byť zachované aspoň minimálne záruky ďalšieho nešírenia tejto informácie, čo možno dosiahnuť len striktným dodržaním povinnosti mlčanlivosti členov orgánu externej kontroly.

Ak si odmyslíme prípady nebezpečných snáh o zneužitie spravodajskej služby, ktoré môžu vzniknúť pri absencii dostatočných právnych záruk, resp. pri nerešpektovaní právnej regulácie vyváženého vzťahu medzi recipientom a spravodajskou službou, je nebezpečenstvo vystavenia spravodajského zdroja odhaleniu najmä tam, kde sa uplatňujú prostriedky dokazovania spôsobom zavedeným pre právne rozhodovacie procesy.

Právne rozhodovacie procesy a ochrana spravodajského zdroja

Ako už bolo naznačené, azda najširšou oblasťou, v ktorej sa informácie z prostredia spravodajských služieb dostávajú do rizika legálneho vyzradenia, sú právne rozhodovacie procesy, v ktorých sa uplatňujú tradičné metódy a inštitúty dokazovania, a v ktorých v súlade s požiadavkami kladenými na riadne fungovanie právneho štátu je súčasne základnou „mantrou“ zachovanie práva na spravodlivý proces a rovnosť zbraní účastníkov konania. Okrem klasického modelu poskytovania informácií z poznatkovej bázy spravodajskej služby sa vývoj, najmä v oblasti rozhodovania orgánov činných v trestnom konaní a tiež orgánov verejnej správy uberá smerom prinášajúcim v tomto ohľade nové výzvy. Tieto sa týkajú najmä rastúcej tendencie využívať informácie zo spravodajskej proveniencie na tú časť štátno-správnych funkcií, v ktorých orgány štátnej správy rozhodujú o právach, právom chránených záujmoch a povinnostiach fyzických a právnických osôb. Deje sa tak najčastejšie prostredníctvom osobitným zákonom uloženej povinnosti spravodajskej služby poskytovať konajúcemu orgánu štátnej správy informácie vzťahujúce sa na vec, ktorá je predmetom konania, najmä informácií o účastníkovi konania. Práve v tejto oblasti dochádza ku konfliktu právom chránených záujmov. Na jednej strane je tu záujem na dosiahnutí účelu právneho rozhodovacieho procesu a na strane druhej na ochrane informácii, ktoré orgán realizujúci procesné úkony dokazovania považuje za podstatné pre dosiahnutie tohto účelu. To, čo možno na účel fungujúcej spravodajskej podpory ochrany a presadzovania záujmov štátu označiť za dostatočné, teda v anglickej terminológii „good enough“, nemusí nevyhnutne postačovať pre účely dokazovania skutočností, pri ktorých je poznanie

skutkového stavu veci potrebné preukázať bez dôvodných pochybností. Na druhej strane rovnako platí, že absencia dôkazu neznamená absenciu hrozby. Záujem na udržaní utajeného charakteru takýchto vstupov spravodajskej služby do právnych rozhodovacích procesov, vrátane zachovania zdroja spravodajských informácií, by však mal predstavovať významný korektív rozsahu i obsahu poskytovaných informácií. Na uvedenie príkladu môže, s využitím už ustálenej judikatúry, poslúžiť správno-právna úprava vo viacerých zákonoch účinných na úseku regulácie migračnej a azylovej politiky Slovenskej republiky. Podľa zákona č. 480/2002 Z. z. o azyle poskytuje Slovenská informačná služba na účely posudzovania žiadosti o udelenie azylu vyjadrenie vo veci žiadosti. Ide o príklad, v ktorom sa z poznatkového fondu spravodajskej služby dostáva do dispozície iného štátneho orgánu informácia, ktorá pochádza z evidencií spravodajskej služby a bola získaná spravodajskou činnosťou, t.j. prostredníctvom spravodajských zdrojov. Účelom je poskytnúť Migračnému úradu SR informačne dostatočne výpovedný podklad, ktorý prispieva k spoľahlivému zisteniu stavu veci, tak ako to vyžaduje dotknutá zásada správneho konania.[2] Ide predovšetkým o tú časť podkladu, ktorá má napomôcť konanie realizujúcemu správnemu orgánu uplatniť správne uváženie v otázke, či žiadateľ nepredstavuje nebezpečenstvo pre bezpečnosť Slovenskej republiky[3]. Ak v konaní o žiadosti dôjde k vydaniu rozhodnutia, pre ktoré je dôvodom pre zamietnutie žiadosti o udelenie azylu konštatovanie, že v osobe žiadateľa o takéto nebezpečenstvo ide, zákon ustanovuje, že v odôvodnení rozhodnutia sa uvedie iba skutočnosť, že „*ide o bezpečnostný záujem Slovenskej republiky*“. Obmedzenie rozsahu, inak správnym poriadkom vyžadovanej konkretizácie dôvodov, zaviedol zákon o azyle práve v snahe ochrániť utajené zdroje spravodajskej služby, z ktorých sa pre úvahu správneho orgánu potrebné informácie získali. Úmysel zákonodarcu v tomto smere bol opakovane predmetom súdneho prieskumu, pričom správne súdy v zásade nepopreli jeho legitimitu a ani legalitu, zároveň však vyslovili viaceré právne názory na požiadavky, za ktorých sa má v správnom konaní aplikovať. Súdy v prospech nielen ochrany spravodajských zdrojov, ale aj ochrany obsahu samotných informácií napr. ustálili, že námietky žalobcu o absencii náležitého odôvodnenia v prípade, že toto obsahovalo len konštatovanie existencie bezpečnostného záujmu Slovenskej republiky, nie sú dôvodné a tvrdeniam žalobcov nevyhoveli. Výslovne a opakovane judikovali, že „ *Dôvod takéhoto znenia predmetnej zákonnej úpravy (§ 52 ods. 2 zákona o azyle) je zrejmý - je to snaha zabrániť zverejneniu prameňov, z ktorých sa dospelo k poznatkom, podľa ktorých konkrétna osoba predstavuje nebezpečie pre bezpečnosť Slovenskej republiky. V prípade, ak by odôvodnenie administratívneho rozhodnutia, ktoré je svojím charakterom verejnou listinou, obsahovalo opis zisteného stavu, došlo by k odkrytiu zdroja poznatkov, samotnej masy poznatkov a spôsobu ich získania, čím by sa v konkrétnej veci zmarilo konanie príslušných štátnych orgánov a vo všeobecnosti by sa aj zverejnili postupy, používané na odhaľovanie konaní, ktoré môžu ohrozovať ústavné zriadenie, územnú celistvosť, zvrchovanosť a bezpečnosť Slovenskej republiky, ktoré vedú napr. k aktivite cudzích spravodajských služieb, k organizovaniu trestnej činnosti a terorizmu, resp. ktoré môžu vážne ohroziť alebo poškodiť hospodárske záujmy Slovenskej republiky.*“. [4]

---

[2]) §3 ods. 4 zákona č. 71/1967 Zb. o správnom konaní (Správny poriadok) v platnom znení.

[3]) §13 ods. 5 písm. a) zákona č. 480/2002 Z. z. o azyle., podľa ktorého sa azyl neudelí, ak „žiadateľa možno odôvodnene považovať za nebezpečného pre bezpečnosť Slovenskej republiky.“.

[4]) Napr. rozsudok KS BA 9Saz/7/2011-42 z 20. apríla 2011, rozsudok KS BA 9Saz/5/2011-27 zo 4. mája 2011.

Medzi povinnosti, ktoré správne súdy zároveň prikázali správnym orgánom v takýchto druhoch administratívnych konaní rešpektovať, je povinnosť správneho orgánu vyjadrenie spravodajskej služby založiť v príslušnom, na konanie sa vzťahujúcom administratívnom spise. Nevyhnutnosť takejto podmienky je právne odôvodnená, inak by zistenie skutkového stavu odporovalo obsahu administratívneho spisu a v prípade súdneho prieskumu by príslušné administratívne rozhodnutie muselo byť zrušené z dôvodu podľa § 250j ods. 3 O.s.p. t.j. pre neúplnosť spisu. Takáto povinnosť správneho orgánu je zároveň dôležitá pre konanie spravodajskej služby, ktorá, zodpovedajúc za ochranu spravodajských zdrojov, musí formulovať svoje vyjadrenie tak, aby ani pri jeho založení do administratívneho spisu - a to napriek jeho podriadeniu pod režim ochrany utajovaných skutočností, k jeho odkrytiu nedošlo.

V otázke prístupu k utajovanej skutočnosti, tvoriacej obsah vyjadrenia spravodajskej služby je zaujímavé poukázať napr. na výsledky rozhodovacej činnosti súdov v oblasti preskúmavania zákonnosti rozhodnutí vydávaných podľa zákona č 404/2011 Z. z. o pobyte cudzincov v znení neskorších predpisov. Súdy, okrem potvrdenia právneho názoru o povinnosti pripojiť utajované informácie do administratívneho spisu uznali, že tieto podliehajú špeciálnemu režimu utajovania a vylúčili, že nahliadanie do týchto podkladov pre rozhodnutie správneho orgánu, či už zo strany žalobcu, t.j. toho koho sa obsahovo týkajú, alebo jeho právneho zástupcu, je automatické. Odkazuje sa pritom na právne dovolenú možnosť jednorázového oboznámenia sa s utajovanou skutočnosťou, avšak rozhodnutie o uplatnení tejto možnosti súdy ponechávajú na „zvážení“ spravodajskej služby, ktorá je ich pôvodcom. Úvaha však ani tu nemôže byť svojvoľná a spravodajská služba musí vždy zohľadniť nielen záujem na utajení konkrétnej informácie, ale tiež záujem na predmete administratívneho konania. Na druhej strane, ak ide o obsah samotnej informácie z poznatkových fondov spravodajskej služby, je dôležité, že súdy dovodili právo žalobcu - predtým účastníka administratívneho konania, dozvedieť sa „*aspoň to, akých skutočností sa týka predmetné podozrenie“.*[5] Ochrany spravodajského zdroja sa v tomto okruhu predmetu súdneho prieskumu judikatúra nedotkla.

Seriózny prístup nielen spravodajských služieb, ale aj orgánov štátnej správy a preskúmavajúcich súdov je v otázke ochrany spravodajských zdrojov dôležitý a hodný ďalšej odbornej diskusie nielen z právneho, ale predovšetkým z hľadiska bezpečnostného. Ide predsa o oblasť, v ktorej sa spravodajský záujem zvyšuje zodpovedajúco rastúcim prejavom radikalizmu v komunitách cudzincov, ale samozrejme aj neznášanlivosti majoritného obyvateľstva voči minorite, či teroristickým útokom, namiereným proti samotnej podstate ústavných základov demokratického štátu a proti bezpečnosti všetkých jeho obyvateľov.

Previerky sudcovskej spôsobilosti a ochrana spravodajských zdrojov

V slovenskej vnútroštátnej úprave sa najnovším podnetom pre riziko stretu záujmu na ochrane spravodajských zdrojov so záujmom transparentného preukázania skutočností, ktoré tvoria obsah produkcie spravodajskej služby, môže stať proces preverovania tzv. sudcovskej spôsobilosti, ktorý zavádza na vykonanie novely Ústavy[6] Slovenskej republiky zákon č. 195/2014 Z. z. V podmienkach

[5]) Napr. Rozsudok KS BA 2S42/08-34 z 15. apríla 2009.
[6]) Ústavný zákon č. 161/2014 Z. z.

fungovania súdnej moci v Slovenskej republike ide nepochybne o jeden z najzávažnejších regulačných nástrojov, ktoré sa zákonodarná moc rozhodla v právnom poriadku SR presadiť. Bez ohľadu na opodstatnené otázky o miere jeho ústavnej a medzinárodnoprávnej prípustnosti[7] ide o právnu úpravu zakladajúcu ďalší priestor pre vznik rizika ohrozenia spravodajských zdrojov. Prijatie stanoviska Súdnej rady SR, či kandidát na vymenovanie za sudcu spĺňa predpoklady sudcovskej spôsobilosti, ktoré dávajú záruku, že funkciu sudcu bude vykonávať riadne sa v zmysle právnej úpravy opiera o podklady rozhodovania, ktoré na tento účel poskytuje Národný bezpečnostný úrad.[8] Zhromažďovanie informácií o sudcovi a o kandidátovi na sudcu podľa § 69a ods. 2 písm. b), c) a e) cit. zákona realizuje Národný bezpečnostný úrad v podstatnej časti z policajných a spravodajských poznatkových fondov. Národným bezpečnostným úradom vyhodnotené informácie sú v zmysle zákonnej úpravy podkladom pre rozhodovanie Súdnej rady SR o splnení predpokladov sudcovskej spôsobilosti. Pokiaľ ide o spravodajské služby, či už Slovenskú informačnú službu alebo Vojenské spravodajstvo, ale aj Policajný zbor, tieto sú povinné v určenej lehote žiadosti Národného bezpečnostného úradu vyhovieť. Ide o právne správne konštruovanú povinnosť, zodpovedajúcu účelu zákonnej právomoci Národného bezpečnostného úradu. Čo však v súvislosti s ochranou spravodajských zdrojov vyvoláva obavu, je ustanovenie druhej vety § 69 a ods. 4 cit. zákona *in fine,* podľa ktorého sú tieto orgány povinné Národnému bezpečnostnému úradu „*umožniť nahliadnutie do písomných materiálov, z ktorých informácie úradu poskytli*.“. V prípade Slovenskej informačnej služby sa evidenciami, z ktorých spravodajská služba relevantné informácie poskytuje, rozumejú evidencie vytvárané a vedené podľa § 17 zákona NR SR č. 46/1993 Z. z. o Slovenskej informačnej službe. Za zmienku stojí, že tu ide o povinnosť spravodajských služieb, ktorá je koncipovaná extenzívnejšie, než v prípade poskytovania súčinnosti pri výkone pôsobnosti Národného bezpečnostnému úradu na úseku bezpečnostných previerok. Súdna rada SR je pred prijatím rozhodnutia o splnení predpokladov sudcovskej spôsobilosti povinná umožniť kandidátovi na vymenovanie za sudcu vyjadriť sa k zisteniam vyplývajúcim z podkladov, ktoré jej boli na tento účel zabezpečené Národným bezpečnostným úradom.[9] Hoci v tomto prípade nejde o súdny rozhodovací proces, možno mať zato, že napriek tomu ide o jeden zo základných pilierov spravodlivého konania uplatňovaný v právnom štáte. Otáznym sa preto stáva spôsob realizácie podmienky, ktorú ako akýsi limitujúci korektív prikazuje zákon pre aplikačnú prax, a ktorý vyžaduje, aby pritom „nedošlo k zásahu do práv tretích osôb a nebol ohrozený zdroj informácií“.[10] Zákon tak síce uznal existenciu rizika ohrozenia zdroja v tomto prípade, ako aj možnosť neželanej ingerencie do práv iného, ale uplatňovanie prijatého zákonného obmedzenia ponechal na aplikačnú prax.

Obdobne si v tejto súvislosti vyžadujú ďalšiu pozornosť s ohľadom na ochranu spravodajských zdrojov ustanovenia týkajúce sa rozsahu podkladov pre konanie

[7]) Napr. Uznesenie Pléna NS SR z 10. júna 2014, uznesenie Súdnej rady Slovenskej republiky č. 299 zo 16. Júna 2014.
[8]) § 69a zákona č. 215/2014 Z. z. v znení zákona č. 195/2014 Z. z.
[9]) § 27ga ods. 5 zákona 185/2002 Z. z. v znení zákona č. 195/2014 Z. z.
[10]) Tamtiež.

o sťažnostiach proti uzneseniu Súdnej rady SR vo veci spĺňania predpokladov sudcovskej spôsobilosti podľa osobitného zákona.[11]

Vzhľadom na krátkosť času účinnosti a tiež vzhľadom na už začaté konanie o súlade právnych predpisov pred Ústavným súdom Slovenskej republiky[12] - a to vo veci súladu viacerých ustanovení zákona č. 195/2014 Z. z., a súvisiacich ustanovení osobitných zákonov[13] s dotknutými ustanoveniami Ústavy Slovenskej republiky, nie je zatiaľ možné pri identifikácii rizík pre spravodajské zdroje vychádzať zo skúseností z aplikačnej praxe, a ani zo záverov súdnej adjudikácie, ale rozbor príslušných zákonných ustanovení nasvedčuje ich reálnej existencii a bude nepochybne predstavovať výzvu pre spravodajské služby, Súdnu radu Slovenskej republiky, Národný bezpečnostný úrad a tiež súdny prieskum v budúcnosti.

Rovnosť zbraní a prekážka poskytnutia informácií z prostredia spravodajskej služby

Už viackrát spomenutá utajenosť zberu informácií je podstatnou črtou práce spravodajskej služby bez ohľadu na to, čo je v konkrétnom prípade objektom spravodajského záujmu a aké prostriedky sa pritom použijú. V tejto súvislosti však treba pripomenúť, že takýto charakter práce nie je vlastný výlučne spravodajským službám, ale aj orgánom ochrany a presadzovania práva, napríklad orgánom činným v trestnom konaní. Ako príklad možno uviesť použitie informačno-technických prostriedkov či iných prostriedkov sledujúcich zabezpečenie informácií, ktoré sa aj podľa slovenskej trestnoprávnej úpravy či osobitného zákona[14], vykonáva utajene.[15] Samozrejme, že nielen proces získavania informácií je utajovaný, ale spravidla aj rezultát tejto činnosti tvorí utajovanú skutočnosť,[16] čo môže taktiež vyvolať závery o existencii prekážky pre možnosť prípustnosti spravodajskej informácie ako dôkazu v trestnom konaní. Ide napríklad o problém oboznamovania sa obvineného, resp. obžalovaného a jeho obhajcu s obsahom dôkazu, ktorý by bol utajovanou skutočnosťou.

---

[11]) § zákon NR SR č. 38/1993 Z. z. o organizácii Ústavného súdu Slovenskej republiky, o konaní pred ním a o postavení jeho sudcov v znení neskorších predpisov.

[12]) Uznesenie Ústavného súdu SR o prijatí návrhu predsedníčky Súdnej rady SR, vedené pod. sp. zn. 1. PL. ÚS 21/2014, zverejnené tl. info. Č. 67/2014 zo 17. septembra 2014.

[13]) Zákon č. 38/1993 Z. z. o organizácii Ústavného súdu Slovenskej republiky, o konaní pred ním a o postavení jeho sudcov v znení neskorších predpisov, zákon č. 185/2002 Z. z. o Súdnej rade Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 215/2004 z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[14]) Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

[15]) § 113 a nasl. TrP § 2 ods. 1 zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

[16]) Podľa § 2 písm. a) zákona č. 215/2004 Z. z. utajovanou skutočnosťou je informácia alebo vec určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred neoprávnenou manipuláciou, ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda Slovenskej republiky svojím nariadením. Samotnú informáciu zákon definuje ako obsah písomnosti, nákresu, výkresu, mapy, fotografie, grafu alebo iného záznamu, obsah ústneho vyjadrenia, obsah elektrické elektromagnetického, elektronického alebo iného fyzikálneho transportného média. Utajovanou skutočnosťou môže byť aj vec - a to hmotný nosič so záznamom informácií, výrobok, zariadenie alebo nehnuteľnosť.

Treba uznať, že tu ide o závažný problém ústavne garantovaného práva na účinnú obhajobu.[17] Bez znalosti obsahu informácie majúcej vzťah k predmetu obvinenia nemožno naplniť ani jednu zo základných zásad trestného konania podľa § 2 ods. 7 TrP. Právna úprava musí zaistiť rovnosť zbraní medzi obžalobou a obhajobou, inak nemožno trestný proces považovať za spravodlivý. Nemožno však konštatovať, že slovenská právna úprava neprináša žiadne riešenie vzťahu medzi verejným záujmom na utajení určitých skutočností a individuálnym právnym záujmom jednotlivca, proti ktorému sa vedie trestné konanie.

Účinná administratívnoprávna úprava na úseku ochrany utajovaných skutočností umožňuje, aby sa napr. obvinený a jeho obhajca oboznámili s utajovanou skutočnosťou v rozsahu nevyhnutne potrebnom pre jej využitie, pričom vtedy požívajú status tzv. inej oprávnenej osoby. Zákon od iných oprávnených osôb nevyžaduje splnenie podmienok, ktoré musia inak spĺňať osoby oprávnené na oboznamovanie sa utajovanými skutočnosťami.[18] Dotknutá právna úprava sa vzťahuje na všetky utajované skutočnosti - vrátane tých, ktorých pôvodcom je spravodajská služba a ktoré obsahujú spravodajské informácie. Právna ochrana takýchto informácií pred ich ďalším sprístupnením nepovolaným osobám sa zabezpečuje formou vyhlásenia o mlčanlivosti a poučením o povinnostiach pri ochrane utajovaných skutočností a možných dôsledkoch ich porušenia. Orgán činný v trestnom konaní, resp. súd, ktorý konanie uskutočňuje, je prípad takého oboznámenia obvineného, resp. obhajcu povinný písomne notifikovať Národnému bezpečnostnému úradu a pôvodcovi utajovanej skutočnosti, napr. spravodajskej službe.[19]

Máte povinnosť mlčať!

Notoricky známa veta „máte právo mlčať“, ktorá vychádzajúc z pozitívno-právne garantovaného práva na právnu ochranu a ktorej účel je eliminovať hrozbu „sebakriminalizácie“, sa v prípade špecifického okruhu osôb, ktorých zamestnanie, povolanie, funkcia alebo osobitný vzťah poskytovania informácii alebo pomoci v prospech spravodajskej služby transformuje súčasne na zákonom uloženú povinnosť mlčať. Na rozdiel od „práva mlčať“ však účelom touto povinnosťou konštituovanej právnej ochrany nie je individuálny záujem toho, kto je ňou viazaný, ale objektom ochrany je verejný záujem. Táto právna povinnosť korešponduje s „právom štátu mlčať“ a sú ňou viazané špeciálne subjekty, ktorých vzťah k štátu zohľadňuje ich pracovnoprávny status - a teda je daný povolaním, zamestnaním, funkciou či ich participáciou na plnení štátnych funkcií právne upraveným spôsobom iným spôsobom. Vo vzťahu k otázke ochrany spravodajských zdrojov to predovšetkým znamená, že príslušníci spravodajskej služby sú viazaní zákonom ustanovenou povinnosťou zachovať mlčanlivosť o skutočnostiach, o ktorých sa dozvedeli v súvislosti s činnosťou spravodajskej služby.

V prípade, že ide o mlčanlivosť vzťahujúcu sa na skutočnosti, o ktorých sa má mlčať v záujme štátu, poskytuje právo túto formu ochrany pred vyzradením či už legálnym alebo nelegálnym dvom zásadným kategóriám informácii. Prvou kategóriou sú utajované skutočnosti a druhou kategóriou sú skutočnosti, o ktorých povinnosťou zaviazaný subjekt nadobudol vedomosť v súvislosti s činnosťou spravodajskej

[17] Čl. 50 ods. 3 Ústavy SR v spojení s čl. 48 ods. 2.
[18] § 35 ods. 2 zákona č. 215/2004 Z. z.
[19] § 35 ods. 4 zákona č. 215/2004 Z. z. a § 161 Trestného poriadku.

služby. Informácie, ktoré sú výsledným produktom spravodajskou službou plnených úloh, sú *per se* objektom právnej ochrany prostredníctvom povinnosti mlčanlivosti a ďalších administratívnych, organizačných, technických či personálnych opatrení zameraných na ich udržanie v tajnosti. *In generalis* sú však určené na legálnu diseminácia do dispozičnej sféry ich zákonných príjemcov. Do oboch spomenutých kategórii informácii právne chránených pred vyzradením však patrí nielen tento druh informácii. Patria sem i informácie obsahovo pokrývajúce spôsob, akým spravodajská služba k získaniu spravodajských informácii dospela. Ide teda o informácie, kto alebo čo bolo zdrojom, z ktorého spravodajská služba získala prinajmenšom vstupné údaje na vytvorenie finálnej spravodajskej produkcie. Na účinné udržanie informácii vzťahujúcich sa na identifikáciu spravodajských zdrojov v tajnosti sú spravodajské služby zvlášť citlivé.

Slovenská zákonná úprava povinnosti zachovávať mlčanlivosť je koncipovaná spôsobom, ktorý sa usiluje právne zaručiť nielen zachovanie tajomstva v záujme štátu, ale aj v záujme fyzických a právnických osôb.[20] Zohľadnenie ochrany individuálneho záujmu prostredníctvom povinnosti zachovávania mlčanlivosti je rozhodujúcou právnou reštrikciou pre spravodajských dôstojníkov vyzradiť okrem iného aj informácie o ľudských spravodajských zdrojoch bez porušenia zákona.

Okrem vzniku následkov v služobno-právnej oblasti je porušenie povinnosti mlčanlivosti o utajovanej skutočnosti tiež kriminalizované prostredníctvom skutkových podstát trestných činov zameraných na ochranu bezpečnosti republiky a ochranu poriadku vo verejných veciach[21] Pri porušení povinnosti mlčanlivosti nedovoleným vyzradením spravodajského zdroja nemožno vylúčiť naplnenie znakov aj ďalších skutkových podstát trestných činov, napr. sabotážneho charakteru.

Anglo-americký príklad dôslednosti pri ochrane osobitne ľudských spravodajských zdrojov tradične vyzdvihuje význam ich trestnoprávnej ochrany - a to napriek zásade *ultima ratio* trestného práva. V zmysle ustanovení o trestných sankciách, ktoré sú súčasťou národno-bezpečnostnej úpravy v Spojených štátoch amerických[22], je vedomé spôsobenie vyzradenia identity agenta v utajení osobou, ktorej táto identita stala známou na základe povolenia oboznamovať sa s utajovanými skutočnosťami neoprávnenej osobe, penalizované finančným trestom alebo trestom odňatia slobody, pričom pripúšťa sa aj súbeh oboch druhov trestov. [23]

Na rozdiel od v zahraničí známych nástrojov trestného postihu nedovoleného vyzradenia spravodajských zdrojov v podobe osobitnej právnej úpravy kriminalizácie takého konania páchateľa, slovenská hmotnoprávna úprava takúto možnosť neposkytuje.

Tiež treba v tejto súvislosti pripomenúť, že vzhľadom na slovenskú právnu úpravu, povinnosťou mlčanlivosti však nie sú viazaní len príslušníci spravodajskej služby, ale nositeľom je každý, kto plní úlohy spravodajskej služby podľa zákona. Všeobecným spôsobom koncipovaný nositeľ tejto právnej povinnosti tak zaisťuje, že sa tak vzťahuje aj na osoby konajúce v prospech spravodajskej služby. Ak teda uvažujeme o ochrane ľudského spravodajského zdroja, je zrejmé, že na tejto ochrane sa prostredníctvom inštitútu legálnej mlčanlivosti podieľa aj samotný zdroj.

---

[20]) Porov. § 23 ods. 1 zákona NR SR č. 46/1993 Z. z.
[21]) § 318 a 319, § 353 Trestného zákona.
[22] National Security Act, Sec. 601. /50 U.S.C. 421/- Protection of identities of certain United States undercover intelligence officers, agents, informants and sources, 1947.
[23])Tamtiež.

Vec právom chránenej dôvery

Na rozdiel od iných druhov spravodajských zdrojov je v prípade HUMINT-u nevyhnutné, aby sa medzi spravodajskou službou a osobou dobrovoľne konajúcou v jej prospech vytvoril vzťah dôvery a aby táto dôvera trvala nielen počas celého času trvania tajnej spolupráce, ale aj po jeho ukončení. Nie jedinou, zato však podstatnou súčasťou tejto dôvery je na strane osoby konajúcej v prospech presvedčenie, že spravodajská služba je schopná zaistiť svojmu tajnému spolupracovníkovi ochranu - a to predovšetkým v podobe utajenia jeho identity a faktu, že v prospech spravodajskej služby koná.

Potreba utajovať je tak nielen vo výlučnom záujme spravodajskej služby, ale tiež prostriedkom ochrany individuálnej bezpečnosti nositeľa spravodajsky relevantnej informácie. V anglo-americkej odbornej terminológii sa vo vzťahu k HUMINT-u akcentuje potreba rešpektovať utajenosť tohto druhu spravodajského zdroja pripájaním adjektíva „covert“, čiže niečo, čo má zostať skryté a k čomu sa otvorene nemá nikto a nič priznávať. Bez ohľadu na riziká späté s ľudskými vlastnosťami, ktoré u každého človeka, vrátane „agentov“ spravodajských služieb determinujú spoľahlivosť a mieru objektivity tohto spravodajského zdroja, je tradične počas celého dejinného vývoja spravodajskej činnosti neodmysliteľnou súčasťou škály spravodajských nástrojov. Jeho „ľudskosť“, ktorá je faktorom občas skôr znižujúcim hodnotu jeho výstupu pre službu, je naopak, faktorom nepochybne zvyšujúcim jeho vlastnú hodnotu a jej ochrana je podstatnou súčasťou zodpovednosti každej spravodajskej služby.

Dôvera, ktorú vkladá osoba dobrovoľne poskytujúca servis v prospech spravodajskej služby, je na rozdiel od iných spravodajských zdrojov, ako napr. SIGINT či OSINT unikátnym charakteristickým znakom tohto druhu zdroja. Odhalenie, či už právom dovolené alebo nedovolené, nemá len nepriaznivé následky voči konkrétnej osobe, ale nepriaznivo ovplyvňuje spôsobilosť spravodajskej služby získavať alebo udržať ďalšie osoby konajúce v jej prospech a tak budovať, resp. zachovať existujúcu agentúrnu sieť. Zásadné oslabenie tejto spôsobilosti by vzhľadom na význam tohto druhu informačno-operatívneho prostriedku pre efektivitu spravodajskej služby mohlo privodiť ujmu na všetkých, spravodajskou podporou zabezpečených záujmoch štátu. Pre spravodajské služby, ktorých operačný záber je navyše v súlade so záujmami ich štátu obmedzenejší čo do rozsahu cieľov aj zdrojov, a ktorých spôsobilosť využívať iné, vo všeobecnosti logisticky a finančne náročnejšie spravodajské zdroje, je tak prirodzene limitovanejšia, stáva sa ľudská agentúrna sieť akýmsi „rodinným striebrom“.

Vecná podstata spočívajúca v dôvodoch legitimizujúcich utajenie ľudských zdrojov a spojená s ochranou zaručenej anonymity osoby konajúcej v prospech spravodajskej služby však nie je zachovaná, ak by sa potreba utajovať zároveň dostatočne netransformovala do podoby právnej garancie jej zachovania. Účinnú právnu ochranu ľudského spravodajského zdroja nemožno, vzhľadom na zvýšené riziko jej ohrozenia v prípade odhalenia jej identity dosiahnuť prostredníctvom všeobecnej zákonnej bázy ponúkanej právnou úpravou ochrany osobných údajov.[24] Ide o špeciálny subjekt vyžadujúci si tak nevyhnutne aj špeciálny, nadstavbový režim právnej ochrany. Vo formálnom zmysle je nepochybné, že prameňom pozitívneho

[24]) Zákon č. 122/2013 Z.z. o ochrane osobných údajov v znení zákona č. 84/2014 Z. z.

práva pre tento osobitný režim právnej reglementácie je súčasťou predmetu úpravy osobitných prostriedkov, ktoré sú zákonom zverené do legálnej dispozície spravodajskej služby. V uvedenom zmysle zákonná úprava výslovne zakotvuje utajenie spolupráce medzi ľudským zdrojom a spravodajskou službou a spoločne s požiadavkou dobrovoľnosti ho vymedzuje ako materiálny pilier pozitívnej legálnej definície ľudského zdroja.[25] Tento definičný znak spravodajského ľudského zdroja pokrýva nielen fakt existencie vzťahu tajnej spolupráce ako takej, ale predovšetkým chráni právne aprobovaným inštitútom utajenia totožnosť osoby, ktorá poskytuje spravodajskej službe pri plnení jej zákonných úloh svoje služby. Význam, ktorý právo kladie tejto forme ochrany osôb konajúcich v prospech spravodajskej služby je vyjadrený v pozitívnom právnom záväzku uloženom spravodajskej službe zabezpečiť ochranu tohto, ako aj ďalších druhov spravodajských zdrojov pred vyzradením a zneužitím. [26]

Výhrada dôležitého záujmu spravodajskej služby ako prekážka spravodlivosti?

Možnosťou, či nedôjde k ohrozeniu zdrojov, zmareniu prebiehajúcej operatívnej činnosti, odkrytiu utajených foriem a metód jej práce, a to s priamou alebo nepriamou implikáciou na bezpečnostné záujmy štátu, sa má vždy spravovať úvaha spravodajskej služby pri rozhodovaní o poskytnutí spravodajskej produkcie do externého prostredia. Azda tradične najťažším a spoločensky aj právne najcitlivejším prípadom je oblasť súčinnosti v oblasti odhaľovania, vyšetrovania trestnej činnosti a zisťovania jej páchateľov. Hoci viac-menej v doktrinálnom aj empirickom prístupe prevláda správnosť presvedčenia o potrebe separácie spravodajskej služby od sústavy orgánov činných v trestnom konaní, nemožno poprieť, že úloha spravodajskej služby pri obstarávaní dôkazov v oblastiach odhaľovania určitých druhov trestnej činnosti je nenahraditeľná. Trestné činy, ktoré patria už tradične do okruhu spravodajského záujmu, ako vyzvedačstvo, sabotáž, teror, úklady proti štátu, terorizmus, t.j. trestné činy, ktorých objektom sú základy štátu a jeho vlastná bezpečnosť, patria do takej oblasti kriminalizovaných skutkov, pri ktorých úplné vylúčenie spravodajskej služby z procesu obstarávania dôkazov zásadne znižuje spôsobilosť štátu dosahovať potrebnú úroveň vlastnej trestnoprávnej ochrany.

Či už v rámci podpory orgánov činných v trestnom konaní, alebo v prípade priameho zapojenia spravodajskej služby do procesu obstarávania dôkazov však vzniká otázka spojená s ochranou spravodajských zdrojov. Tak spravodajská služba, ako aj orgány činné v trestnom konaní musia v rámci symbiotického pôsobenia v oblasti boja proti kriminalite riešiť bolestivú dilemu, pretože čím viac obsažnejších informácii s dôkaznou relevanciou z prostredia spravodajskej služby pochádza, tým väčšie je riziko ohrozenia spravodajských zdrojov. Nielen z vecného hľadiska, ale tiež pri právnom nazeraní na túto dilemu sa do vzájomnej kolízie dostávajú dva dôležité verejné záujmy, oba však vybavené zákonnou ochranou.

Poskytovanie spravodajských informácií o trestnej činnosti orgánom činným v trestnom konaní slovenský zákonodarca upravil v osobitnom ustanovení § 2 zákona o SIS, a to oddelene od režimu poskytovania informácií orgánom politickej decíznej sféry.

---

[25]) Napr. § 11 ods. 4 zákona č. 46/1993 Z. z.
[26]) Napr. § 10 ods. 2 zákona č. 46/1993 Z. z.

Akcent na ochranu toho, čo má vo vyššom, ale výlučne zákonom uznanom záujme zostať utajené - a to dokonca aj pred orgánmi činnými v trestnom konaní - nachádza svoje legislatívne vyjadrenie v ustanovení § 2 ods. 7 zákona o SIS. Slovenskej informačnej službe sa tu ukladá povinnosť vždy pred poskytnutím spravodajských informácií skúmať, či dôsledkom poskytnutia spravodajskej informácie nevznikne ohrozenie, medzi iným, aj spravodajských zdrojov. Podstata realizácie tejto zákonnej povinnosti spravodajskej služby spočíva v uplatnení obligatórnej úvahy o nielen naplnení zákonom dovoleného účelu poskytnutia spravodajskej produkcie konkrétnemu príjemcovi[27], ale v prípade informácií o trestnej činnosti, aj o existencii zákonom vymedzených vnútro-bezpečnostných obmedzení pre uvoľnenie informácie do prostredia polície a prokuratúry. Ak by malo poskytnutie spravodajskej informácie za následok ohrozenie zákonom aprobovaného vnútro-bezpečnostného záujmu (napr. osoby konajúcej v prospech služby, metód či foriem činnosti a pod.), zákon postihuje takýto prípad zákazom uvoľnenia spravodajskej informácie do externého prostredia. Podobný právny režim možno nájsť aj v práve iných európskych štátov s porovnateľnou právnou úpravou spravodajských služieb.[28] V tomto kontexte sa samozrejme naskytuje viacero otázok zasahujúcich do právneho režimu súčinnosti štátnych orgánov tak ako je tento upravený § 3 TrP.

Uvoľnenie spravodajskej informácie na účel trestného konania však, vzhľadom na zásady spravodlivého prejednania veci[29] a najmä zásadu rovnosti zbraní[30] a kontradiktórnosti konania, vždy vedú k vzniku rizika, že utajovaný obsah spravodajskej informácie bude vystavený možnosti sprístupnenia obvinenému a ďalším osobám, ktorým takýto prístup trestno-procesná úprava inak musí garantovať.

V tejto súvislosti sa azda dá len zopakovať rutinné vyjadrenie, že riešenie nie je univerzálne a vždy si vyžaduje osobitný prístup so zohľadnením konkrétnych okolností. Spoločne s otázkou prístupu strany, proti ktorej sa vedie trestné konanie k utajovaným informáciám, a ktorých odhalenie v konaní naráža na bezpečnostný záujem, možno sa však pri riešení inšpirovať aj výsledkami rozhodovacej činnosti Európskeho súdu pre ľudské práva v Štrasburgu.

Ako učebnicový príklad možno citovať rozsudok Európskeho súdu pre ľudské práva v prípade Fitt proti Spojenému kráľovstvu zo 16. februára 2000, týkajúci sa sťažnosti č. 29777/96, či v prípade Jasper proti Spojenému kráľovstvu, týkajúci sa sťažnosti č. 27052/95. V konaniach o sťažnostiach sa súd musel okrem iného zaoberať otázkou možnosti utajiť pred obhajobou určité dôkazy a podmienkami, za ktorých platná úprava záruk spravodlivého procesu, tak ako sú tieto zakotvené v Európskom dohovore o ľudských právach a základných slobodách, akceptuje takéto utajenie dôkazov za právne únosné.

V zmysle čl. 6 ods. 1 Dohovoru sa vyžaduje, aby orgány činné v trestnom konaní oznámili obhajobe všetky relevantné dôkazy, ktoré majú k dispozícii, ako v prospech, tak aj v neprospech obžalovaného. Vo vzťahu k takto zaručenému právu však bol zároveň vyslovený záver, že právo na oznámenie relevantných dôkazov nie

---

[27]) § 2 ods. 7 prvá veta zákona NR SR č. 46/1993 Z. z.

[28]) Napr. podľa § 8 ods. 3 zákona č. 153/1994 Sb. o zpravodajských službách v Českej republike - „Zpravodajské služby předávají policejním orgánum informace o zjištěních, která náleží do oboru jejich pusobnosti, to neplatí, jestliže by poskytnutí ohrozilo duležitý zájem sledovaný příslušnou zpravodajskou službou“.

[29])§ 2 ods. 7 Trestného poriadku

[30]) Čl. 47 ods. 3 Ústavy Slovenskej republiky, § 2 ods. 14 Trestného poriadku.

je absolútne. V podstate bol judikovaný právny záver, že povinnosť orgánov činných v trestnom konaní oznámiť dôkazy obhajobe je právne konformným spôsobom obmedzená. Ide v podstate o prípad konkurujúcich si záujmov. Z pohľadu Dohovorom zaručeného práva na spravodlivý proces bolo akceptované, že v niektorých prípadoch môže byť nevyhnutné zatajiť obhajobe určité dôkazy. Súd pripustil, že k zatajeniu dôkazov pred obhajobou môže dôjsť vtedy, ak v konkrétnom prípade prevládne iný, konkurujúci záujem, pričom ide buď o individuálny záujem na ochrane základných práv iného jednotlivca, alebo o dôležitý verejný záujem. Vzhľadom na takýto záver je podstatné zaoberať sa jednak vymedzením dôležitého verejného záujmu a jednak podmienkami, za splnenia ktorých tento záujem prevládne. Na prvom mieste v rámci identifikácie takéhoto dôležitého verejného záujmu bola uznaná národná bezpečnosť. Z pohľadu dôkazov, ktoré by boli reprezentované napr. spravodajskými informáciami majúcimi vzťah k predmetu trestného konania a zároveň k národnej bezpečnosti, je takýto záver rozhodujúci.

Veľmi významnou časťou právneho názoru súdu v citovaných prípadoch sťažností je požiadavka na dostatočnú kompenzáciu všetkých ťažkostí spôsobených obhajobe v dôsledku obmedzenia jej práva na prístup k niektorým dôkazom z dôvodu dôležitého verejného záujmu, a to postupom sledovaným súdnymi orgánmi. Významnou zárukou tu je možnosť a povinnosť sudcu posudzovať v každom momente konania nutnosť oznámenia dôkazov obhajobe. Súd vychádzal z toho, že sudca uskutočňujúci konanie má povinnosť počas celého procesu verifikovať, či utajenie dôkazov nebolo v rozpore so spravodlivosťou. Samozrejme, že splnenie týchto podmienok si vyžaduje, pokiaľ ide o samotné utajené dôkazy,, aby sudca bol vždy oboznámený so všetkými dôkazmi a mal k dispozícii zrozumiteľné dôvody, pre ktoré si dôležitý verejný záujem na utajení dôkazu vyžaduje zamedzenie prístupu obhajoby. Sudca musí mať prístup aj k dôkazom, ktoré sú utajovanou skutočnosťou.

V rámci administratívnoprávnej úpravy ochrany utajovaných skutočností v Slovenskej republike sudcovi takýto prístup zaručuje aj status osoby s osobitným postavením podľa § 34 ods. 1 písm. f) zákona o ochrane utajovaných skutočností. V prípade spravodajských informácií je potrebné upozorniť na fakt, že vyššie vysvetlené prekážky poskytnutia spravodajských informácií podľa § 2 ods. 7 zákona o SIS sa týkajú orgánov činných v trestnom konaní, nie však súdu. Zároveň súd je jediným externým subjektom so zákonne garantovaným prístupom k spravodajským informáciám, uloženým spravodajskou službou v jej evidenciách a informačných systémoch podľa § 17 ods. 3 cit. zákona o SIS.

Druhým predpokladom je uvedenie dôvodov utajenia. Ak by dôkazom v konaní mala byť spravodajská informácia utajená v súlade so záujmom štátu na ochrane národnej bezpečnosti, samotné konštatovanie pôvodcu (napr. spravodajskej služby) o existencii záujmu na ochrane národnej bezpečnosti nepostačuje na uznanie tohto dôvodu za faktor určujúci nevyhnutnosť obmedzenia prístupu obhajoby k nemu. Dôvody, ktoré by mal mať súd k dispozícii v tejto súvislosti, by mali zrozumiteľne identifikovať ujmu, ktorá by odhalením takého dôkazu obhajobe reálne ohrozila bezpečnostné záujmy štátu. V rámci slovenského právneho poriadku možno tu vychádzať zo zákonného vymedzenia jednotlivých stupňov utajenia skutočností, ktoré majú byť chránené v záujme štátu. Napr. ak by išlo o informáciu so stupňom utajenia „Tajné“, mohlo by jej odhalenie obhajobe spôsobiť ohrozenie zahraničnopolitického postavenia, obrany, bezpečnosti a záujmov štátu v medzinárodnej a ekonomickej oblasti, a tým by mohla vzniknúť vážna ujma záujmom Slovenskej republiky. Pôvodca by v tomto prípade mal súdu predložiť také vecne

špecifikované súvislosti či okolnosti, aby tento mohol uplatniť kvalifikovanú úvahu o riešení konkurenčných záujmov v celom priebehu konania. Len ich dostatočná znalosť totiž umožní súdu splnenie požiadavky na zaistenie spravodlivého procesu aj v prípade prevahy dôležitého verejného záujmu na utajení dôkazu nad individuálnym záujmom obhajoby.

Slovenská trestno-procesná úprava primárne vychádza z rešpektovania verejného záujmu na utajovaní niektorých informácií, resp. iných skutočností (napr. vecí a objektov). Deje sa tak napriek tomu, že sú dôležité pre trestné konanie, napr. prostredníctvom zákazu výsluchu svedka alebo výnimkou z povinnosti predložiť listinu alebo vec dôležitú pre trestné konanie, ak sa jej obsah týka okolnosti, na ktorú platí zákaz výsluchu svedka. Zámer zákonodarcu rešpektovať takýto záujem možno vidieť aj v ďalších ustanoveniach Trestného poriadku, najmä ustanovením výnimky zo zásady verejnosti súdneho konania, zákazu vyhotovovať zvukové alebo obrazové záznamy a písomné poznámky zo strany predsedu senátu, či požiadavky na prijatie opatrení, aby boli zachované utajované skutočnosti pri nazeraní do spisov. Na druhej strane však zároveň umožňuje prostredníctvom uplatnenia inštitútu oslobodenia od povinnosti mlčanlivosti dosiahnuť výpoveď svedka, inak zaviazaného povinnosťou mlčanlivosti o utajovaných skutočnostiach, alebo napr. vydanie veci, ak dôjde k oslobodenie od povinnosti zachovať vec v tajnosti.

V prípade informácií a vecí, ktorých pôvodcom, resp. držiteľom je spravodajská služba, možno citovať už spomenutú právnu úpravu zákona o SIS. Podľa § 23 ods. 2 zákona o SIS je riaditeľ oprávnený rozhodovať o zbavení mlčanlivosti príslušníkov služby, ako aj každého, kto plnil úlohy spravodajskej služby a je zaviazaný zachovávať mlčanlivosť o skutočnostiach, ktoré sa v tejto súvislosti dozvedel. Riaditeľ Slovenskej informačnej služby tak môže urobiť na základe žiadosti orgánov činných v trestnom konaní. Ak ide v trestnom konaní o výsluch svedka, je oprávnenie riaditeľa Slovenskej informačnej služby uplatniť úvahu pri rozhodovaní o oslobodení od povinnosti mlčanlivosti obmedzené. Dôvody odopretia oslobodiť takúto osobu od povinnosti zachovávať mlčanlivosť o utajovanej skutočnosti sa môžu zakladať len na ohrození obrany štátu alebo bezpečnosti štátu, alebo hrozbe inej rovnako vážnej škody.[31] Zákon vtedy ukladá povinnosť uviesť dôvody na odopretie oslobodenia.

V práve Slovenskej republiky došlo v otázkach právnej regulácie na úseku získavania informácií nevyhnutných na zamedzovanie a odhaľovanie trestnej činnosti ako aj obstarávanie dôkazov v spojení s prácou nielen orgánov činných v trestnom konaní, ale aj celého bezpečnostného aparátu štátu k významným zmenám. Tieto zmeny v porovnaní s predchádzajúcim právnym stavom znamenali extenziu právne konzistentných dôkazných prostriedkov získavaných na širšom zákonnom základe ako poskytuje trestno-procesná úprava.

Záver

Štát je sprevádzaný počas svojej existencie prácou spravodajcov rovnako dlho, ako je jeho fungovanie spojené s potrebou tvorby a ochrany vlastného práva. Pre nás, ktorí sme sa rozhodli venovať svoj profesijný život práci pre štát - a to práve v jeho spravodajských službách - je nepochybne dobrou správou, že kým tu bude štát, budú tu aj spravodajské služby. Rovnako pozitívne je, že štát si

[31] § 129 ods. 1 Trestného poriadku.

s presadzovaním hodnôt, na ktorých je postavený, stále viac uvedomuje potrebu zodpovednej právnej regulácie aj takej dôležitej oblasti, ako je oblasť činnosti spravodajských služieb. A hoci nie je táto činnosť často pod ťarchou negatívnej skúsenosti občanov z totalitnej minulosti štátu, alebo jednoducho pre rôzne zlyhania spravodajskej služby, ktoré sa stali verejne známymi, vnímaná vždy kladne, je dôležité, aby spravodajské služby efektívne ochránili záujmy, na ktorých ochranu boli zriadené. Rovnako dôležité však je to, aby ich efektivita nedominovala nad legalitou, ale aby oba tieto základné princípy spravodajskej činnosti zostali v rovnovážnom a vzájomne sa podporujúcom vzťahu. Funkciou spravodajských služieb je chrániť štát a právo a funkciou práva je tiež poskytnúť spravodajským službám ochranu predovšetkým toho, čo je pre ne najdôležitejšie, a tým sú ich utajené zdroje. Aj tento príspevok mal ambíciu prispieť k širšej diskusii o tom, kde sa v slovenských podmienkach schopnosti obidvoch týchto funkcií nachádzajú a aké sú možné výzvy pre ich zlepšenie v budúcnosti.

I. Cibula: Legendovanie ako spôsob ochrany spravodajských zdrojov

PhDr. Igor Cibula *(1942) – Publicista, expert v oblasti spravodajských služieb. Ako spravodajský dôstojník začínal na 1.správe FMV (1968-1970). Po rehabilitácii v roku 1990 pokračoval v spravodajskej kariére na Úřade pro zahraničné styky a informace. V období 1993-1995 bol riaditeľom rozviedky SIS. V rokoch 2006-2007 prednášal na Fakulte politických vied a medzinárodných vzťahov Univerzity Mateja Bela v Banskej Bystrici o spravodajských službách. Od roku 2008 na túto tému prednáša na Fakulte práva Paneurópskej vysokej školy. V roku 2006 inicioval založenie Asociácie bývalých spravodajských dôstojníkov na Slovensku.*

V poslednom období sme zaregistrovali v medzinárodnej spravodajskej komunite viacero závažných únikov spravodajských informácií, ktoré významnou mierou poškodili národnú bezpečnosť dotknutých štátov a potvrdili nedostatočnú efektívnosť systémovej ochrany v životne dôležitých bezpečnostných záležitostiach. Hlavne v niektorých nepublikovaných prípadoch došlo k neautorizovanému prezradeniu zdrojov spravodajských informácií. Následkom takýchto situácii nebýva výlučne iba prezradenie štátneho tajomstva a poškodenie štátnych záujmov, ale aj vznik rizika, že dôjde k odhaleniu nenahraditeľných spravodajských zdrojov. V uvedenom kontexte sa javí ako odôvodnená prax, že zákonným adresátom spravodajských informácií sa neposkytujú zdroje týchto informácií, resp. zakrýva sa spôsob ich získania v konkrétnom záujmovom prostredí. Existujú však výnimky z tohto všeobecného pravidla, a to pri poskytovaní niektorých mimoriadne dôležitých spravodajských informácií predstaviteľom exekutívy na najvyššej úrovni. Obvykle sa tak stáva v krízových momentoch, keď rozhodovanie zodpovedného predstaviteľa štátnej moci na základe spravodajskej informácie môže byť spojené s rizikovými alternatívami ohrozenia krajiny. Niekedy adresát mimoriadne závažnej spravodajskej informácie si vyžaduje konkrétnu charakteristiku zdroja, pretože poskytnutá informácia sa vymyká z rámca doterajších poznatkov o probléme.

Distribúcia spravodajských informácií ich zákonným adresátom pozná viacero konkrétnych prípadov, keď došlo k nežiaducemu úniku prísne utajovaných informácií, a preto v záujmy ochrany ich pôvodu je nevyhnutné zakrývať ich zdroje dômyselnou legendou. Na úvod sa žiada spomenúť konkrétne príklady, keď spravodajská služba poskytla adresátovi významnú informáciu, ale zámerne neuviedla skutočný zdroj tejto informácie, aby tak zabránila potenciálnemu prezradeniu zdroja, prípadne naplnila aj iný zámer.

Prvý príklad pochádza z obdobia spred štyridsiatich rokov, keď medzištátne vzťahy vtedajšieho Česko-Slovenska so Spolkovou republikou Nemecko vážne zaťažoval spor o tzv. nulitu Mníchovskej zmluvy, ktorou si vodca nacistického Nemecka A. Hitler v roku 1938 vynútil u európskych mocností súhlas s územným okliešťením Československej republiky. Ešte pred skončením 2. svetovej vojny spojenci Česko-Slovenska deklarovali neplatnosť Mníchovskej zmluvy od okamihu jej podpísania, teda tzv. nulitu - pretože česko-slovenská vláda sa podriadila jej podmienkam pod nátlakom jej signatárov. Ale všetky povojnové vlády v Bonne zastávali názor, že zmluva z Mníchova je v podstate platná. Pritom argumentovali viacerými dôvodmi, predovšetkým ohľadmi na občiansko-právne a majetkovo-právne vzťahy bývalých sudetských Nemcov, ktorí boli pôvodne občanmi Československej republiky. Spor o výklad Mníchovskej zmluvy bránil nadviazaniu normálnych

diplomatických stykov na úrovni veľvyslanectiev medzi Česko-Slovenskom a Spolkovou republikou Nemecko. Od februára 1968 až do decembra 1973 vlády oboch krajín komunikovali iba prostredníctvom svojich obchodných zastupiteľstiev v Prahe a V Bonne.

Až v roku 1971 sa predstavitelia Spolkovej republiky Nemecko a Česko-Slovenska dohodli, že spor o tzv. nulitu Mníchovskej zmluvy vyriešia rokovaniami na úrovni expertov, ktoré striedavo prebiehali na obchodných zastupiteľstvách oboch krajín v Bonne a v Prahe. Tieto rokovania sa úspešne skončili v decembri 1973 podpísaním Zmluvy o vzájomných vzťahoch medzi ČSSR a SRN, ktorá kompromisnou formuláciou o neplatnosti Mníchovskej zmluvy ukončila spor o tzv. nulite Mníchova a umožnila nadviazať vzájomné diplomatické styky na úrovni veľvyslanectiev.

Nie zanedbateľnú úlohu pri formovaní postojov a postupov československej strany na rokovaniach s predstaviteľmi SRN zohral fakt, že sa československej rádiorozviedke podarilo prelomiť šifru, ktorou boli kryptované pokyny západonemeckým diplomatom v Prahe, ako majú argumentovať a taktizovať pri vyjednávaniach o tzv. nulite Mníchovskej zmluvy. Vtedajší najvyšší československí predstavitelia, vrátane generálneho tajomníka ÚV KSČ a prezidenta republiky G. Husáka a predsedu vlády L. Štrougala, rozhodovali o pokynoch pre československú delegáciu na základe podkladov, ktoré boli získané vďaka kryptológom rádiorozviedky. Napriek tomu, že išlo o dôveryhodných adresátov na najvyššej úrovni, vedenie rezortu ministerstva vnútra – kam patrila aj rádiorozviedka – rozhodlo o tom, že pri prezentácii získaných informácií sa nebude adresátom uvádzať skutočný spôsob ich nadobudnutia. Aby sa predišlo riziku, keby sa nemeckej kontrarozviedke podarilo získať z prostredia adresátov informáciu o tom, že československí vyjednávači už pred rokovaním poznajú pozície ich protistrany – alebo by sa samotní československí diplomati prezradili vlastnou neopatrnosťou – rádiorozviedkou získané informácie boli Husákovi i Štrougalovi prezentované ako výsledok agentúrnej činnosti spravodajskej služby. Takáto legenda by usmernila Nemcov na hľadanie cudzieho zdroja medzi pracovníkmi obchodného zastupiteľstva v Prahe, ale neviedla ich k tomu, aby zmenili používanú šifru.

Druhý príklad legendovania spravodajského zdroja sa týka zverejnenia informácií o vojenských aspektoch výskumu a vývoja jadrových technológií v Iráne. Konkrétne ide o tlačovú konferenciu v polovici augusta 2002 vo Washingtone, na ktorej predstavitelia Národnej rady iránskeho odporu – čo je exilová frakcia iránskych Ľudových mudžahedínov – oznámili, že pri meste Natanz buduje Irán závod na výrobu jadrového paliva. Oficiálne uvedenú správu potvrdil americký State Departement v decembri 2002; napriek odvolaniu sa na iránske opozičné zdroje v svetovej spravodajskej komunite sa považuje za pravdepodobné, že informáciu získali spravodajské služby Spojených štátov amerických, ale podsunuli ju iránskej opozícii, aby tak zakryli vlastný zdroj informácie. Až v septembri 2010 sa objavil v izraelskom denníku The Jerusalem Post článok, kde sa písalo o tom, že poznatky o projekte jadrových zariadení pri Natanz získali americké a izraelské spravodajské služby, ktoré zámerne prvotnú informáciu o tomto objave verejne prezentovali prostredníctvom iránskej exilovej organizácie. Zrejmým motívom takéhoto postupu bol záujem USA nepriznať verejne svoje špionážne aktivity, zamerané na vývoj nukleárnych technológií v Iráne - a zároveň legitimizovať konanie Medzinárodnej

organizácie pre atómovú energiu, ktorá ako jediná inštitúcia disponuje oprávnením vykonávať inšpekciu v prípadoch, keď ide o porušenie konvencie o nešírení jadrových zbraní.

Zakrytie informačného zdroja spravodajskej služby pri prezentácií informácií adresátovi pomocou legendy má viacero dôvodov. V minulosti sa nie raz preukázalo, že nie každý kompetentný predstaviteľ exekutívy disponuje schopnosťou zabezpečiť zodpovedné používanie štátnych tajomstiev - a to sa týka aj utajovaných spravodajských zdrojov. Dokazuje to napr. aféra okolo bývalej dôstojníčky CIA Valerie Plame, ktorej spravodajskú identitu prezradil vo svojom komentári Robert Novak v denníku Washington Post (14. júla 2003). Išlo o manželku amerického diplomata Josepha Wilsona, ktorý spochybnil tvrdenie prezidenta Georgea Busha o irackých nákupoch obohateného uránu v africkej republike Niger. Vyšetrovanie preukázalo, že dekonšpirácia Valerie Plame bola politická pomsta kvôli odhaleniam jej manžela, za ktorou stála Bushova administratíva, vrátane viceprezidenta Dicka Cheneyho. Po škandalóznych peripetiách Valerie Plame v roku 2007 svoju spravodajskú kariéru dobrovoľne ukončila. Podľa jej kolegov v CIA bola to schopná a pracovitá úradníčka.

Nezodpovedný, resp. nekompetentný prístup k zakrývaniu spravodajských zdrojov ilustruje tiež prípad z obdobia prvej vlády Mikuláša Dzurindu. V júli 1999 premiér pri predkladaní návrhu na odvolanie prezidenta Fondu národného majetku Ľudovíta Kaníka argumentoval obsahom zaznamenaných telefonických rozhovorov s majiteľom spoločnosti Nafta Gbely. Podľa vyjadrenia vtedajšieho vicepremiéra Pavla Hamžíka z obsahu dôverného materiálu bolo zrejmé, že pochádzal zo SIS. Na tlačovej konferencii to potvrdil samotný premiér Dzurinda, ktorý prezentoval novinárom argumenty proti prezidentovi FNM Ľ. Kaníka s vysvetlením, že boli získané odposluchom Kaníkových telefonických rozhovorov. Postup premiéra Dzurindu vyvolal pochybnosti o jeho politických praktikách a odôvodnené otázky, či predseda vlády je oprávnený disponovať prepismi nahrávok odpočúvaných telefonátov a oboznamovať s ich obsahmi vládu. Neskôr táto aféra bola použitá proti Dzurindovi v iných kauzách.

Prípady Valerie Plame i Ľudovíta Kaníka svedčia o tom, že niektorí politici sa nie vždy pri využívaní spravodajských informácií riadia imperatívom ochrany spravodajských zdrojov, ale prioritne uprednostňujú svoje politické ciele a záujmy. Neautorizované odkrývanie spravodajských zdrojov, teda úniky ohrozujúce utajenú identitu ľudských zdrojov, technických prostriedkov a špeciálnych technológií si vyžaduje regulačný rámec, ktorý zahrnuje aj legendovanie ako určitý špecifický spôsob ochrany spravodajských zdrojov. V tomto kontexte sa žiada uviesť názor dlhoročného funkcionára CIA, právnika Johna Rizza, že „prakticky žiadne tajomstvo nezostane tajomstvom večne a utajená existencia nových tajomstiev sa neustále kráti“. Napriek tejto, tak povediac zákonitosti, efektívne fungovanie spravodajských služieb v značnej miere závisí od toho, ako dokážu chrániť svoje zdroje.

Únik spravodajských informácií, spojený s prezradením ich zdroja môže v niektorých prípadoch ohroziť aj život informátora spravodajskej služby alebo umožní spravodajskému protivníkovi, aby sa chránil pred technickými prostriedkami, odhaľujúcimi jeho tajomstvá. Adresátom spravodajských informácií sa obvykle nešpecifikujú ich zdroje konkrétne; nie je však nepochopiteľné, ak sa adresáti na

najvyššej úrovni exekutívy bližšie zaujímajú o pôvod informácií, ktoré sa obsahom a významom vymykajú z bežného informačného stereotypu. Takéto mimoriadne situácie pri prezentovaní spravodajskej informácie jej zákonnému adresátovi sú predvídateľné, a preto si možno na tento účel vopred pripraviť vhodnú legendu na zakrytie spravodajského zdroja. Cieľom takejto legendy je predísť tomu, aby aj pri neautorizovanom úniku spravodajskej informácie nedošlo k odkrytiu jej zdroja. Kvalifikovaní adresáti spravodajskej informácie sa spravidla nezaujímajú o jej zdroj; napriek tomu pred prezentovaním informácie jej adresátovi je potrebné počítať s nepredvídateľnými okolnosťami a byť na takéto okolnosti pripravený. Pri prezentovaní osobitne citlivej spravodajskej informácie môže jej adresát požadovať okolnosti jej pôvodu, ale aj v takomto prípade by identita zdroja mala zostať tabu!

Úvahy o tom, ako legendovanie zaštiťuje spravodajské zdroje pred odhalením, nastoľujú otázku, či takýto postup spravodajskej služby výlučne slúži na ochranu nástrojov národnej bezpečnosti alebo tiež aj na zakrytie zneužívania štátnej moci. Aktuálna prax úniku informácií, ktoré získali spravodajské služby, nedáva na túto otázku jednoznačnú odpoveď. Je evidentné, že vlády majú životný záujem nielen na utajovaní informácií spravodajských služieb, ale aj zdrojov týchto informácií, pretože si to vyžaduje ich ochrana. Na druhej strane verejnosť má záujem na tom, aby štátne utajovanie neohrozovalo demokraciu. Dilemu tohto problému sa pokúsila vyjadriť docentka Právnickej fakulty Adelaidskej univerzity Gabriele Applebyová: „Potrebujeme uznať úlohu, ktorú zohrávajú úniky a konfrontovať sa s dilemami, ako môžeme podporovať a chrániť vynášačov (leakers) bez toho , aby sme zbytočne obetovali záujmy národnej bezpečnosti“.

Sotva možno poprieť, že prax legendovania zdrojov spravodajských informácií pred ich zákonnými adresátmi vychádza zo skúseností, že únik informácií môžu ovplyvniť aj náhodné okolnosti, ktoré bývajú nepredvídateľné. Najmä v súvislosti s informáciami s politickým kontextom nemožno vylúčiť napr. zlyhanie profesionálnej lojality osôb, ktoré systematicky alebo len náhodne prichádzajú do styku s utajovanými skutočnosťami. Ilustruje to známy prípad agenta FBI Williama Felta, ktorý pod metaforickým označením Deep Throat (Hlboké hrdlo) fungoval ako tajný zdroj novinárov Boba Woodwarda a Carla Bernsteina (Washington Post) v afére Watergate. Neautorizovaný únik informácií z fondov FBI vyvolal škandál, ktorý viedol k rezignácii prezidenta Richarda Nixona v roku 1974 a spustil proces významných legislatívnych reforiem v spravodajskej komunite Spojených štátov amerických. Škandál Watergate zohral historickú úlohu pri presadzovaní a udržiavaní spravodlivosti a pravidiel demokracie v USA.

Na záver sa žiada položiť si otázku: ohrozuje štátne utajovanie demokraciu ? Takto začal svoju knihu odborný asistent Katedry politológie Univerzity v Princetone Rahul Sagar: „Tajomstvá a úniky: Dilema štátneho tajomstva“. Podľa jeho názoru utajovanie je podstatným aspektom vodcovstva. Kľúčom k problému je zabezpečiť, aby sa exekutívne utajovanie používalo zodpovedne. V takomto rámci treba viesť diskusiu a hľadať odpoveď aj na otázku, či legendovanie ako spôsob ochrany spravodajských zdrojov zodpovedá potrebám ochrany národnej bezpečnosti a jej inštitúcií, ku ktorým patria tiež spravodajské služby. Rahul Sagar poukázal v spomínanej knihe na to, že jediné nástroje, ktoré máme na monitorovanie používania štátnych tajomstiev, nezapadajú pohodlne do našich „morálnych

a politických hodnôt, najmä nie do kľúčových demokratických štandardov.“ A týka sa to aj legendovania, ktorým chránime informačné zdroje spravodajských služieb.

P. Púčik: Identita zdroje a zásada "potřeba znát"

Peter Púčik *(1945) - Studoval na MGIMO v letech 1964-1969 arabštinu a oblast Blízkého a Středního východu; poté krátce pracoval na Federálním ministerstvu zahraničních věcí. Do roku 1979 odborný pracovník Orientálního ústavu ČSAV. Další léta topič a řidič autobusu. V období 1985-1989 byl ve Výzkumném ústavu matematických strojů v Praze. Po listopadu 1989 opět krátce FMZV a od roku 1990 až do léta 1999 příslušník československých a českých zpravodajských služeb. Přednášel na Prague Security Studies Institute v Praze.*

Bonmot "potřeba znát" v anglické či německé verzi (*need to know* resp. *Kenntnis nur wenn nötig*) byl ke shlédnutí na zdech školících středisek či na drobných upomínkových předmětech jako pokus vštípit adeptům i partnerům zásadu hlásající zhruba toto: I když jste prověřeni, seznámíte se jen s tím, co potřebujete nezbytně ke své práci.

Aniž bychom se pouštěli do právních rozborů, zdá se být zřejmé, že jednotlivé národní právní úpravy vztahující se k ochraně utajovaných informací či předpisy Severoatlantické aliance nebo Evropské unie neřeší a ani nemohou zcela řešit situace ochrany identity zdroje zpravodajské služby. I když budeme striktně dodržovat postupy nastavené zákony a dalšími právními předpisy, v praxi s nimi nevystačíme. Zcela běžně se tak činnost zpravodajských služeb, zejména v oblasti operativní činnosti a ochrany zdroje dostává do kolize s právní úpravou, která je na jedné straně příliš restriktivní a na straně druhé nedokáže postihnout detailní problémy z praxe. Zpravodajské služby se tak v menší či větší míře snaží do právní úpravy včlenit alespoň určité výjimky, které by jim umožnily tuto citlivou oblast zajistit (např. umožnění přístupu k utajované informaci osobě bez prověření).

Chod služby, především operativy přináší denně množství poznatků, které by měly být nějakým způsobem utajovány. U některých toho lze dosáhnout formálním zařazením mezi "utajované informace" a následným zacházením dle zákona a prováděcích předpisů.

Objem informací spadajících do režimu utajení však netvoří jen informace, řádně zaevidované, řízeně distribuované a ukládané v souladu s předpisy. Patří sem nejen to, co je možno si přečíst, ale i to co lze spatřit, slyšet a zažít. Tyto poznatky, vlastně zacházení s nimi, lze formalizovat obtížně. Nakonec tuto "šedou zónu" vyřešil zákonodárce i služby institutem mlčenlivosti. Jako je tomu například v ustanovení § 45 odst. 1 písm. c) zák.č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, které stanoví povinnost zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděl při výkonu služby; to neplatí, jestliže byl příslušník této povinnosti zproštěn služebním funkcionářem, nestanoví-li zvláštní právní předpis jinak.

Služby tento problém řeší trvale a zpravidla jsou to vnitřní předpisy, jejichž tvorba a zejména dodržování dává službě řád a bezpečnost výkonu operativní činnosti. Zásada "potřeba vědět" je doplněna organizačním principem, pro které máme anglický výraz "c*ompartmentalization"*.

Všechny utajované informace nebo lépe řečeno tajnosti služby jsou důležité,

ale některé jsou důležitější. Není sporu o tom, že přední místo mezi nimi zaujímá identita zdroje zpravodajských poznatků a jejich ochrana. Debata může být o tom, **kdo** uvnitř služby má mít k těmto údajům přístup, **protože je nezbytně potřebuje znát**.

Na první pohled se může zdát, že příspěvek na téma "utajování zdrojů uvnitř služby" je vlastně zbytečný. Každému je jasné, že krytí zdrojů zpravodajských poznatků je z povahy věci zcela evidentní a nesporné. Bližší pohled na praxi by však ukázal, že jde o záležitost nejednoznačnou, někdy rozpornou a často narážející na rámec nedokonalých či nedodržovaných pravidel, resp. vnitřních předpisů.

Možná bude vhodné představit si zcela hypotetickou situaci, v níž se ocitne vedení zpravodajské služby malé země , jež stojí před zadáním zreformovat službu, zabývající se doposud analýzou otevřených zdrojů či drobnými intrikami. Zajímat nás bude nastavení pravidel, jež zajistí dlouhodobý zisk z toku zpravodajských poznatků, nepřerušovaný periodickými maléry.

Osvícené vedení tuší, že čím dokonaleji zakope své zdroje, tím déle bude mít klid od politiků i médií. Po určité době, strávené debatami, pátráním po tom, jak se to dělalo dřív a jak to dělají jinde, se ukáže, že problém je složitější, či jak se dnes říká strukturovanější.

Aspektů ochrany zdroje je celá řada, všechny musí být řešeny současně a musí tvořit ucelený systém, který je v souladu se zvoleným či okolnostmi vnuceným *modem operandi* (zdrojem, jehož identitu chráníme může být kmenový příslušník služby, občan vlastní země, obyvatel státu cílového či občan třetí země). Pokusme se o stručný a jistě neúplný výčet těchto aspektů:

a) *bezpečnost evidenční*
b) *problém finančního zajištění operativní činosti*
c) *otázky technického vybavení a výcviku*
d) *operativní podpora a zabezpečení v terénu*
e) *vstup produkce do informačního toku služby*
f) *zpětná vazba a úkolování*
g) *identita zdroje a kontakty s dalšími službami státu*
h) *spolupráce se zahraničními partnery*

Chybné nastavení v kterémkoliv z uvedených aspektů může vést k nedozírným následkům, přinejmenším pro zúčastněné a zejména pro náš zdroj. Pojednejme tedy o těchto aspektech z hlediska uplatnění zásady "potřeba vědět" podrobněji, přestože některé z nich se zdají být opět triviálními. Pro zjednodušení zcela opomineme sféry čistě "nelegální" rozvědky i produkci deklarovaných či zcela nedeklarovaných představitelů služby.

"Evidenční" bezpečnost zdroje

Zřejmě nejjednodušší je řešení v případě, kdy je zdrojem osoba stojící zcela mimo službu. Ať už se jedná o občana vlastní země, třetího státu nebo cílového, není žádný důvod, aby jeho pravá identita opouštěla vlastní operativní pracoviště, které je s ním ve styku. Důsledné používání krycího jména (pokud možno odlišného od názvu

či označení zdroje pro potřeby dalšího zpracování produkce) by mělo být dostatečné. Přitom pravá totožnost se spolu s množstvím jiných identit může v databázích služby objevovat jako důsledek vlastního tipování, podnětů z vnějšku či od liaison. Pokud lze zabránit vzniku příslovečného černého puntíku u jména (dejme tomu z hlediska blokace) a zajistit zejména rozumné legendování odpovědí na dotazy od jiných služeb, domácích či cizích, pak je evidenční ochrana dostačující.

Složitější je situace, kdy zdrojem je kmenový příslušník služby, působící zpravidla pod přirozeným krytím v profesi, která mu poskytuje přístup ke kýženým informacím nebo alespoň k jejich nositelům. Sama tato praxe je dost rozporná, často budí odpor zejména u "čistých" příslušníků oněch profesí a pochopitelně v médiích i u politiků, zejména opozičních. Nicméně z historie tyto případy známe a není nutno se tohoto řešení předem vzdávat. Pouze na to musí být služba po organizační stránce připravena. Není sporu, že takový příslušník musí být z povahy věci evidován kompletně – debata může být pouze o tom, kde má být personální svazek uložen a kým spravován. Nabízí se možnost vytvoření zvláštního personálního pracoviště tak, aby nebylo možné si ze standardních dat dovodit jeho vztah k působišti,úkolování a produkci.

Z hlediska evidenční bezpečnosti ovšem není lhostejné, zda "náš" člověk byl nejdříve kmenovým příslušníkem a pak se vypracoval do výšin své druhé profese nebo opačně, byl již hvězdou oboru a potom jej zlákala zpravodajská kariéra. První případ je nesporně složitější, neboť klade na člověka i organizaci značné nároky s nejistým výsledkem. V případě druhém, kdy přijdeme již k zavedenému člověku, vznikají problémy spíše v jiných souvislostech, zejména v oblasti výcviku, než s bezpečností"evidenční ".

Bezpečnost financování činnosti zdroje

Kdosi v minulosti řekl, že můžeme mít jakoukoliv tajnou službu, jenom ne levnou. V globálu to bezesporu platí, ale méně je již známo, že přímé operativní výdaje tvoří pouhý zlomek celkových nákladů na chod služby, jak mandatorních, tak i provozních. Nicméně se ví, že právě tyto náklady přitahují pozornost managementu a stejně tak jsou středem zájmu kontrolních orgánů. Výši a účelnost vynaložených financí proto operativa musí neustále zdůvodňovat mimo jiné i návazností na kvalitu a množství produkce. Řádná evidence i vnitřní kontrola jsou proto nezbytným předpokladem.

Zdroj a jeho činnost není gratis a jejich financování se může stát kamenem úrazu i z bezpečnostního hlediska. Řešení mohou být různá a některá jsou účinnější, než jiná z pohledu ochrany identity zdroje. Lze například oddělit do různých finančních evidencí vlastní financování zdroje (např. odměny a náklady krytí) a zajištění vlastní produkce zdroje. Lze jí třeba přidělit krycí jméno operace a dále pod tímto názvem můžeme onu produkci i prezentovat. Na ní je možno účtovat náklady spojení, osobní kontakty se zdrojem, materiální vybavení a pod. Pojítkem mezi svazkem zdroje a svazkem operace bohužel musí zůstat krycí jméno zdroje a zde je právě výhodné mít zavedené ještě druhé (třeba alfanumerické) označení zdroje. I takto můžeme zajistit, že zásada "need to know" neulehčí eventuelní tvůrčí účetnictví. Nabízí se pak i varianta název operace pozměnit. Pro odběratele není podstatné vědět, máme li jeden zdroj nebo více ve stejném oboru, ale obsah a věrohodnost

předávaných informací. Tato různá opatření pro účely ochrany zdroje ve věci vykázání vynaložených finančních prostředků nemohou a ani nesmí mít vliv na možnost provedení řádné kontroly financí.

Technické vybavení zdroje a jeho krytí

Tento aspekt utajování identity zdroje uvnitř služby uvádíme spíše pro úplnost komplexní ochrany zdroje. Jde v podstatě o to, že výbava dnešního zpravodajce v terénu většinou předpokládá určité množství technických prostředků, zejména komunikačních. V této souvislosti může vznikat riziko, že při výběru techniky a zejména při nácviku jejího využití přijde náš zdroj do kontaktu i s jinými než operativními pracovníky. Až na zcela mimořádné výjimky jde o zbytečné rozšíření okruhu osob se znalostí identity zdroje. Obecně platí, že prostředky informačních technologii patří vždy mezi potenciálně inkriminující a dekonspirující markanty.

K této věci snad jednu krátkou obecnou poznámku k výcviku. Nedomníváme se, že nezbytné (až na nutné výjimky z pravidla) vystavovat náš zdroj plejádě školitelů z různých oborů operativní problematiky a tím dále rozšiřovat okruh osob obeznámených se zdrojem. V praxi skutečně platí, že nedokonalý výcvik je horší než žádný a přirozené krytí je nejlepší. Zdroji je třeba spíše připomínat, co dělat nemá, než obráceně.

Operativní podpora zdroje v terénu

V této oblasti se zcela jednoznačně projevuje otázka kapacitních možností jednotlivých služeb, kdy velké služby mají pro tyto účely vycvičené speciální týmy k zajištění schůzkové činnosti a malá služba takovými strukturami nevládne a musí tedy svoji činnost zajišťovat jinak.

Většina malých služeb nepředpokládá poskytování přímé operativní podpory svých zdrojů přímo v terénu a tak do úvahy připadá zejména zajištění schůzkové činnosti v třetích zemích. V dané situaci se jako vhodnější jeví skromné nasazení operativní podpory za využití příslušníků, kterým je zdroj znám a nedochází tak k jeho dalšímu rozkrývání.

Vstup produkce zdroje do informačního toku služby

Až dosud jsme se zabývali převážně “technickými” aspekty dodržování zásady “potřeby vědět”. Jejich dodržování pouze snižuje riziko exponování našeho zdroje uvnitř služby. Nyní však přecházíme k daleko obtížnější otázce a tou je bezpečné začlenění získaných poznatků do informačního toku. Jde jak o vlastní poznatkový fond (třeba databáze) tak zejména o výstupy služby určené oprávněným adresátům. Tady už nejde jen o ochranu identity zdroje uvnitř služby, ale i o nechtěně vytvářené povědomí širšího a někdy i neurčitého okruhu osob o možnostech zdroje v dané oblasti. To se týká jak vlastní analytiky tak i adresátů výstupu.

Primárním účelem existence služeb je získávání informací a od tohoto účelu se pak odvíjí snaha o získání zdrojů těchto informací, avšak získáním informací a jejich postoupením do informačního toku se otázka ochrany zdroje dostává do zcela nové roviny.

Tento vývoj je zcela přirozený a v podstatě nevyhnutelný, avšak z hlediska operativní činnosti do značné míry i nepříjemný. Důsledkem tlaku na operativu je pak určité napětí mezi ní a analytikou. Jeho překonání je posléze obtížné a ne vždy trvalé. Platí to zřejmě více pro služby malé, s omezeným záběrem a množstvím zdrojů. Nepoměr mezi vlastní produkcí a zdánlivou záplavou poznatků, získanou službou z neoperativních zdrojů informací je viditelný. K tomuto stavu pak přispívá často neochota operativy sdílet s analytikou jakékoliv detaily kolem možností a přístupu zdroje. Zpravidla je snahou, aby se analytik spokojil se stručnou klasifikací přístupu a spolehlivosti pramene. Analytik se však nutně musí vyrovnat s verifikací zpracovávané informace, aby mohl pokročit dál a postoj operativy nese úkorně.

Jednou z možností jak předávat poznatky mezi operativou a analytikou je existence vlastního prvotního "analytického" pracoviště přímo v rámci operativy. Jeho posláním by především mělo být redigovat produkci zdroje, tj. dát ji formu, jež dostatečným způsobem zdroj "odosobní" směrem dovnitř služby. Ve vztahu ke zdroji pak tato analytika operativy opět rediguje požadavky na produkci. Toto pracoviště rovněž nemusí být nutně seznámeno s vlastní identitou zdroje, ale musí mít jasno ve věci jeho přístupu a věrohodnosti.

Na formu a obsah výstupu pro adresáty pochopitelně nemá operativa žádný nebo minimální vliv a často ani neví, jak se s poznatkem naložilo. Toto je další úskalí, neboť odběratelem nejsou pouze vysocí státní úředníci, u nichž se dá jistá míra profesionality očekávat, ale zejména vrcholní politici. Někdy se jedná o osoby, které s informacemi ze zpravodajských zdrojů ještě neumí zacházet, chápou je jako politický trumf a nikoli jako vzácnou příležitost vhledu do trochu jiného světa, která má pomoci při přijetí rozhodnutí či poskytnout informační podporu. Pokud je výstup koncipován bez ohledu na citlivost zdroje informací, povědomí o tom, že "tam" máme svého člověka se šíří již mimo službu. Brzy si najde cestu třeba do médií a to bude ten lepší případ.

Mezi vládou a službami v řadě zemí stojí těleso, pověřené jejich koordinací a někdy též finálním zpracováním výstupů. Může být dokonce i profesionální a být u dodavatelů ve vážnosti. V každém případě by mělo mít k dispozici více informací, než mají jednotlivé služby a snad i jakýsi rozhled a nadhled. Na této úrovni již na postavení jednotlivého zdroje příliš nezáleží a důležitá je pouze jeho spolehlivost. Není to však diskusní klub a už vůbec ne v rovině operativní. Jednou odevzdaný výstup tak žije vlastním příběhem.

Je třeba si uvědomit, že všechny tyto činnosti se odehrávají v konkurenčním prostředí ne vždy se milujících služeb a současně, že informace hozené do tzv."velké vany" pocházejí z velmi diferencovaných zdrojů. Operativní informace jsou nutně v menšině a vyžadují zvláštní zacházení. Tento problém se obdobně týká i SIGINT-u.

Zpětná vazba a úkolování

Komunikace mezi zdrojem a jeho centrálou, jmenovitě operativou není jednosměrná. Zpětná vazba, hodnocení předaných informací, žádosti o doplnění či vysvětlení určitých aspektů zprávy – to vše je standardní postup.Samozřejmě, není

jedno, zda tato komunikace probíhá v reálném čase anebo v kratších či delších intervalech, navíc nepravidelných.

Organizace zpětné vazby směrem ke zdroji a jeho úkolování mají vztah k diskutovanému problému. Analytikova reakce je samozřejmě důležitá. Jeho posláním je maximálně verifikovat, objektivizovat informaci a uvést ji buď do požadovaných souvislostí nebo pouze splnit konkrétní zakázku oprávněného zadavatele. Jeho požadavky jsou a musí být neosobní, bez vztahu k subjektivním podmínkám zdroje, ovšem často bez znalosti prostředí atd. Zcela jistě existují analytici, kteří jsou ve věci reálií či znalosti prostředí více erudováni, než operativa, zejména ti, kteří danou oblast studovali již před nástupem do služby. Avšak ani tento stav nesmí a nemůže být důvodem pro změnu bezpečnostních zásad a pravidel. Operativec řídící zdroj má k dotyčnému vztah zcela jiný a je svým způsobem odpovědný za jeho bezpečnost. Zpravidla jej zná nejen jako zdroj, ale i jako člověka. Tento operativec ví, že obsah i formu zpětné vazby musí nějakým způsobem modifikovat, tzv. "přešít na tělo zdroji". Měl by vědět, zda je zdroj schopen bez rizika zjistit odpovědi na doplňující otázky a zda vůbec má přirozený přístup do prostředí, kam je úkolován.

Významnou úlohu zde hraje již zmíněný způsob komunikace. Tento aspekt nemusí analytika vůbec zajímat a stejně tak pro něj nejsou podstatné další detaily operativní práce. Nicméně, každý analytik po určité době zjistí jakýsi systém v odezvách a ve svých nárocích na operativu se tomu přizpůsobí. Úkolování a zpětná vazba mohou fungovat hladce po delší dobu, zejména pokud je poptávka především po informacích spíše analyzujících a doplňujících chápání současné situace spolu s umírněnými prognózami. Vše se však mění v okamžicích vzniku nenadálé situace, první krize, teroristického útoku apod. Na službu se valí požadavky a nemožnost je splnit v požadovaném čase se musí složitě omlouvat. Příčinou tohoto stavu často může být právě zavedený způsob komunikace nebo vlastní zaměření zdrojů.

Podobně může dopadnout i úkolování ad hoc, tedy k záležitostem urgentním, avšak často mimo možnosti zdroje a spojené se zvýšeným rizikem. Na jednorázové úkolování může připadnout vlastní analytika, nápad může přijít od zákazníka, ale i od partnerské služby. Co lze vysvětlit a rozmluvit kolegům, nefunguje u oprávněného zadavatele. Výsledkem takového tlaku může být splnění zadání, avšak s nulovou hodnotou. Některé zdroje v některých teritoriích prostě nerady zarmucují své řídící operativce a tak něco pošlou.

Identita zdroje a kontakty s ostatními službami státu

Identita zdroje může být v ohrožení i mimo vlastní službu ve vlastní zpravodajské komunitě a ze strany specializovaných policejních útvarů. Příčina je zcela jasná již na první pohled. Zjednodušíme-li to, pak všichni loví víceméně ve stejném rybníku. Zájem uvedených složek je v podstatě o stejný typ lidí, ovšem cílové prostředí jejich eventuálního dalšího působení se liší. Týká se to především cizinců, ale předmětem pozornosti jsou i jisté skupiny vlastních občanů, majících například osobní, profesní či odborný vztah k zájmovým oblastem činnosti služby.

V případě fáze tipování, prověřování a prvotních kontaktů je dost možné, že v prostředí malé země se záměry služeb a specializovaných policejních útvarů dříve nebo později protnou. U nadějných kandidátů se jedná o možnost hraničící s jistotou.

Například v České republice byl předlistopadový systém blokací a vzájemných lustrací z různých důvodů opuštěn a v současných podmínkách a vzhledem k existující struktuře zpravodajsko-bezpečnostní komunity lze usuzovat, že by jeho případné vytvoření a fungování bylo více než náročné.

Nepříjemná situace nastává, pokud se zdroj služby stane svým chováním podezřelým pro bezpečnostní službu, či v horším případě pro policii. Zájem kontrarozvědky může vzbudit právě to, proč si zdroje ceníme. Například jeho rodinné zázemí či kontakty do vyšších pater moci a vlivu v jeho vlasti. Současně je takřka rutinně zvažováno o jeho možné příslušnosti k cizí službě. Vzhledem k tomu, že ke skutečnému dotažení případu bývá většinou daleko, není vše ztraceno a podle situace je možné přijmout odpovídající opatření. Pokud však zdroj má skutečný problém, např. s policií, lze mu těžko radit či dokonce pomoci, aniž by byl jeho vztah ke službě ohrožen. Současně je nezbytné, aby operativa zvážila možná rizika další spolupráce se zdrojem.

Spolupráce se zahraničními partnery

Převážný díl spolupráce s partnerskými službami v zahraničí se nijak nevztahuje k ochraně identity zdroje. Informační výměnu představují většinou analytické zprávy, neodkazující se na zdroj poznatků. Vlastně se ani neočekává, že by byl zdroj upřesněn. Je zcela běžné, že z důvodu ochrany zdroje bývají tyto označovány jako získané z jiného typu zdroje, např. *SIGINT-u*. Výjimky, kdy označení zdroje je uváděno jako *HUMINT,* se vyskytují vzácně a jsou spíše projevem důvěry ze strany partnera nebo v některých případech toto může být motivováno snahou dosáhnout reciprocity.

Zájem o náš zdroj může být vyvolán nechtěně reakcí na poznatek, který byl rutinně předán partnerům a vzbudil větší zájem, než bylo očekáváno. Kruh požadavků na upřesnění původní zprávy i dotazy na záběr zdroje se zužuje. Někdy se partneři uspokojí předáváním svých požadavků, jindy projeví přímo zájem o sdílení zdroje či jeho vytěžování.

Může tak dojít k paradoxním situacím, kdy vlastní analytika identitu zdroje nezná, ale zahraniční partner ano, pokud je tento postup ku prospěchu obou zainteresovaných stran. Jindy se může stát, že se zdrojem nemůže služba udržovat bezpečný kontakt, či jej smysluplně úkolovat a tento druh spolupráce je prostě nezbytnou nutností. Zásada “need to know” však porušena není.

Shrnutí

Po nástinu problému identity zdroje versus zásada “potřeba znát” se pokusme stručně shrnout, co z něj zatím vyplývá.

Jednotlivé aspekty se dělí na dvě zcela odlišné skupiny. Otázky evidenční, finanční, technické i operativní jsou v zásadě řešitelné na úrovni vnitřních předpisů a aplikovaných postupů, které však musí být striktně dodržovány. Předpokladem je dostatečné personální zázemí operativy - zejména administrativní a technické, oddělené od podobných útvarů, sloužících daleko většímu zbytku služby. “Potřeba vědět” je zabudovaná do organismu konkrétního pracoviště.

Otevřeným a zatím nepojednaným zůstává problém vztahu vnitřní bezpečnosti a jejího fungování vůči operativě. V některých službách bývá pravidlem zapojit vnitřní bezpečnost přímo do některých operací, zejména při zajištění schůzek a pod.

Druhou skupinu aspektů tvoří problémy spojené s produkcí zdroje. Zcela jistě je tok zpravodajských poznatků usměrňován interním předpisem, nicméně i zde by mělo vstupovat do hry něco jako "kultura služby", korektnost vůči partnerům spojená s trváním na "need to know" a samozřejmě odpovídající úroveň mezilidských vztahů. Prostě něco, co se vytváří a buduje složitěji než pouhý interní předpis. Přijetí a uplatnění "potřeby vědět" je v tomto prostředí dlouhodobější záležitostí. Je-li pravdou, že intelektuální výkvět služby by měl být zpravidla zaměřen na zpracování produkce, je tu naděje na postupné vytvoření této "kultury služby".

Na závěr je třeba uznat, že argumenty ve prospěch liberálněji vykládané "potřeby vědět" zde nezazněly, ovšem pouze proto, že je autor nezná. Striktnější vymezení okruhu operativců se znalostí identity zdroje se zdá být jediná reálná možnost ochrany bezpečnosti zdroje a v určitém směru i obrana proti jeho nereálnému úkolování .

Pro operativce ve vztahu ke zdroji platí to, co řekl lišák Malému princovi : "Stáváš se navždy zodpovědným za to, co sis ochočil.". [1]

[1] *Le Petit Prince* (1943), Antoine de Saint-Exupéry, éd. Gallimard jeunesse, coll. Hors luxe, 1951 (ISBN 2-07-010502-4), chap. 21, p. 72

L. Csipák: Ochrana agentúrnych zdrojov pri schôdzkovej činnosti

Ladislav Csipák *(1965) – Ako operatívny dôstojník pôsobil v spravodajských službách od roku 1987 kontinuálne až do roku 2003. Po celé uvedené obdobie sa zameriaval hlavne na problematiku medzinárodného terorizmu. Svoju odbornosť spravodajského špecialistu na boj proti terorizmu zdokonaľoval v rámci viacerých školení a kurzov v CIA, v britskej MI6 a v Mossade. V rámci spolupráce SIS so zahraničnými partnermi riadil niekoľko úspešných medzinárodných bilaterálnych operácií zameraných proti teroristom. V súčasnosti pôsobí v súkromnej sfére.*

Úvod

Vybudovanie akcieschopnej agentúrnej siete je zložitý proces. Jeho prvou časťou je výber, previerka a získavanie spolupracovníka. Druhá časť je omnoho závažnejšia - a to je riadenie spolupracovníkov. Najdôležitejšie agentúrne zdroje tvoria spolupracovníci (agentúra) a spravodajskí dôstojníci. Keď narazíte na človeka, ktorý nepije, nestojí o sex, nepotrebuje peniaze, nemá žiadne problémy a so svojim životom je spokojný, tak jeho získanie k spolupráci sa nemôže podariť. Zložitosť riadenia spolupracovníkov (agentúrnej siete) je podmienená špecifickosťou povahy spravodajských služieb, predovšetkým ich utajovaným charakterom, ale aj odlišným charakterom jednotlivých spolupracovníkov. Výchova dospelých ľudí je vysoko náročná činnosť, pre ktorú je nutné vytvoriť podmienky a zvoliť citlivý prístup. V procese výchovy spolupracovníci sú vedení k základným zásadám konšpirácie a spravodajskej činnosti. Keď spolupracovníci dokážu využiť v praxi spravodajské metódy, konšpiráciu na získavanie informácií, tak ich ochrana sa zvyšuje a riziko dekonšpirácie (vyzradenia) sa znižuje na minimum.

Príprava na schôdzku

Keď hovorím o príprave na schôdzku, mám na mysli prípravu spravodajského dôstojníka na stretnutie so spolupracovníkom. Najefektívnejším spôsobom riadenia spolupracovníkov je bezprostredný styk spravodajského dôstojníka so spolupracovníkom na schôdzke. Schôdzky so spolupracovníkom je nutné naplánovať v pravidelných intervaloch. Najvhodnejšie je to aspoň raz za tri mesiace, samozrejme okrem mimoriadnych schôdzok, ktoré podľa operatívnej situácie nastanú. Obsahom práce, ktorú je nutné pred každým stretnutím so spolupracovníkom uskutočniť, zahrnuje naštudovanie zadaných úloh, ktoré od poslednej schôdzky mal splniť, ako aj vypracovanie a zadanie nových úloh, ktoré spolupracovník má plniť. Prípadne je potrebné znovu preveriť informácie, ktoré analytický odbor vyhodnotil ako informácie nízkej kvality, prípadne vysokej kvality – zistiť, ako boli získané, aké spravodajské postupy zvolil spolupracovník, aké zásady konšpirácie boli použité. Treba tiež naplánovať termín ďalšej schôdzky. Efektívnosť schôdzky však závisí aj na tom ako sa spolupracovník pripraví na schôdzku, ako sa mu podarilo splniť zadané úlohy. Dôkladná príprava na schôdzku, presné zadanie nových úloh do budúcej schôdzky ušetrí čas a znižuje riziko ďalších komplikácií v prípade vyzradenia identity spolupracovníka.

Výber vhodného miesta na schôdzku

V rámci prípravy na schôdzku veľmi dôležitým prvkom je výber vhodného miesta na schôdzku. Určité zásady z minulosti spravodajskej práce v súčasnom období sú už zastarané. Spravodajský dôstojník by mal vytypované vhodné miesta na schôdzkovú činnosť so spolupracovníkmi, ktoré vyhovujú zásadám spravodajskej práce. Keď na schôdzke majú byť odovzdané citlivé materiály, najvhodnejším miestom schôdzky je konšpiračný byt *(tzv. safehouse)*. Sú určité podmienky, ktoré znevýhodňujú postavenie spravodajského dôstojníka (napr. v byte spolupracovníka, v zamestnaní spolupracovníka, kde je na tzv. „domácej pôde"), a preto by sa ich mal vyvarovať. Schôdzky na neutrálnej pôde sú pre obe strany výhodné a prijateľné. Najvhodnejším, ale aj najpopulárnejším miestom schôdzkovej činnosti sú reštaurácie. Spravodajský dôstojník by mal mať vytypované vhodné reštaurácie na schôdzku so spolupracovníkom. Pri vytypovaní by mali platiť určité spravodajské zásady. Reštaurácie by nemala byť monitorovaná kamerovým systémom. Reštaurácia by mala mať aspoň dva vchody na opačných stranách budovy. Spravodajský dôstojník by mal mať prehľad o otváracích hodinách, poznatky o spoločnosti, ktorá navštevuje reštauráciu, ďalej poznať parkovacie možnosti, dostupnosť s MHD, vhodné obdobie, keď je najmenej návštevníkov v reštaurácii. Samozrejme, platí zásada, že v tej istej reštaurácii sa neplánujú schôdzky aj s ďalšími spolupracovníkmi, aby nedošlo k situácii, že pri náhodnej návšteve ďalší spolupracovník by odhalil identitu práve schôdzkujúceho spolupracovníka so spravodajským dôstojníkom. Tieto všetky opatrenia znižujú riziko dekonšpirácie spolupracovníkov a tým sú chránené agentúrne zdroje.

Ochrana zdrojov počas schôdzky

Na schôdzku by mal pravodajský dôstojník vždy chodiť podľa kritérií spravodajských zásad. Mal by kontrolovať celú svoju trasu počas cesty na schôdzku. Pred konaním schôdzky - aspoň 30 minút - by mal skontrolovať miesto konania schôdzky (aké osoby sa v reštaurácii alebo v kaviarni nachádzajú). Následne zaujať postavenie, odkiaľ môže nepozorovane sledovať príchod spolupracovníka na schôdzku a tým preveriť jeho prípadné sledovanie. Spravodajský dôstojník vždy na miesto schôdzky príde ako druhý, aby sa nevystavil ako terč pre sledovanie, prípadne útok na vlastnú osobu. Schôdzka sa začína tým že spolupracovník podá vyčerpávajúcu správu o splnených úlohách od poslednej schôdzky, aké výsledky dosiahol a aké postupy použil pri získavaní informácií. Spravodajský dôstojník potom analyzuje dosiahnuté výsledky, prípadne poukáže na chyby pri použitých postupoch, ktoré spolupracovník zvolil. Spolupracovník môže podávať správy aj písomne, tým sa zaistí aj náležitá konšpirácia, ich rozhovor si nevypočujú ostatní návštevníci reštaurácie alebo obsluhujúci personál. Tým sa predíde aj skresleniu informácií pri písaní záznamu o schôdzke spravodajského dôstojníka so spolupracovníkom. Záznam o schôdzke treba formulovať tak, aby nebolo možné ustanoviť na základe odovzdaných správ identitu spolupracovníka. Aj tu platí pravidlo, že ak spolupracovník počas schôdzky pod zámienkou (toaleta, zabudnuté veci v aute a pod.) prerušenia schôdzky chce odísť, schôdzka by mala byť okamžite ukončená a odchádzať by mali spolu so spravodajským dôstojníkom (spolupracovník by mohol spravodajského dôstojníka vystaviť dokonšpirácii pred médiami, podsvetím, políciou alebo prípadnému fyzickému útoku).

Kontrola agentúrnych zdrojov po schôdzke

Nedeliteľnou súčasťou práce so spolupracovníkmi je ich kontrola. Pomocou spolupracovníkov sa získavajú spravodajské informácie, ktoré vyžadujú spoľahlivosť. Preto spravodajské zásady vyžadujú systematickú kontrolu spolupracovníkov. Cieľom tejto kontroly je získanie optimálnych záruk, že spolupracovník nie je dekonšpirovaný, nie je zradca, podáva pravdivé informácie, svedomite plní uložené spravodajské úlohy. V priebehu kontroly spolupracovníka zisťujeme predovšetkým jeho spoľahlivosť, úroveň jeho spravodajskej práce, spôsob získavania informácií, skutočné motívy spolupráce. Hlavné poslanie previerky spolupracovníka spočíva vo včasnom odhalení dablérov, provokatérov, dezinformátorov, ktorým sa podarilo preniknúť do agentúrneho aparátu. Preverovanie spolupracovníkov vykonávame vždy pred získaním spolupracovníka na spoluprácu, pri nižších stupňoch spolupráce, pri spolupracovníkoch z nepriateľského prostredia (teroristické organizácie, zločinecké skupiny), spolupracovníkoch, ktorí boli získaní na základe kompromitujúcich materiálov a pri cudzincoch.

Ochranné prvky pri styku s agentúrnymi zdrojmi

Spravodajský dôstojník musí dohodnúť so spolupracovníkom niekoľko spôsobov spojenia tak, aby vytvoril podmienky pre utajenie schôdzkovej činnosti. Dokonca je účelné tieto spôsoby po čase obmieňať. Pri prerušení alebo obnovení schôdzky je dôležité pripraviť správnu legendu pre obnovenie a zvoliť dohodnutý náhradný termín, náhradné miesto a čas na schôdzku. Spravodajský dôstojník je povinný vypracovať plán spojenia s každým spolupracovníkom. V pláne spojenia si spravodajský dôstojník stanoví miesto a termín plánovanej schôdzky, miesto a termín náhradnej schôdzky, náhradné spôsoby spojenia (heslo, ktorým sa môže ohlásiť nadriadený alebo iný spravodajský dôstojník, ktorý preberá riadenie spolupracovníka). *(Ako príklad by som uviedol z knihy Petra Tótha Komando 52 – spolupracovníka Rubensa nakontaktoval po rokoch iný spravodajský dôstojník s dohodnutým heslom „ Pozdravuje Vás Igor“ a spolupracovník nakoniec súhlasil s pokračovaním spolupráce).* Okrem plánovaných schôdzok so spolupracovníkom je nutné dohodnúť aj spojenie na mimoriadnu schôdzku (dohodnuté heslo, čas, náhradné miesto), keď si to operatívna situácia vyžaduje. Mimoriadnu schôdzku môžeme vykonať len s preverenýmdlhoročným spolupracovníkom, ktorý je spoľahlivý. Pri používaní mŕtvej schránky je dôležité, aby spolupracovník dal spravodajskému dôstojníkovi okamžite znamenie o tom, že mŕtva schránka je naplnená (heslo, email, sms). Tieto ochranné prvky so spolupracovníkmi slúžia na ochranu oboch hlavných agentúrnych zdrojov (spolupracovníci, spravodajský dôstojníci) pred vyzradením, prípadne ich ohrozením.

Činnosť spravodajských služieb na cudzom území ohrozujúca agentúrne zdroje

Spravodajskí dôstojníci pri styku so spolupracovníkmi musia vždy dodržiavať základné zásady spravodajskej činnosti - a to konšpiratívnosť, plánovitosť a operatívnosť. Pri spravodajskej činnosti sa najčastejšie používa osobný styk so spolupracovníkmi. Tento spôsob styku má veľa predností. Umožňuje dôsledne uplatnenie zásad riadenia, výchovy a kontroly spolupracovníka. Zásada

konšpiratívnosti vychádza zo skutočnosti, že celá činnosť spravodajskej služby musí byť utajená pred verejnosťou. Preto spojenie spravodajských dôstojníkov a ich spolupracovníkov musí byť utajené pred nepovolanými osobami (v tomto prípade nepovolané osoby sú aj kolegovia). Konšpiráciu môže ovplyvniť veľa faktorov (nevhodne zvolené miesto schôdzky, náhoda, dopravná nehoda), preto niekedy treba improvizovať, vymýšľať vopred dohodnuté legendy, prípadne dohodnúť scenár pre nepredvídateľné prípady. Pri nedodržaní zásad konšpirácie môžu vzniknúť ďalekosiahle následky, z ktorých najnebezpečnejšia je dekonšpirácia spravodajského dôstojníka, alebo spolupracovníka. Pri dekonšpirácii spolupracovníka hrozí strata ďalších možností získavať informácie zo záujmového prostredia. Prípadná dekonšpirácia pred cudzou spravodajskou službou sa môže prejaviť v snahe o preverbovanie dekonšpirovaného spolupracovníka. Všetky zásady konšpirácie treba maximálne dodržiavať pri schôdzkovej činnosti so spolupracovníkmi; na cudzom území (v zahraničí) tieto zásady platia dvojnásobne.

Nechránené „agentúrne zdroje“

Laická verejnosť slovom agent označuje nielen spravodajských dôstojníkov, ale i spolupracovníkov spravodajskej služby. Spolupracovníkom spravodajskej služby sa stáva človek, ktorého spravodajský dôstojník vytypoval, preveril, naverboval, je evidovaný v databáze spravodajskej služby a vykonáva sa s ním pravidelná schôdzková činnosť. Spravodajský dôstojník okrem spolupracovníkov môže využívať aj rôzne „pomocné“ zdroje na získavanie informácií. Tieto pomocné zdroje nie sú spolupracovníci spravodajskej služby v klasickom zmysle. Niekedy sú to jednorazové konzultácie; môže to byť využitie pomocných zdrojov pod legendou kriminálnej polície, pod rôznymi inými legendami, s ktorými spravodajský dôstojník získa potrebné informácie. Tieto pomocné zdroje nepodliehajú žiadnym zásadám konšpirácie, nepodliehajú ani žiadnym kritériám ochrany. Rozvojom technických možností nastali aj netradičné posuny v zásadách spravodajskej práce. Rôzne smartfóny, sociálne siete či komunikácia cez internet prinášajú progresívne zmeny aj do spravodajskej práce. Ako príklad by som uviedol prípad slovenského občana Mateja Valúcha, ktorého cez sociálnu sieť „naverbovala“ cudzia spravodajská služba, pre ktorú išiel plniť úlohy do Iránu, kde bol neskoršie za špionáž zatknutý. Je to nový fenomén v spravodajskej práci – „verbovanie“ cez internet. Samozrejme, nejde o klasické verbovanie podľa spravodajských zásad a nejde o spolupracovníka spravodajskej služby, ktorý podlieha konšpiratívnej ochrane. Je to „pomocný“ zdroj, ktorého cudzia spravodajská služba vyslala do záujmového prostredia (nikdy sa osobne nestretli – spravodajský dôstojník a „spolupracovník“), aby plnil úlohy. Samozrejme, že takým spôsobom nemenovaná spravodajská služba mohla osloviť aj niekoľko tisíc ľudí cez sociálne siete a mohla ich týmto spôsobom vyslať do záujmového prostredia, aby plnila zadané úlohy. Momentálne sa stalo veľmi populárnym verbovanie cez sociálne siete. Teroristická organizácia ISIL úspešne verbuje nových bojovníkov cez sociálne siete. Ale to už je kapitola na inú prednášku.

J. Ivor - M. Vlha: Využitie spravodajských informácií v prípravnom trestnom konaní

Prof. JUDr. Jaroslav Ivor, DrSc. *(1952) - Absolvent Právnickej fakulty UK v Bratislave. V rokoch 1977-2001 pracoval vo viacerých výkonných a riadiacich funkciách na úseku policajného vyšetrovania, naposledy ako generálny riaditeľ sekcie vyšetrovania a kriminalistiko-expertíznych činností Policajného zboru. V roku 1994 bol vymenovaný do hodnosti generála. Pedagogicky pôsobil na Právnickej fakulte UK, Akadémii PZ v Bratislave a od roku 2004 na Fakulte práva Paneurópskej vysokej školy, v súčasnosti ako dekan Fakulty práva PEVŠ. V roku 1998 habilitoval na docenta v odbore trestné právo a v roku 2004 bol vymenovaný za profesora v odbore bezpečnostné služby.*

JUDr. Martin Vlha , PhD. *(1986) – Absolvent magisterského štúdia na Fakulte práva Bratislavskej vysokej školy práva (Paneurópska vysoká škola), absolvent doktorandského štúdia v odbore trestné právo na rovnakej fakulte a absolvent odboru Medzinárodné vzťahy a diplomacia na Vysokej škole veřejných vztahů. Pôsobí ako odborný asistent na Ústave verejného práva Fakulty práva PEVŠ; venuje sa najmä otázkam trestného práva a kriminalistiky.*

Tak ako sa vyvíjajú prostriedky a nástroje boja proti najrôznejšej trestnej činnosti, tak isto sa vyvíja aj samotná trestná činnosť a vyskytujú sa nové druhy trestných činov. V súčasnej dobe sú v celosvetovom meradle diskutované a riešené najzávažnejšie formy trestnej činnosti, a to najmä terorizmus a organizovaná trestná činnosť. Spomedzi organizovanej kriminality predstavujú vážne problémy obchodovanie s ľuďmi, s drogami, zbraňami, či pranie špinavých peňazí.

Nielen uvedenými formami trestnej činnosti, ale aj so všetkými ostatnými sa zaoberajú orgány činné v trestnom konaní, a to najmä polícia. Polícia je špecializovaný ozbrojený štátny orgán, ktorého jednou z úloh je odhaľovanie a boj s trestnou činnosťou.

Terorizmus a organizovaný zločin majú svoje špecifické rysy, ktoré častokrát znemožňujú použitie tradičných prostriedkov trestnoprávnej praxe. Medzi takéto rysy patrí napríklad rozdeľovanie úloh v rámci rôznych kriminálnych zoskupení, individuálna zodpovednosť ich členov, zastupiteľnosť jednotlivých členov, či utajenie ich činnosti. Významnou črtou je tiež prelínanie legálnych a nelegálnych aktivít kriminálneho zoskupenia a schopnosť znemožňovať prácu polície a ďalších orgánov.

Uvedené skutočnosti odôvodňujú, že štát musí neustále prostredníctvom svojich zainteresovaných subjektov reagovať na rozmach najrôznejších protispoločenských fenoménov. S týmto úzko súvisí využívanie rôznych sofistikovaných prostriedkov, pretože ako už bolo uvedené, „tradičné“ trestnoprávne prostriedky už nestačia. Práve takýmito modernými prostriedkami disponujú spravodajské služby.

V Slovenskej republike existujú dve spravodajské služby. Slovenská informačná služba (základný právny rámec predstavuje zákon č. 46/1993 Z.z. o Slovenskej informačnej službe- ďalej ako „zákon o Slovenskej informačnej službe“)

a Vojenské spravodajstvo (základný právny rámec predstavuje zákon č. 198/1994 Z.z. o Vojenskom spravodajstve – ďalej ako „zákon o Vojenskom spravodajstve“). S prihliadnutím na čas, kedy boli spomínané zákony prijímané, je možné konštatovať, že zákonodarca vychádzal pri ich koncipovaní z tradičného poňatia spravodajských služieb ako zložiek verejnej správy, ktoré nemajú žiadne výkonné právomoci.

Ako Slovenská informačná služba, tak Vojenské spravodajstvo vykonávajú úlohy, ktoré im zverujú uvedené zákony. Konkrétne úlohy sú vymedzené zhodne v § 2 oboch právnych predpisov. V súlade s právnou úpravou je úlohou oboch spravodajských služieb okrem iného získavanie, sústreďovanie a vyhodnocovanie informácií o najrôznejších činnostiach ohrozujúcich ústavné zriadenie, územnú celistvosť a zvrchovanosť Slovenskej republiky, o činnostiach smerujúcich proti bezpečnosti Slovenskej republiky, aktivitách cudzích spravodajských služieb, ako aj o skutočnostiach spôsobilých vážne ohroziť alebo poškodiť hospodárske záujmy Slovenskej republiky.

V kontexte tohto príspevku je na mieste upozorniť na ďalšiu z úloh spravodajských služieb, a to získavanie, sústreďovanie a vyhodnocovanie informácií o organizovanej trestnej činnosti a terorizme (aj napriek tomu, že zákon o Vojenskom spravodajstve organizovanú trestnú činnosť nespomína). V prípade, ak spravodajské služby v rámci plnenia svojich úloh získajú takéto informácie, dochádza k prieniku činností orgánov činných v trestnom konaní a spravodajských služieb.

Ustanovenie § 196 ods. 1 zákona č. 301/2005 Z.z. Trestný poriadok (ďalej ako „Trestný poriadok“) uvádza, že orgány činné v trestnom konaní zisťujú skutočnosti nasvedčujúce spáchanie trestného činu z trestných oznámení. Podnety na začatie trestného konania môžu však pochádzať aj z vlastných zistení orgánov činných v trestnom konaní, či z informácií, ktoré im odovzdali napríklad služba kriminálnej polície alebo aj spravodajské služby. Už pred začatím trestného stíhania je teda možné vidieť dôležitosť informácií, ktoré získala spravodajská služba, pričom v tomto štádiu trestného konania neslúžia ako dôkaz, ale majú význam z pohľadu začatia trestného konania. Spolupráca orgánov činných v trestnom konaní a spravodajských služieb je preto z pohľadu odhaľovania najzávažnejších foriem trestnej činnosti veľmi dôležitá.

V súvislosti so získavaním informácií od zdrojov spravodajských služieb, konkrétne pri výsluchu svedka, je dôležité upozorniť ešte na jeden veľmi dôležitý aspekt vyplývajúci z ustanovenia § 129 ods. 1 Trestného poriadku. V zmysle tohto ustanovenia platí zákaz výsluchu, tzn. že svedok nesmie byť vypočúvaný o okolnostiach, ktoré tvoria utajovanú skutočnosť. Zákon však výsluch svedka (v tomto prípade príslušníka spravodajskej služby) pripúšťa za podmienky, že táto osoba bude od povinnosti zákazu vypovedať príslušným orgánom oslobodená. Inými slovami je nevyhnutný súhlas SIS, resp. Vojenského spravodajstva na výsluch osoby. Ak sa tak nestane a súhlas nebude daný, orgány činné v trestnom konaní ani súdy nemôžu takúto osobu vypočuť.

Informácie týkajúce sa trestnej činnosti (zákon o Slovenskej informačnej službe zvýrazňuje najmä informácie o organizovanej trestnej činnosti) spravodajské služby poskytnú príslušným orgánom Policajného zboru a prokuratúre. Dôležitý je

v tejto súvislosti fakt, že spravodajské služby poskytnú informácie len za predpokladu, že právny záujem na ich poskytnutí je väčší ako záujem na ich neposkytnutí. Inými slovami poskytnú informácie len za podmienky, že ich poskytnutím nedôjde:

- k ohrozeniu plnenia konkrétnej úlohy informačnej služby alebo
- k odhaleniu zdrojov a prostriedkov informačnej služby alebo
- k odhaleniu totožnosti jej príslušníkov alebo
- k odhaleniu osôb konajúcich v prospech informačnej služby.

Snaha ochrániť zdroje spravodajskej služby, jej príslušníkov a osoby konajúce v jej prospech je tu zjavná. Je potrebné však podotknúť, že v rámci trestného konania môže byť takýmto osobám (svedkom) poskytovaná ochrana prostredníctvom inštitútu utajených svedkov (v literatúre uvádzaní aj ako anonymní svedkovia – ide o synonymá). Trestný poriadok v § 136 upravuje tri stupne utajenia identity svedka. Osoby konajúce v prospech spravodajských služieb spadajú do tretieho, najvyššieho stupňa utajenia. Ich výpoveď prichádza do úvahy v zásade len vo výnimočných prípadoch, najmä keď nie sú k dispozícii žiadne iné dôkazy. Ak k takémuto výsluchu dôjde, takejto osobe sa poskytne legenda a je vypočutá prostredníctvom technických prostriedkov určených na prenos obrazu a zvuku.

Problematika využívania anonymného svedka bola viackrát prejednávaná aj na európskej úrovni. Konkrétne sa využitím anonymného svedka na národnej úrovni zaoberal Európsky súd pre ľudské práva (ďalej ako ESĽP). V tomto kontexte obžalovaní namietali predovšetkým porušenie článku 6 ods. 3 písm. d) Európskeho dohovoru o ochrane ľudských práv a základných slobôd, ktorý znie: „Každý, kto je obvinený z trestného činu, má právo vypočúvať alebo dať vypočúvať svedkov proti sebe a dosiahnuť predvolanie na vypočúvanie svedkov vo svoj prospech za rovnakých podmienok, ako v prípade svedkov proti nemu.“

Rozhodnutia ESĽP nemalým spôsobom pomohli k zdokonaleniu právnej úpravy členských štátov v tejto oblasti a k správnemu využívaniu inštitútu anonymného svedka. Spomedzi rozhodnutí ESĽP spomeňme napríklad prípad WINDISCH proti Rakúsku z roku 1990. V tomto prípade rakúsky súd rozhodol o vine sťažovateľa na základe výpovedí dvoch anonymných svedkov, ktorí jednak nevypovedali pred súdom a jednak obhajoba nemala možnosť ich vypočuť. ESĽP konštatoval v odôvodnení rozsudku, že bolo porušené právo na spravodlivý proces p. Windischa takto: „Všetky dôkazy musia byť v zásade vykonávané v prítomnosti obvineného v rámci verejného jednania s ohľadom na kontradiktórnosť konania. Avšak použitie výpovede z predsúdneho konania, ako dôkazu nie je samo o sebe nekonzistentné s čl. 6 ods. 1 a ods. 3 písm. d) Európskeho dohovoru za podmienky, že budú rešpektované práva obhajoby. Platí pravidlo, že obvinenému musí byť poskytnutá primeraná a náležitá možnosť vypočúvať svedka, či už v okamihu podania výpovede svedka alebo v neskoršom štádiu konania.“

Podobne ESĽP rozhodol aj v prípade TAAL proti Estónsku z roku 2005. V tomto prípade bol odsudzujúci rozsudok estónskeho súdu založený iba na výpovedi anonymného svedka z prípravného konania. Keďže obhajobe nebolo umožnené zúčastniť sa výpovede tohto svedka, či klásť mu otázky v neskorších

štádiách procesu, ESĽP jednomyseľne rozhodol o porušení čl. 6 ods. 1 a ods. 3 Dohovoru. Vo všeobecnosti ESĽP opakovane vo svojich rozhodnutiach konštatoval, že je neprípustné odsúdenie založiť výlučne, resp. v prevažnej miere, len na anonymných výpovediach bez predloženia iných dôkazov (napr. rozhodnutie vo veci DOORSON proti Holandsku, VAN MECHELEN proti Holandsku).

Spomeňme ešte jeden prípad z roku 2011. ESĽP vo veci AL-KHAWAJA A TAHERY proti Spojenému kráľovstvu uviedol, že rozhodnutie založené výlučne alebo v rozhodujúcej miere na svedectve osoby, ktorú nemal obžalovaný možnosť osobne vypočúvať, nie je automatickým porušením čl. 6 Dohovoru za predpokladu, že obžalovanému sú poskytnuté dostatočné záruky na to, aby mohol navrhnúť dôkazy, ktorými by anonymné svedectvo spochybnil. Platí, že prekážky, na ktoré naráža obhajoba v súvislosti s výpoveďami anonymných svedkov (nemôže spochybniť jeho vierohodnosť, zaujatosť, sledovať jeho bezprostredné reakcie), by mali byť kompenzované určitými zárukami v konaní pred súdom. Medzi tieto záruky patrí okrem iného dodržanie princípu subsidiarity, v zmysle ktorého by práva obhajoby mali byť obmedzované len v nevyhnutnom rozsahu, alebo dodržanie už spomínaného princípu zákazu výlučného použitia dôkazov založených na anonymných svedectvách. Podľa rozhodnutia ESĽP vo veci ELLIS, SIMMS a MARTIN proti Veľkej Británii bolo právo na obhajobu dodržané aj za situácie, kedy došlo k odsúdeniu členov organizovanej zločineckej skupiny (aj) na základe výpovede anonymných svedkov, spomedzi ktorých jeden mal dokonca väzby na konkurenčnú zločineckú skupinu, a to s prihliadnutím na skutočnosť, že obhajca, sudca a členovia poroty boli priamo účastní pri podávaní svedectiev týchto svedkov, t.j. boli zaistené relatívne silné procesné záruky umožňujúce posúdenie vierohodnosti a spoľahlivosti takýchto svedectiev.

V rámci trestného konania orgány činné v trestnom konaní a súdy spoznávajú skutok, ktorý je predmetom daného trestného konania, tak, že tento skutok rekonštruujú prostredníctvom zákonom upraveného postupu, ktorým je dokazovanie. Dokazovanie a informácie získané spravodajskými službami nešli vždy „ruka v ruke“. Dôvodom bola legislatíva. Zákon č. 141/1961 Zb. o trestnom konaní súdnom (Trestný poriadok) , účinný až do roku 2005, v § 89 ods. 2 považoval „za dôkaz všetko, čo môže prispieť k náležitému objasneniu veci a čo bolo získané zákonným spôsobom“. Tento fakt spôsoboval z pohľadu spolupráce spravodajských služieb a orgánov činných v trestnom konaní viaceré problémy. Nie málokrát totiž dochádzalo k situáciám, že spravodajské služby získali informácie nasvedčujúce alebo dokonca potvrdzujúce spáchanie trestného činu, avšak vzhľadom na legislatívny „nedostatok“ nebolo možné tieto informácie v rámci trestného konania využiť. Chýbala totiž možnosť, ako tieto informácie „sprocesniť“ a „vyrobiť“ z nich dôkazy, ktoré by mohli byť využité a akceptované v procese dokazovania v rámci trestného konania.

K výraznej zmene v tomto smere došlo v roku 2003 prijatím zákona č. 163/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov, známym aj ako zákon o ochrane pred odpočúvaním. Tento bol z pohľadu využívania informácií získaných spravodajskými službami v trestnom konaní významný v tom smere, že zjednotil podmienky používania informačno - technických prostriedkov orgánmi štátu (Policajný zbor SR, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa) okrem ich použitia v rámci trestného konania (úpravu obsahuje Trestný poriadok).

Tento zákon taktiež vypustil zo Zákona o Slovenskej informačnej službe, ako aj zo Zákona o Vojenskom spravodajstve ustanovenia § 12, 13 a 14, ktoré dovtedy upravovali použite informačno – technických prostriedkov.

Za najzásadnejší prínos z pohľadu tohto príspevku považujeme fakt, že tento zákon zaviedol možnosť využiť spravodajské informácie získané na základe použitia informačno – technických prostriedkov ako dôkaz v trestnom konaní. Túto možnosť upravuje v § 7 ods. 1 a ods. 2 takto: „Kópiu zvukového, obrazového alebo zvukovo-obrazového záznamu (ďalej len "záznam"), ktorý bol vyhotovený použitím informačno-technického prostriedku, možno postúpiť len vecne a miestne príslušnému štátnemu orgánu, ak záznam môže byť dôkazom v konaní vedenom pred príslušným štátnym orgánom v medziach jeho zákonom ustanovenej právomoci. Vecne a miestne príslušný štátny orgán, ktorému bol záznam postúpený, nesmie vyhotoviť kópiu záznamu ani záznam alebo jeho prepis poskytnúť k nahliadnutiu či skopírovaniu inej osobe, inému štátnemu orgánu alebo orgánu územnej samosprávy alebo inej samosprávy.“ V prípade „ak sa majú informácie získané použitím informačno-technického prostriedku použiť ako dôkaz v trestnom konaní, vyhotoví orgán štátu písomný záznam s uvedením údajov o mieste, čase a zákonnosti použitia informačno-technického prostriedku; k písomnému záznamu orgán štátu priloží záznam a jeho doslovný prepis. Informácie získané použitím informačno-technického prostriedku, ktoré sa nevzťahujú na dôvody jeho použitia uvedeného v žiadosti, sa môžu použiť ako dôkaz v trestnom konaní, len ak sa týkajú trestnej činnosti, v súvislosti s ktorou možno použiť informačno-technický prostriedok.“

Na tento výrazný posun nemohol nezareagovať „nový“ rekodifikovaný Trestný poriadok. Trestný poriadok účinný od 1. januára 2006 v § 189 ods. 2 rozšíril pôvodnú definíciu, čo možno použiť ako dôkaz v trestnom konaní takto: „Za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona.“ Týmto zákonom je predovšetkým už spomínaný zákon o ochrane pred odpočúvaním. Nemenej dôležitá je aj druhá veta citovaného ustanovenia, kde sú exemplifikatívne vymenované dôkazné prostriedky, pričom nechýbajú medzi nimi ani informácie získané použitím informačno-technických prostriedkov.

Vďaka tejto právnej úprave tak bola „zlegalizovaná“ možnosť využitia informácií získaných spravodajskými službami ako dôkazov v trestnom konaní. Naproti tomu, celkom iná situácia je v Českej republike, kde v súlade s judikatúrou Ústavného súdu, konkrétne nálezom I. ÚS 3038/07, spravodajské odposluchy nie je možné použiť ako dôkazy v trestnom konaní. Predmetný nález dôvodí tento záver najmä odlišným zákonným režimom a účelom zákonov regulujúcich spravodajské odposluchy a trestno-právne odposluchy a tiež skutočnosťou, že český trestný poriadok neupravuje možnosť použiť ako dôkaz odposluch získaný na základe iných zákonov v prípadoch, kedy má byť narušená sloboda súkromia. Spravodajské odposluchy tak nedosahujú „garančných kvalít“ vyžadovaných trestným poriadkom, a teda ich nemožno považovať za získané zákonným spôsobom.

O značnom prínose uvedených legislatívnych zmien v rámci boja proti najzávažnejším formám kriminality svedčia aj verejne publikované správy o činnosti Slovenskej informačnej služby. Pre porovnanie uvedieme údaje za posledné tri roky, t.j. za roky 2011, 2012 a 2013.

V roku 2011 podala SIS celkovo 531 žiadostí o použitie informačno-technických prostriedkov, pričom sudcovia vydali 530 súhlasov na ich použitie a len jedna žiadosť bola zamietnutá. Jedna žiadosť nebola z technických príčin realizovaná. Celkovo bolo teda realizovaných 529 použití informačno – technických prostriedkov . K 31.12.2011 z hľadiska dosiahnutia zákonom uznaného účelu a cieľa na ktorý slúžia, bolo vyhodnotených 339 prípadov. Zákonom uznaný účel a cieľ bol dosiahnutý pri 299 použitiach informačno-technických prostriedkov a nebol dosiahnutý v 40 prípadoch. K 31.01.2012 nebolo možné vyhodnotiť zvyšných 190 realizovaných prípadov.

V roku 2012 podala SIS celkovo 218 žiadostí o použitie informačno-technických prostriedkov, pričom sudcovia vydali 216 súhlasov na ich použitie a dve žiadosti SIS boli odmietnuté. Z realizovaných 216 použití informačno-technických prostriedkov bolo z hľadiska dosiahnutia zákonom uznaného účelu a cieľa, na ktorý slúžia, vyhodnotených 195 prípadov. Zákonom uznaný účel a cieľ bol dosiahnutý pri 165 použitiach informačno-technických prostriedkov a nebol dosiahnutý v 30 prípadoch.

V roku 2013 SIS podala celkovo 235 žiadostí o použitie informačno-technických prostriedkov, pričom sudcovia vydali 230 súhlasov na ich použitie a 5 žiadostí SIS o použitie informačno-technických prostriedkov bolo odmietnutých. Z celkového počtu 230 realizovaných použití informačno-technických prostriedkov boli z hľadiska dosiahnutia zákonom uznaného účelu a cieľa, na ktorý slúži, vyhodnotené všetky prípady použitia informačno-technických prostriedkov. Zákonom uznaný účel a cieľ bol dosiahnutý pri 217 prípadoch použitia informačno-technických prostriedkov a nebol dosiahnutý v 13 prípadoch.

Bližšie informácie o používaní informácií získaných spravodajskými službami v rámci trestného konania nám nie sú vzhľadom na ich charakter k dispozícii. Možnosť ich využitia v rámci trestného konania, za zákonom presne stanovených podmienok, však vítame a slovenskú právnu úpravu považujeme v tomto smere v porovnaní s českou za progresívnejšiu.

P. Zeman: Ochrana zdroje je posvátná, ale má i negativní dopady

RNDr. Petr Zeman *(1947) – Signatár Charty 77. Po novembri 1989 pôsobil na vedúcich postoch v kontrarozviedke. Bol tiež riaditeľom Úradu pro zahraniční styky a informace (1998-2001). Prednášal o spravodajských službách na Masarykovej univerzite v Brne. Podieľal sa aj na činnosti Ústavu strategických studií Univerzity obrany v Brne. Je autorom a hlavným koordinátorom spracovania publikácie Česká bezpečnostní terminologie. Významnou mierou zhrnul a rozpracoval poznatky z oblasti terminológie, fungovania a členenia spravodajských služieb. Venoval sa problematike transformácie spravodajských štruktúr v postkomunistických krajinách.*

Jsem rád, že letošní sympozium obrací pozornost k praktické rovině zpravodajské činnosti.Nepochybuji, že všichni dnešní referující se absolutně shodnou na tezi, že ochrana zdrojů a jejich identity zdrojů je ústředním pravidlem zpravodajské činnosti. Dá se říci, že je to jedno z ústředních paradigmat zpravodajců, chápané jako posvátný eticko-profesní příkaz číslo jedna. Budu hovořit o *lidských* zdrojích (spolupracovnících, informátorech), i když mnohé, co uvedu, platí beze zbytku i při ochraně zdrojů a metod při sběru zpravodajských informací *technickými* prostředky; ostatně zmiňuji se o tom níže. Ochrana lidských zdrojů je součástí řízení lidských zdrojů.

Obdobný, byť ne vždy natolik rigorózní přístup k ochraně svých informačních zdrojů zaujímají kriminalisté. A rovněž novináři, zejména investigativní chrání identitu zdroje, i za cenu soudního popotahování.

Myslím, že nemusím detailně rozebírat, **proč** chránit identitu zdrojů. Řeknu to stručně a populárně, a záměrně použiji (gramaticky) první osobu jednotného čísla.

Když nebudu identitu lidských zdrojů náležitě držet v tajnosti:

- mohou mé zdroje dojít k těžké úhoně,
- nepodaří se mi získat zdroje nové,
- ztratím výhodu nad protivníkem / protihráčem,
- zničím si vlastní pověst.

Dnešní doba bohužel nepřeje tradičním ctnostem zpravodajských služeb, jako je kázeň, diskrétnost, mlčenlivost a loajalita ke službě. Ale zdá se mi, že ochrana zdroje natolik vrostla do nitra zpravodajského důstojníka, že mezi nejrůznějšími prohřešky bývalých či stávajících zpravodajců prozrazení identity zdrojů se objevuje nejméně často. Zásada chránit zdroj a jeho identitu se do duše nového zpravodajce vtiskne brzy, snadno a pevně. Příčinu vidím v psychologickém sklonu, který se pokusím popsat níže.

Jestliže *já sám* se s dotyčným zdrojem utajeně scházím, kladu mu otázky, dávám mu úkoly a zapisuji příslušné reporty (nebo dokonce jestliže jsem zdroj sám osobně pro spolupráci získal!), zřetelně cítím, že jsem s oním zdrojem-člověkem spojen osobními pouty a odpovědností. Současně jsem si vědom, jak jsem si získání dříve skryté informace svým vlastním úsilím odpracoval.

Současně kolem sebe vidím, jak lidé nedbale zacházejí s osobními, citlivými a důvěrnými informacemi, jak rádi tlachají, pomlouvají, baví se o jiných a sytí se klepy o nich, ***svou* práci se rozhodnu bedlivě střežit. Je to přece produkt mého úsilí** a cosi jako **„můj majetek“**.

A tak se zpravodajec-nováček rychle a dobrovolně podrobí pravidlům konspirovaného styku, psaní zamlžených reportů, krycích jmen atp. Pochopí a úzkostlivě dodržuje zásadu nezbytné znalosti *(need to know)* – v našem případě identitu zdroje. Proto taky akceptuje stejné chování blízkých kolegů.

Psychologický sklon **udržet vlastní tajemství** se střetá s jiným psychologickým sklonem, puzením ke **zvědavosti a indiskrétnosti**. Myslím, že oba biologicko-psychologické sklony spojuje postavení člověka jako sociálního tvora, který ve své societě potřebuje zaujmout a posléze si udržet postavení, jež mu poskytne nějaké **výhody nad druhými**. (Pro citlivější duše podotýkám, že to nevylučuje altruistické chování.)

Opakuji - spravodajci „efektivně rozštěpí" svůj psychologický vztah k tajemstvím: své (a naše) chránit, cizí získávat. A tajemství zahrabané nejhlouběji, které nevyplave ani při uřeknutích či v opilosti, je identita ***mých*** zdrojů.[1]

Připomeňme též, že když se po roce 1989-1990 v postkomunistických zemích začaly zveřejňovat seznamy spolupracovníků bývalých komunistických tajných služeb, vedlo to ke ztížení práce nových služeb, k neochotě občanů spolupracovat z obavy z dehonestujícího zveřejnění. Příslušníkům nových služeb to tehdy paradoxně poskytlo další výchovnou profesně-etickou lekci jak být opatrný, jak chránit zdroj a zda lze dodržet dané sliby.

Operativní ochrana identity a bezpečnosti lidského zdroje informací zahrnuje specifické profesní postupy a organizační opatření (definované interními směrnicemi[2]).

Znamená to mj.:

- omezit počet zasvěcených (**princip nezbytné znalosti**), včetně komplikovaného přidělování přístupových práv uvnitř organizace (kompartmentace),
- praktikovat konspirovaný styk se zdrojem[3],
- získané informace vhodné pro další informační tok v reportech[4] sanitizovat, tj. oprostit od možnosti uhodnout, kdo je zdroj,
- provádět klamné operace, tj. odvádět pozornost jinam.

---

[1] A naopak, čím vzdálenější je jiné (*cizí*) pracoviště zpravodajského nebo kriminalistického zaměření, tím častěji je v uzavřených komunitách zpravodajské a policejní branže oblíbeným předmětem zábavy „kdo tam u nich koho zverboval" atd. A toto je jeden z důvodů, proč operativci velmi neochotně zapisují identitu zdrojů do lustrovatelných databází, ačkoliv dobře vědí, proč jsou takové databáze účelné.

[2] Směrnice tohoto druhu není ani nezbytné utajovat. Viz například britský úřední dokument Covert Human Intelligence Sources (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97958/code-practice-human-intel.pdf).

[3] Některé rozvědky dodržují zásadu, že **obsah** informace od zdroje je ze zahraničí na domovskou centrálu zaslán jedním kanálem (jednou šifrou, jedním způsobem…), zatímco **okolnosti** setkání reportuje kanálem zcela odlišným. Při vhodné formulaci obou dokumentů lze dosáhnout toho, že když protivník zachytí jeden z nich, dozví se jen málo.

[4] Ani v dokumentech **uvnitř** operativního pracoviště není zdroj pojmenováván pravým občanským jménem. Místo „s Abú Músou se sejdu v Bejrútu" se napíše „schůzku s Malíkem uskuteční OP v Břeclavi"… Ti, kdo mají vědět, vědí, kdo je Malík a kde leží Břeclav.

Středoevropské zpravodajské služby mají podle mého názoru jedno společné **organizační paradigma**. Role a organizační postavení **dvou** souvisejících **pracovišť** jsou výrazně odděleny. Jedni lidé sbírají utajeně skryté informace od lidských zdrojů; to je operativa, též zvaná HUMINT. Jiní lidé zpracovávají přicházející neanalyzované informace (*pieces of Information*) do takové podoby zpravodajské informace (*intelligence*), jež může být předána zákazníkům[5]; to je analytika.

Ve střední Evropě je obvyklé, že analytici ústředního analytického pracoviště, zaměření na určitý **tematicky definovaný problém** nebo na **určité teritorium**, obdrží **všechny** získané informace daného zaměření, ale **neznají identity** zdrojů než pod kódem (zpravidla alfanumerickým, třeba A123) nebo krycím jménem (zpravidla jednoslovným, třeba Jumbo).[6] Nevím, zda tento středoevropský model je ten nejlepší možný; má svá plus i minus.[7] Nicméně středoevropský model vyžaduje, aby na pracovišti HUMINT-u, neboli na operativě, se interně pěstovala tzv. **operativní analytika**. V praxi bývají spory o tom, jakou má onen operativní analytik úlohu a jaké kompetence. Podle mého názoru jednoznačně **má znát identitu zdroje** a analyzovat *právě to*, co se ústřední analytické pracoviště (analýza problému či teritoria) nedozví, protože je to ani nezajímá. Interní analytik uvnitř operativy se zabývá tím, jak probíhá styk se zdrojem, jaká je lidská situace onoho zdroje, jaké má slabiny, co to znamená pro bezpečnost spolupráce, jaká je situace v jeho okolí, v jeho zemi. Hledá ale také známky nesolidnosti zdroje, přítomnosti zavádějících informací. Operativní analytik je tedy podle mého pojetí *současně* podporou řídícímu operativci, podporou zdroji, trochu bezpečnostním důstojníkem i tak trochu kontrarozvědčíkem. Oproti řídícímu operativci (*handler, runner*) **není** operativní analytik „zatížen" osobní vazbou[8] ke zdroji, vztahem, jenž někdy zaslepuje.

Na okraj tohoto tématu nutno doříci: sanitizace a odosobňování zdrojů v informačním toku uvnitř služby nelze přehánět ad absurdum. Dobrý zpravodajský analytik (tj. ten na analytickém pracovišti) rozpozná celkový obraz i ze souboru zlomků a okrajových náznaků. Po delší době může nakonec identitu zdroje určit (zpravidla v tichosti, aniž při tom hne brvou).

Ve fázi přípravy zpravodajské zprávy pro zákazníka (vysokého státního úředníka nebo pro politika) se text sdělení znovu přeformulovává. Ve výsledné podobě se zamlží identita zdroje, mnohdy se záměrně zamění SIGINT za HUMINT a naopak, dokument se např. proloží tvrzeními „naše utajené zdroje v plné míře potvrdily domněnku známého komentátora (novin)"[9]. A to uděláme i politikovi, jemuž věříme;

---

[5] Zde nemám na mysli takticko-operační zpravodajce vojenské, ani situaci v policii, tedy obsluhu agentů řízených kriminalisty.

[6] Někdy, v případě velmi citlivých zdrojů, operativa informace od jednoho zdroje dokonce připíše zdrojům několika. Je pravda, že takový postup analytikům ztíží možnost posoudit spolehlivost zdroje.

[7] Mám za to – i když relevantní informace o vnitřních vztazích uvnitř zpravodajských služeb jsou k dispozici jen zřídka – že anglosaské organizace nejsou v oddělení rolí operativy a analytiky tak rigorózní. Britský *desk officer* se mírně blíží shora popsanému operativnímu analytikovi.

[8] Le Carré, Tajný společník (správně přeloženo: Tajný poutník), str. 10 českého překladu, upraveno. Smiley vypráví o vztahu ke zdroji: „K tradičnímu pojetí služby s představou *operativce* jako učitele, pastýře, rodiče a přítele dodal roli majetkového a manželského poradce, odpustkáře, společníka a ochránce. Ať muž, nebo žena, řídící *operativec* je člověk nadaný schopností vzít jakoukoliv špatnost jako všední záležitost, a tím se stát v představách svého agenta jeho skutečným partnerem."

[9] Trochu to přeženu: Ideální výsledná zpravodajská zpráva vypadá tak, že po uběhnutí cca 5 let (kdy paměť veřejnosti na detaily odezní) je možno její obsah v úplnosti zveřejnit… Identita pro ni použitých zdrojů a metod avšak nechť zůstane utajena 70 let!

nikoli osobně kvůli němu, ale kvůli jeho úřednickému okolí, jež *nikdy* nejsme s to monitorovat v úplnosti.

To, co jsem výše uváděl o lidském zdroji, platí i o dalších metodách (disciplínách) utajeného získávání informací. Specifická metoda záchytu v COMINT-u (obecněji ve všech technických INT-ech) se musí chránit někdy ještě důsledněji než totožnost člověka. Nejde tu o životy, ale o velké peníze.

Znamená to mj.:

- omezit počet zasvěcených (princip nezbytné znalosti), opět včetně komplikovaného přidělení přístupových práv,
- získané informace vhodné pro další informační tok v reportech svádět na jiné zdroje, tj. oprostit od možnosti uhodnout, kudy se odposlouchává[10],
- provádět klamné operace, včetně popírání jistých dovedností[11].

Je zřejmé, že utajování, ochranné postupy, zásada nezbytné znalosti, kompartmentace a sanitizace jsou:

- Za prvé: samy o sobě **pracné**. Z toho plyne zlozvyk je dělat nedůsledně.
- Za druhé: Zásady utajování z principu snižují efektivitu informačního toku, zpomalují jej a někdy mu i brání.
- Za třetí: Navíc návyk *na need to know* psychologicky ovlivňuje zpravodajce tak, že zapomínají, že rčení má ještě druhou polovinu: *need to share*, tj. **nezbytnost sdílet**. Málokterý ze zpravodajců přemýšlí takto[12]: **kdo ještě by měl toto vědět, komu by se ještě tato informace mohla hodit**?
- Za čtvrté: jako v každém komplikovaném a obtížně kontrolovatelném poli, utajovací postupy mohou svést některé spolupracovníky i kmenové zpravodajce k přibarvování produktu šizení nebo dokonce k sebeobohacování, bohužel. Není-li tento nešvar páchán systematicky a ve velkém, je pramalá šance na to přijít.

Posvátná ochrana zdroje je nutnou podmínkou efektivní zpravodajské práce. Je nezbytná, ale jak jsem uvedl, **má i některé neblahé důsledky.**

[10] Ať si protivník raději myslí, že máme pět informátorů v jeho generálním štábu, než aby přišel na to, že jsme mu napíchnuli kabel.

[11] Například vysílat šifrované depeše do teritoria, kde toho času ani „nikoho nemáme“. Nebo znejisťovat veřejnost tím, že se jisté dovednosti popírají jako fyzikálně nemožné.

[12] Zde leží jeden z důvodů opakovaného selhávání zpravodajských služeb. Kdesi „v systému“ klíčová informace k mání je, ale nedoputuje na potřebné místo… Je to věčný problém, pro nějž neexistuje definitivní řešení.

Závery zo sympózia

1. Lektori sympózia sa zhodujú na zásade, že ochrana informačných zdrojov a hlavne ochrana identity zdrojov je ústredným pravidlom utajovaného zberu a využívania skrytých informácií spravodajských služieb. Legitimita ochrany informačných zdrojov spravodajských služieb je základom regulačného rámca ochrany štátnych tajomstiev.
2. Zborník príspevkov zo sympózia bude poskytnutý funkcionárom a expertom štátnych inštitúcií, ktorí sa zaoberajú problematikou distribúcie utajovaných informácií a ich ochranou.
3. Zborník príspevkov zo sympózia bude k dispozícii poslancom - členom výborov Národnej rady SR na kontrolu činnosti spravodajských služieb, aby sa mohli kompetentnejšie venovať problematike spravodajských služieb.
4. Možno považovať za spoločensky prínos tradíciu medzinárodných sympózií o spravodajských službách na pôde Fakulty práva Paneurópskej vysokej školy, pretože tieto podujatia otvárajú aktuálne otázky spravodajskej komunity a umožňujú študentom hlbšie chápať problematiku spravodajských služieb.
5. Zahraničným a domácim lektorom patrí vysoké ocenenie za obetavosť a ochotu bez nároku na odmenu prezentovať svoje názory na sympóziu; vysoké uznanie si zaslúži osemročná aktivita Asociácie bývalých spravodajských dôstojníkov a rovnako aj spolupráca s Fakultou práva Paneurópskej vysokej školy, ktorá vytvára materiálne a organizačné zázemie týmto podujatiam.

Bratislava 4. decembra 2014