Miroslav Brvnišťan

Stav právnej úpravy ochrany utajovaných informácií EÚ ako predpoklad ich efektívnej ochrany a zabezpečenia konzistentnosti obdobnej právnej úpravy členských krajín EÚ[1]

Anotácia: Článok sa zaoberá vybranými aspektmi systému ochrany utajovaných informácií EÚ, jeho aktuálnym stavom a vývojom. Realizácia možných opatrení v oblasti ochrany utajovaných informácií EÚ priamo závisí od ochoty jednotlivých členských krajín zabezpečiť konzistentnosť pravidiel a bezpečnostných štandardov. Analýza systému ochrany informácií EÚ v jeho komplexnosti vytvára široký priestor na zamyslenie sa nad možnosťami jeho zefektívňovania s priamymi dôsledkami na systémy ochrany informácií jednotlivých členských štátov. Európska integrácia a jej prehlbovanie môže byť kľúčovým činiteľom pre ďalšie zefektívňovanie ochrany informácií utajením ako substantívneho nástroja ochrany spoločných európskych záujmov.

Kľúčové slová: utajovaná informácia, bezpečnostná situácia, bezpečnostné riziká, ochrana informácií Európskej únie, bezpečnostná dohoda, integrácia EÚ.

Úvod

Ochrana informácií Európskej únie (ďalej len EÚ) je vo všeobecnosti vnímaná ako integrálna súčasť bezpečnostných systémov jednotlivých členských krajín, úzko súvisiaca s realizáciou spoločných európskych záujmov, ako aj záujmov jednotlivých členských krajín. Zároveň to znamená, že oblasť ochrany "národných" utajovaných skutočností je takmer nemožné posudzovať bez porozumenia širších súvislosti, majúcich priamy vzťah k opatreniam prijímaným na úrovni EÚ. Nejednoznačnosť európskej integrácie a jej imanentných cieľov, odlišné postoje, záujmy a právne prostredie členských krajín ovplyvňujú inštitucionálne a právne prostredie EÚ vrátane ochrany informácií prostredníctvom režimu utajenia. Do úvahy je potrebné brať aj meniace sa bezpečnostné prostredie a nové bezpečnostné výzvy, ktoré kladú bezprecedentný tlak na bezpečnosť ako takú, nevynechajúc bezpečnosť systému ochrany informácií, špecificky systém ochrany informácií utajením (ďalej len **OIU**).

Nové bezpečnostné hrozby atakujú zabehnuté národné a medzinárodné (nadnárodné) bezpečnostné mechanizmy často až na hranicu ich zlyhania. Vytvárajú tým elementárne predpoklady pre adekvátnu reakciu na rôznych úrovniach riadenia štátov a nadnárodných zoskupení bez ohľadu na to, či ide o rozhodovanie politické alebo odborné. Sme svedkami procesov, pri ktorých sa meniace bezpečnostné prostredie stáva výzvou, na ktorú je ťažké nájsť odpoveď v rámci existujúcich bezpečnostných mechanizmov.

Situáciu komplikuje aj fakt, že postoje a zámery jednotlivých členských štátov, rôznych lobistických zoskupení, politikov, orgánov a inštitúcií EÚ sú nesúrodé, čo podmieňuje prijímanie rôznych kompromisov a náhradných riešení.

Samotný vznik EÚ a integračný proces nových členských krajín do EÚ ovplyvnil výrazným spôsobom fungovanie bezpečnostných mechanizmov EÚ zameraných na ochranu informácií. Jedným z dôvodov je najmä fakt, že v dôsledku procesu integrácie dochádza priamo k obmedzeniu a odovzdaniu niektorých výlučných právomocí členských krajín EÚ v prospech EÚ. Postupne sa aj bezpečnosť členských krajín a realizácia ich bezpečnostných záujmov stáva integrálnou súčasťou bezpečnostných opatrení v rámci EÚ.[2] Členské krajiny sa podieľajú na činnosti orgánov EÚ a vznikajúcich (plánovaných) bezpečnostných štruktúr, čím priamo zabezpečujú konzistentnosť

[1] Tento príspevok je podporovaný Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV – 16-0521.

[2] Podrobnejšie v Ustanoveniach o spoločnej bezpečnostnej a obrannej politike, čl. 42, Zmluva o Európskej únii.

a koordinovanosť svojich vnútroštátnych („interných“) opatrení s opatreniami realizovanými prostredníctvom EÚ. Spôsob, akým dokážu členské krajiny zosúladiť svoje „interné“ kroky s krokmi prijímanými v rámci EÚ, určuje tiež celkovú efektívnosť spoločného EÚ systému bezpečnosti a ochrany informácií utajením.

To, čo bolo historicky budované ako záruka bezpečnosti a stability, je v súčasnosti často vnímané ako znak nemohúcnosti a aj neschopnosti reagovať primerane na nové bezpečnostné výzvy. Tento stav bol čiastočne predvídateľný a logický, minimálne s ohľadom na viaceré historické skúsenosti.[3] Určitým prekvapením však je systematické nepripúšťanie si tohto stavu a snáď aj určitá snaha o predstieranie funkčnosti súčasných bezpečnostných mechanizmov a bezpečnostného systému. Pripustenie zaostávania v oblasti bezpečnosti informácií by bolo predsa neprijateľné a nepredstaviteľné.

Oblasť ochrany informácií utajením je podľa nášho názoru kľúčová z hľadiska bezpečnosti EÚ. V minulosti existovali viaceré pokusy a návrhy na zmeny v bezpečnostnom systéme EÚ, niektoré sa aj uskutočnili.[4] Súčasná bezpečnostná situácia a vývoj naznačujú, že je potrebné byť neustále pripravený čeliť novým bezpečnostným výzvam a hrozbám.

V súlade s uvedeným sa preto budeme zaoberať analýzou súčasného systému OIU EÚ, ktorý je možné na prvý pohľad vnímať jednotne a konzistentne, no v skutočnosti ide o zložitý a komplexný systém pozostávajúci z viacerých podsystémov. Tieto vznikali v rôznych etapách európskej integrácie a ich opodstatnenie sa postupne menilo a vyvíjalo v súlade so záujmami členských krajín. Pri posudzovaní možností ďalšieho rozvoja systému OIU EÚ vo väzbe na možné prehlbovanie integrácie EÚ sa zameriame najmä na popísanie vzťahu „vývoj EÚ verzus záujmy členských krajín“ a jeho koherentnosť. Realizácia záujmov členských krajín bude určujúcim faktorom pre pochopenie vývoja systému OIU a jeho súčasného stavu a zároveň nástrojom na načrtnutie možného vývoja do budúcnosti.

1 Východiská vývoja a základy systému ochrany informácií EÚ

Základy súčasného systému ochrany informácií Slovenskej republiky (ďalej len SR) boli vytvorené najmä po II. svetovej vojne, práve v čase, kedy vznikali aj základy Severoatlantickej aliancie (ďalej len NATO) a Európskej únie. Principiálne rovnaké východiská z hľadiska požiadaviek na bezpečnosť informácií a vtedajšej globálnej bezpečnostnej situácie boli rozpracované rôzne, nielen tzv. východ verzus západ,[5] ale situácia sa odlišne vyvíjala aj z pohľadu NATO a EÚ. Napr. bezpečnostná politika NATO upravujúca oblasť ochrany informácií je konzistentný dokument, ktorý systematicky upravuje ochranu informácií. Systém bezpečnosti informácií EÚ je omnoho komplikovanejší, čo pramení z celkovej nejednoznačnosti cieľov EÚ v oblasti bezpečnosti a ich postupného vývoja. Uvedené je možné považovať za dôvod prečo je systém ochrany informácií EÚ neprehľadný, zložitý a aj neefektívny. Vývoj bezpečnostného systému EÚ však neustále pokračuje, často však skôr s ohľadom na partikulárne (národné) politicko-bezpečnostné záujmy členských krajín, než skutočné (a spoločné) bezpečnostné záujmy. V tomto kontexte by určujúcimi, okrem bezpečnostných a politických záujmov, mali byť faktory ako dôsledné poznanie bezpečnostnej situácie, jej analyzovanie a definovanie bezpečnostných hrozieb. Až následne by mali byť prijímané opatrenia v súlade s politickými a bezpečnostnými záujmami a možnosťami ich realizácie.

---

[3] Poznámka autora: V súčasnosti je možné za takúto výzvu považovať odchod Veľkej Británie z EÚ, najmä preto, že táto bola jedným z kľúčových tvorcov bezpečnostného systému EÚ pre ochranu informácií.

[4] Poznámka autora: Za takýto krok je možné považovať aj kodifikáciu bezpečnostných pravidiel Európskej Rady a Komisie v roku 2004, týkajúcich sa ochrany utajovaných informácií EÚ, ako súčasť podmienených zmien súvisiacich s rozširovaním EÚ.

[5] Bližšie v BRVNIŠŤAN, M. 2013. Ochrana utajovaných skutočností v spektre historického vývoja, Bratislava: Tlačiareň Ministerstva vnútra SR, str. 11 a 55.

"Odlišnosti" členských krajín EÚ, ako faktor zohrávajúci kľúčovú rolu pri budovaní kompatibility bezpečnostných systémov členských krajín, je potrebné brať do úvahy pri uvažovaní o spoločnej realizácii bezpečnostných záujmov na úrovni EÚ. Často ide snáď len o dôsledok historických procesov a skúseností, ktoré však majú závažné dôsledky pre budovanie spoločného bezpečnostného systému. Obdobne, jednotlivé členské krajiny nezdieľajú rovnaké pohľady a názory na aktuálne bezpečnostné riziká.[6] Vývoj v oblasti spoločnej bezpečnosti EÚ v ostatnom období poukazuje na možné zmeny. Viacerí politici sa čoraz častejšie vyjadrujú na margo spoločnej bezpečnosti EÚ a navrhujú riešenia. Napr. taliansky premiér Matteo Renzi vyzval na zriadenie vlastnej spravodajskej služby EÚ. Uviedol, že ak má EÚ spoločnú menu, musí mať aj spoločný bezpečnostný a spravodajský systém.[7] Ostatný vývoj v EÚ a vyjadrenia aj iných vrcholných predstaviteľov potvrdzujú tieto tendencie. Francúzsky prezident Macron už v roku 2017 vyzval na vytvorenie spoločného európskeho vojenského projektu, zatiaľ čo nemecká kancelárka Merkelová vo svojom prejave v Európskom parlamente v novembri 2018 uviedla, *„že by sme mali pracovať na vízii vytvorenia skutočnej európskej armády*". Smerovanie k bezpečnostnej a obrannej únii bolo jednou z priorít Komisie. Niektoré nedávne opatrenia EÚ na posilnenie spolupráce v oblasti obrany a bezpečnosti tomu nasvedčujú:

- Lisabonskou zmluvou sa ustanovila spoločná obranná politika EÚ (článok 42 ods. 2 ZEÚ). V zmluve sa však jasne definuje aj význam národnej obrannej politiky vrátane členstva v NATO alebo neutrality.
- EÚ začala vykonávať ambiciózne iniciatívy s cieľom zabezpečiť viac zdrojov, podporiť efektívnosť, uľahčiť spoluprácu a podporiť rozvoj spôsobilostí.
- Stála štruktúrovaná spolupráca (PESCO - Permanent Structured Cooperation) začala v decembri 2017 a od júna 2019 sa na nej zúčastňuje 25 členských štátov EÚ s platnými záväzkami vrátane európskeho zdravotníckeho velenia, systému námorného dozoru, tímov rýchlej kybernetickej reakcie a vzájomnej pomoci v oblasti kybernetickej bezpečnosti, ako aj spoločnej spravodajskej školy EÚ.
- Európsky obranný fond (EOF) začal fungovať v júni 2017. Po prvýkrát sa tak európsky rozpočet používa na spolufinancovanie spolupráce v oblasti obrany a tento fond by sa mal stať súčasťou budúceho dlhodobého rozpočtu EÚ (2021-2027). Európsky obranný fond bude dopĺňať vnútroštátne investície a poskytovať praktické aj finančné stimuly pre spoločný výskum, spoločný vývoj a nadobúdanie obranných zariadení a technológií.

Navrhované opatrenia je možné efektívne uskutočniť len za predpokladu hlbšej integrácie, a teda realizácie nie národných, ale širších spoločných záujmov. V budúcnosti sa dá očakávať väčší prenos kompetencií (národných) na nadnárodné zoskupenia, a to aj v oblasti obrany a bezpečnosti.

Neefektívne a pomalé riadenie v oblasti bezpečnosti a byrokratizácia sa prejavujú v neschopnosti bezpečnostných systémov efektívne identifikovať hrozby a následne správne a včas reagovať na aktuálne hrozby. Uvedené je možné považovať za jedno z najzásadnejších bezpečnostných rizík súvisiacich s rozvojom a riadením bezpečnostných systémov, najmä v časoch enormného nárastu množstva informácií a kybernetických hrozieb, terorizmu a kybernetického terorizmu, rôznych asymetrických a hybridných hrozieb. Ochrana informácií v takomto komplikovanom a nejednotnom prostredí je náročná a s ohľadom na vynakladané prostriedky neefektívna, a preto je potrebné zjednocovanie a prísna štandardizácia.

Nesúlad strategických dokumentov a ich neaktuálnosť ide ruka v ruke s riadením bezpečnostného systému, určujúcim jeho dlhodobé smerovanie. Pri bližšom pohľade na riadenie

[6] Ako príklad môže poslúžiť bezpečnostné riziko v oblasti personálnej bezpečnosti – spolupráca s niektorými štruktúrami bývalej štátnej polície v krajinách východnej Európy. Uvedené riziko väčšina členských krajín nepozná, no rovnaká informácia (napr. utajovaná informácie EU Confidential) sa môže nachádzať vo viacerých členských krajinách, pričom jej môže byť na základe dodržiavania minimálnych štandardov poskytnutá odlišná ochrana.

[7] Podrobnosti na www.aktuality.sk, 12.1.2015.

bezpečnostného systému SR je možné konštatovať, že zásadný dokument (bezpečnostno-politický), ktorý by mal určovať smerovanie rozvoja bezpečnostného systému - Bezpečnostná stratégia SR,[8] je zastaraný, čím je spochybnený samotný cieľ. Argumenty, že dokument je univerzálny a jeho aktualizácia nie je potrebná, neobstoja. Ak má plniť svoje primárne poslanie, je potrebné, aby takýto dokument bol aktuálny a v praxi využívaný a jeho realizovanie kontrolované.[9] Aktuálnosť by mala byť posudzovaná nielen z hľadiska časového, ale aj z hľadiska komplementárnosti k iným strategickým dokumentom, ktoré sa týkajú partikulárnych oblastí bezpečnosti a nadnárodných zoskupení.[10] Tieto dokumenty by mali byť vnímané ako celok, ktorý definuje celkové smerovanie bezpečnostného systému SR a zároveň jeho miesto v bezpečnostnom systéme nadnárodného zoskupenia - EÚ. Na dosiahnutie uvedeného je však potrebné zosúladiť najmä oblasti realizácie záujmov SR (definovať národné záujmy a záujmy SR realizované v rámci nadnárodných zoskupení), nakoľko bez tohto kroku nie je možné pristúpiť k potrebným zmenám v systéme ochrany informácií vo väzbe na strategické dokumenty.

Nová Bezpečnostná stratégia SR by mala zareagovať na aktuálne zmeny v geopolitickej a bezpečnostnej situácii v euroatlantickom a eurázijskom priestore. Zároveň by mala brať do úvahy nové strategické dokumenty nielen nadnárodných zoskupení, ale aj jednotlivých krajín, napr. Stratégiu národnej bezpečnosti Ruskej federácie, Bezpečnostnú stratégiu USA. Až následne je možné pristúpiť k špecifikácii národnej bezpečnostnej politiky pre oblasť ochrany informácií utajením.

2 Súčasný systém ochrany utajovaných informácií EÚ

Systém OUI EÚ sa nevyvíjal systematicky a v zásade až do súčasnej doby plne nereflektuje požiadavky zodpovedajúce miere európskej integrácie.[11] Jeho základy pochádzajú z počiatkov budovania EÚ, kedy ciele budovania EÚ boli odlišne stanovené.

Je zrejmé, že miera realizácie spoločných záujmov jednotlivých členských krajín prostredníctvom EÚ stále nedosiahla takú úroveň, aby vytvorila dostatočný tlak na definovanie spoločného, jednotného európskeho systému OUI.

Súčasný stav v oblasti predpisov OUI EÚ je možné predstaviť prostredníctvom stručnej analýzy vybraných nosných predpisov EÚ pre oblasť OUI. Tieto boli postupne prijímané najmä ako dôsledok (nutnosť) rozširovania EÚ - požiadaviek nových členských krajín na jednoznačnú záväznosť predpisov v oblasti ochrany informácií. Ich priama záväznosť a aplikovateľnosť je často diskutovaná, preto neposkytujú jednoznačný právny rámec pre právnu úpravu oblasti ochrany informácií EÚ. Ako je aj z úvodných ustanovení jednotlivých analyzovaných dokumentov zrejmé, pri ich tvorbe sa vychádzalo z ustanovení zmlúv a predpisov upravujúcich interné pravidlá alebo rokovacie poriadky inštitúcií EÚ. Riešenie, ktoré sa takto prijalo je síce právne odôvodniteľné, no zároveň poskytuje priestor na rôzne úvahy spochybňujúce ich záväznosť, a to najmä vo vzťahu k členským krajinám.

1. **Zásadným pre oblasť OUI bol vznik Európskeho spoločenstva pre atómovú energiu - ESAE**. Realizácia spoločných záujmov v oblasti energetickej nezávislosti, výskumu v oblasti

[8] Bezpečnostná stratégia SR, 2005.

[9] Poznámka autora: Aby sa v budúcnosti neopakovala takáto situácia, bolo by žiaduce nájsť mechanizmus, ktorý by viedol k pravidelnej aktualizácii bezpečnostnej stratégie. Príkladom by mohlo byť riešenie aplikované v USA, kde na základe zákona kongres USA raz ročne prejednáva správu o národnej bezpečnosti, na základe ktorej sa upravujú strategické dokumenty.

[10] Napr. Stratégia kybernetickej bezpečnosti EÚ, Bezpečnostná stratégia NATO.

[11] Pozri bližšie: BRVNIŠŤAN, M. 2013. Ochrana utajovaných skutočností v spektre historického vývoja, Bratislava: Tlačiareň Ministerstva vnútra SR, str. 54.

atómovej energie a rozvoja nukleárneho priemyslu boli nosnými myšlienkami, na ktorých sa budúce členské štáty zhodli.[12] Došlo k vzniku potreby vzájomnej výmeny špecifických a vysoko citlivých informácií, ktoré boli spravidla v rámci jednotlivých krajín utajované. Zdieľanie takýchto informácií a vytvorenie zodpovedných orgánov spoločenstva predpokladá už samotná zakladacia zmluva ESAE,[13] čo je zároveň možné považovať za základ opatrení pre vznikajúcu oblasť OUI v rámci spoločenstiev. Na základe zmluvy o ESAE (článok č. 24, 25 a 217)[14] bola Radou EÚ na návrh Európskej komisie schválená **smernica Euratom č. 3.**[15] Smernica implementovala uvedené články Zmluvy zakladajúcej ESAE a definovala základy OUI vytvorením potrebnej bezpečnostnej štruktúry a orgánov na čele s Bezpečnostným úradom Európskej komisie. Týkalo sa to však iba informácií získaných ESAE alebo vymieňaných medzi členskými krajinami v súlade so Zmluvou o ESAE. Takéto informácie boli označované ako „Euratom utajované informácie" (Euratom Classified Information, v skratke „ECI").[16] Jednotlivé stupne utajenia poskytujú rôzny stupeň ochrany spoločným európskym záujmom. Napríklad stupeň utajenia označovaný ako Eura-Prísne tajné znie: *„neoprávnené poskytnutie informácií by malo mimoriadne vážne dôsledky pre obranné záujmy jedného alebo viacerých členských štátov"* alebo pre stupeň Eura-Dôverné: *„neoprávnené poskytnutie informácií by poškodilo obranné záujmy jedného alebo viacerých členských štátov*". Je zrejmé, že takto definované stupne ochrany majú viacero zaujímavých konzekvencií. V prvom rade ide o určitý rozpor zo zameraním ESAE, kde sa primárne neuvádzajú obranné záujmy. Uvedené môže byť dôsledkom prebrania bezpečnostného systému ZEÚ, ktorý mal obranné a hospodárske ciele. V druhom rade sa v definíciách stupňov utajenia uvádzajú dôsledky pre jeden alebo viaceré členské štáty, a teda nie pre dané spoločenstvo krajín (EÚ ako takú), čo je pravdepodobne vyjadrením postoja členských krajín k spoločnej OUI, keďže je v podstate nahrádzaná systémami OUI jednotlivých členských krajín. V treťom rade je tým zrejme vyjadrený postoj k ochrane spoločných záujmov v tak citlivej oblasti ako je spoločná obrana. Tento stav bol zapríčinený priklonením sa k možnosti realizovať spoločné obranné záujmy v rámci Severoatlantickej aliancie.[17]

Napriek tomu, uvedená smernica platí nezmenene aj v súčasnosti. Ostatné citlivé informácie členských krajín nemali z hľadiska ESAE právny rámec. Ak dochádzalo k výmene takýchto informácií, tak len na základe bilaterálnych dohôd medzi jednotlivými členskými štátmi, ktoré vytvorili právny rámec zastrešujúci výmenu utajovaných informácií aj v nastávajúcom období.

2. **Rozhodnutie Rady Európskej únie (ďalej len Rada) z 23.9. 2013, č. 2013(488)EU,** ktorým sa prijímajú bezpečnostné smernice Rady.
Rozhodnutie bolo spracované na základe :

- článku 240(3) Zmluvy o fungovaní EÚ, (Rada a Komisia môžu prijať interné pravidlá);
- článku 24 Rozhodnutia Rady z 1. 12. 2009 č. 2009/937/EU, ktorým sa prijíma rokovací poriadok Rady.

---

[12] Objavovali sa však aj názory na budovanie vlastných atómových síl, nakoľko krajiny ako Francúzsko a Veľká Británia sa nechceli spoliehať na ochranu len prostredníctvom „atómového dáždnika" USA, NATO history. Bližšie pozri:www.members.tripod.com, 2008.

[13] Článok 24 zmluvy o založení ESAE.

[14] Článok 24 hovorí o ochrane informácií, ktoré spoločenstvo získa ako výsledok výskumu a prezradenie ktorých by mohlo poškodiť záujmy členských štátov, a preto tieto majú byť predmetom ochrany bezpečnostným systémom; zároveň v ods. 1 sa navrhuje prijať bezpečnostné smernice, ktoré stanovia bezpečnostné stupne; článok 25 stanovuje princípy komunikácie medzi EK a členskými štátmi a dodržiavanie bezpečnostných označení; v článku 217 sa hovorí, že prijatie potrebných smerníc sa má uskutočniť do 6 mesiacov po nadobudnutí platnosti zmluvy.

[15] Smernica (Euratom) č. 3, Úradný vestník Európskej únie sp. v. L 17/58 z 6.10.1958.

[16] Článok 1 bod 1 Smernice Euratom č. 3, ktorou sa implementuje článok 24 Zmluvy zakladajúcej The European Atomic Energy Community.

[17] Pozri bližšie BRVNIŠŤAN, M. 2013. Ochrana utajovaných skutočností v spektre historického vývoja, Bratislava: Tlačiareň Ministerstva vnútra SR, str. 55.

Už z citovaných úvodných ustanovení rozhodnutia je zrejmé, že ochrana informácií Rady nemá reálny základ v zakladajúcich zmluvách. Systémovo sa odvíja len z ustanovení Zmluvy o fungovaní EÚ, ktoré Rade umožňujú prijať interné pravidlá. To je často aj skutočnosť, na ktorú členské štáty poukazujú, pokiaľ ide o záväznosť pravidiel Rady v oblasti bezpečnosti utajovaných informácií.

Zámerom rozhodnutia Rady bolo vytvoriť *mutadis mutandis* nový právny rámec pre komplexný bezpečnostný systém na ochranu utajovaných informácií EÚ. V úvodných ustanoveniach sa napriek tomu kladie aj dôraz na jasné vyjadrenie záväznosti a aplikácie tohto predpisu členskými krajinami, ktoré má už zo svojej povahy „rozhodnutie Rady" prednosť pred vnútroštátnym právom.

Napriek jednoznačnej záväznosti rozhodnutí Rady z hľadiska právnej teórie a zohľadňujúc pravidlo prednosti únijného práva pre právom vnútroštátnym vrátane priamej aplikovateľnosti rozhodnutia Rady, resp. priameho účinku, je v bode 3 Preambuly uvedené, že: „*Členské štáty by v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi a v rozsahu potrebnom pre fungovanie Rady mali dodržiavať toto rozhodnutie, keď ich príslušné orgány, personál alebo dodávatelia manipulujú s utajovanými skutočnosťami EÚ, aby sa každému poskytlo ubezpečenie o tom, že pre utajované skutočnosti EÚ je zabezpečená rovnaká úroveň ochrany"*.

Uvedené ustanovenie je potrebné vnímať aj v kontexte článku 1 ods. 2 tohto rozhodnutia, ktorý znie: „*Tieto základné zásady a minimálne štandardy sa vzťahujú na Radu a Generálny sekretariát Rady a členské štáty ich dodržiavajú v súlade so svojimi príslušnými vnútroštátnymi zákonmi a inými právnymi predpismi, aby sa každému poskytlo ubezpečenie o tom, že pre utajované skutočnosti EÚ je zabezpečená rovnaká úroveň ochrany"*.

Z uvedených ustanovení je zrejmý dôraz na jasné definovanie vzťahu tohto rozhodnutia Rady k všeobecne záväznými právnym predpisom členských krajín. Takisto je zrejmé, že právna konštrukcia úvodných ustanovení predpokladá, že členské krajiny a ich vnútroštátne predpisy sú v súlade s týmto rozhodnutím. Predpokladá sa, že každý členský štát vyvinie úsilie na dodržiavanie stanovených minimálnych štandardov.

Štruktúra a obsah rozhodnutia je principiálne totožná s predchádzajúcimi rozhodnutiami Rady č. 2001(264)ES a č.2011(292)EÚ. Člení sa na dve základné časti.

Prvá časť obsahuje preambulu a úvodné, všeobecné ustanovenia týkajúce sa systému zabezpečenia OUI, definície a popis základných nástrojov ochrany a charakteristiku jednotlivých oblastí OUI. Dôležitým je vymedzenie systémových nástrojov ochrany informácií, z ktorých je zrejmé, tak ako aj v prípade predpisov NATO, že ochrana informácií prostredníctvom ich utajenia je založená na manažmente rizík (napr. kriminálne aktivity, špionáž, sabotáž alebo terorizmus) a následnom flexibilnom prijímaní vhodných opatrení.

Druhá časť obsahuje prílohy týkajúce sa jednotlivých oblastí OUI:

1. Personálna bezpečnosť
2. Fyzická bezpečnosť
3. Správa utajovaných informácií
4. Ochrana utajovaných informácií EÚ v informačných systémoch
5. Priemyselná bezpečnosť
6. Výmena utajovaných informácií s tretími štátmi a medzinárodnými organizáciami.

V kontexte zmienených vykonávacích predpisov (nie sú záväzné a ani priamo aplikovateľné, na rozdiel od samotného rozhodnutia Rady) je zrejmé, že dôraz je kladený na umožnenie fungovania jednotného rámca ochrany utajovaných informácií zdieľaných v rámci EÚ a v záujme EÚ. A to bez ohľadu na to, či ide o informácie inštitúcií EÚ, agentúr, štruktúr alebo členských krajín EÚ – dôležitý je kontext s aktivitami EÚ.

Prakticky to znamená, že členské krajiny môžu vytvárať EÚ utajované informácie a tieto zdieľať s inštitúciami EÚ, agentúrami a inými „štruktúrami EÚ", a zároveň si takéto informácie aj medzi sebou vymieňať.

Na koordináciu bezpečnosti v rámci Rady a jej pôsobnosti bola pod generálnym sekretariátom vytvorená Bezpečnostná kancelária Generálneho sekretariátu Rady a takisto

Bezpečnostný výbor Rady, pozostávajúci zo zástupcov národných bezpečnostných úradov členských krajín.

Návrhy rozhodnutí Rady a prípadných vykonávacích predpisov schvaľuje Bezpečnostný výbor Rady konsenzom. V prípade, že ide o rozhodnutia Rady, sú tieto návrhy posúvané na schválenie cez Antici Group (poradná skupina národných expertov) do COREPER (Comité des Representantes Permanentes - Výbor stálych zástupcov – zástupcovia členských krajín).

Rozhodnutie Rady č. 2013(488)EU zároveň zrušilo predchádzajúce rozhodnutia Rady č. 2001(264)EC a č. 2011(292)EC, pričom všetky utajované informácie sú chránené automaticky podľa nového predpisu.

3. **Rozhodnutie Komisie z 13. marca 2015 č. 2015/444/EÚ, Euratom o bezpečnostných predpisoch na ochranu utajovaných informácií EÚ.** Rozhodnutie Komisie bolo prijaté so zreteľom na:

- Zmluvu o fungovaní Európskej únie, a najmä článok 249 (Komisia môže prijať interné pravidlá),
- Zmluvu o založení Európskeho spoločenstva pre atómovú energiu, a najmä na jej článok 106,
- Protokol č. 7 o výsadách a imunitách Európskej únie pripojený k zmluvám, a najmä na jeho článok 18.

Rozhodnutie Komisie č. 2015/444/EÚ - Euratom tvorí prílohu Rokovacieho poriadku Komisie a priamo v bode č. 3 a 4 jeho úvodných ustanovení sa konštatuje, že Rada, Komisia a Európska služba pre vonkajšiu činnosť (ďalej len EEAS) sa zaviazali, že budú dodržiavať rovnaké bezpečnostné normy. Čo prakticky znamená, že Komisia a EEAS vypracujú svoje predpisy v súlade s rozhodnutím rady č. 2013(488)EU. Zámerom bolo v súlade s rozhodnutím Rady vytvoriť jednotný systém OUI platný pre Komisiu, jej inštitúcie, zastúpenia. Zároveň je v úvodných ustanoveniach (bod 4) výzva smerom ku všetkým inštitúciám, agentúram, orgánom a úradom vrátane Európskeho parlamentu, aby sa zapojili do dodržiavania týchto noriem. Táto formulácia zároveň naznačuje určitú vágnosť definovania problematiky a vyplývajúcich interných vzťahov zohľadňujúc chýbajúce definovanie problematiky v zmluvách. Je to v podstate na dobrovoľnosti všetkých zúčastnených vytvoriť a akceptovať jednotné pravidlá. Tzv. "zlatý bezpečnostný štandard" poskytuje práve Rozhodnutie Rady č. 2013(488)EU.

Štruktúra dokumentu a jeho obsah korešponduje s dokumentom Rady, sú tu však naviac upravené niektoré špecifiká Komisie, ako nadnárodného permanentného a kolektívneho orgánu EÚ disponujúceho najmä oprávneniami v oblasti tvorby komunitárneho práva.

Rozhodnutie Komisie sa odvoláva na viacero ustanovení zmlúv, čím sa rozširuje a posilňuje záväznosť tohto rozhodnutia vo vzťahu k členským krajinám. Zároveň, tak ako v prípade Rady, je toto Rozhodnutie komisie včlenené do rokovacieho poriadku Komisie, je jeho prílohou. Takisto možno konštatovať, že do jeho prijatia bola oblasť OUI v rámci Komisie pokrývaná rôzne, spravidla na základe interných pokynov a usmernení.

Na koordináciu bezpečnosti v rámci Komisie a jej pôsobnosti voči rôznym Komisiou zriaďovaným agentúram bolo vytvorené Bezpečnostné riaditeľstvo a zároveň ako poradný orgán Poradná skupina Komisie pre bezpečnostnú politiku, pozostávajúca zo zástupcov národných bezpečnostných úradov členských krajín.

4. **Rozhodnutie vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku zo dňa 19. apríla 2013 č. 2013/C 190/01 o bezpečnostných pravidlách EEAS (ďalej len Rozhodnutie EEAS**).

Rozhodnutie EEAS bolo prijaté so zreteľom na:

- Rozhodnutie Rady č. 2010/427/EÚ z 26. júla 2010 o organizácii a fungovaní Európskej služby pre vonkajšiu činnosť (ďalej len „EEAS"),
- Stanovisko výboru uvedeného v článku 9 ods. 6 rozhodnutia vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku z 15. júna 2011 o bezpečnostných pravidlách EEAS.

Napriek tomu, že EEAS je funkčne autonómnym orgánom EÚ, mala by mať bezpečnostné pravidlá v súlade s článkom 10 ods. 1 rozhodnutia Rady 2010/427/EÚ. Vysoký predstaviteľ Únie

pre zahraničné veci a bezpečnostnú politiku by mal rozhodovať o bezpečnostných pravidlách EEAS, ktoré zahŕňajú všetky aspekty bezpečnosti, pokiaľ ide o fungovanie EEAS, aby služba mohla účinne riadiť oblasť ochrany informácií.

Bezpečnostné pravidlá EEAS by mali pomôcť dosiahnuť súdržnejší komplexný všeobecný rámec EÚ, ktorým by sa zaistila ochrana utajovaných skutočností EÚ, pričom by mali vychádzať z bezpečnostných pravidiel Rady a Komisie a zachovávať s nimi maximálny možný súlad.

EEAS, Rada a Komisia sa zaviazali, že budú uplatňovať rovnaké bezpečnostné normy na ochranu utajovaných skutočností EÚ.

Čl. 1 písm. e) definuje záujmy EEAS ako*:„bezpečnostné záujmy EEAS zahŕňajú personál EEAS, objekty EEAS, závislé osoby, fyzický majetok vrátane komunikačných a informačných systémov, informácie a návštevníkov"*. Takto jednoznačne definované záujmy ešte neboli v žiadnom inom predpise inštitúcií EÚ.

Zaujímavé je riešenie kategórie citlivých informácií, kde je priamo stanovené, že takéto informácie existujú ako aj rámcový spôsob ich ochrany. Čl. 3 bod 3 tohto rozhodnutia znie: *„Vzhľadom na ochranu **citlivých neutajovaných informácií** musia byť bezpečnostné opatrenia v rámci EEAS úmerné čo do citlivosti a/alebo účinku ich nepovoleného vyzradenia na záujmy EÚ"*. Oblasť citlivých informácií nebola doteraz upravená na úrovni rozhodnutia.

Rozhodnutím o bezpečnostných pravidlách EEAS sa stanovuje všeobecný bezpečnostný rámec.

Pri tvorbe tohto rozhodnutia sa vychádzalo z čl. 10 ods. 1 Rozhodnutia Rady zo dňa 26. júla 2010 o organizácii a fungovaní Európskej služby pre vonkajšiu činnosť, ktoré znie: „*Vysoký predstaviteľ po porade s Bezpečnostným výborom Rady rozhodne o bezpečnostných nariadeniach EEAS a prijme všetky vhodné opatrenia, aby sa zabezpečilo, že EEAS efektívne riadi riziká týkajúce sa jej personálu, fyzického majetku a informácií a že plní svoju povinnosť starostlivosti a zodpovednosti v tomto ohľade. Tieto nariadenia sa vzťahujú na všetkých členov personálu EEAS a delegácií Únie bez ohľadu na ich administratívne postavenie alebo pôvod"*.

Zároveň sa v ďalších odsekoch konštatuje, že v rámci tohto rozhodnutia bude EEAS v súvislosti s OUS uplatňovať bezpečnostné opatrenia ustanovené v prílohe k rozhodnutiu č. 2001/264/ES (predchodca v súčasnosti platného nariadenia Rady č. 2013/488/EU), a takisto uplatňovať ustanovenia rozhodnutia Komisie o bezpečnosti č. 2015/444/EÚ/Euratom.

5. **Rozhodnutie Rady zo dňa 30. novembra 2009, ktorým sa prijímajú pravidlá o dôvernosti informácií Europol-u č. 2009/968/JHA**

Uvedené rozhodnutie priamo ilustruje zložitosť vzťahov v rámci EÚ, pričom nie je ojedinelé a tvorí integrálnu súčasť pravidiel ochrany informácií EÚ. Obdobným spôsobom majú prijaté pravidlá ohľadom ochrany informácií (vrátane utajovaných) aj iné inštitúcie a agentúry EÚ, zriaďované rôznym, často neštandardným spôsobom, a často aj s nie celkom zrejmou záväznosťou voči členským krajinám. Napríklad Európsky parlament (Rozhodnutie úradu Európskeho parlamentu č. 2011/C 190/02, týkajúce sa pravidiel pokrývajúcich nakladanie s dôvernými informáciami Európskym parlamentom), ESA – Európska vesmírna agentúra, FRONTEX – Európska agentúra pre pohraničnú a pobrežnú stráž, EDA - Európska obranná agentúra a iné.
Rozhodnutie Rady o dôvernosti informácií Europol-u bolo prijaté v súlade s čl. 40 rozhodnutia Rady o zriadení Europol-u, ktoré pojednáva o opatreniach týkajúcich sa výmeny utajovaných skutočností súvisiacich s činnosťou Europol-u.

Je potrebné uviesť, že rozhodnutím Rady o zriadení Europol-u (*de facto* sa Europol stal agentúrou Rady, subjektom financovaným zo všeobecného rozpočtu EÚ) sa odstránil v prvom rade neštandardný stav týkajúci sa jeho postavenia ako samostatnej organizácie EÚ. V druhom rade sa tým zjednodušil legislatívny proces prijímania pravidiel fungovania Europol-u a ich záväznosti a vymožiteľnosti voči napr. členským krajinám, keďže sú vydávané ako rozhodnutia Rady.

V kontexte pravidiel ochrany utajovaných informácií je zrejmé, že i keď Europol-u bola ponechaná určitá samostatnosť prejavujúca sa v niektorých špecifikách ochrany informácií vrátane

utajovaných, je zrejmé, že Europol musí aplikovať všeobecné pravidlá Rady stanovené v rozhodnutí Rady č. 2013(488)EU.

Na príklade Europol-u je jasne vidieť tak častú nepraktickosť, neefektívnosť a zbytočnú komplikovanosť vzťahov a fungovania EÚ. Týka sa to o to viac oblasti ochrany informácií utajením, kedy by sa mal automaticky predpokladať jednotný a jasný rámec fungovania.

Tento príklad zároveň dostatočne ilustruje zložitosť tvorby predpisov pre oblasť utajovaných informácií EÚ, kedy sa neexistencia jednotného právneho rámca, záväzného pre „všetkých", odvíjajúceho sa od zakladajúcich zmlúv EÚ, nahrádza viacerými špecifickými a často nejednotnými pravidlami.

6. **Dohoda medzi vládami členských štátov Európskej únie, ktoré sa zišli na zasadnutí Rady o ochrane utajovaných skutočností, ktoré sa vymieňajú v záujme Európskej únie, platná od 1. decembra 2015 (330/2015 Z. z.), ďalej len dohoda.**

Situácia pred prijatím Dohody nebola z pohľadu budovania jednotného systému ochrany utajovaných informácií EÚ jednoduchá. Prijatiu Dohody predchádzalo množstvo snáh o prehodnotenie a prepracovanie systému OUI EÚ. Z prehľadu je vidieť, že vývoj a aktuálny stav v oblasti OUI nebol systematický. Riešenia a postupne prijímané dokumenty sú dôkazom, že ideálne riešenie nie je jednoduché dosiahnuť. Samotná EÚ je "projekt vo vývoji".

Vytvorenie jednoznačného a komplexného právneho rámca pre ochranu informácií nebolo z hľadiska vývoja EÚ prioritou. Systém OUI vždy "nejako" fungoval. Problémy sa prehlbovali postupne a zvýraznili sa až so vstupom nových členských krajín z východnej Európy. V prístupovom procese (aproximácia práva EÚ) sa poukazovalo najmä na nejasnú právnu záväznosť predpisov upravujúcich oblasť ochrany utajovaných informácií, čo v čase keď táto oblasť bola pokrývaná len internými predpismi jednotlivých inštitúcií bolo vcelku legitímne. Zaujímavým sa preto javí krátky pohľad do minulosti EÚ a legitímna otázka: Ako sa so záväznosťou vysporiadali "staré" členské krajiny? Odpoveď na takto položenú otázku by pravdepodobne mohla byť predmetom samostatnej štúdie. No s ohľadom na špecifiká vývoja EÚ možno odpoveď nájsť v komplikovanom systéme vzájomných bezpečnostných zmlúv. Pravdepodobne členské krajiny takto našli určitú odpoveď a postačovala im. Nové členské krajiny, pôvodom z východného bloku, však v procese aproximácie práva EÚ narážali na stav, kedy bolo vyžadované prispôsobiť národný systém ochrany informácií systému EÚ, no keďže tento nebol právne jednoznačne upravený, bolo potrebné vykonať zmeny. V zásade, od roku 2001 možno datovať obdobie, kedy prebiehali odborné diskusie ako tento stav systematicky riešiť. Čiastkovým výsledkom bola transformácia interných pravidiel Rady a Komisie do právne záväzných foriem - rozhodnutí. No ako sa ukázalo, proces hľadania efektívneho riešenia tým len začal. Nájsť správne a v členských štátoch priechodné riešenie nebolo jednoduché. O to viac, že s prehlbujúcou sa EÚ integráciou, nárastom množstva informácií a technickým a technologickým pokrokom bolo zrejmé, že je potrebné nájsť efektívnejšie riešenie.

Ako už bolo načrtnuté za najproblematickejšie bolo považované riešenie záväznosti už zmienených dokumentov Rady, Komisie. Zatiaľ čo nové členské štáty, ktoré vstúpili do EÚ v roku 2004 a 2007, prijali bezpečnostné predpisy Rady a Komisie ako súčasť *acquis,* staré členské krajiny ich považovali za záväzné len do tej miery, ktorá bola nevyhnutná pre fungovanie Rady a Komisie. Uvedený nesúlad zvýrazňuje aj skutočnosť, že tieto predpisy do roku 2001 ani neexistovali a oblasť OUI EÚ bola upravená len internými predpismi Rady a Komisie. V podstate až prístupový proces nových členských krajín poukázal na potrebu riešenia situácie so záväznosťou týchto predpisov. Zároveň sa zistilo, že bezpečnostná architektúra systému OUI EÚ, ako taká, je nevyhovujúca. Bezpečnostný výbor Rady sa situáciou viackrát zaoberal, no bez riadneho poverenia nebolo možné začať hľadať riešenie.

S ohľadom na uvedené, COREPER dňa 5. 12. 2007 poveril Bezpečnostný výbor Rady (Coucil Security Commitee, ďalej len CSC[18]) revíziou právneho rámca upravujúceho OUI EÚ a prípravou návrhu riešenia tejto oblasti jednotnejším spôsobom.

Neformálne rokovania začali v roku 2008 v Štokholme. Zástupcovia členských krajín a Generálneho sekretariátu Rady EÚ (ďalej len GSC) sa zhodli, že zakladajúce zmluvy neobsahujú žiadny právny základ, ktorý by umožnil upraviť ochranu OUI právnym nástrojom záväznejším než už uvedené rozhodnutia Rady a Komisie. Ako bolo konštatované, v podstate jedinou oblasťou, ktorá by sa dala samostatne upraviť nariadením alebo smernicou by bola oblasť priemyselnej bezpečnosti, ktorá má väzby na jednotný vnútorný trh. Takáto "dvojkoľajnosť" však nebola prijateľná. S ohľadom na uvedené bolo konštatované, že jediným riešením je prepracovať súčasné predpisy Rady a Komisie a zaistiť ich záväznosť multilaterálnou dohodou. Návrh dohody bol vypracovaný zástupcami francúzkeho bezpečnostného úradu.

S výnimkou niektorých ustanovení - článok 3, 4 ods.2 a 5 ods. 2, členské štáty v procese rokovaní dosiahli konsenzus. Proces schvaľovania bol však rozhodnutím CSC pozastavený pokiaľ nebudú prepracované vtedy platné predpisy Rady a Komisie, tak aby tieto boli v súlade s navrhovanými ustanoveniami dohody. Zároveň sa ich novelizáciou odstránili niektoré nedostatky, na ktoré poukazovala prax. Ich definitívne znenie bolo odsúhlasené na rokovaní CSC v Bruseli 17. októbra 2009. Podpis dohody bol síce naplánovaný na koniec roku 2009, no niektoré štáty mali stále zásadný problém so znením úvodných článkov Dohody (najmä článok 3). Podpis dohody sa uskutočnil až 4. mája 2011 po tom, čo boli schválené bezpečnostné predpisy Rady a Komisie.

<u>K jednotlivým ustanoveniam Dohody uvádzame podrobnejšie:</u>

Preambula:
Preambula deklaruje zhodu zmluvných strán na spolupráci, ktorá môže vyžadovať vzájomnú výmenu utajovaných informácií v záujme EÚ, a to medzi členskými krajinami a takisto medzi členskými krajinami (zmluvnými stranami) a orgánmi EÚ alebo agentúrami, inštitúciami či úradmi, ktoré zriadila. Cieľom bolo vytvoriť rámec na postupné nahradenie systému vzájomných bezpečnostných zmlúv a vytvoriť priestor na postupné zefektívňovanie právneho prostredia.
Preambula ďalej zdôrazňuje želanie zmluvných strán prispieť k zavedeniu súdržného a komplexného všeobecného rámca pre ochranu utajovaných informácií v záujme EÚ.

Článok 1

Po prvýkrát je jednotným právnym rámcom zastrešená OUI EÚ a zreteľne popísané oblasti ochrany informácií, ktorých sa týka. Účelom Dohody je zabezpečiť, aby zmluvné strany chránili utajované skutočnosti:
a) **s pôvodom v inštitúciach Európskej únie alebo v agentúrach, orgánoch alebo úradoch zriadených Európskou úniou,** pričom tieto skutočnosti sa poskytli zmluvným stranám alebo sa s nimi vymieňali;

Ustanovenie zjednocuje proces tvorby a označovania UI a jasne definuje stav, kedy pravidlá Rady sú určujúcimi pre systém OUI EÚ.

b) **s pôvodom v štátoch, ktoré sú zmluvnými stranami, pričom tieto skutočnosti sa poskytli inštitúciám Európskej únie alebo agentúram, orgánom alebo úradom zriadeným Európskou úniou;**

Predmetné ustanovenie je možné považovať za prelomové, keďže po prvýkrát je jasne uvedené, že členské krajiny môžu vytvárať utajované informácie EÚ. Zákon o OUS je v príkrom rozpore s predmetným ustanovením, nakoľko neumožňuje takýto proces. Naopak zákon o OUS

[18] Poznámka autora: Členmi výboru sú okrem zástupcov Generálneho sekretariátu Rady aj zástupcovia členských krajín, spravidla na úrovni riaditeľov národných bezpečnostných úradov, zástupcovia Komisie a ad hoc prizývaní zástupcovia agentúr EÚ.

považuje EÚ za cudziu moc, čo je v zásade nepredstaviteľné v kontexte samotného členstva a zámermi Dohody, ktorú SR ratifikovala.

c) **s pôvodom v štátoch, ktoré sú zmluvnými stranami, na účely ich poskytnutia alebo vzájomnej výmeny v záujme Európskej únie, pričom sa označí, že na tieto skutočnosti sa vzťahuje táto dohoda;**

Prínosom predmetného ustanovenia je, že priamo vytvorilo prostredie na vzájomnú výmenu UI medzi členskými krajinami bez potreby uzatvárania vzájomných bilaterálnych bezpečnostných dohôd. Určitou podmienkou je len, že tieto informácie sú vytvorené v "záujme EÚ" a označené adekvátnym stupňom utajenia. Pri vytváraní konštrukcie tohto ustanovenia sa predpokladal pozitívny vývoj v zjednocovaní záujmov jednotlivých členských krajín, založený na postupnom prehlbovaní EÚ integrácie. V ideálnom prípade by to mohlo znamenať, že členské krajiny by si v súlade s predmetným ustanovením tejto Dohody mohli vymieňať všetky utajované informácie. *De facto* by tým došlo k odstráneniu potreby uzatvárania bilaterálnych dohôd medzi členskými krajinami.

Vzájomná výmena a ochrana UI je podľa tohto ustanovenia Dohody založená na dodržiavaní tzv. minimálnych bezpečnostných štandardov EÚ stanovených v rozhodnutí Rady, a teda, že členské krajiny sú si navzájom isté ako budú vymieňané informácie chránené vrátane aplikácie možných sankcií v prípadoch zneužitia alebo nedodržania minimálnych štandardov.

Zákon o OUS však takýto proces neumožňuje ako už bolo uvedené pri objasnení podstaty predchádzajúceho ustanovenia Dohody.

Zaujímavou skutočnosťou je aj existujúca dvojkoľajnosť vo vzťahu k možnostiam vzájomnej výmeny UI medzi členskými krajinami, ako priama konzekvencia prijatia Dohody. Dvojkoľajnosť vyplýva zo situácie, že napr. SR má uzatvorené bezpečnostné dohody o vzájomnej ochrane utajovaných skutočností snáď so všetkými členskými krajinami EÚ.[19] To znamená, že si môže vymieňať UI s členskými krajinami bez ohľadu na ustanovenia Dohody - ak sú adekvátne označené (podľa § 3 zákona o OUS). Zároveň je však obdobný proces umožnený aj prostredníctvom Dohody, no vymieňané informácie musia byť označené podľa pravidiel EÚ. Takýto stav neprispeje práve k praktickému fungovaniu systému OUI, no minimálne umožní "osvieteným" členským krajinám zefektívniť proces vzájomnej výmeny. To však nie je situácia SR.

d) **ktoré poskytli inštitúciám Európskej únie alebo agentúram, orgánom alebo úradom zriadeným Európskou úniou tretie strany** alebo medzinárodne organizácie, pričom tieto skutočnosti sa poskytli zmluvným stranám alebo sa s nimi vymieňali.

Predmetné ustanovenie vytvára podmienky pre systém výmeny UI medzi EÚ a tretími stranami a zjednocuje ochranu informácií tretích strán poskytnutých EÚ.

Záver

Analýza predpisov vybraných inštitúcií a agentúr EÚ poukazuje na zložitosť vzťahov v EÚ, pokiaľ ide o bezpečnosť informácií režimom utajenia. Z hľadiska systému ochrany informácií nedošlo prijatím Lisabonskej zmluvy k zásadným zmenám. Napriek viacerým zmenám a doplneniam právneho rámca EÚ, inštitucionálneho fungovania EÚ a „miery integrácie" sa tieto zmeny zásadným spôsobom nedotkli systému ochrany informácií, nevytvorili iné, ako už zmienené princípy a ustanovenia zavedené pôvodnými zakladajúcimi zmluvami. Zmluva o založení ESAE zostala nedotknutá, napriek zrušeniu tzv. trojpilierového systému. Znamená to, že záväzky pre členské krajiny v oblasti OUS vyplývajúce z tejto zmluvy ostávajú aj v súčasnosti zachované (platná smernica Euratom č. 3).

[19] Pozri bližšie zoznam bezpečnostných dohôd na www.nbusr.sk.

Možno konštatovať, že bez primeraného právneho rámca definovaného v zmluvách o EÚ je ochrana informácií zbytočne zložitá, prebyrokratizovaná a často spochybňovaná. Jej právna záväznosť a vynútiteľnosť vo vzťahu k členským krajinám zodpovedá stavu fungovania EÚ v súčasnosti. Pokusy o definovanie spoločných záujmov len poukazujú na tento problém, ktorý bez hlbšej integrácie EÚ nie je možné efektívne riešiť. Zásadné zmeny mohli priniesť dokumenty Zmluva zakladajúca ústavu pre Európu[20] a Lisabonská zmluva,[21] no ako bolo uvedené, nestalo sa tak. Jediným pôvodným a právne jednoznačne záväzným dokumentom zmluvného charakteru, ktorý vytvára podmienky na zabezpečenie ochrany informácií utajením EÚ je Zmluva o založení Európskeho spoločenstva pre atómovú energiu, i keď iba v špecifickej oblasti atómových informácií.

Pomyselnú "strechu" a právny rámec sa podarilo vytvoriť až Dohodou medzi vládami členských štátov Európskej únie, ktoré sa zišli na zasadnutí Rady o ochrane utajovaných skutočností, ktoré sa vymieňajú v záujme Európskej únie. Vytvoril sa tým jednotný, no stále príliš komplikovaný, právny rámec. Situáciu je potrebné vnímať aj v kontexte existencie množstva vzájomných bilaterálnych zmlúv medzi jednotlivými členskými krajinami EÚ riešiacimi ochranu "národných" utajovaných informácií.

Ochrana informácií režimom utajenia EÚ je v súčastnosti príliš komplikovaný nástroj určený pre zaistenie bezpečnosti dôležitých informácií. Stojí preto pred množstvom nových výziev, a to aj v kontexte meniaceho sa bezpečnostného prostredia a dynamických bezpečnostných hrozieb. Súčasný stav je neudržateľný. Na viacero systémových nedostatkov bolo poukázané, pričom je zrejmé, že cesta, ktorá bola v tejto oblasti započatá pri vzniku základov EÚ bola v rámci súčasného právneho stavu naplnená a možnosti vyčerpané.

Ďalšie kroky EÚ by mali v kontexte postupného prehlbovania integrácie EÚ smerovať k zadefinovaniu oblasti ochrany informácií do základných zmlúv. Odstránil by sa tým súčasný komplikovaný a absolútne neflexibilný systém. Zmeny by mali zohľadňovať dôsledky a stav integrácie EÚ v jednotlivých oblastiach. Napríklad oblasť spoločnej bezpečnostnej a obrannej politiky znamená aj spoločný prístup k ochrane dôležitých informácií vznikajúcich pri realizácii spoločných záujmov. Tieto je potrebné chrániť jednotne v rámci celej EÚ. V prípade zistenia nových bezpečnostných rizík je nutné reagovať jednotne a na centrálnej úrovni byť schopný prijať opatrenia na ochranu informácií, ktoré sú realizované rovnako a rýchlo vo všetkých členských krajinách EÚ.

Rozvoj a zmeny akéhokoľvek systému bezpečnosti informácií vrátane systému bezpečnosti informácií by mali byť založené na dôkladnom poznaní. Do budúcnosti je preto potrebné sa vyhnúť situáciám, ktoré je možné parafrázovať slovným spojením „nový motor do starého auta". Postupné prehlbovanie integrácie EÚ by malo ísť ruka v ruke so zmenami právneho rámca. Štandardizácia, flexibilita, dôraz na spoločné záujmy, jednotnosť a rovnaký odborný jazyk sú možné témy, o ktorých sa bude v budúcnosti intenzívne diskutovať v záujme hľadania efektívnych riešení budovania jednotného systému bezpečnosti utajovaných informácií na úrovni EÚ.

Európska integrácia a jej prehlbovanie môže byť kľúčovým činiteľom pre ďalšie zefektívňovanie ochrany informácií utajením ako substantívneho nástroja ochrany spoločných európskych záujmov. Je zrejmé, že v záujme bezpečnosti EÚ vzniká potreba vytvorenia priestoru na relevantnú diskusiu na rôznych úrovniach EÚ vrátane zapojenia národných bezpečnostných inštitúcií a akademickej obce.

---

[20] Zmluva zakladajúca Ústavu pre Európu, Úradný vestník Európskej únie C 310 zo 16. 12. 2004, táto zmluva nebola v ratifikačnom procese schválená, a preto nenadobudla právoplatnosť.

[21] Lisabonská zmluva (tiež tzv. Lisabonská reformná zmluva), ktorá dopĺňa Zmluvu o EÚ a zmluvu zakladajúcu Európske spoločenstvo, Úradný vestník Európskej únie C 306 17.12.2007, nadobudla platnosť 1. 12. 2009.

Literatúra

Bezpečnostná politika NATO - Security within the North Atlantic Treaty Organization (NATO), C-M(2002)49, NATO Archives – public version, 2017

Bezpečnostná stratégia NATO. [online] Dostupné z: www.mosr.sk

Bezpečnostná stratégia SR. 2005. [online] Dostupné z: www.mosr.sk

BRVNIŠŤAN, M. 2013. Ochrana utajovaných skutočností v spektre historického vývoja, Bratislava: Tlačiareň Ministerstva vnútra SR, s. 160. ISBN 978-80-8054-561-1

BRVNIŠŤAN, M. Možnosti ochrany informácií SR, In: Zborník príspevkov z VI. medzinárodnej vedeckej konferencie v Banskej Bystrici 6. – 7. februára 2013, II. Zväzok, Fakulta politických vied a medzinárodných vzťahov UMB, 2013. ISBN 978-80-557-0497-5, str. 556 – 565

Európska bezpečnostná stratégia. [online] Dostupné z: www.mosr.sk

NEČAS, P., UŠIAK, J. Nový prístup k bezpečnosti štátu na začiatku 21. storočia, In: Vedecká monografia, Akadémia ozbrojených síl generála M. R. Štefánika v Liptovskom Mikuláši, 2010, ISBN 978-80-8040-401-7

POTÁSCH, P. a kol. 2019. Ochrana právne privilegovaných informácií vo vybraných režimoch verejného práva. Woltwers Kluwer ČR, a.s., 224 strán, ISBN 978-80-7598-866-9

Rozhodnutie Rady Európskej únie z 23.9. 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií, Úradný vestník Európskej únie, sp. v. L 141/17 z 27.5. 2011

Key words: classified information, security situation, security risks, European Union information protection, security agreement, EU integration

Summary

The article deals with selected aspects of the EU classified information protection system, its current status and development. The implementation of possible measures for the protection of EU classified information depends directly on the willingness of individual Member States to share common values, thus ensuring consistency of rules and security standards. The analysis of the EU information protection system in its complexity creates a wide area of reflection on how to make it more effective, with direct implications for Member States' information protection systems. European integration and its deepening may be a key factor in further streamlining the protection of information by confidentiality as a substantive instrument for the protection of common European interests.

JUDr. Miroslav Brvnišťan, PhD.
Akadémia Policajného zboru v Bratislave
Sklabinská 1
Bratislava,
Tel.:+421903993119
e-mail: brvnistan@yahoo.com

Recenzenti: prof. JUDr. Peter Polák, PhD., JUDr. Matej Kostrec, PhD.