

**Možnosti využitia informačno-technických prostriedkov podľa Zákona
o ochrane súkromia pred odpočúvaním^[1]**

***Possibilities of using information and technical means according to the Act on
Protection of Privacy from Interception***

Doc. PhDr. JUDr. Marcela Tittlová, PhD.

Paneurópska vysoká škola, Fakulta práva, Ústav verejného práva

Anotácia

Informačno-technické prostriedky predstavujú skupinu moderných, ofenzívnych a do garantovaných práv dotknutých osôb významne zasahujúcich inštitútov. Kým v rovine procesnej je ich právna úprava podrobovaná často pomerne ostrej kritike, neprocesná rovina naproti tomu často ostáva nepovšimnutá. Podmienky využitia informačno-technických prostriedkov sú pritom v mnohom veľmi podobné a podobný je aj účel a spôsob ich využitia s tým rozdielom, že v rovine procesnej vedú k preverovaniu existujúcich podozrení z trestnej činnosti, kým v rovine neprocesnej smerujú k odhaľovaniu latentnej kriminality a k ochrane najvýznamnejších záujmov Slovenskej republiky.

Annotation

Information and technical resources represent a group of modern, offensive and guaranteed institutions of significant interference. While at the procedural level their legislation is often subjected to quite sharp criticism, on the other hand, the non-procedural level often remains unnoticed. The conditions for using information and technical means are very similar in many respects, and the purposes and way of using them are similar, with the exception that in the procedural level they lead to the screening of existing criminal offenses, while in the non-procedural level they tend to detect latent crime and to protect the most important interests of the Slovak Republic.

Kľúčové slová

neprocesná rovina, informačno-technické prostriedky, účel použitia, oprávnené subjekty, rozsah použitia.

Key words

non-process plane, information and technical means, purpose of use, authorized entities, scope of use.

Úvod

Ustanovenia Zákona o ochrane súkromia upravuje možnosti a podmienky použitia informačno-technických prostriedkov v neprocesnej rovine presne vymedzeným druhom orgánov. V súvislosti s týmto zavádza legálnu definíciu toho, čo sa na tieto účely rozumie informačno-technickými prostriedkami. Zákonodarca exemplifikatívne vypočítava, že sú to najmä elektrotechnické, rádiatechnické, fototechnické, optické, mechanické, chemické a iné prostriedky a zariadenia alebo ich súbory používané utajeným spôsobom s cieľom:

- vyhľadávania, otvárania, skúmania a vyhodnocovania poštových zásielok a iných dopravovaných zásielok,
- získavania obsahu správ prenášaných prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie,
- vyhotovovanie obrazových, zvukových, obrazovo-zvukových alebo iných záznamov.

Aj podľa tohto je vidieť, že v mnohom sa uvedená definícia približuje vymedzeniu informačno-technických prostriedkov v ustanoveniach Trestného poriadku (zákon č. 301/2005 Z. z. v znení neskorších predpisov, ďalej len „Trestný poriadok“). Prirodzene, kým v rovine procesnej ide o využívanie zaisťovacích inštitútov, ktoré majú povahu dôkazných prostriedkov smerujúcich k získaniu relevantných informácií, v rovine neprocesnej je to súčasť širšej stratégie smerujúcej k odhaľovaniu latentnej časti kriminality. Tým je determinovaný jednak rozsah, ale aj špecifiká využívania informačno-technických prostriedkov v tejto neprocesnej línii, na podklade ustanovení Zákona o ochrane súkromia pred odpočúvaním.

Je zrejmé, že za informačno-technické prostriedky je teda možné považovať uvedené prostriedky a zariadenia a ich súbory, ktoré slúžia na konkrétny účel. Vyhľadávanie, otváranie, skúmanie a vyhodnocovanie poštových a iných zásielok, získavanie obsahu správ, ktoré sa prenášajú prostredníctvom elektronických komunikačných sietí vrátane telefonickú komunikáciu, a aj vyhotovovanie obrazových, zvukových a obrazovo-zvukových a iných záznamov predstavuje konkrétnu činnosť, ktorá sa za pomoci týchto prostriedkov realizuje. Vzhľadom na to, že využitie tejto špeciálnej techniky na uvedené účely je priamo nevyhnutné, aj tieto činnosti sa zvyknú (podľa povahy a označenia používanej techniky) označovať za informačno-technické prostriedky.

1. Spôsob a účel použitia informačno-technických prostriedkov v neprocesnej rovine

Zákonná (legálna) definícia sama predkladá spravodajské, utajené použitie informačno-technických prostriedkov na uvedené účely. Dotknuté osoby nemajú v čase ich použitia vedomosť o tom, že takto špeciálne skonštruovaná technika sa vo vzťahu k nim alebo vo vzťahu k ich činnosti využíva. To je priamo zákonný základ, od ktorého sa odvíja očakávaný prínos použitia informačno-technických prostriedkov, teda získanie objektívnych, neskreslených, záujmami tretích osôb nepozmenených informácií a poznatkov. Za pomoci špeciálne skonštruovanej techniky – informačno-technických prostriedkov je možné vyhľadávať, otvárať, skúmať a vyhodnocovať obsah poštových a iných dopravovaných zásielok.

Čiastočne kriticky možno uviesť, že hoci samotné tieto prostriedky sa označujú ako prostriedky informačno-technické, svojou povahou ide len o konkrétnu činnosť, ktorá sa realizuje prostredníctvom osobitne skonštruovanej techniky, ktorá ma povahu informačno-technických prostriedkov. Preto aj uvedené činnosti sa označujú ako informačno-technické prostriedky, hoci priamo takúto povahu nemajú resp. toto ich označenie sa odvodzuje od techniky, ktorá sa na tieto účely využíva.

V tejto súvislosti sa poštovou zásielkou, ktorú je možné takto vyhľadávať, následne otvoriť, skúmať jej obsah a vyhodnocovať, sú akékoľvek oznámenia v písomnej forme alebo iné veci, ktoré majú byť dodané adresátovi a ktoré sú označené adresou adresáta. Poštové zásielky vyberá a následne distribuuje poštový podnik podľa poštových podmienok. Poštovou zásielkou však nie je len listová zásielka (najmä korešpondencia, reklamná zásielka alebo slepecká zásielka), ale sú to aj všetky balíky, periodické zásielky a taktiež aj poštové poukazy. Okrem takto vymedzených poštových zásielok, ktoré sú na prepravu podané a ďalej distribuované poštovým podnikom, to však môžu byť aj všetky ďalšie zásielky, ktoré sú podané na prepravu a je možné ich prepravovať a následne doručovať konečnému adresátovi prostredníctvom iných doručovateľov. Je to v podstate každá zásielka, ktorá je podaná na prepravu, ktorú je možné prepravovať a doručovať adresátovi.^[2]

Korešpondencia je oznámenie v písomnej forme na akomkoľvek druhu fyzického média, ktoré sa má dodať na adresu uvedenú na ňom alebo na obálke. Korešpondenciou je aj účet, faktúra, finančný výkaz alebo iná správa nerovnakého obsahu a formy, ktoré súvisia so záväzkovými alebo inými vzťahmi medzi odosielateľom a adresátom. Korešpondenciou nie je kniha, katalóg, noviny a iná periodická tlač, a to ani vtedy, ak sú obsahom listovej zásielky.

Informačno-technické prostriedky je možné využiť aj na získavanie obsahu akýchkoľvek správ prenášaných prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie. V tomto zmysle sa elektronickou komunikačnou sieťou rozumie funkčne prepojená sústava prenosových systémov, a ak je to potrebné, prepájacích alebo smerovacích zariadení vrátane sieťových prvkov, ktoré nie sú aktívne, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním paketov, internetu a mobilných pozemských sietí, sietí na rozvod elektrickej energie v rozsahu, v ktorom sa používajú na prenos signálov, sietí pre rozhlasové a televízne vysielanie a káblových distribučných systémov bez ohľadu na druh prenášaných informácií.^[3]

Elektronické komunikácie zabezpečujú výmenu alebo prenos informácií najmä vo forme obrazu, zvuku alebo textu po elektronických komunikačných sieťach. Telefónna komunikácia sa realizuje v rámci telekomunikačnej prevádzky, ktorá predstavuje prenos signálu realizovaný prostredníctvom telekomunikačného zariadenia. Je to technické zariadenie, ktoré umožňuje vysielanie, prenos, smerovanie, príjem, prepojenie alebo spracovanie signálov a informácií vo forme obrazu, zvuku alebo dát prostredníctvom vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, ako aj pridružené prostriedky. Pôjde najmä o prenos signálu telefónom, telefaxom, mobilnými telefónom, posielanie krátkych textových správ, komunikáciu prostredníctvom vysielacky, pageru, komunikácia prostredníctvom elektronickej pošty (komunikáciu prostredníctvom e-mailu).^[4]

V konečnom dôsledku, informačno-technické prostriedky podľa tohto ustanovenia je možné využívať aj na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových a iných záznamov. Ide o akékoľvek záznamy, ktoré umožňujú zachytávať obraz, zvuk, prípadne ich vzájomnú kombináciu.

V tejto súvislosti možno len dodať, že uvedená legálna definícia je veľmi podobná, takmer zhodná s tou, ktorá je obsiahnutá v § 10 ods. 21 Trestného poriadku. V tomto zmysle sa za informačno-technické prostriedky považujú elektrotechnické, rádiatechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri:

- odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach,
- obrazových, zvukových alebo obrazovo-zvukových záznamoch alebo
- vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.

2. Subjekty oprávnené využívať informačno-technické prostriedky a rozsah použitia

Ustanovenia zákona o ochrane súkromia pred odpočúvaním upravujú možnosti využitia informačno-technických prostriedkov v súlade s podmienkami a s v súlade s pravidlami, ktoré upravuje tento zákon v ďalších svojich ustanoveniach. Ide o prostriedky, ktoré sa využívajú na konkrétny účel, zasahuje sa nimi do práv a právom chránených záujmov dotknutých osôb bez ich súhlasu a na ich použitie sú oprávnené konkrétne štátne orgány. Podľa tohto zákona môžu informačno-technické prostriedky využívať tieto orgány štátu:

- a) Policajný zbor SR,
- b) Slovenská informačná služba,
- c) Vojenské spravodajstvo,
- d) Zbor väzenskej a justičnej stráže a
- e) Finančná správa.

Je vidieť, že v porovnaní s procesnou rovinou, ide o širší výpočet subjektov, ktoré môžu využívať informačno-technické prostriedky. Kým v trestnom konaní ide o orgány činné v trestnom konaní, pre ktoré vykonávajú informačno-technické prostriedky príslušné útvary Policajného zboru SR, v rovine neprocesnej s ohľadom na formuláciu účelu ich použitia, je tento výpočet podstatne širší, čo možno hodnotiť nepochybne pozitívne.

Využitie informačno-technických prostriedkov týmito orgánmi štátu je zároveň limitované rozsahom ich pôsobnosti, ktorú upravujú osobitné predpisy. Na základe § 36 Zákona č. 171/1993 Z. z. o Policajnom zbore SR v znení neskorších predpisov (ďalej len „ZoPZ“) má možnosť tento zbor používať informačno-technické prostriedky na dosiahnutie konkrétneho účelu.^[5] Konkrétne Policajný zbor využíva informačno-technické prostriedky:^[6]

- pri plnení úloh v boji proti terorizmu,
- v boji proti legalizácii príjmov z trestnej činnosti a financovaniu terorizmu pri odhaľovaní trestnej činnosti organizovanej v spojení s cudzinou a organizovanej trestnej činnosti súvisiacej s nedovolenou výrobou, držaním a rozširovaním omamných a psychotropných látok, jedov, prekursorov a jadrových materiálov, s falšovaním a pozmeňovaním peňazí, známok a cenných papierov,

- pri odhaľovaní iných zločinov, pri poskytovaní ochrany a pomoci ohrozenému svedkovi a chránenému svedkov,
- pri operatívnej ochrane legalizanta a agenta pri odhaľovaní daňových únikov a nezákonných finančných operácií,
- pri odhaľovaní úmyselných trestných činov podľa druhého a tretieho dielu ôsmej hlavy druhej časti Trestného zákona, za ktoré možno uložiť trest odňatia slobody s hornou hranicou najmenej dva roky,
- pri odhaľovaní iných úmyselných trestných činov, ktorých stíhanie upravuje medzinárodná zmluva, ktorou je Slovenská republika viazaná, a pri zisťovaní ich páchatel'ov a pátraní po nich.

Takisto Slovenská informačná služba je oprávnená na základe § 10 ods. 1 Zákona č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov (ďalej len „ZoSIS“) používať informačno-technické prostriedky pri plnení úloh, ktoré sú jej podľa § 2 ZoSIS zverené a v rozsahu svojej pôsobnosti (§ 2 ods. 1 a 2 ZoSIS). Slovenská informačná služba v zmysle tohto získa, sústreďuje a vyhodnocuje informácie o:

- činnosti ohrozujúcej ústavné zriadenie, územnú celistvosť a zvrchovanosť Slovenskej republiky,
- činnosti smerujúcej proti bezpečnosti Slovenskej republiky,
- aktivite cudzích spravodajských služieb,
- organizovanej trestnej činnosti,
- terorizme vrátane informácií o účasti na terorizme, jeho financovaní alebo podporovaní,
- politickom a náboženskom extrémizme, extrémizme prejavujúcom sa násilným spôsobom a škodlivom sektárskom zoskupení,
- aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu, nelegálnej medzinárodnej preprave osôb a migrácii osôb,
- skutočnostiach spôsobilých vážne ohroziť alebo poškodiť hospodárske záujmy Slovenskej republiky,
- ohrození alebo úniku informácií a vecí chránených podľa osobitného predpisu alebo medzinárodných zmlúv alebo medzinárodných protokolov,
- získa, sústreďuje a vyhodnocuje informácie o aktivitách, ktoré vznikajú v zahraničí a smerujú proti ústavnému zriadeniu a bezpečnosti Slovenskej republiky, a informácie potrebné na realizáciu jej zahraničnopolitických záujmov.

Vojenské spravodajstvo môže z dôvodu plnenia svojich úloh taktiež využívať informačno-technické prostriedky podľa Zákona č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov (ďalej len „ZoVS“). Konkrétne je mu toto oprávnenie zverené na základe § 10 ods. 1 ZoVS v rozsahu pôsobnosti Vojenského spravodajstva podľa § 1 ZoVS a v zmysle zákonných úloh podľa § 2 ZoVS.

Vojenské spravodajstvo plní úlohy týkajúce sa spravodajského zabezpečenia obrany, obranyschopnosti a bezpečnosti Slovenskej republiky. Na tieto účely získava, sústreďuje a vyhodnocuje informácie dôležité pre zabezpečenie obrany a obranyschopnosti Slovenskej republiky na území Slovenskej republiky a v zahraničí zamerané na:

- činnosti ohrozujúce suverenitu, ústavné zriadenie, zvrchovanosť, územnú celistosť a obranyschopnosť Slovenskej republiky,
- aktivity cudzích spravodajských služieb,
- terorizmus, jeho financovanie alebo podporovanie, kybernetický terorizmus,
- vlastizradu, sabotáž a záškodníctvo,
- politický extrémizmus alebo náboženský extrémizmus, extrémizmus prejavujúci sa násilným spôsobom a škodlivú propagandu, ak súčasne ohrozuje plnenie úloh ozbrojených síl a extrémizmus profesionálnych vojakov,
- škodlivé sektárske zoskupenia, ak ohrozujú plnenie úloh ozbrojených síl a škodlivé sektárske zoskupenia profesionálnych vojakov,
- organizovanú trestnú činnosť a trestnú činnosť proti obrane Slovenskej republiky,
- nelegálne obchodovanie s výrobkami obranného priemyslu, so zbraňami hromadného ničenia alebo s položkami dvojakého použitia,
- nelegálnu medzinárodnú prepravu osôb,
- skutočnosti spôsobilé vážne ohroziť alebo poškodiť vojensko-hospodárske záujmy Slovenskej republiky,
- ohrozenie alebo únik údajov obsahujúcich utajované skutočnosti,

Zbor väzenskej a justičnej stráže má možnosť využívať informačno-technické prostriedky na základe § 23 a § 24 Zákona č. 4/2001 Z.z. o Zbore väzenskej a justičnej stráže v znení neskorších predpisov (ďalej len „ZozVJS“) v súvislosti s oprávneniami, ktoré plní pri odhaľovaní trestnej činnosti, a to na úseku boja proti terorizmu a organizovanému zločinu, s cieľom predchádzať a odhaľovať pripravovanú trestnú činnosť alebo trestnú činnosť spáchanú obvinenými vo výkone väzby alebo odsúdenými vo výkone trestu odňatia slobody, trestnú činnosť príslušníkov Zboru väzenskej a justičnej stráže alebo zamestnancov tohto zboru. Na tieto účely má Zbor väzenskej a justičnej stráže oprávnenie používať informačno-technické prostriedky, no zásadne v jeho objektoch. Tieto prostriedky môže využívať pri odhaľovaní trestnej činnosti, ako už bolo uvedené, no tiež len za podmienky, že zabezpečovanie nevyhnutných dôkazov pre trestné konanie by bolo iným spôsobom neúčinné alebo podstatne sťažené (podmienka subsidiarity použitia). Informačno-technické prostriedky sa nesmú použiť, ak ide o styk obvineného alebo odsúdeného s obhajcom.

Finančná správa je oprávnená používať informačno-technické prostriedky podľa § 13 ods. 2 písm. b.) Zákona č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov a nadväzne na to podľa ustanovenia § 14 tohto zákona. Tieto prostriedky môžu používať ozbrojení príslušníci finančnej

správy zaradení na finančnom riaditeľstve a ozbrojení príslušníci finančnej správy zaradení na Kriminálnom úrade finančnej správy na účely:

a) odhaľovania zločinov spáchaných v súvislosti s porušením colných predpisov alebo daňových predpisov v oblasti dane z pridanej hodnoty alebo spotrebných daní,

b) zisťovania páchatel'ov vyššie uvedených zločinov.

Zbor väzenskej a justičnej stráže a takisto aj orgány Finančnej správy majú možnosť využívať informačno-technické prostriedky na konkrétne vymedzené účely. Nemajú však k dispozícii dostatok špecializovaných technických zariadení a ich súborov na to, aby mali možnosť používať informačno-technické prostriedky, čo je ale v rámci ich činnosti a na konkrétne účely nevyhnutné.

Vzhľadom na to, aby aj tieto orgány štátu mali možnosť využívať informačno-technické prostriedky tak, ako im to zákon umožňuje, zaviedla sa povinnosť Policajného zboru technicky zabezpečiť ich použitie. Technicky si teda použitie informačno-technických prostriedkov Zbor väzenskej a justičnej stráže a ani orgány Finančnej správy nezabezpečujú sami.

Písomný súhlas zákonného súdu udelený Zboru väzenskej a justičnej stráže a orgánom Finančnej správy následne tieto orgány predkladajú Policajnému zboru. Policajný zbor pre tieto orgány štátu technicky zabezpečuje na podklade predloženia písomného súhlasu zákonného sudcu použitie informačno-technických prostriedkov.

Ostatné orgány štátu, teda najmä Policajný zbor, Slovenská informačná služba a čiastočne aj Vojenské spravodajstvo si zabezpečujú použitie informačno-technických prostriedkov po splnení podmienok ustanovených týmto zákonom sami.

Vojenské spravodajstvo si v rozsahu svojej pôsobnosti a na plnenie zákonom zverených úloh má možnosť samo technicky zabezpečovať použitie informačno-technických prostriedkov. Výnimkou z tohto pravidla je možnosť využitia informačno-technických prostriedkov pri získavaní obsahu správ, ktoré sa prenášajú prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie. Na tieto účely pre Vojenské spravodajstvo zabezpečuje použitie informačno-technických prostriedkov Policajný zbor. Technicky zabezpečí ich použitie na základe:

- predloženia žiadosti o ich použitie a technické zabezpečenie ich použitia,
- predloženia písomného súhlasu zákonného sudcu s použitím týchto informačno-technických prostriedkov.

Týmto spôsobom došlo k odstráneniu nedostatkov vyskytujúcich sa v aplikačnej praxi a k zabezpečeniu riadneho a bezproblémového využívania informačno-technických prostriedkov ako neoddeliteľnej súčasti Vojenského spravodajstva pri plnení jeho zákonných úloh. Policajnému zboru sa tu súčasne ukladá povinnosť technicky zabezpečovať použitie informačno-technického prostriedku (pri získavaní obsahu správ, ktoré sa prenášajú prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie) pre Vojenské spravodajstvo.

Vojenské spravodajstvo totiž nemá k dispozícii všetky potrebné technické zariadenia používané ako informačno-technické prostriedky, ktorých zaobstaranie a následná prevádzka si vyžaduje značné

nároky na rozpočtové prostriedky. Pôvodne teda nebolo možné, aby Vojenské spravodajstvo ako oprávnený subjekt priamo zo zákona o ochrane pred odpočúvaním malo možnosť pri plnení úloh využívať všetky druhy informačno-technických prostriedkov a bez komplikácií a vyžadovania súčinnosti. Tento nedostatok sa odstránil práve zavedením povinnosti Policajného zboru technicky zabezpečiť použitie uvedeného informačno-technického prostriedku pre Vojenské spravodajstvo.

3. Účel použitia informačno-technických prostriedkov v neprocesnej rovine

Účel, na ktorý je možné využiť informačno-technické prostriedky podľa Zákona o ochrane súkromia pred odpočúvaním upravuje § 3 tohto zákona. Ich použitie je totiž možné iba v prípadoch, ak je to nevyhnutné s ohľadom na konkrétny, v tomto ustanovení formulovaný účel. To, že ich použitie na tieto účely je nevyhnutné, to je potrebné posudzovať v kontexte konkrétnej situácie tak, ako použitie nutné, nutne potrebné. Použitie informačno-technických prostriedkov podľa tohto zákona je možné len v prípade, ak je to v demokratickej spoločnosti nevyhnuté z dôvodu:

- a) zabezpečenia ochrany ústavného zriadenia,
- b) zabezpečenia vnútorného poriadku a zahraničnopolitických záujmov štátu,
- c) zaistenia bezpečnosti a obrany štátu,
- d) získavania informácií zo zahraničných zdrojov,
- e) predchádzania a objasňovania trestnej činnosti alebo
- f) ochrany práv a slobôd iných a ak dosiahnutie tohto účelu inak by bolo neúčinné alebo

podstatne sťažené.

Ako sme vyššie naznačili, tomuto účelu plne zodpovedá šírka alebo rozsah subjektov, ktoré majú možnosť využívať informačno-technické prostriedky na účely plnenia svojich zákonných úloh, ale aj s cieľom ochrany základných ľudských práv všeobecne a na účely ochrany právneho a demokratického štátu ako takého.

Použitie informačno-technických prostriedkov na dosiahnutie sledovaného účelu zároveň podlieha splneniu podmienky subsidiarity. Použitie informačno-technických prostriedkov podľa tohto ustanovenia je teda možné len v prípade, ak sa ich použitím sleduje konkrétny (vyššie taxatívne uvedený) cieľ a tento cieľ, resp. účel ich použitia nie je možné dosiahnuť inak alebo ak by jeho dosiahnutie inak, inými prostriedkami bolo podstatne sťažené. Plne sa tak rešpektuje skutočnosť, že informačno-technické prostriedky predstavujú moderné a ofenzívne inštitúty, ktoré silno zasahujú do oblasti základných ľudských práv dotknutých osôb. Ich využívanie je síce možné, ale len na konkrétne účely a po splnení podmienky, že uvedený účel ich použitia sa nedá dosiahnuť bez takto intenzívneho zásahu do ľudských práv alebo ak by jeho dosahovanie inými prostriedkami bolo podstatne sťažené.

Ustanovenie § 3 Zákona prezentuje prejavy zásad proporcionality a legitimacy používania informačno-technických prostriedkov. Pritom možno dodať, že neodmysliteľnou požiadavkou použitia informačno-technických prostriedkov je naplnenie zásady legality, ktorej obsahom je požiadavka na existenciu podkladu umožňujúceho použiť informačno-technické prostriedky.

Z podmienky legality plyní požiadavka na existenciu normy, ktorá umožňuje použitie informačno-technických prostriedkov, a tým spôsobom umožňuje zasahovať do garantovaných práv. Tento zásah

musí byť jednak možný, no musí byť aj predvídaný vnútroštátnym právom. Existencia „zákona“, ktorý umožňuje použitie týchto prostriedkov, sa v zmysle čl. 8 ods. 2 Dohovoru interpretuje pomerne široko a v každom prípade materiálne (a vo význame stricto sensu). V tomto prípade ide priamo o právnu úpravu o sile zákona, no ESĽP vo svojej judikatúre pod tento pojem dovoľuje zahrnúť aj ďalšie právne predpisy, ako aj judikatúru a názory právnej vedy. Na strane druhej nepostačuje len existencia právnej praxe, prípadne interné a nezáväzné smernice a iné podobné normy prijaté na úrovni ministerstva.

So zásadou legality je úzko spojená aj už formulovaná požiadavka na nevyhnutnosť zásahov v podobe použitia informačno-technických prostriedkov. Požiadavka na nevyhnutnosť takéhoto zásahu v demokratickej spoločnosti by sa mala prelínať do vnútroštátnej úpravy v podobe dôslednej úpravy podmienok a pravidiel použitia týchto inštitútov.^[7] Informačno-technické prostriedky považuje ESĽP vo svojej judikatúre za nástroje tajného dohľadu nad jednotlivcami a ich správaním sa, ktoré sú typické pre policajné a nie pre demokratické štáty. V podmienkach demokratických štátov je ich použiteľnosť možná len v prípade, ak je to celkom nevyhnutné z dôvodu ochrany demokratického zriadenia.

Nevyhnutnosť sa nedá zamieňať s užitočnosťou, vhodnosťou, prijateľnosťou alebo rozumnosťou použitia.^[8] Požiadavka na nevyhnutnosť spočíva v naliehavej spoločenskej potrebe a nutnosti zodpovedať stanovenému cieľu (legitímnemu cieľu). Toto zhodnotenie je prirodzene veľmi subjektívne a pre zmluvné strany poskytuje určitý priestor pre voľnú úvahu. Tento priestor je však obmedzený.

Voľná úvaha v posúdení sa odvíja najmä od zhodnotenia povahy zásahu, od rozsahu zásahu, od situácie, za ktorej dôjde k zásahu, od naliehavosti a spoločenskej potreby zasiahnuť do garantovaných práv. Zásahy do garantovaných práv sú v kontexte požiadavky nevyhnutnosti subsidiárne a prostredníctvom týchto inštitútov majú povahu ultima ratio. Ich využitie je možné len vtedy, ak je to nevyhnutné, teda ak sa nedá rovnaký cieľ a účel dosiahnuť inými, spravidla miernejšími prostriedkami.^[9]

Legitimita použitia informačno-technických prostriedkov zahŕňa úvahu o tom, či ide o také nástroje, na podklade ktorých štátne orgány zasahujú do práva na súkromie a rodinný život, ktoré zodpovedajú požiadavkám a cieľom formulovaným v čl. 8 ods. 2 Dohovoru. Predmetné ustanovenie Dohovoru umožňuje štátnym orgánom zasahovať do garantovaných práv (právo na súkromie, rodinný život, tajomstvo prepravovaných správ) za podmienky, že tento zásah je:

a) v súlade so zákonom a súčasne (kumulatívne)

b) je nevyhnutný v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.

Použiteľnosť informačno-technických prostriedkov podľa tohto zákona teda spĺňa požiadavky na ich použiteľnosť podľa čl. 8 ods. 2 Dohovoru. Dovoľuje orgánom štátu zasahovať do garantovaných práv za podmienok, ktoré ustanovuje tento zákon a na dosiahnutie konkrétneho účelu, ak je použitie takýchto nástrojov na dosiahnutie tohto účelu nevyhnutné. Požiadavka legitimacy (požiadavka legitímneho cieľa) nespôsobuje zásadnejšie problémy, keďže záujmy na ochrane poriadku a bezpečnosti štátu a aj prevencia zločinnosti sú dostatočne široko formulované tak, že pokrývajú celú škálu prípadov a získavania dôkazov. Legitímny cieľ tak môže v konkrétnom prípade predstavovať záujem na zaistení

národnej bezpečnosti, záujem na ochrane ľudských práv, záujem na zachovaní hospodárskeho blahobytu.^[10] Toto ustanovenie teda formuluje konkrétne limity, konkrétne medze – účel, ku ktorého dosiahnutiu musia zásahy do dotknutých práv smerovať na to, aby v prípade zákonnosti a aj po splnení testu proporcionality mohli byť prípustné.^[11]

Požiadavka proporcionality zásahov sa prejavuje v hľadaní a dodržiavaním určitej rovnováhy medzi právami, ktoré sú k dispozícii, a možnosťami výberu konkrétnych druhov prostriedkov smerujúcich k naplneniu sledovaného (legitímneho) cieľa. Samotný zásah musí byť nevyhnutný (teda ak stanovený cieľ nie je možné dosiahnuť iným spôsobom, to znamená pomocou miernejších prostriedkov) a jeho realizácia musí zodpovedať nutnej spoločenskej potrebe – dosahovaniu sledovaného cieľa v kontexte podstaty práva, ktoré má byť na tieto účely obmedzené.^[12] Je tak nutné skúmať splnenie testu proporcionality, resp. to, či takýto zásah prejde testom proporcionality vzhľadom na následok – vzhľadom na zásah do garantovaných práv. „Zásada proporcionality je všeobecným testom riešenia kolízie základných práv, prípadne verejných dohier, teda aj kolízie verejných dohier a základných práv kolidujúcich s právom na súkromie.“^[13]

Informačno-technické prostriedky je podľa ustanovení Zákona o ochrane súkromia pred odpočúvaním možné na stanovený účel a po splnení požiadavky subsidiarity využívať primárne na území Slovenskej republiky. Takto majú možnosť využívať informačno-technické prostriedky Policajný zbor, Zbor väzenskej a justičnej stráže, orgány Finančnej správy, Slovenská informačná služba a Vojenské spravodajstvo. V prípade Slovenskej informačnej služby a Vojenského spravodajstva sa povoľuje, aby tieto subjekty využívali informačno-technické prostriedky aj mimo nášho územia, a to v rozsahu úloh, ktoré majú podľa ich zákonnej úpravy plniť. V zmysle § 2 ods. 2 ZoSIS je do pôsobnosti Slovenskej informačnej služby zverené aj získavanie, sústreďovanie, vyhodnocovanie informácií o aktivitách, ktoré vznikajú síce v zahraničí, ale ktoré smerujú proti ústavnému zriadeniu a bezpečnosti Slovenskej republiky, a taktiež informácií, ktoré sú potrebné na realizáciu zahraničnopolitických záujmov Slovenskej republiky. Vojenské spravodajstvo plní na základe § 2 ods. 2 ZoVS úlohy, ktoré mu plynú z medzinárodných zmlúv a dohôd, ktorými je Slovenská republika viazaná, a aj úlohy podľa ďalších právnych predpisov. Obmedzenie základných ľudských práv a slobôd, ktoré sú použitím týchto prostriedkov dotknuté, je možné len v takom rozsahu a na takú dobu, ako je to nevyhnutné na dosiahnutie sledovaného účelu, na dosahovanie ktorého sa tieto prostriedky podľa tohto ustanovenia používajú. Ide o jeden z prejavov zásady primeranosti v súvislosti s využívaním informačno-technických prostriedkov na podklade Zákona.

4. Osobitné podmienky využívania informačno-technických prostriedkov v neprocesnej rovine

Zákonodarca ustanovuje osobitné podmienky pre informačno-technické prostriedky, ktoré sa používajú pri odpočúvaní a zaznamenávaní telekomunikačných služieb. Telekomunikačnou službou je možné rozumieť činnosti, obsahom ktorých je prenos informácií a dát tretej osobe prostredníctvom telekomunikačného zariadenia alebo prostredníctvom telekomunikačnej siete.

Za telekomunikačnú službu sa považuje aj prenájom telekomunikačného okruhu. Telekomunikačné služby môžu mať povahu verejnú alebo neverejnú. Verejné telekomunikačné služby sú také,

z poskytovania ktorých nie je vopred vylúčený žiadny záujemca o jej využitie (teda je všeobecne dostupná každému). Verejné telekomunikačné služby sú najmä verejná telefónna služba a verejná služba prenosu dát. Neverejnou telekomunikačnou službou sa rozumie nekomerčná komunikačná služba, ktorá je určené len pre vlastné potreby konkrétnej, uzavretej, skupiny užívateľov.

Z dôvodu odpočúvania a zaznamenávania telekomunikačnej služby sa môže využívať len taký informačno-technický prostriedok, ktorý:

- umožní okamžite identifikovať koncové telekomunikačné zariadenie, ktoré bolo použité na odpočúvanie a zaznamenávania telekomunikačnej služby,
- neumožní vymazanie údajov identifikujúcich toto zariadenie a
- neumožňuje vymazanie času odpočúvania a zaznamenávania telekomunikačnej služby.

Ide o dôležité parametre informačno-technických prostriedkov, ktoré umožňujú efektívne využitie týchto prostriedkov, získať prostredníctvom nich dôležité informácie a zaručiť ich pravosť a nepozmenenie. Ide o parametre smerujúce k získaniu dôležitých informačných údajov a v konečnom dôsledku aj k preskúmaniu zákonnosti použitia informačno-technického prostriedku.

Informačno-technické prostriedky môžu podľa zákona o ochrane súkromia pred odpočúvaním používať vymedzené druhy štátnych orgánov. Niektoré majú možnosť zabezpečovať si ich technickú realizáciu samé (Policajný zbor, Slovenská informačná služba, čiastočne Vojenské spravodajstvo), iné ich využívajú prostredníctvom technického zabezpečenia Policajným zborom (Zbor väzenskej a justičnej stráže, orgány Finančnej správy, čiastočne Vojenské spravodajstvo). Každý zo štátnych orgánov, ktorý má možnosť využívať informačno-technické prostriedky a ich použitie si aj technicky zabezpečuje, musí mať dostatočne zabezpečenú aj personálnu základňu a organizáciu používania týchto prostriedkov. Je potrebné mať na zreteli, že jednak sa pomocou ich použitia intenzívne zasahuje do garantovaných ľudských práv a súčasne sa pomocou ich použitia získavajú citlivé a často dôkazne využiteľné informácie. Vzhľadom na to, každý orgán štátu, ktorý má možnosť využívať informačno-technické prostriedky podľa tohto zákona a súčasne, ktorý si zabezpečuje ich technickú stránku použitia, musí mať zamestnanca alebo príslušníka (prípadne viacerých), ktorý zabezpečuje úlohy spojené s týmto technickým zabezpečením. Tento zamestnanec alebo príslušník určeného orgánu štátu (alebo viacerí), je povinný podrobiť sa psychofyziologickému overeniu pravdovravnosti, a to v lehotách, ktoré určuje vedúci oprávneného orgánu štátu.

Psychofyziologické overovanie pravdovravnosti je proces, prostredníctvom ktorého je možné identifikovať osoby využívajúce nepravdovravné správanie na základe výsledkov prístroja, tzv. „polygrafu“ (senzor box). Tento prístroj vizuálne a priebežne zaznamenáva simultánne zmeny v kardiovaskulárnom, respiračnom a elektrodermálnom systéme počas prezentácie podnetu. V priebehu vyšetrenia špecialista vedie so subjektom štruktúrované interview, na základe ktorého sa formulujú otázky testového formátu. Počas odpovedí subjektu na tieto testové otázky sa zaznamenávajú jeho fyziologické reakcie, ktoré sa následne numericky a digitálne vyhodnotia. Na základe celkovej analýzy sa určí pravdovravnosť alebo nepravdovravnosť osoby.

Niektoré osobitné úpravy vyslovene upravujú povinnosť príslušníkov zboru alebo zamestnancov podrobiť sa takémuto vyšetreniu. Podľa § 20a ZoVS má príslušník aj zamestnanec Vojenského

spravodajstva povinnosť podrobiť sa psychologickému vyšetreniu a psychofyziológickému overeniu pravdovravnosti na základe rozhodnutia riaditeľa Vojenského spravodajstva. Odmietnutie splnenia tejto povinnosti (odmietnutie podrobiť sa tomuto overeniu) sa považuje za porušenie povinnosti, závažné porušenie služobnej disciplíny alebo závažné porušenie pracovnej disciplíny.

5. Zhodnotenie možností využívania informačno-technických prostriedkov v neprocesnej rovine

V podmienkach modernej a integrovanej informačnej spoločnosti sa spôsoby páchania nie len trestnej činnosti, ale všeobecne činnosti protispoločenskej, v mnohom zakladajú na vyžívaní moderných informačných a komunikačných prostriedkov, aplikácií, ako aj virtuálnej reality. Je zrejmé, že prvky modernej spoločnosti nachádzajú uplatnenie aj v spôsoboch páchania sa súčasne aj to, že takto sa zásadnejším spôsobom komplikujú možnosti poznávania latentnej časti kriminality, ako aj postupy jej odhaľovania a dokazovania v trestnom konaní, ochrana ľudských práv a záujmov štátu. Zisťovanie a poznávanie kriminálne relevantného správania sa, rovnako tak aj možnosti jeho odhaľovania v trestnom konaní, ochrana ľudských práv a spoločenských záujmov v najširšom slova zmysle, záujmov štátu, sú významným spôsobom sťažené a v mnohých prípadoch si priamo vyžadujú využívanie moderných a ofenzívnych nástrojov, k akým je možné zaraďovať aj informačno-technické prostriedky. Ich využitie je možné jednak v rovine procesnej, na základe ustanovení Trestného poriadku, ako aj v rovine neprocesnej a to na základe ustanovení osobitných predpisov, okrem iného aj ustanovení Zákona o ochrane súkromia pred odpočúvaním.

Je možné vidieť, že povaha a charakter informačno-technických prostriedkov tak, ako sú vymedzené v tejto neprocesnej línii, sa v mnohom približuje ich definovaniu v ustanoveniach Trestného poriadku. Hoci tieto procesné ustanovenia sú často predmetom kritiky z dôvodu nedostatočnej ochrany garantovaných práv dotknutých osôb, v dôsledku vytvárania viacerých teoretických i aplikačných problémov, rovina neprocesná ostáva viac menej nepovšimnutá. Pritom rozsah možností využívania informačno-technických prostriedkov v tejto línii je podstatne širší, ako je tomu v rovine procesnej. Aj z toho dôvodu nutne možno formulovať požiadavku na exaktnosť tejto úpravy, keďže v čase využívania týchto prostriedkov neprebiehajú spravidla žiadne procesné šetrenia. O to dôslednejšie je potrebné pristupovať k hodnoteniu tejto neprocesnej úpravy a k možnostiam, ktoré konkrétnym orgánom štátu táto úprava dáva, poskytuje, nakoľko týmto spôsobom nepochybne dochádza k zásahu do základných ľudských práv a slobôd dotknutých osôb, ktoré nemajú ani len postavenie osôb obvinených v trestnom konaní.

V porovnaní s procesnou úpravou, v tomto prípade je rozsah subjektov, ktoré majú možnosť využívať informačno-technické prostriedky podstatne širší. Pritom, samotné označenie „informačno-technické prostriedky, ktoré sa v mnohom prekrýva s procesným vymedzením týchto nástrojov, nie je celkom vhodné či správne. Vo svojej podstate je to konkrétna činnosť, ktorá sa realizuje pomocou špeciálnej techniky, prostredníctvom špeciálnych prostriedkov a zariadení, ktoré umožňujú utajene získavať informácie o dotknutých osobách, ich činnosti, komunikácii. Vzhľadom na využitie takejto techniky, aj pre uvedené prostriedky resp. vo svojej podstate činnosti, sa zaužívalo označenie „informačno-technické prostriedky, hoci to nie je celkom správne resp. presné označenie.

Okruh subjektov resp. štátnych orgánov, ktoré majú možnosť využívať v neprocesnej rovine informačno-technické prostriedky, je širší ako v rovine procesnej a to s ohľadom na účel, ktorý sa využitím týchto prostriedkov sleduje. Kým v rovine procesnej ide o odhaľovanie a dokazovania vybraných druhov trestných činov, v rovine neprocesnej je podstatne širšie formulovaný účel použitia. Celkovo je to súčasť širšej stratégie odhaľovania latentnej kriminality, ale týmto účelom sa smeruje aj k ochrane právneho a demokratického poriadku, celkovo k ochrane základných ľudských práv a slobôd. V kontexte účelu, na ktorý sa tieto prostriedky vymedzujú, možno pozitívne hodnotiť to, že ich využitie je umožnené tým štátnym orgánom, ktoré z povahy svojho postavenia a vzhľadom na charakter svojej činnosti majú smerovať k ochrane týchto dôležitých hodnôt.

Pozitívnym aspektom tejto úpravy je celý rad podmienok, na ktorých splnenie sa viaže používanie informačno-technických prostriedkov v neprocesnej línii. Tu je problematický hlavne utajený spôsob ich použitia a absencia vedomosti dotknutých osôb o ich používaní, hoci nie sú spravidla začaté žiadne procesné (trestno-procesné) postupy a šetrenia. Pri zdôvodnení požiadavky dosahovať účel použitia týchto prostriedkov možno povedať, že v podstate každý môže byť utajeným spôsobom sledovaný, jeho komunikácia i pohyb môžu byť podrobené sledovaniu, odpočúvaniu a rovnako to platí o korešpondencii osôb. Ide o prostriedky, ktoré sú typické pre policajné a nie demokratické a právne štáty. Ak teda aj v právnej úprave majú existovať takéto nástroje tajného sledovania jednotlivcov, potom musia byť súčasne vytvorené podmienky pre ich zákonné použitie a systém garancií ochrany dotknutých práv jednotlivcov. Okrem požiadavky zákonného použitia, je to primárne formulácia konkrétneho účelu, na ktorý sa dajú uvedené prostriedky využívať. Možno uviesť, že účel použitia tak, ako je formulovaný v predmetnom ustanovení a tak, ako je analyzovaný vyššie, je pomerne všeobecnou formuláciou, ktorá vytvára priestor pre individualizáciu účelu používania. Pod takto vymedzený účel sa dá subsumovať skutočne rad dôvodov použitia a preto aj v konkrétnom prípade by tento účel mal byť na jeho podmienky riadne konkretizovaný (čo sa rozumie ochranou verejného poriadku, bezpečnosti a pod. v danom prípade), aby sa dal skutočne preskúmať. Tento účel je doplnený o požiadavky subsidiarity a nutne aj proporcionality, takže v každom prípade je nutné zvažovať možnosti využívania iných miernejších zásahov do garantovaných práv. Táto podmienka by mala byť aj v konkrétnom prípade, v návrhu na použitie konkrétneho prostriedku, uvedená tak, aby mohla byť riadne preskúmaná. To je veľmi podobné ako je tomu v prípade účelu použitia, ktorý sa formuluje pomerne všeobecne, ale mal by byť konkretizovaný v žiadosti o použitie a premietat sa v súhlase s použitím.

Ku garanciam ochrany práv dotknutých osôb v súlade s použitím informačno-technických prostriedkov v neprocesnej rovine prispieva aj formulácia požiadavky proporcionality, ktorá by sa mala tiež v premietat v žiadosti o povolenie použitia. Pomocou testu proporcionality totiž asi najlepšie možno preskúmať primeranosť použitia konkrétneho prostriedku v určitej situácii a na konkrétny účel.

Všeobecne možno povedať, že právna úprava použitia informačno-technických prostriedkov v neprocesnej rovine predstavuje širšie možnosti využívania týchto nástrojov v podstate tajného dohľadu nad jednotlivcami. Túto šírku je možné vidieť v okruhu subjektov, ktoré majú možnosť využívať v neprocesnej línii informačno-technické prostriedky a rovnako tak v účele, na ktorý je možné ich použitie. Tento sa dopĺňa o požiadavky subsidiarity a proporcionality. Hoci ide o širšie možnosti využitia, tieto a priori nemožno hodnotiť negatívne, nakoľko na plnenie úloh štátu a vybraných orgánov štátu (za zabezpečenie ich činnosti) je potrebné, aby disponovali potrebnými informáciami. Aj tu ale treba zdôrazniť požiadavku na existenciu dostatočných garancií ochrany práv dotknutých osôb, ktoré

sú budované práve pomocou podmienok ich použitia. A hoci mnohé z nich sú formulované pomerne všeobecne a teda aj dosť vágne, je to najmä konkrétna činnosť subjektov žiadajúcich o povolenie ich používania, ako aj rozhodovacia činnosť zákonného sudcu, aby jednak v žiadosti, ale aj v súhlase s použitím boli dostatočne špecifikované (nie len zo zákona prepísané vágne formulácie) dôvody a okolnosti, pre ktoré sa o ich použitie žiada a pre ktoré sa ich použitie povoľuje.

Záver

Zákon o ochrane súkromia pred odpočúvaním upravuje podmienky a možnosti používania informačno-technických prostriedkov, pričom ich použitie zveruje vymedzeným orgánom štátu. Ide o neprocesnú líniu ich využívania, ktorá má v rámci širšej stratégie boja s trestnou činnosťou smerovať k odhaľovaniu latentnej kriminality a v širšom kontexte k ochrane najvýznamnejších záujmov Slovenskej republiky.

Použitím informačno-technických prostriedkov v neprocesnej línii dochádza k intenzívnym zásahom do základných a garantovaných ľudských práv, najmä do práva na súkromie, rodinný život a pod. Jednoznačne sa určuje, že obmedziť garantované práva je možné len činnosťou orgánov verejnej moci a aj to nie všetkých, ale len tých, ktorým tieto prostriedky k dispozícii dáva priamo toto ustanovenie. Ide o tie orgány štátu, ktoré podľa osobitných zákonov majú výslovne priznané oprávnenie použiť informačno-technický prostriedok. Informačno-technické prostriedky v zmysle ich legálnej definície podľa tohto zákona nemôžu ani držať a ani používať orgány územnej samosprávy ani súkromné bezpečnostné služby a ani iné fyzické alebo právnické osoby.

Faktom je, že pokiaľ ide o využívanie informačno-technických prostriedkov, Zákon o ochrane súkromia vymedzuje tak rozsah oprávnený subjektov, účel použitia, ako aj ďalšie zákonné podmienky. V mnohom sú veľmi podobné, ako je tomu v línii procesnej, no v tomto prípade sú súčasťou koordinovaného neprocesného postupu vybraných orgánov štátu (nie orgánov činných v trestnom konaní na účely preverovania trestných oznámení a zabezpečovania dôkazov pre trestné konanie).

Zoznam použitých zdrojov:

Čentěš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava : C. H. Beck, 2013.

Holländer, P. Zásada proporcionality: jednosměrná ulice, nebo hermeneutický kruh? Na příkladech veřejných dober a základních práv kolidujících s právem na soukromí. In Šimíček, V. Právo na soukromí. Brno : Masarykova univerzita, 2011.

Ivor, J., Polák, P., Záhora, J.: Trestné právo procesné I. Všeobecná časť. Bratislava: Wolters Kluwer, 2017.

Peťovský, M., Odlerová, M.: Zákon o Policajnom zbore. Aplikčná prax. Plzeň: Aleš Čeněk, 2018.

Tittlová, M.: Zákon o ochrane súkromia pred odpočúvaním. Komentár. Bratislava: Wolters Kluwer, 2018.

Tittlová, M., Medelský, J.: Zákon o Policajnom zbore SR. Komentár. Bratislava: Wolters Kluwer, 2016.

Zákon č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov.

Trestný poriadok, zákon č. 301/2005 Z. z. v znení neskorších právnych predpisov.

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) v znení neskorších.

Zákon č. 4/2001 Z. z. o Zbore väzenskej a justičnej stráže v znení neskorších predpisov.

Zákon č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.

Zákon č. 461/1993 Z. z. v Slovenskej informačnej službe v znení neskorších predpisov.

Rozsudok ESĽP z 25. marca 1983 vo veci Silver proti Spojenému Kráľovstvu.

Rozsudok ESĽP zo 6. septembra 1978 vo veci Klass a ostatní proti Nemecku.

Rozsudok ESĽP vo veci Funke proti Francúzsku.

Poznámky pod čiarou

[1] 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) v znení neskorších predpisov (v ďalšom texte len „Zákon“ alebo „Zákon o ochrane súkromia“) Táto štúdia bola podporovaná Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-16-0521

[2] Tittlová, M.: Zákon o ochrane súkromia pred odpočúvaním. Komentár. Bratislava: Wolters Kluwer, 2018, s. 32

[3] Ivor, J., Polák, P., Záhora, J.: Trestné právo procesné I. Všeobecná časť. Bratislava: Wolters Kluwer, 2017, s. 421 a nasl.

[4] Tittlová, M.: Zákon o ochrane súkromia pred odpočúvaním. Komentár. Bratislava: Wolters Kluwer, 2018, s. 32 a nasl.

[5] Tittlová, M., Medelský, J.: Zákon o Policajnom zbore SR. Komentár. Bratislava: Wolters Kluwer, 2016, s. 109 a nasl.

[6] Peťovský, M., Odlerová, M.: Zákon o Policajnom zbore. Aplikčná prax. Plzeň: Aleš Čeněk, 2018, s. 94 a nasl.

[7] Rozsudok ESĽP zo 6. septembra 1978 vo veci Klass a ostatní proti Nemecku, ods. 49

[8] Rozsudok ESĽP z 25. marca 1983 vo veci Silver proti Spojenému Kráľovstvu, ods. 97

[\[9\]](#) Rozsudok ESĽP zo 6. septembra 1978 vo veci Klass a ostatní proti Nemecku, ods. 49

[\[10\]](#) Rozsudok ESĽP vo veci Funke proti Francúzsku, ods. 52

[\[11\]](#) Rozsudok ESĽP vo veci Funke proti Francúzsku, ods. 52

[\[12\]](#) Čentéš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava : C. H. Beck, 2013, s. 44

[\[13\]](#) Holländer, P. Zásada proporcionality: jednosměrná ulice, nebo hermeneutický kruh? Na příkladech veřejných dober a základních práv kolidujících s právem na soukromí. In Šimíček, V. Právo na soukromí. Brno : Masarykova univerzita, 2011, s. 46