ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

DIPLOMOVÁ PRÁCE

Právní úprava a důkazní využití odposlechů v trestním řízení

Plzeň, 2013 **Ivo Kartus**

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra trestního práva

DIPLOMOVÁ PRÁCE

Právní úprava a důkazní využití odposlechů v trestním řízení

Vedoucí diplomové práce:

Prof. JUDr. Jan Musil, CSc.
Katedra trestního práva

Zpracoval:

Ivo Kartus
Studijní program: Právo a právní věda
Studijní obor: Právo

Plzeň, 2013

„Prohlašuji, že jsem diplomovou práci na téma Právní úprava a důkazní využití odposlechů v trestním řízení zpracoval samostatně. Veškeré prameny a zdroje informací, které jsem použil k sepsání této práce, byly citovány v poznámkách pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury“.

V Benešově, dne 15. března 2013 …….

Touto cestou děkuji Prof. JUDr. Janu Musilovi, CSc. za pomoc při výběru tématu a za konzultační pomoc při řešení odborných problémů a otázek týkajících se vlastního zpracování diplomové práce.

OBSAH DIPLOMOVÉ PRÁCE

1. Úvod

Pachatelé na celém světě zdokonalují svou trestnou činnost a snaží se být co nejdále od vlastní oběti trestného činu. Proto využívají nové a stále se dokonalejší formy trestné činnosti. Jedná se především o internetové podvody, podvodné textové zprávy (SMS) prostřednictvím mobilních telefonů či emailové pošty. Těchto technických vymožeností ovšem pachatelé využívají i ke komunikaci, plánování trestné činnosti, čímž značně ztěžují nasazování operativně pátracích prostředků. V nedávných dobách se pachatelé museli domlouvat osobně, většinou na veřejném místě a tak do jisté míry ulehčovali činnost policistům, kteří prováděli operativní rozpracování. S vývojem techniky i demokracie se ale stávalo, že právě ty složky, které by měly chránit majetek a zdraví občanů, byly mnohdy i několik kroků za pachateli. V důsledku tohoto vývoje se policisté často potýkají s nízkou a zastaralou úrovní technického vybavení, s nálezy soudů nebo neschopností zákonodárců vytvořit takový zákon, který by byl „ušit“ na míru orgánům, které mají chránit občany vlastního státu. Problematika vlastního technického vybavení je záležitostí resortu (ministerstva), které má jednotlivé složky ve své gesci. Za zásadní je tudíž nutné považovat vlastní zákonné úpravy, které se týkají ochrany celé společnosti.

Tématem této diplomové práce je problematika právní úpravy a důkazního využití odposlechů v trestním řízení. Problematika využívání odposlechů v praxi a obava z jejich zneužití, je jedním z problémů, které přineslo období demokracie. Rozhodně nelze souhlasit se zneužíváním tohoto operativního prostředku. Některé případy zneužívání odposlechů v minulosti i v poměrně nedávné době našeho nově vzniklého demokratického státu jsou neoddiskutovatelné, ať už se jednalo o zneužití při nasazování odposlechů nebo únik informací – přepisů odposlechů. Téměř ve všech případech se jednalo o pochybení jednotlivců a nikoliv systému. Někteří byli exemplárně potrestáni, jiní unikli pouze s nízkým trestem. Při studiu některých odůvodnění proč nelze odposlech nasadit bylo zjištěno, že některé exekutivní složky státu povolení nevydají s odůvodněním, aby bylo využito jiných prostředků ke zjištění pachatele (policisté při objasňování sériové trestné činnosti ale mnohdy nemají možnost získat jiné důkazní materiály o skutečnosti, že se jedná o sériovou trestnou činnost, protože jiné informace z míst trestné činnosti prostě nejsou k dispozici).

Je proto možné konstatovat, že stát by v těchto záležitostech měl více hájit svá práva, a to i za cenu omezení některých práv vlastních občanů.

Jsem si samozřejmě vědom, že §88 a §88a trestního řádu je jedním ze zásahů do státem chráněných a deklarovaných základních práv a svobod, ale i přesto si dovolím tvrdit, že odposlech a záznam telekomunikačního provozu představuje jednu z nejvýznamnějších metod operativní činnosti, bez níž si současné trestní řízení lze jen stěží představit.

V této diplomové práci bude zmíněna také činnost jednotlivých subjektů oprávněných využívat odposlech při jeho vyžadování.

Cílem této práce je zdůraznit význam a důležitost odposlechu a záznamu telekomunikačního provozu při objasňování trestné činnosti pachatelů, srovnání možností, využití a postavení odposlechů v sousedních státech a v neposlední řadě se tato práce zabývá i problematikou provádění a dokumentování nasazovaných odposlechů u jednotlivých specializovaných útvarů Policie ČR.

2. Vysvětlení pojmu

V současném moderním světě využívají technických vymožeností (mobilní telefonní síť, SKYPE, emailová pošta, SMS zprávy) při páchání trestné činnosti téměř všichni pachatelé. Proto je odposlech telekomunikačního provozu jeden z velmi důležitých operativních prostředků v boji s trestnou činností. Další velmi důležitou formou při zjišťování sériové trestné činnosti je výpis z telekomunikačního provozu a lokalizační údaje. Výše uvedené formy operativně pátrací činnosti (fáze prověřování) byly v minulosti velmi významnou měrou omezeny, resp. bylo přesně stanoveno, na jaké trestné činy je možno odposlech nasadit případně zjistit telekomunikační provoz z míst trestné činnosti, a to na základě nálezu Ústavního soudu, který tento způsob boje proti organizované trestné činnosti značně omezil. V současné době dochází k narovnání – novelizaci zákona o telekomunikačním provozu, kdy je zpětně uložena povinnost všem operátorům mobilních a pevných telefonních sítí uchovávat data o provedeném telekomunikačním provozu pro orgány činné v trestním řízení (6 měsíců zpětně), dále tato novelizace snižuje horní hranici trestu odnětí svobody z 8 let na 3 roky. Tento významný posun v boji proti trestné činnosti v budoucnosti zcela jistě prokáže, že tento krok byl správný.

V právním řádu České republiky nenalezneme vymezení pojmu **telekomunikační provoz**, a to i přesto, že je tento pojem velmi často užíván. Pojem telekomunikační provoz lze najít v komentářích k trestnímu řádu, a to **v tomto znění:** „Pod pojmem telekomunikační provoz se rozumí telefon, telefax, mobilní telefony, vysílačky, ale i jiná telekomunikační zařízení.“ Bezprostředně související pojmy s pojmem telekomunikační provoz nalezneme v zákoně č. 127/2005 Sb. (§136/ods.20a) o elektronických komunikacích. Jedná se zejména o pojmy **telekomunikační služba, telekomunikační síť** a **telekomunikační zařízení.**

Odposlech a záznam telekomunikačního provozu (dále jen odposlech) je velmi důležitou složkou v boji proti nejzávažnějším formám páchání trestné činnosti. Mezi ně se řadí zejména organizovaný zločin, drogová kriminalita nebo korupce.

Odposlech jako takový je samozřejmě velkým zásahem do ústavně i mezinárodně chráněných základních práv a svobod. Při použití odposlechů musí být postupováno velmi obezřetně, a pokud je již odposlech nasazen, musí stále probíhat kontrola, zda nebyl tímto úkonem porušen zákon či nedošlo ke zneužití provozních a lokalizačních údajů v rámci operativní činnosti policie a je-li i nadále zajištěna ochrana soukromí a osobních údajů.

V současné době mohou být odposlechy nařízeny pro **trestné činy – zločiny**, za které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby 8 let, dále pro trestný čin **pletichy v insolvenčním řízení, porušení předpisů o pravidlech hospodářské soutěže, sjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě, zneužití pravomoci úřední osoby nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje Českou republiku mezinárodní smlouva**, a to například trestné činy, které se týkají **drogové kriminality, CITES** (Úmluva o mezinárodním obchodu s ohroženými druhy volně žijících živočichů a planě rostoucích rostlin, viz. Washingtonská úmluva).

3. Právní vývoj odposlechu a záznamu telekomunikačního provozu

Prvním zákonem, který upravoval postavení soudů a jejich pravomocí byl Řád soudu trestního, který byl vydán dne 23. května 1873 jako říšský zákoník. Tento zákon se nazýval Zákoník říšský pro království a země v radě říšské zastoupené[1]. A to pod číslem 119/1873(v současné době platný v Rakouské republice). Tento zákon se dá považovat za položení základů dalších zákonů v oblasti trestního práva. V tomto zákoně není řešena problematika odposlechů, neboť vzhledem k malé technické vyspělosti tehdejší společnosti toto nebylo nutné.

Další vývoj ve věcech trestních se datuje na den 12. července 1950 a jedná se o zákon číslo 87/1950 Sb. Tento dokument se nazýval Zákon o trestním řízení soudním (trestní řád). Vývoj tohoto zákona byl samozřejmě ovlivněn společenskými událostmi z roku 1948. I v tomto trestním řádu nebyla problematika odposlechu zapracována tak

[1] http://alex.onb.ac.at/cgi-content/alex?aid=rbo&datum=1873&size=45&page=417 dne 9.3.2013

jako v následujícím zákoně číslo 64/1956 Sb., který byl vydán dne 19. prosince 1956. V tomto zákonném znění nebyly odposlechy jako takové zákonem upraveny nebo vymezeny, ale bylo využíváno dikce zákona o dokazování, konkrétně se jedná o Hlavu I. - Obecná ustanovení, § 2, odst. 7, 8.

Přirozeným vývojem společnosti a vzrůstající úrovní technického vybavení došlo i k úpravě trestního řádu tehdejší Československé socialistické republiky. Nový trestní řád – zákon číslo 141/1961 Sb. byl vydán dne 29. listopadu 1961. V této době byly využívány operativní úkony složkami, jako byl například Sbor národní bezpečnosti (SNB) a Státní bezpečnost (StB) a jiné exekutivní složky státu tyto možnosti využívání neměly. V tomto období bylo využívání odposlechů velmi odlišné od současné doby. Odlišnost byla zejména technického rázu (tzv. zvonky). Odposlech byl zaznamenáván na magnetofony a byl prováděn v reálném čase. Obsah hovorů se zálohoval na magnetofonové pásky nebo kazety, ty pak byly policejními orgány vyhodnocovány. V této době neexistovala mobilní komunikace a de facto se jednalo pouze o odposlechy pevných linek. Takový způsob zadokumentování by v současné demokratické době nebyl možný, protože nakládáním se záznamy o odposleších by bylo možné lehce manipulovat. Teprve s nástupem demokracie došlo k novelizaci trestního řádu (novela č. 178/1990 Sb.), ve kterém byl do zákona číslo 141/1961 Sb. zapracován § 88 - „ odposlech telefonních hovorů“

Po zahájení trestního stíhání pro zvlášť závažný úmyslný trestný čin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, může předseda senátu a v přípravném řízení prokurátor nařídit odposlech telefonních hovorů, pokud lze důvodně předpokládat, že jimi budou sděleny významné skutečnosti pro trestní řízení. Nelze však provádět odposlech telefonních hovorů mezi obhájcem a obviněným.[2]
Příkaz k odposlechu telefonních hovorů musí být vydán písemně a odůvodněn. Současně v něm musí být stanovena doba, po kterou bude odposlech telefonních hovorů prováděn. Odposlech zajistí orgán sboru národní bezpečnosti.[3]

[2] Ust. § 88 odst. 1 zák. č. 178/1990Sb., kterým se mění a doplňuje trestní řád, ve znění účinném od 01. 07. 1990.
[3] Ust. § 88 odst. 2 zák. č. 178/1990Sb., kterým se mění a doplňuje trestní řád, ve znění účinném od 01. 07. 1990.

Je-li vedeno trestní stíhání pro jiný trestný čin, než je uveden v odstavci 1, může orgán činný v trestním řízení nařídit odposlech telefonních hovorů jen se souhlasem účastníka odposlouchávané telefonní stanice. [4]
Má-li být záznam telefonního hovoru užit jako důkaz, je třeba k němu připojit protokol s uvedením údajů o místě, času, způsobu a obsahu provedeného záznamu, jakož i o osobě, která záznam pořídila.[5]

Tímto paragrafovým zněním byla poprvé v trestním řádu zakotvena problematika odposlechů ve výše uvedeném paragrafu. Poprvé došlo k jasnému vymezení, jakým způsobem se budou odposlechy vyžadovat a jakým způsobem s nimi bude nakládáno. Současně je zakázán odposlech mezi obhájcem a obviněným, jsou zde přesně stanoveny náležitosti příkazu o odposlechu a jsou zároveň stanoveny podmínky pro využití odposlechů jako důkazního prostředku. V této novele není však ještě řešen institut ochrany osobních údajů v návaznosti na § 88 a způsob uchovávání odposlechů. Tato mezera byla ovšem upravena a doplněna nařízením policejního prezidenta.

S rychlým rozvojem demokratického státu docházelo i k novelizacím zákonů, které rodící se demokratická společnost nutně potřebovala pro svůj vývoj. Tento vývoj se samozřejmě dotkl i trestního řádu, který byl několikrát novelizován. Novelizací číslo 292/1993 Sb. došlo ke změně v názvu paragrafu 88 a to na „odposlech a záznam telekomunikačního provozu“.

Změny nevyplývaly pouze z vývoje politického a společenského, ale většina změn reagovala na velmi rychle se rozvíjející technické vybavení - zejména pak telekomunikační techniky. Společnost se nově setkala s faxy, mobilními telefony a jinými telekomunikačními zařízeními (e-maily, SKYPE, ICQ), proto je zcela logické, že i vývoj trestního řádu musel bezpodmínečně reagovat na tento technický rozvoj.

Základní princip - nemožnost odposlechu mezi obhájcem a obviněným zůstává nezměněn, ale stanovuje se například délka odposlechů, jednoznačné podmínky pro vydání příkazu k odposlechu i to, kdo takovéto odposlechy může provádět. Bylo také jasně stanoveno, za jakých podmínek může být záznam telekomunikačního provozu užit jako důkaz.

[4] Ust. § 88 odst. 3 zák. č. 178/1990Sb., kterým se mění a doplňuje trestní řád, ve znění účinném od 01. 07. 1990.
[5] Ust. § 88 odst. 4 zák. č. 178/1990Sb, kterým se mění a doplňuje trestní řád, ve znění účinném od 01. 07. 1990.

Příkaz k odposlechu a záznamu telekomunikačního provozu musí být vydán písemně a odůvodněn. Současně v něm musí být stanovena doba, po kterou bude odposlech a záznam prováděn a která nesmí být delší než 6 měsíců. Odposlech a záznam telekomunikačního provozu provádí policejní orgán.[6]

Pokud při odposlechu a záznamu nebyly zjištěny skutečnosti významné pro trestní řízení, je nutno záznamy předepsaným způsobem zničit.[7]

Vzhledem k velmi rychlému rozvoji celé společnosti došlo k dalším novelizacím trestního řádu - například v novele číslo 152/1995 Sb., byl upraven institut nemožnosti odposlechu mezi obhájcem a obviněným a rozšířen o část, která se zabývá nakládáním s těmito hovory. Jednoznačně bylo stanoveno, že takový odposlech musí policejní orgán přerušit, zničit předepsaným způsobem. Tato novela také stanovila nemožnost použití hovoru mezi obhájcem a obviněným jako důkazu.

V roce 2001 došlo k další novelizaci institutu odposlechu, a to novelou číslo 265/2001 Sb., ve které byl znovu novelizován § 88. V této novelizaci je upraveno, kdo odposlech a záznam telekomunikačního provozu provádí.

Příkaz k odposlechu telefonních hovorů musí být vydán písemně a odůvodněn. Současně v něm musí být stanovena doba, po kterou bude odposlech telefonních hovorů prováděn. Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení policie české republiky.[8]

Tato novelizace stanovuje, že Policie české republiky jako jediná může provádět odposlechy, a to i pro ostatní orgány činné v trestním řízení (BiS, VoZ, GIBS, atd.)

Další významnou změnou bylo rozšíření institutu odposlechů o tzv. poskytnutí údajů o uskutečněném telekomunikačním provozu. Toto ustanovení § 88a aplikuje rozvoj operativní práce orgánů činných v trestním řízení, které tyto údaje využívají

[6] Ust. § 88 odst. 2 zák. č. 292/1993Sb., novela trestního řádu, ve znění účinném od 01. 01. 1994.
[7] Ust. § 88 odst. 5 zák. č. 292/1993Sb., novela trestního řádu, ve znění účinném od 01. 01. 1994.
[8] Ust. § 88 odst. 2 zák. č. 265/2001Sb., novela trestního řádu, ve znění účinném od 01. 01. 2002.

k natipování možných pachatelů trestné činnosti a zároveň napomáhají zjistit, zda se jedná o sériovou trestnou činnost. Jedná se o velmi potřebný nástroj proti pachatelům.

Příkaz, který je vydán na základě nařízení předsedy senátu a v přípravném řízení na návrh státního zástupce soudcem, může být vydán pouze ze zákonných důvodů, písemně a jeho opodstatnění náležitě odůvodněno.

Ustanovení § 88a) zní:

Je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, nařídí předseda senátu a v přípravném řízení soudce, aby je právnické nebo fyzické osoby, které vykonávají telekomunikační činnost, sdělily jemu a v přípravném řízení buď státnímu zástupci, nebo policejnímu orgánu. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn.[9]
Příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat.[10]

Další změny, kterými muselo znění paragrafů 88 a 88a projít, proběhly na základě Nálezů Ústavního soudu České republiky v roce 2011. Konkrétně se jednalo o návrh poslanců Poslanecké sněmovny Parlamentu České republiky na zrušení ustanovení § 97 odst. 3,4 zákona číslo 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a vyhlášky číslo 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě způsobu jejich předávání orgánům oprávněným k jejich využívání. Předmětný nález Ústavního soudu byl vyhlášen dnem 31. března 2011, kdy byly prováděcí vyhlášky a dotčená ustanovení fakticky zrušeny dnem vyhlášení tohoto nálezu ve Sbírce zákonů. Dnem 1. října 2012 byly výše uvedené paragrafy novelizovány, právnickým a fyzickým osobám bylo znovu nařízeno uchovávat údaje o provedených telekomunikačních provozech, a to po dobu 6 měsíců zpětně. U § 88 byly změněny

[9] Ust. § 88a odst. 1 zák. č 265/2001Sb., změna trestního řádu, ve znění účinném od 01. 01. 2002.
[10] Ust. § 88a odst. 2 zák. č. 265/2001Sb., změna trestního řádu, ve znění účinném od 01. 01. 2002.

podmínky, za kterých lze nadsadit odposlechy, a to při vyšetřování úmyslného trestného činu s horní hranicí trestní sazby min. 8 let.

Paragraf 88a je podrobněji rozebrán v kapitole 5 - Rozbor nálezu Ústavního soudu ve věci §88 a §88a trestního řádu.

4. Současné postavení odposlechu a záznamu telekomunikačního provozu v trestním řízení

Tato kapitola se zaměřuje na výklad praktického použití odposlechu a činnosti konkrétních orgánů policie, které s odposlechy jako takovými pracují, vyžadují je a na jejich základě usvědčují pachatele trestné činnosti.

V ustanovení § 88 je uvedeno, že provádění odposlechů mají v kompetenci příslušné orgány Policie ČR, které je zajišťují pro orgány činné v trestním řízení. Který z orgánů činných v trestním řízení může tedy být žadatelem k nasazení odposlechu? Oprávněnými žadateli jsou policisté služebně zařazeni u oprávněných subjektů, kterými jsou útvary Služby kriminální policie a vyšetřování (dále jen SKPV). Konkrétně se jedná o:

• odbory ÚSKPV Policejního prezidia ČR,

• útvar pro odhalování organizovaného zločinu SKPV (dále jen ÚOOZ),

• národní protidrogovou centrálu SKPV (dále jen NPC),

• útvar speciálních činností SKPV (dále jen ÚSČ),

• útvar odhalování korupce a finanční kriminality SKPV (dále jen ÚOKFK),

• úřad dokumentace a vyšetřování zločinů komunismu SKPV (dále jen ÚDV),

• odbory SKPV Policie ČR krajských ředitelství,

• oddělení SKPV územních odborů a městských ředitelství Policie ČR.

Realizaci odposlechu a záznamu telekomunikačního provozu v rozsahu § 88 trestního řádu zajišťuje v podmínkách Policie ČR výhradně Útvar zvláštních činností

služby kriminální policie a vyšetřování Policie České republiky (dále jen ÚZČ), který jediný provádí a technicky zabezpečuje odposlech.

Útvar zvláštních činností pracuje v nepřetržitém režimu, přijímá požadavky výhradně ze svých pracovišť a posílá je dále příslušnému operátorovi, nemá přímý kontakt z jiných součástí PČR nebo s jinými oprávněnými subjekty, dohlíží na správný průběh aktivace a deaktivace zadaných telefonních čísel, nemá oprávnění samostatně editovat požadavky a nemá přístup k výstupním informacím. Toto jsou obecné charakteristiky útvaru zvláštních činností ve vztahu k prováděným odposlechům.

Existují ale konkrétní bezpečnostní prvky, které jsou součástí tzv. bezpečnostního systému vyžadování odposlechů ÚZČ, kterými jsou:

- Existence spisového materiálu ke každému odposlechu, který je uložen na třech různých místech – expozitura ÚZČ, zadavatel, příslušný soud.
- Editování požadavku je možné pouze z pracoviště, na kterém je veden spisový materiál ke konkrétnímu odposlechu.
• Editování požadavku pouze oprávněnou osobou po její individuální identifikaci („zalogování“).
• Aktivace odposlechu je prováděna pracovištěm, které nemá možnost požadavek editovat a nemá možnost poslouchat záznamy.
• Přítomnost informací o prováděném odposlechu ve všech částech systému (na všech pracovištích).
• Automatické zpracování záznamů na tom pracovišti, na které jsou směřovány technologií operátora.
• Jakékoliv přístupy do systému, v kterékoliv části, jsou možné pouze po individuální identifikaci.
• Logy všech přístupů jsou archivovány a centrálně dostupné.
• Povinnost operátorů uchovávat veškeré údaje o aktivaci a deaktivaci odposlechů pro potřeby kontrolního orgánu PSP ČR.

Při vyžadování úkonů dle §88 odst. 1 trestního řádu je policejní orgán povinen postupovat následujícím způsobem:

Nejprve zpracuje žádost o vydání příkazu k odposlechu a záznamu telekomunikačního provozu na speciálním formuláři, kterou poté konzultuje na

speciálním pracovišti PČR (ÚZČ) z pohledu technické proveditelnosti a kapacitních možností.

Získá-li policista předběžný souhlas, předloží žádost ke schválení příslušnému nadřízenému. Žádost je zpracována na příslušném stupni utajení a vztahuje se k číslu jednacímu trestního spisu nebo k číslu jednacímu vyžádané právní pomoci.

Po schválení nadřízeným předá žádost cestou státního zástupce soudci, který je příslušný vydat příkaz. Písemnou žádost vyhotoví zpravidla v pěti výtiscích, které obdrží soudce, státní zástupce, specializované pracoviště a oprávněný žadatel (založeny ve spisovém materiálu). Policejní orgán v písemné žádosti uvede informace k případu a zdůvodní nutnost použití odposlechu a záznamu telekomunikačního provozu.

Policisté si často stěžují na přehnanou přísnost soudců, kteří mají odposlech nařídit, soudci často vyžadují velmi obsáhlé zdůvodnění a často až přehnané informace, které by měly dostatečně odůvodnit podezření na konkrétní osobu, která má být odposlouchávána. Policisté se často domnívají, že se soudci v dnešní době obávají tento úkon nařídit.

Na straně soudců stojí však Ústavní soud, který formální hodnocení podkladů pro povolení odposlechu mnohokrát řešil a dospěl k závěru, že při nařízení odposlechu nelze setrvat stroze na formálních náležitostech a zcela vynechat posouzení materiálních podmínek pro nařízení odposlechu. Pouze záznam odposlechu telekomunikačního provozu, který byl proveden na základě příkazu, který plně obsahuje všechny informace, je v souladu s ústavním pořádkem procesně použitelným důkazem v trestním řízení.[11]

Pokud soudce shledá žádost jako dostatečnou, nařídí písemně (formou příkazu) odposlech a záznam telekomunikačního provozu, ve kterém mimo jiné jednoznačně identifikuje odposlouchávané telefonní číslo a stanoví dobu, po kterou je provádění odposlechu a záznamu telekomunikačního provozu povoleno. Písemný příkaz soudce k odposlechu a záznamu telekomunikačního provozu předloží policejní orgán specializovanému pracovišti. Teprve na základě těchto dokumentů založí specializované pracoviště spis odposlechu a záznamu telekomunikačního provozu, ve kterém eviduje veškeré písemnosti vzniklé v souvislosti s prováděním akce. **Bez splnění kterékoliv z výše uvedených podmínek je provádění odposlechu a záznamu telekomunikačního provozu nerealizovatelné.**

[11] Srov. blíže s: Rozsudek Ústavního soudu ze dne 23.května 2007, sp. zn. 615/06

Odlišný je postup při vyžadování úkonů dle § 88 odst. 5 trestního řádu, kdy je odposlech prováděn na základě souhlasu osoby, do jejichž práv a svobod má být zasahováno. V takovém případě se k písemné žádosti připojuje příkaz policejního orgánu a souhlasné stanovisko účastníka odposlouchávané stanice. Po doručení žádosti a příkazu k odposlechu a záznamu telekomunikačního provozu je stanoven způsob provedení a zajištění odposlechu a způsob předávání takto získaných informací. Po ukončení odposlechu je jeho výsledek policistou vyhodnocen. Policista zpravidla z ÚZČ dostane ke spisu v elektronické podobě záznamy hovoru, které musí sám vyhodnotit (označí jako „zájmové“ hovory). Přístup k těmto záznamům má pouze on, avšak může přístup povolit například kolegům, kteří na vyšetřování věci spolupracují. Obsahuje-li některý záznam skutečnosti významné pro trestní řízení, požádá policista do 20 dnů ÚZČ o uschování všech dosud nepředaných záznamů. Jestliže při odposlechu záznamu nejsou zjištěny skutečnosti významné pro trestní řízení, zničí policista předepsaným způsobem všechny již předané záznamy a požádá ÚZČ, aby stejně zničil i záznamy dosud nepředané.

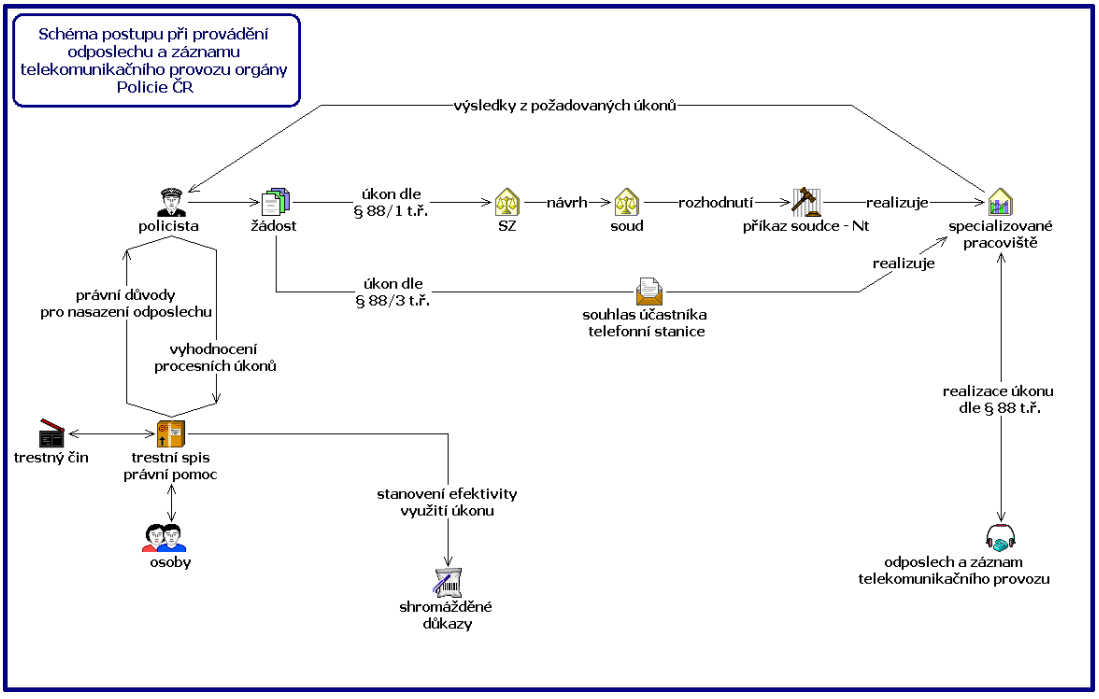
Protokol o zničení záznamů pak ÚZČ policistovi zašle. To, že se často stane, že takový postup nedokáže vždy policejní orgán zastat, řeší ve svém rozsudku Ústavní soud, který uvádí, že pokud z jakéhokoli důvodu nedojde k řádnému zničení odposlechu a záznamu telekomunikačního provozu, například v důsledku špatné či nedostatečné práce orgánů činných v trestním řízení, nelze s nimi disponovat. Jde o materiály, které vlastně nelze v trestním řízení použít. Dle ustanovení §88 odst. 7 trestního řádu, je nutno záznamy předepsaným způsobem zničit, a to ve všech formách, v nichž se nacházejí ve spise. Tato povinnost tedy není vyčerpána zničením CD nosičů s uvedenými záznamy, pokud současně zůstaly ve spisu založeny například v listinné podobě. Ke zničení má přitom dojít ex officio a nikoliv až na návrh.[12]

Má-li být některý záznam použit jako důkaz v trestním řízení, vyhotoví k němu ten, kdo záznam pořídil, protokol s náležitostmi uvedenými v § 88 odst. 6 trestního řádu. Policista musí také vyhotovit přepis rozhovoru, který byl zaznamenán, a to buď doslovný nebo formou záznamu, kde popisuje rozhovor, ve kterém uvede např., jaké informace byly v rozhovoru uvedeny a kdo je uvedl. Přepis také může obsahovat legendu, protože řada pachatelů trestných činů používá pro různé situace a věci různé zašifrované termíny, jak je známo například u tzv. „kapříků“ v souvislosti s

[12] Srov. blíže s: Rozsudek Ústavního soudu ze dne 27.září 2007, sp.zn. 789/06

vyšetřováním korupce, či argot používaný mezi dealery drog a jejich výrobci. Například v Polsku existují znalci, kteří právě k takovým přepisům vytvářejí legendy. Otázku identifikace mluvčího řešil také Nejvyšší soud, který v rozsudku uvádí, že jiné podmínky než uvedené v ustanovení §88 odst. 6 trestního řádu pro provedení důkazu odposlechem stanoveny nejsou a není tedy ani stanoveno, jakým způsobem má být uživatel telekomunikačního zařízení, příp. další osoby jako účastnící odposlouchávaného rozhovoru ztotožněni. Osoby, jejichž hovory byly na odposlechovém zařízení zaznamenány lze ztotožnit i za pomoci údajů uváděných v jednotlivých hovorech, skutečností, které těmto údajům odpovídají, souvislostí mezi hovory na různých odposlouchávaných telefonních stanicích atd. Soud tedy není povinen opatřovat si srovnávací hlasové vzorky, vyžadovat odborné vyjádření atd.[13]

Pro lepší orientaci v praktické problematice slouží níže uvedené schéma postupu při provádění odposlechu a záznamu tel. provozu orgány PČR.



Zdroj: www.mvcr.cz/soubor/analyza-odposlechu-2007-doc.aspxs

Velmi důležitou součástí jsou údaje, které jsou přikládány a zachycovány na datovém nosiči společně s provedeným odposlechem telekomunikačního provozu. Zde je nutné nejdříve osvětlit pojmy, které souvisejí s mobilními telekomunikacemi.

[13] Srov. blíže s: Rozsudek Nejvyššího soudu České republiky ze dne 14.dubna 2005, sp.zn. 7 Tz 196/2004

Jako první je zkratka „IMEI“, která pochází z anglického termínu International Mobile Equipment Identity. Jde o unikátní číslo přidělené výrobcem mobilní telefonu. Tato čísla jsou mobilními operátory uložena v interních systémech. Po nahlášení například krádeže mobilního telefonu operátorovi je možné dané „IMEI“ číslo zablokovat pro další použití v mobilní síti. Toto číslo je patnáctimístné a lze je zapsat ve formátu ZZnnnn-MM-nnnnnn-X. První skupina „IMEI“ čísla se nazývá, type approval code (TAC), kde první dvě čísla určují kód země (ZZ). Druhá skupina (MM) je kód výrobce mobilního telefonu. Poslední číslo (X) se vetšinou nevyužívá a je předdefinováno na nulu.

Formát „IMEI“ čísla je tedy následovný:

• TAC – Type Approval Code (6 číslic z toho první dvě jsou kódem země)

• FAC – Final Assembly Code (2 číslice, které charakterizují výrobce)

• SNR – Serial Number (6 číslic, což je sériové číslo telefonu)

• SP – Spare (1 číslice, většinou předdefinována na nulu)

Na většině mobilních telefonů či jiných mobilních zařízení např. dnes již hojně využívaných tabletů a podobně lze zjistit „IMEI“ číslo zadáním kódu *#06#. Pro přehlednost přikládám tabulku jednotlivých výrobců mobilních telefonů s kódy FAC.

kód FAC	Výrobce
01, 02, 65	AEG
07, 40	Motorola
10, 20	Nokia
30	Ericsson
40, 41, 44	Siemens
50	Bosch
51	Sony, Siemens, Ericsson
60	Alcatel
70	Sagem
75	Dancall
80	Philips
85	Panasonic

Odborný článek – Bezpečností teorie a praxe 2/2011 (Mgr. Bc. Pavel Málek)

SIM karta – SIM je zkratka pocházející z anglického Subscriber Identity Module, tato účastnická karta slouží pro identifikaci účastníka v mobilní síti. Na SIM kartě je

uloženo číslo IMSI, které jednoznačně identifikuje účastníka na celém světě, ať už se přihlásí do jakékoliv mobilní sítě. Toto číslo se nepoužívá jako telefonní číslo. Každé SIM kartě je přiřazeno MSISDN číslo účastníka mobilního telefonu. SIM karty jsou nejčastěji používány v síti GSM, ale také v sítích UMTS. SIM karta také obsahuje svoji paměť, kam se ukládají textové zprávy SMS, telefonní čísla a někdy také další aplikace.

MSISDN je celosvětově originální číslo, které identifikuje SIM kartu v mobilní síti GSM nebo UMTS. Přidělování těchto čísel se řídí číslovacím plánem E. 164, který definovala Mezinárodní telekomunikační unie. MSISDN se většinou uvádí v mezinárodním formátu telefonního čísla i s mezinárodním přestupným znakem (nejčastěji + nebo 00), kupříkladu české MSISDN ve tvaru +420 xxx xxx xxx, samotný přestupný znak, ale není součástí MSISDN. Toto číslo může mít maximální délku 15 číslic a tvoří ho kód země následovaný národním telefonním číslem, které se skládá z kódu mobilní sítě a čísla v příslušné síti.

Celkem je tedy MSISDN tvořeno ze 3 částí:
Country Code (CC) – jedno až trojciferný kód země (ČR – tzn. 420)
National Destination Code (NDC) – národní směrové číslo, které určuje mobilní síť v dané zemi (ČR – např. 723)
Subscriber Number (SN) – účastnické číslo, které určuje konkrétní SIM kartu v dané mobilní síťi (ČR - 006 589)

Dnešní trestná činnost pachatelů je velmi sofistikovaná a pachatelé jsou velice dobře obeznámeni s postupy policie. Mnohdy jsou i lépe technicky vybaveni, z tohoto důvodu nutí nebo alespoň by měli nutit orgány činné v trestním řízení k tomu, aby z opatřeného důkazu vytěžili maximum informací a skutečností, které budou moci být použity k prokázání viny pachatele trestné činnosti. Z toho vyplývají možnosti vyžádání výpisů v souvislosti s §88a trestního řádu.

• výpis konkrétní SIM karty – jedná se o výpis na jedno účastnické číslo, ze kterého je možné zjistit *tzv. prohazování telefonů,* to znamená, že zájmová osoba využívá více mobilních přístrojů, ale stále se stejnou SIM kartou. Tento způsob se objevuje především u majetkové a drogové kriminality,

• výpis na IMEI kód – tímto výpisem je monitorováno jedno konkrétní mobilní zařízení a tímto postupem mají orgány činné v trestním řízení možnost zjistit vkládání různých SIM karet. Tento postup se použije v případě předpokladu, že majitel zařízení často mění telefonní čísla pro ztížení možnosti odposlechu. Toto praktikují zejména pachatelé organizované, násilné nebo majetkové trestné činnosti,

• výpis na přenosovou buňku – tento způsob je využíván v případech, kdy dochází na různých místech, dle modu operandi, k podobné trestné činnosti a je zde snaha o ustanovení shodných telekomunikačních zařízení, která byla používána na místě trestných činů,

• kombinace jednotlivých výpisů případně jejich postupné vyžadování dle zjištěných informací. Jedním výpisem je možné zjistit jiné číslo či jiný mobilní telefon a pomocí druhého výpisu se zjišťují další navazující informace.

Pro úplnost je třeba zmínit, že všechny typy výpisů a z nich zjištěné informace poskytují přímý důkaz o pohybu věci (mobilní telefon, SIM karta, nebo i více mobilních zařízení), nikoliv však o pohybu konkrétní osoby.

V této souvislosti je třeba zmínit rozhodnutí Nejvyššího soudu ČR 4Tz 17/2009, kterým bylo judikováno, že odposlech a záznam telekomunikačního provozu, zejména obsah hovoru, nemůže být považován za důkaz tehdy,pokud z výpisu vyplývá, že volající žádá po zájmové osobě nebo po obviněném například formou argotického vyjadřování „*PIKO*“ , „*BUČO*“apod. Z rozhodnutí Nejvyššího soudu vyplývá, že je nutné vést další dokazování, že mezi obviněným a zájmovou osobou se skutečně jednalo o drogách a ne o něčem jiném.

Z výše uvedeného tedy vyplývá, že lze zjistit výměnu telefonního přístroje, do něhož je vložena zájmová SIM karta. Dále lze zjistit pohyb karty během telefonního hovoru, a pokud se mění počáteční i koncová přenosová buňka lze tím určit i směr pohybu karty a samozřejmě i místo, kde se karta nacházela.

4.1. Podmínky pro nasazení odposlechu

Podle ustanovení § 88 odst. 1 z. č. 141/1961 Sb. je možné nařídit odposlech a záznam telekomunikačního provozu, je- li vedeno trestní řízení (ve smyslu tohoto

zákona – trestního řádu) pro zvlášť závažný zločin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva.

Co je zvlášť závažný zločin definuje trestní zákoník v ustanovení § 14 odst. 3:

Zločiny jsou všechny trestné činy, které nejsou podle trestního zákona přečiny; zvlášť závažnými zločiny jsou ty úmyslné trestné činy, na něž trestní zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně deset let.[14]

Odposlech je tedy možné nařídit u úmyslných trestných činů, u kterých zákon stanoví trest odnětí svobody s hranicí trestní sazby nejméně deset let.

Odposlech a záznam telekomunikačního provozu lze také nařídit u trestných činů, jejichž stíhání zavazuje vyhlášená mezinárodní smlouva.[15]
Jedná se také o další obecné skutkové podstaty trestných činů, např. trestný čin obecného ohrožení podle § 272 odst. 1 trestního zákoníku, trestný čin ublížení na zdraví podle
§ 146 odst. 1, 2, 3 trestního zákoníku, trestný čin omezování osobní svobody podle § 171 odst. 1, 2, 3 trestního zákoníku v návaznosti na mezinárodní úmluvy.[16] [17]

Dalším kritériem pro provádění odposlechů – vydání příkazu k jeho uskutečnění v trestním řízení - je důvodný předpoklad, že nařízeným odposlechem budou získány významné skutečnosti pro právě vedené trestní řízení, které nelze pro sledované účely získat jinak nebo by jejich dosažení bylo ztížené.

Skutečnostmi významnými pro trestní řízení jsou především skutečnosti uvedené v ustanovení § 89 odst. 1 písm. a) až c) event. i e) trestního řádu, a to:

---

[14] Ust. § 14 odst. 3 zák. č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

[15] Např. trestné činy: Ublížení na zdraví podle ust. § 146 odst. 1, 2e) tr. zákoníku v návaznosti na Mezinárodní úmluvu o odstranění všech forem rasové diskriminace č. 95/1974 Sb.; Odběr tkáně, orgánu a provedení transplantace za úplatu podle ust. § 166 odst. 1, 2 tr. zákoníku v návaznosti na Úmluvu o lidských právech a biomedicíně, č. 96/2001 Sb.m.s.,a Dodatkový protokol k Úmluvě o lidských právech a biomedicíně, č. 5 97/2001 Sb.m.s.; Prostituce ohrožující mravní vývoj dětí podle ust. § 190 tr. zákoníku v návaznosti na Úmluvu o právech dítěte č. 104/1991 Sb., Podplácení podle ust. 332 tr. zákoníku v návaznosti na Trestně právní úmluvu o korupci, č. 70/2002 Sb.m.s., č. 43/2009 Sb.m.s.

[16] Úmluva o zabránění a trestání trestných činů proti osobám požívajícím mezinárodní ochrany včetně diplomatických zástupců č. 131/1978 Sb., Mezinárodní úmluva proti braní rukojmí, č. 36/1988 Sb., Protokol o boji s protiprávními činy násilí na letištích sloužících mezinárodnímu civilnímu letectví, č. 138/2002 Sb.m.s., Úmluva o značkování plastických trhavin pro účely detekce, č. 6/2003 Sb.m.s., Mezinárodní úmluva o potlačování teroristických bombových útoků, č. 80/2001 Sb.m.s., Mezinárodní úmluva o potlačování činů jaderného terorismu, č. 57/2007 Sb.m.s., Evropská úmluva o potlačování terorismu, č. 552/1992 Sb., Úmluva o zabránění a trestání zločinů genocidia, č. 32/1955 Sb., Mezinárodní úmluva o otroctví č. 165/1930 Sb., a Dodatková úmluva o odstranění otroctví, obchodu s otroky a institucí a praktik podobných otroctví, 7. září 1956, Ženeva.

[17] Šámal, P. a kol.: *Trestní řád, komentář*. 6. vyd. Praha: Nakladatelství C.H. Beck, rok. 2008

a) zda se stal skutek, v němž je spatřován trestný čin,
b) zda tento skutek spáchal obviněný, případně z jakých pohnutek,
c) jaké podstatné okolnosti měly vliv na posouzení nebezpečnosti činu,
e) jaké podstatné okolnosti umožnily stanovení následku a výše škody způsobené trestným činem.

Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů trestního řízení Policie České republiky. Orgány činnými v trestním řízení se rozumějí soud, státní zástupce a policejní orgán. Policejními orgány se pak rozumějí útvary Policie České republiky. V řízení o trestných činech policistů a zaměstnanců zařazených k Policii České republiky má postavení policejního orgánu Inspekce Policie České republiky. Stejné postavení mají v řízení o trestných činech příslušníků ozbrojených sil pověřené orgány Vojenské policie, v řízení o trestných činech příslušníků Vězeňské služby České republiky pověřené orgány této služby, v řízení o trestných činech příslušníků Bezpečnostní informační služby pověřené orgány Bezpečnostní informační služby, v řízení o trestných činech příslušníků Úřadu pro zahraniční styky a informace pověřené orgány Úřadu pro zahraniční styky a informace a v řízení o trestných činech příslušníků Vojenského zpravodajství pověřené orgány Vojenského zpravodajství. Tím není dotčeno oprávnění státního zástupce podle § 157 odst. 2 písm. b). Postavení policejních orgánů mají i pověřené celní orgány v řízení o trestných činech spáchaných porušením celních předpisů a předpisů o dovozu, vývozu nebo průvozu zboží, a to i v případech, kdy se jedná o trestné činy příslušníků ozbrojených sil nebo ozbrojených sborů a služeb a dále porušením právních předpisů při umístění a pořízení zboží v členských státech Evropských společenství, je-li toto zboží dopravováno přes státní hranice České republiky, a v případech porušení předpisů daňových, jsou-li celní orgány správcem daně podle zvláštních právních předpisů. Není-li dále stanoveno jinak, jsou uvedené orgány oprávněny ke všem úkonům trestního řízení patřícím do působnosti policejního orgánu.[18]

Z dostupných studijních materiálů se lze dočíst o odposleších mezi obhájcem a obviněným. Tuto problematiku řeší zejména §88 odst.1. Provádění odposlechů a záznam telekomunikačního provozu mezi obhájcem a obviněným je podle ustanovení

[18] Srov. blíže s: Ust. § 12 odst. 1 zák. č. 141/1961Sb., trestní řád, ve znění pozdějších předpisů.

88 trestního řádu nepřípustné. Zjistí-li policejní orgán při odposlechu a záznamu telekomunikačního provozu, že obviněný komunikuje se svým obhájcem, je povinen záznam odposlechu bezodkladně zničit a informace, které se v této souvislosti dozvěděl nijak nepoužít. Protokol o zničení záznamu je povinen založit do spisu.

Ve věci nařízení odposlechů a při vyžadování operačních údajů od poskytovatelů telekomunikačních služeb je podstatné správné podání všech žádostí a příkazů. Všechny náležitosti musí striktně odpovídat znění zákona a splňovat formální náležitosti úkonu. Tyto náležitosti nelze dovozovat pouze ze záměru nebo znění vydaného opatření. V případě formálního pochybení hrozí, že důkaz provedený na základě chybného příkazu bude považován za nezákonný a v daném řízení tedy za nepoužitelný. Je nutné dodržet několik náležitosti, kterými jsou:

• přesná a odůvodněná specifikace trestného činu, není však přípustné pouze účelově používat jinou právní kvalifikaci z důvodu možného nasazení operativních prostředků,

• pokud není vedeno trestní řízení pro zvlášť závažný zločin a jako legální podklad pro vydání příkazu je odkaz na text mezinárodní smlouvy, pak je třeba přesně citovat znění mezinárodní smlouvy, která zavazuje Českou republiku ke stíhání takového jednání, včetně poukazu na konkrétní článek mezinárodního dokumentu,

• kdy a jakým způsobem bylo zahájeno trestní řízení případně trestní stíhání. Pro vydání příkazu a pro následné využití i v řízení před soudem není rozhodné procesní postavení osoby, zda je tedy podezřelá nebo obviněná, jestliže je tato skutečnost uvedena a zároveň jsou splněny všechny náležitosti dle § 88 trestního řádu. Je nutno upozornit, že samotné trestní oznámení nemůže být podkladem pro postup dle § 158 odst. 3 trestního řádu, a tedy ani pro nařízení odposlechu, případně pro postup dle § 88 či §88a trestního řádu – vždy je nutno zkoumat a vyhodnocovat další okolnosti,

• v případě, že postup dle §88 a §88a trestního řádu má být proveden ještě před zahájením trestního stíhání, je třeba do žádosti, ale i do příkazu uvést skutečnosti předpokládané v ustanovení § 158 odst. 3 písm. i) trestního řádu a tyto skutečnosti řádně odůvodnit,

• přezkoumatelným způsobem odůvodnit, jaké informace mohou být odposlechem zjištěny,

• přezkoumatelným způsobem odůvodnit, proč nemůže být informace či důkaz získán jinou cestou, případně proč by jiný způsob opatření takový postup podstatně ztěžoval,

• v žádostech, návrzích a příkazech striktně rozlišovat to, kdo je a) účastníkem telekomunikačního provozu, což je každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvou na poskytování těchto služeb, a kdo je b) uživatelem telekomunikačního zařízení, což je každá osoba, která využívá nebo žádá veřejně dostupnou elektronickou komunikaci (tyto definice vyplývají ze zákona o veřejných telekomunikacích). Na užívání těchto pojmů je třeba klást zřetel při možném postupu dle §88 odst. 5 trestního řádu, kdy záměna osoby dávající souhlas by způsobila nepoužitelnost takto zjištěné informace, přičemž je vyloučeno následné doplnění souhlasu osobou jinou.

• je nutno zajistit, aby již z odůvodnění příkazu k odposlechu telekomunikačního provozu byly zřejmé okolnosti odůvodňující podezření proti konkrétní osobě; za nezákonný důkaz je totiž považován i odposlech, který je proveden na podkladě nedostatečně odůvodněného příkazu, případně jeho odůvodnění neobsahuje konkrétní skutečnosti ohledně identifikace osob, přestože již byly v době nařízení známy,

• pokud jsou v návrhu a následně v příkazu tvrzeny nějaké skutečnosti, musí být doloženy ve spisovém materiálu; v případě, že tyto skutečnosti ze spisu jasně nevyplývají, nemohou být použity pro povolení odposlechu. Stejně tak nemůže být následně využito tvrzení o důkazech vyplývajících z provedených odposlechů, pokud nejsou řádně zařazeny do spisového materiálu,

• zajistit naplnění zákonné dikce podstatných náležitostí protokolu o provedeném odposlechu dle §88 odst. 6 trestního řádu, kdy postačuje uvedení údajů o čase uskutečnění jednotlivých hovorů, číslech a osobách uživatelů účastnických stanic, tedy o osobách volajících a volaných,

• ze strany policejních orgánů a státních zástupců musí být kladen důraz i na to, aby soudní rozhodnutí neboli příkaz obsahoval všechny náležitosti výše uvedené a na doplnění obsahu rozhodnutí případně trvat,

• při zohlednění časového hlediska pro další využití opatřeného záznamu o odposlechu telekomunikačního provozu v rámci dalšího trestního řízení je nutno počítat s tím, že lhůta k odtajnění a fyzickému zpracování CD činí nejméně 10 dnů.[19]

4.2. Podmínky pro nasazení odposlechu dle mezinárodních smluv

Trestní řád upravuje problematiku odposlechu převážně v §88 a §88a). Oproti odposlechu uskutečňovanému na základě §88 trestního řádu, který směřuje k odposlouchávání budoucí komunikace, směřuje ustanovení §88a) trestního řádu k zaznamenávání komunikace již v minulosti uskutečněné.[20] Nejedná se o telefonní hovory, které nemohou být zaznamenány a nejsou předmětem telekomunikačního tajemství. Dále trestní řád upravuje problematiku odposlechů v ustanovení § 437a) trestního řádu, ve kterém se jedná o tzv. **PŘESHRANIČNÍ** odposlech.

V ustanovení § 437a) odst. 1 trestního řádu je uvedeno:

Umožňuje-li vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, aby byl z cizího státu prováděn odposlech telekomunikačního provozu na území České republiky bez její technické pomoci, je k rozhodování o udělení souhlasu s provedením odposlechu nebo s jeho pokračováním a k souvisejícím úkonům příslušný krajský soud v Praze; je-li v cizím státě provádějícím odposlech trestní řízení ve stadiu před podáním obžaloby, rozhodne na návrh státního zástupce krajského státního zastupitelství v Praze. Souhlas s provedením odposlechu nebo s jeho pokračováním lze udělit pouze při splnění podmínek uvedených v § 88.(§437a odst. 1 zák. č. 141/1961sb.)

[19] Málek, P.: Odposlechy trochu jinak. Část 2., Bezpečnostní teorie a praxe, 2011, s. 104 – 105.
[20] Císařová, D., Fenyk, I., Kloučková, S.: Trestní právo procesní, 3. aktualizované a rozšířené vyd. Praha: Nakladatelství LINDE PRAHA a.s., 2004. str. 286.

V ustanovení § 437a) odst. 2 trestního řádu je dále uvedeno:

Umožňuje-li vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, aby byl z České republiky prováděn odposlech telekomunikačního provozu na území cizího státu bez jeho technické pomoci, státní zástupce a po podání obžaloby soud informuje cizí stát o předpokládaném nebo prováděném odposlechu (§437a odst. 1 zák. č. 141/1961sb.).

4.3. Podmínky pro nasazení odposlechu a záznamu telekomunikačního provozu dle §66 §68 zákona číslo 273/2008 Sb.

Policie České republiky nemá v současné době možnost nasadit odposlechy ve fázi prověřování dle zákona č.273/2008 Sb. o Policii České republiky. Ta zde byla počátkem 90. let dvacátého století. Vývojem demokracie v našem státě byla tato možnost policejním orgánům odebrána a možnost nasazení odposlechů a záznamů telekomunikačního provozu je možná pouze na základě ustanovení § 88 a 88a tr. řádu. Tato změna byla dána přirozeným vývojem a rozvojem nově vzniklé demokratické společnosti, která čerpala zkušenosti od vyspělých demokracií a zejména pak ze zkušeností okolních států, jako jsou např. Rakousko nebo Spolková republika Německo.

Policii tudíž zůstala pouze možnost využít ustanovení § 66a §68 zákona č. 273/2008 Sb.
jedná se o následující znění:

§ 66
Získávání informací z evidencí

(1) Policie může v rozsahu potřebném pro plnění konkrétního úkolu žádat od správce evidence nebo zpracovatele poskytnutí informací z evidence provozované na základě jiného právního předpisu. Správce evidence nebo zpracovatel poskytne informace bezplatně, nestanoví-li jiný právní předpis jinak. Správce evidence nebo zpracovatel jsou povinni žádosti bez zbytečného odkladu vyhovět, nestanoví-li jiný právní předpis pro poskytnutí informací policii jiný režim19).

(2) Policie může v rozsahu potřebném pro plnění konkrétního úkolu žádat od správce evidence nebo zpracovatele poskytnutí informací z databáze účastníků veřejně dostupné telefonní služby, agendového informačního systému evidence občanských průkazů, agendového informačního systému evidence cestovních dokladů, agendového informačního systému evidence diplomatických a služebních pasů, agendového

informačního systému evidence obyvatel, evidence údajů o mýtném, katastru nemovitostí, základního registru obyvatel, základního registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci, základního registru územní identifikace, adres a nemovitostí, základního registru agend orgánů veřejné moci a některých práv a povinností, informačního systému územní identifikace, registru silničních vozidel, centrálního registru silničních vozidel, registru historických a sportovních vozidel, registru řidičů a centrálního registru řidičů způsobem umožňujícím dálkový a nepřetržitý přístup; v případě agendového informačního systému evidence občanských průkazů a agendového informačního systému evidence cestovních dokladů lze informace poskytnout pouze způsobem umožňujícím nepřetržitý přístup; v případě databáze účastníků veřejně dostupné telefonní služby se informace poskytne ve formě a v rozsahu stanoveném jiným právním předpisem20).

(3) Policie může v případech stanovených zákonem a v rozsahu potřebném pro plnění konkrétního úkolu žádat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis[21] jinak. Tyto osoby jsou povinny žádosti vyhovět bez zbytečného odkladu, ve formě a v rozsahu stanoveném jiným právním předpisem.

(4) Policie žádá o poskytnutí informací podle odstavců 1 až 3 pouze způsobem, který umožní policii uchovávat identifikační údaje o útvaru policie nebo o policistovi, který o poskytnutí informací žádal, a o účelu, k němuž bylo o poskytnutí informací žádáno, nejméně po dobu 5 let. O skutečnostech podle věty první jsou správce evidence nebo zpracovatel povinni zachovávat mlčenlivost.

(5) Za účelem zajištění ochrany osoby, o níž lze důvodně předpokládat, že by mohl být ohrožen její život nebo zdraví, za účelem pátrání po hledané anebo pohřešované osobě nebo za účelem zabránění vyzrazení činnosti policie mohou policie nebo ministerstvo požadovat od zpracovatele nebo správce evidence vedené na základě jiných právních předpisů, aby policii oznamovali každý výdej osobních údajů.

Ustanovení výše uvedeného paragrafu je využíváno k získání informací, které se týkají konkrétního účastnického čísla. Jedná se tedy o informace, které jsou doplňující a napomáhají dotvořit celkový obraz o místě trestného činu nebo podezřelém. Dotazem u specializovaného útvaru PČR – ÚZČ, který žádost policejního orgánu zpracuje a postoupí příslušným operátorům telekomunikačních služeb.
Různou kombinací dotazů je možné od operátorů získat informace ke konkrétnímu telefonnímu číslu.

[21] *Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů*

a) zjištění operátora
b) zjištění majitele telefonního čísla
c) zjištění IMEI mob. telefonu, IMSI telefonního čísla
d) zjištění data a místa zakoupení SIM karty
e) zda nebyla SIM karta zakoupena ve spojitosti s jiným účastnickým číslem, uživatelem např. za bonusové body, komplexní balíček atd.
f) dle zjištěného IMEI telefonního přístroje je možné následně zjistit další možné SIM karty, které byly do telefonního přístroje vloženy a naopak

§ 68
Pátrání po osobách a věcech

(1) Policie provádí jako součást plnění svých úkolů pátrání po osobách a věcech s cílem zjistit, kde se tyto osoby nebo věci nacházejí, nebo identifikovat osoby, mrtvoly, části lidského těla anebo kosterního nálezu neznámé totožnosti.

(2) Policie může žádat pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly poskytnutí provozních a lokalizačních údajů od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis20) jinak. Informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem20).

(3) Policie může pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě žádat od

a) banky předávání dat o době a místě použití elektronického platebního prostředku hledané nebo pohřešované osoby,

b) zdravotní pojišťovny nebo poskytovatele zdravotních služeb poskytnutí informací o době a místě poskytnutí zdravotních služeb této osobě.

(4) Informace získané podle odstavců 2 a 3 lze použít pouze pro účely zjištění doby a místa pobytu osoby.

(5) Policie může za účelem zjištění totožnosti neznámé mrtvoly žádat poskytnutí údajů ze zdravotnické dokumentace.

Tento paragraf je využíván v případech, kdy věc nesnese odkladu, z čehož je patrné, že toto ustanovení se týká zejména, jestliže je ohrožen život nebo zdraví osob, zejména pak osob v pátrání nebo u pohřešovaných osob. Policejní orgán může zjistit informace k telefonnímu číslu, o které je možno požádat pouze na základě dle §88a tr. řádu. Informace nejsou totožné (s § 88a Tr.ř.), ale jsou do určité míry omezeny a uzpůsobeny k co nejrychlejšímu nalezení osoby v pátrání.

Obsah informací, které jsou poskytovány policejnímu orgánu:

a) informace o příchozích a odchozích hovorech sledovaného čísla
b) ustanovení buňky mobilního operátora a azimuty signálu

Informace o provozu a lokalizaci telefonního čísla jsou poskytovány bez obsahů hovorů či obsahu SMS zpráv.

V minulých letech (2011-2012) bylo využití těchto ustanovení značně omezeno nálezem Ústavního soudu Pl 24/2010 ze dne 22. 3. 2011. Proto byli mobilní operátoři nuceni omezit rozsah poskytovaných služeb. Dnem 1. října 2012 je znovu možnost vyžadovat tyto informace, a to na základě novelizace zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů.

5. Rozbor nálezu Ústavního soudu ve věci §88 a §88a Trestního řádu

Dne 26. 3. 2010 se skupina 51 poslanců Poslanecké sněmovny Parlamentu České republiky domáhala zrušení ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a změny některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále též jen „napadená ustanovení“), a vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání (dále též jen „napadená vyhláška“ či souhrnně též jen „napadená právní úprava“). Podstatu námitek navrhovatelé sami shrnuli tak, že shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu v takovém rozsahu, v jakém jej vymezují napadená ustanovení a napadená vyhláška, představují neproporcionální zásah do základních práv uvedených v Listině základních práv a svobod (dále jen „Listina“) a v Úmluvě o ochraně lidských práv a základních svobod (dále jen „Úmluva“), konkrétně základních práv garantovaných čl. 7 odst. 1, čl. 10 odst. 2 a 3 a čl. 13 Listiny a čl. 8 Úmluvy. Dle navrhovatelů lze tento zásah navíc považovat za porušující podstatné náležitosti demokratického právního státu, k nimž lze přiřadit i zásadu proporcionality ve smyslu čl. 4 odst. 4 Listiny. Svá tvrzení navrhovatelé podepřeli následujícími argumenty:

I. A) Shromažďování údajů o komunikaci jako zásah do soukromého života

Obsahem napadaných ustanovení je uložení povinnosti fyzickým a právnickým osobám, které zajišťují veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací (tedy především telefonních operátorů a poskytovatelů internetového připojení), po dobu 6 až 12 měsíců uchovávat provozní a lokalizační údaje (desítky údajů) o veškeré telefonní a faxové komunikaci, e-mailové a SMS komunikaci, návštěvách webových stránek a využívání některých internetových služeb, specifikované v napadené vyhlášce a na žádost jsou povinny je poskytovat oprávněným orgánům. Dle navrhovatelů výše uvedené údaje, jejich shromažďování, uchovávání a předávání státním orgánům nepochybně spadají pod ochranu čl. 8 Úmluvy. V této souvislosti odkázali na celou
řadu rozhodnutí Evropského soudu pro lidská práva (dále jen „ESLP“) i Ústavního soudu.

tudíž:

Uchovávání provozních a lokalizačních údajů nelze považovat za takový zásah, neboť tyto údaje jsou nepřetržitě uchovávány a státním orgánům jsou k dispozici a mohou si je v budoucnu dle příslušných předpisů vyžádat a využívat. Uchovávání shora uvedené sady údajů tak s sebou nese latentní nebezpečí dalších bezprostředních zásahů státních orgánů. Navíc nelze přehlédnout, že stát neuchovává provozní a lokalizační údaje sám, ale využívá k tomu soukromých osob poskytujících telekomunikační služby, přičemž riziko z možného zneužití uchovávaných údajů velkým počtem soukromých osob pohybujících se v oblasti telekomunikačních služeb je vyšší než při jejich uchovávání státem.

Jedním ze základních požadavků ESLP, vyvinutých výkladem podmínky zákonného podkladu státních zásahů do soukromého života, je předvídatelnost a dostupnost tohoto zákonného podkladu. Důvodem je legitimní a logický požadavek, aby jednotlivci byli předem seznámeni s okolnostmi, kdy stát může výjimečně do jejich soukromého života zasáhnout, a mohli přizpůsobit své jednání tak, aby se tomuto zásahu bylo možné vyhnout. Plošný charakter uchovávání provozních a lokalizačních údajů však takovou možnost omezuje, až vylučuje.

Proto v souladu s čl. 8 odst. 2 Úmluvy přistoupili k posouzení přiměřenosti daného opatření, které hodnotili jednak z hlediska závažnosti a rozsahu zásahu do

základních práv jednotlivců, v daném případě do práva na soukromí, dále z hlediska legitimity cíle, k jehož dosažení má omezení základních práv sloužit, a z hlediska přínosu těchto zásahů. V neposlední řadě jeho užití konfrontovali s nebezpečnými aspekty, které jsou s tím spojeny, zejména pak nebezpečí zneužití uchovávaných údajů.

I. B) Závažnost a rozsah zásahu do práva na soukromí

Předně navrhovatelé konstatovali, že zavedení povinnosti uchovávat provozní a lokalizační údaje představuje závažný zásah do soukromí, poněvadž tyto údaje otevírají široké možnosti jejich použití a jejich zkombinování s dalšími údaji může způsobit velmi citelné důsledky pro soukromý život dotčených osob. Povinnost uchovávat provozní a lokalizační údaje v takovém rozsahu má prakticky za následek vyloučení existence nekontrolované a nemonitorované telekomunikace, což je nutno považovat za obzvlášť intenzivní zásah do soukromí všech osob užívajících telekomunikační prostředky (telefonie, užívání služeb internetu), které se v současnosti již nevyužívají pouze ke komunikaci mezi lidmi, ale zasahují široké spektrum každodenních činností (nakupování, bankovní operace, aj.). Z uchovávaných údajů tak lze dovodit celou řadu dalších (v řadě případů velmi citlivých) údajů a informací o dané osobě a jejím soukromí. V řadě případů lze z identity adresáta telefonátu nebo e-mailu odhalit citlivý údaj o odesílateli (např. pokud je adresátem lékař-specialista), podobně lze z navštívených internetových stránek zjišťovat informace o názorovém smýšlení, zdravotním stavu nebo sexuální orientaci dané osoby. Velké množství informací lze získat rovněž z lokalizačních údajů o pohybu mobilního telefonu (respektive jeho držitele), zvláště v kombinaci s lokalizačními údaji o pohybu dalších mobilních telefonů (údaj o tom, kdo se kde a kdy s kým setkal apod.). Na základě uchovávaných údajů tak lze sestavit komunikační a pohybový profil jednotlivce, z kterého lze získat nejen údaje o jeho minulých aktivitách, ale s vysokou mírou pravděpodobnosti i správně předvídat jeho aktivity v budoucnosti, což rovněž představuje významný zásah do práva na ochranu soukromí a korespondence jednotlivců. Pl. ÚS 24/10.

I. C) Legitimita cíle a přínos zásahu do základních práv

Navrhovatelé dále ve svém návrhu polemizovali s legitimitou cíle přijetí napadené úpravy. Z důvodové zprávy vlády k ustanovení § 97 zákona o elektronických komunikacích vyplývá, že účelem ust. § 97 je čelit zvyšujícím se bezpečnostním

rizikům a zajištění bezpečnosti a obrany České republiky, přičemž bližší odůvodnění chybí. Navrhovatelé jsou toho názoru, že podle čl. 8 odst. 2 Úmluvy je zásah do soukromí přípustný ve vztahu k boji s kriminalitou pouze tehdy, pokud slouží k předcházení zločinnosti. „Preventivní, všeobecné uchovávání telekomunikačních údajů bez existence konkrétního důvodu míří zejména do minulosti a může tak sloužit hlavně k objasňování již spáchaných trestných činů“. Zásah do soukromí za účelem objasnění již spáchaného trestného činu je tak dle navrhovatelů v rozporu s čl. 8 Úmluvy. Navíc údaje jsou uchovávány bez existence konkrétního podezření. Optikou napadených ustanovení je tak každá osoba považována za podezřelou bez existence konkrétních okolností, které by k tomuto podezření opravňovaly, což je v právním státě nepřípustné. Navrhovatelé rovněž upozornili (s odkazem na konkrétní případy ze zahraničí) na skutečnost, že vyhodnocování údajů o telekomunikačním provozu s sebou přináší rovněž nebezpečí jejich chybné interpretace a podezřívání či obvinění nevinného člověka. Může totiž dojít k záměně osoby, která komunikaci skutečně prováděla s osobou, která např. uzavřela smlouvu s telefonním operátorem nebo s poskytovatelem internetu.

Všechny námitky, které skupina poslanců předala Ústavnímu soudu, byly vzaty na vědomí a orgány státní správy provedly vyhodnocení, na základě kterých byly napadené zákony či paragrafy upraveny v souladu s nálezem Ústavního soudu Pl 24/2010 ze dne 22. 3. 2011.

Zejména se to týkalo:

Zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a na zrušení vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

Během tohoto legislativního procesu došlo k velmi výraznému omezení využívání ustanovení trestního řádu § 88a a zákona o Policii č. 273/2008 Sb., kde se jednalo o § 66 a§ 68 a. Policie jako taková tímto rozhodnutím ztratila jeden z důležitých nástrojů v boji s trestnou činností. Stávalo se, že v mnoha případech před zavedením napadené právní úpravy, ztroskotávalo vyšetřování, odhalování a stíhání závažných

trestných činů na nemožnosti získat požadované údaje z důvodu, že již taková data nebyla k dispozici. Tento stav byl velmi závažný, přestože výrokem Ústavního soudu nebyla dotčena přímo činnost orgánů činných v trestním řízení, které postupují ve smyslu zákona 141/1961 Sb., o trestním řízení soudním. Stejně tak Policie ČR neztratila své oprávnění získávat informace formou dožádání ve smyslu ustanovení § 8 odst.) trestního řádu a stejně zůstalo v platnosti ustanovení § 66 osdt.3) zákona č.273/2008 Sb., o Policii ČR.

Z výše uvedeného tudíž vyplývá, že postup Služby kriminální policie a vyšetřování při vyžadování údajů o uskutečněném telekomunikačním provozu, který získává cestou Útvaru zvláštních činností SKPV byl v důsledku shora uvedeného nálezu beze změny, a to i po vyhlášení nálezu Ústavního soudu ve sbírce zákonů a nebyl tedy dotčen způsob ani forma vyžadování, tak jak interně stanovuje závazný pokyn policejního prezidenta č. 30 ze dne 21. dubna 2009, ve znění pozdějších předpisů o plnění úkolů v trestním řízení a závazný pokyn policejního prezidenta č. 225 ze dne 31. prosince 2008, ve znění pozdějších předpisů, kterým se upravuje postup při vyžadování odposlechu a záznamu telekomunikačního provozu a údajů o uskutečněném telekomunikačním provozu.

Dne 1. srpna byl prezidentem republiky podepsán zákon, kterým se mění zákon o elektronických komunikacích a některé další zákony (dále jen „novela“). Novela nabyla účinnosti dnem 1. října 2012 a nově upravuje poskytování provozních a lokalizačních údajů oprávněným subjektům, včetně nového znění § 88a trestního řádu (uveden níže). Tímto legislativním vývojem byla kontinuita předmětného oprávnění orgánů činných v trestním řízení zachována.

§ 88a

(1) Je-li třeba pro účely trestního řízení vedeného pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), pro trestný čin podvodu (§ 209 trestního zákoníku), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), pro trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), pro trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), pro trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), pro trestný

čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené, nařídí v řízení před soudem jejich vydání soudu předseda senátu a v přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn, včetně konkrétního odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje. Vztahuje-li se žádost ke konkrétnímu uživateli, musí být v příkazu uvedena jeho totožnost, je-li známa.

(2) Státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvního stupně po pravomocném skončení věci informuje o nařízeném zjišťování údajů o telekomunikačním provozu osobu uživatele uvedenou v odstavci 1, pokud je známa. Informace obsahuje označení soudu, který vydal příkaz k zjištění údajů o telekomunikačním provozu, a údaj o období, jehož se tento příkaz týkal. Součástí informace je poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k zjištění údajů o telekomunikačním provozu. Informaci podá předseda senátu soudu prvního stupně bezodkladně po pravomocném skončení věci, státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a a policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem podle § 174 odst. 2 písm. e).

(3) Informaci podle odstavce 2 předseda senátu, státní zástupce nebo policejní orgán nepodá v řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, spáchaném organizovanou skupinou, v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny, v řízení o trestném činu účasti na organizované zločinecké skupině (§ 361 trestního zákoníku), nebo pokud se na

spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno, nebo pokud je proti osobě, jíž má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel tohoto nebo jiného trestního řízení, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv nebo svobod osob.
(4) Příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat.".

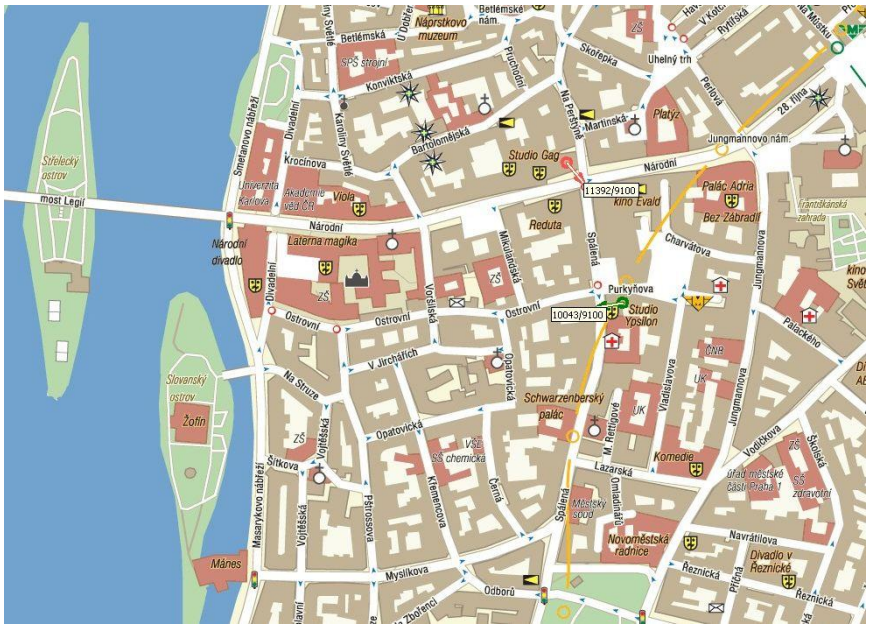
Jako možný příklad využití jednotlivých ustanovení § 88 a §88a zákona 141/1961 Sb., o trestním řízení soudním, dále pak ustanovení § 66 zákona č.273/2008 Sb., o Policii ČR uvádím případ, ve kterém by nebylo možné bez využití výše uvedených zákonných možností dojít k odhalení a předcházení trestné činnosti pachatelů a jejich následné zadržení.

Jednalo se o skupinu zahraničních pachatelů, kteří se dlouhodobě zdržovali na území ČR. Tito pachatelé využívali anonymity velkého města a tak bylo jejich odhalení poměrně složité. Analýzou trestné činnosti ze všech částí republiky došli policisté k přesvědčení, že se jedná o jednu skupinu osob. Tato fakta byla zjištěna právě na základě ustanovení § 88a tr. řádu a následně § 66 zákona o Policii ČR. Vyhodnocením těchto informací a následném nasazení odposlechu a záznamu telekomunikačního provozu dle § 88 tr. řádu, byli zjištěni a ustanoveni skuteční pachatelé, kteří prováděli zvlášť závažnou trestnou činnost.

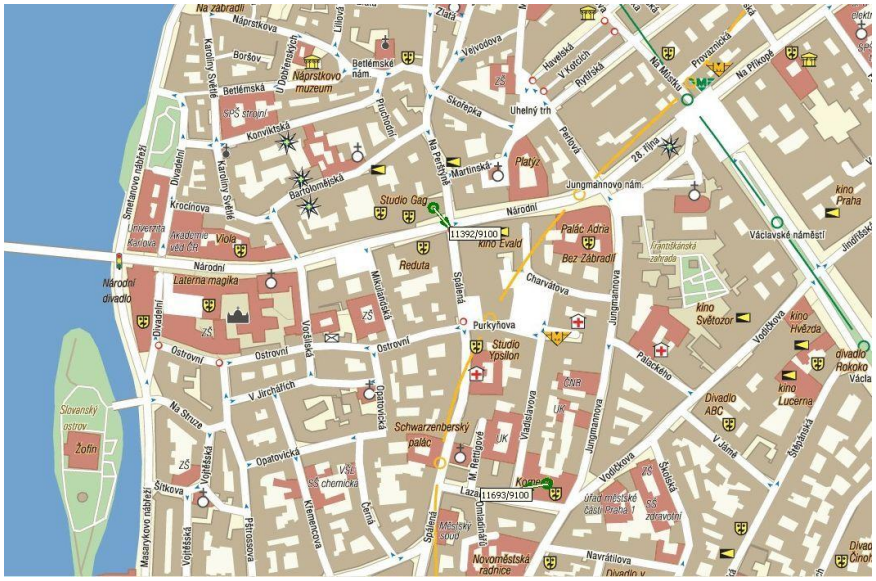
Pachatelé využívali k vzájemné komunikaci právě mobilní telefony, do kterých vkládali několik SIM karet, které využívali na různý typ páchání trestné činnosti. Tyto karty rozdělovali na běžnou komunikaci s rodinnými příslušníky, na tipování objektů, do kterých chtěli provést vloupání a na karty tzv. „čisté", které používali při vlastních vloupáních. Celkem tito pachatelé použili 40 SIM karet, které měnili dle potřeby.

Činnost, respektive výskyt pachatelů na místě trestné činnosti, kterou jinak popírali, je zobrazena na obrázcích č. 1a 2. Následné vyhodnocení situace bezprostředně po vloupání je vyobrazeno na obrázku č.3.

Nutno podotknout, že bez možnosti nasazení odposlechu a záznamu telekomunikačního provozu by nebylo možné odhalit tuto skupinu pachatelů nebo by se podařilo dokázat jen malý zlomek její trestné činnosti.



obr. č.1 - Na tomto obrázku je vidět pohyb pachatelů, kteří se chystají provést vloupání do směnárny. Jeden pachatel je zobrazen jako červený a druhý jako žlutý bod. Zobrazené šipky jsou de facto buňky jednotlivých operátorů, které zaznamenaly hovory pachatelů. (zdroj PP PČR)

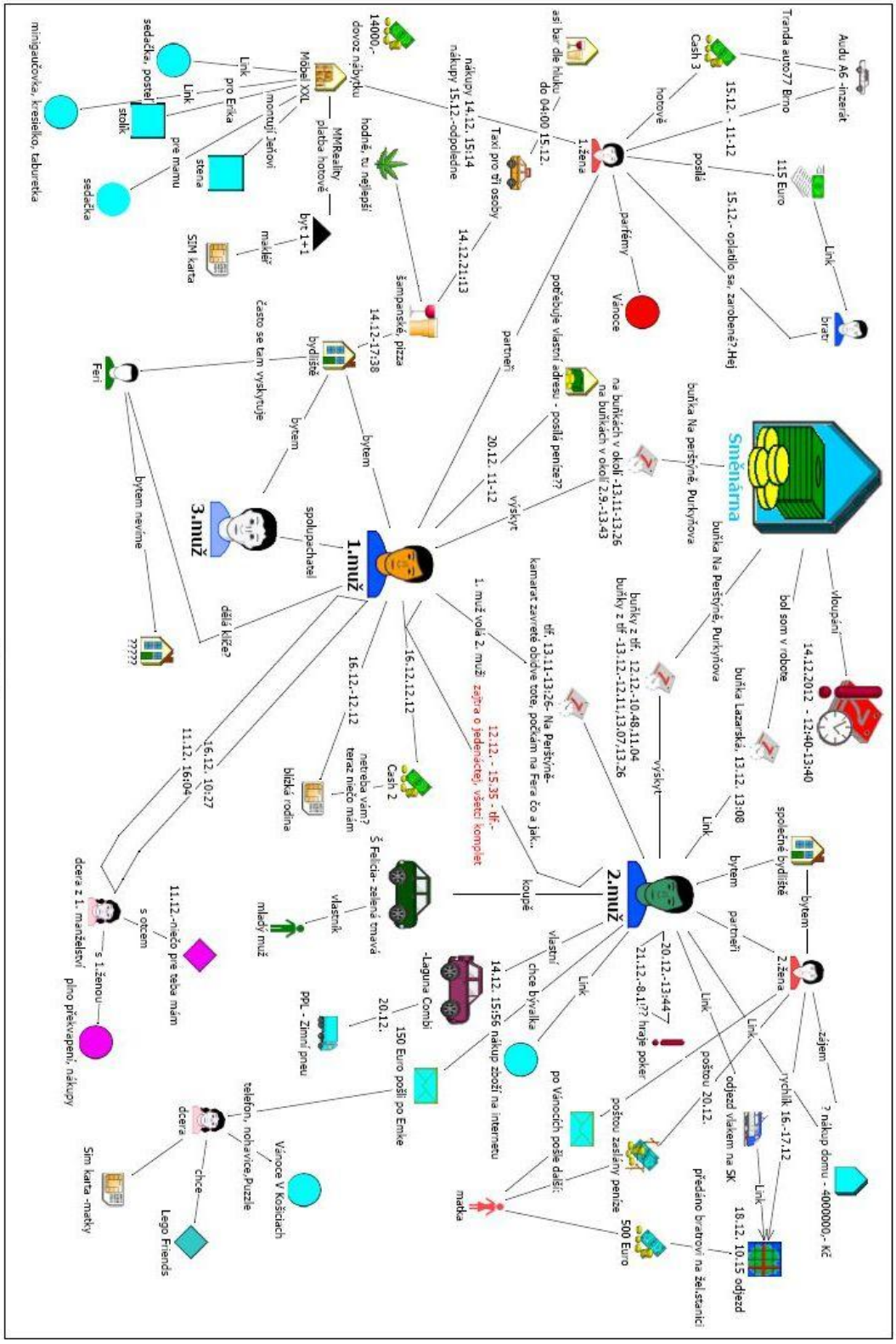


obr. č. 2

Obrázek č. 2 je podobný s obr. č. 1, ale hovory mezi pachateli zaznamenávají jiné buňky. Nutno podotknout, že pachatelé svůj výskyt na místě trestného činu jednoznačně popírali, ale při vlastní realizaci u nich byly zajištěny právě tyto mobilní telefony a to včetně SIM karet. (zdroj PP PČR)

Na dalším snímku (obr. č. 3) je vyobrazen telekomunikační provoz pachatelů a jejich rodinných příslušníků. V tomto případě bylo policii známo, že před provedeným vloupáním bylo na účtech pachatelů a jejich rodinných příslušníků pouze malé množství finančních prostředků a stav některých účtů těchto pachatelů vykazoval debetní stav. Po provedeném vloupání došlo k velkým nákupům, odesílání peněz do zahraničí rodinným příslušníkům, byli kontaktováni prodejci osobních automobilů a také jeden z pachatelů začal vyjednávat o koupi bytu do osobního vlastnictví. Na tomto analytickém grafu je také patrno, že rodinní příslušníci oznamují svým rodinám úspěch, plánují oslavu a nakupují drogy.

Legenda k obr. č. 3: muž 1 – 3 jednotliví pachatelé



obr. č. 3 (zdroj PP PČR)

Právě tyto nástroje, kterými disponuje Policie ČR, jsou jedny z nemnoha prostředků, kterými je možné pachatele usvědčit z páchání trestné činnosti, dokázat i na základě mnoha nepřímých důkazů, že trestný čin spáchal právě ten či onen konkrétní pachatel. Existují sice další možnosti jak usvědčit pachatele, ale nasazení odposlechu a záznam telekomunikačního provozu je jedním z hlavních a nejdůležitějších prostředků orgánů činných v trestním řízení. Bez tohoto prostředku by nebylo tedy ani možné předejít dalším trestným činům, které pachatelé plánují, tak jak tomu bylo i v tomto případě, kdy bylo prokazatelně zjištěno, že se pachatelé připravují na spáchání dalšího obdobného trestného činu.

V tomto konkrétním případě byli pachatelé po provedeném vloupání zadrženi, a tak se podařilo snížit výši možné škody, která by jinak byla značného rozsahu. Finanční hotovost byla zajištěna a následně vrácena majiteli.

6. Odposlechy v rámci mezinárodního práva

Tato kapitola se zaměřuje na uvedení konkrétních příkladů postupu a právní úpravy odposlechu a záznamu telekomunikačního provozu v zemích sousedících s Českou republikou. Sledovat postupy právě v těchto státech se jeví jako velmi vhodné vzhledem k faktu, že čeští pachatelé nebo pachatelé z okolních států páchají trestnou činnost nejen na územích svých států, ale jejich trestná činnost je mnohdy rozšířena i do sousedních zemí.

Spolková republika Německo

Ve Spolkové republice Německo je odposlech a záznam telekomunikačního provozu nařízen výhradně soudem na návrh státního zástupce. Pouze ve výjimečných případech (pokud hrozí nebezpečí prodlení) může odposlech či záznam

telekomunikačního provozu povolit státní zástupce. Pokud ale nařízení státního zástupce není potvrzeno soudem během tří pracovních dní, tak pozbývá platnosti.[22]

Odposlech a záznam telekomunikačního provozu lze provést, jestliže pachatel spáchal skutečnost, u které je podezření ze spáchání těžkého trestného činu nebo trestného činu, u kterého je pokus či příprava trestná, tak jak je zakotveno v § 100a/odst.2 německého trestního řádu. V paragrafu 100a/odst.2 německého trestního řádu je dále přesně specifikováno o jaké trestné činy se jedná (např. podplácení poslanců dle § 108e, živnostenského přechovávačství, praní špinavých peněz a zastírání neoprávněně získaných majetkových hodnot podle § 261/odst. 1,2 a 4, dále trestné činy proti hospodářské soutěži či trestný čin podplácení podle § 332 a 334).

Použití pořízených odposlechů v jiné trestní záležitosti je ve Spolkové republice Německo řešeno v rámci daleko obecnějšího institutu tzv. „náhodných nálezů“, které se ale nezaměřuje pouze na odposlechy, ale i na jiné instituty, protože poznatky získané odposlechem v původním trestním řízení souvisí i jinou trestní věcí.

V § 477/odst.2 StPO je zakotveno:

„Je-li opatření podle tohoto zákona přípustné jen při podezření z určitých trestných činů, pak mohou být poznatky získané takovým opatřením bez souhlasu dotčené osoby použity jako důkaz v jiné trestní věci pouze k odhalení takových trestných činů, k jejichž odhalení podle tohoto zákona by takové opatření smělo být nařízeno“

Samotné nařízení smí být vydáno pouze proti podezřelé osobě nebo proti osobám, o kterých je možno se domnívat, že přijímají nebo předávají sdělení určená pro podezřelého nebo pokud podezřelá osoba používala jejich mobilní telekomunikační zařízení. Tyto získané informace ze soukromého života nesmí být nijak použity. Záznam o odposlechu je nutné zničit bez odkladu a tuto skutečnost je třeba zaznamenat do spisu.

Nemožnost odposlechu komunikace obviněného s obhájcem je vyvozována z ustanovení §148/StPO a §148 odst. 1, který zní:

„Obviněnému je povolen, i když není na svobodě, písemný a ústní styk s obhájcem.“

[22] §100a odst. 1, německého trestní řádu,(Strafprozeβordung), dále jen StPO.

Příkaz je možné vydat nejdéle na dobu tří měsíců a tento úkon lze prodloužit vždy o další tři měsíce, pokud přetrvává předpoklad, že důvody k nařízení odposlechu trvají nadále. Nařízení musí být vydáno písemně. Nezbytnými náležitostmi ve výroku rozhodnutí je třeba uvést jméno a adresu dotčeného, proti komu opatření směřuje, dále telefonní číslo nebo jiné označení odposlouchaného spojení nebo konečného zařízení. Pominou-li však důvody vedoucí k vydání nařízení, je třeba ukončit opatření bez zbytečného odkladu. Ukončení opatření i s jeho výsledkem je třeba oznámit nařizujícímu soudu (100b/odst.4).

Účastníci, kterých se odposlech týká, musí být o opatření informováni. Ke sdělení takové informace nedojde v případě, že převažuje nutnost chránit oprávněné zájmy dotčené osoby. Informace je poskytnuta, jakmile to je možné bez ohrožení účelu vyšetřování, života, zdraví, osobní svobody osob nebo značných majetkových hodnot (§101/odst.5). Nedojde-li ke sdělení takové informace během dvanácti měsíců po skončení opatření, je pro další odklad třeba soudní souhlas. Soud může povolit upuštění od sdělení, pokud předpoklady sdělení s pravděpodobností hraničící s jistotou nenastanou, a to ani v budoucnosti.

Spolkový soudní dvůr v řadě rozhodnutí dovoluje sledovat „stopy“ z odposlechu k získání dalších důkazů, to znamená, že samotné odposlechy nemohou být použity přímo jako důkaz, ale na jejich základě je přípustné získávat důkazy další.

Rakouská republika

V Rakousku, stejně jako v ostatních státech s rozvinutou demokracií, je odposlech a záznam telekomunikačního provozu nařízen výhradně soudem po předchozím návrhu státního zástupce. Trestní řád jako takový je součástí Sbírky spolkových zákonů, které vydává Správní soudní dvůr.

Odposlech telekomunikačního provozu v Rakousku je legislativně upraven v trestním řádu, jedná se o novelizovaný § 135 tr. řádu BGBl č.631/1975 (novelizován BGBl I č.2011/33 s účinností od 01. dubna 2012) ve spojení s § 92 zákona o telekomunikacích a jeho přesné znění je Zabavení korespondence, poskytování

informací o údajích z přenosu zpráv, informace o údajích, které se uchovávají a odposlech zpráv.

zákonné znění

§ 135

Zabavení korespondence, poskytování informací o údajích z přenosu zpráv, informace o údajích, které se uchovávají a odposlech zpráv

(1)

Zabavení korespondence je přípustné, pokud je to nutné, k objasnění úmyslně spáchaného trestného činu, za který hrozí trest odnětí svobody na více než jeden rok, a pokud se obviněný z takového činu nachází ve vazbě, anebo pokud z tohoto důvodu bylo nařízeno jeho předvedení anebo zatčení.

(2)

Informace o údajích z telekomunikačního provozu je přípustné poskytnout,

1. *pokud a po dobu, dokud existuje důvodné podezření, že osoba, které se informace týká, by mohla jinou osobu unést nebo se jí zmocnit, a pokud se informace o údajích vztahuje na takovou zprávu, ze které lze usuzovat, že v době omezení svobody bude obviněným předána, přijata nebo odeslána,*
2. *pokud lze očekávat, že to přispěje k objasnění úmyslně spáchaného trestného činu, za který hrozí trest odnětí svobody na více než šest měsíců, a majitel technického zařízení, jehož určením nebo cílem byl nebo bude přenos zpráv, s poskytnutím údajů výslovně souhlasí, nebo*
3. *pokud lze očekávat, že to přispěje k objasnění úmyslně spáchaného trestného činu, za který hrozí trest odnětí svobody na více než jeden rok a kdy na základě určitých skutečností lze usuzovat, že takto mohou být zjištěny údaje vztahující se k obviněnému*
4. *pokud na základě určitých skutečností lze očekávat, že takto bude moci být zjištěn pobyt obviněného, který uprchl anebo který se zdržuje na neznámém místě, kdy tento obviněný je důvodně podezřelý z trestného jednání, za které hrozí trest odnětí svobody na více než jeden rok.*

(2a)

Informace o údajích, které se uchovávají (§§ 102a a 102b zákona o telekomunikacích) je přípustné poskytovat v případech, uvedených v odstavci 2 body 2 až 4.

(3)

Odposlech přenosu zpráv je přípustný,

1)v případech, uvedených v odstavci 2 bod 1,

2)v případech, uvedených v odstavci 2 bod 2, pokud majitel technického zařízení, jehož určením nebo cílem byl nebo bude přenos zpráv, s odposlechem souhlasí,

3)pokud je to nutné k objasnění úmyslně spáchaného trestného činu, za který hrozí trest odnětí svobody na více než jeden rok, anebo pokud by jinak bylo podstatně ztíženo objasnění nebo zabránění trestné činnosti, páchané nebo plánované v rámci zločinného nebo teroristického spolčení nebo kriminální organizace (§§ 278 až 278b tr. řádu) a

a)

majitel technického zařízení, jehož účelem nebo cílem byl nebo bude přenos zpráv, je důvodně podezřelý z úmyslně spáchaného trestného činu, za který hrozí trest odnětí svobody na více než jeden rok, anebo ze spáchání trestného činu dle §§ 278 až 278b tr. zákona, nebo

b)

na základě určitých skutečností lze usuzovat, že osoba, která je důvodně podezřelá z činu uvedeného pod písm. a) bude technické zařízení používat anebo s ním bude navázáno spojení;

4) v případech, uvedených v odstavci 2 bod 4.

Instituty jako například nemožnost odposlechu mezi obhájcem a obviněným jsou stejné jako v okolních státech nebo v České republice. Obdobná je i lhůta, která se zpravidla stanovuje na dobu 3 měsíců a na základě přínosu z doposud nařízených odposlechů je prodlužována.

Zákon o telekomunikacích, sbírka spolkových zákonů I č. 70/2003 ve znění pozdějších předpisů

(1)

Ustanovení tohoto paragrafu platí pro zpracování a přenos osobních údajů ve spojení s poskytováním veřejných komunikačních služeb ve veřejných komunikačních sítích, včetně veřejných komunikačních sítí, které podporují přístroje pro shromažďování dat a identifikaci těchto přístrojů. Pokud tento spolkový zákon neurčuje jinak, použijí se na skutkové podstaty upravené tímto spolkovým zákonem ustanovení zákona o ochraně dat 2000, sbírka zákonů I č.. 165/1999.

Ustanoveními tohoto oddílu zůstávají nedotčena ustanovení trestního řádu.

Dále jsou v tomto paragrafovém ustanovení vyloženy některé pojmy, které se týkají zpracování a přenosu osobních údajů ve spojení s poskytováním veřejných komunikačních služeb ve veřejných komunikačních sítích.

Jsou to například:

a. "provozní údaje" údaje, které jsou zpracovávány za účelem přenosu zprávy na komunikační síť nebo za účelem fakturace tohoto procesu;
b. "přístupové údaje" taková údaje, které při vstupu účastníka na veřejnou komunikační síť vznikají u provozovatele a jsou potřebné k jejich zařazení v určitém časovém okamžiku pro komunikaci směrem k účastníkovi prostřednictvím použité adresy na síti;
c. "obsahová údaje" obsah přenášených zpráv
d. “údaje o poloze” údaje, které jsou zpracovávány komunikační sítí nebo komunikační službou, a která udávají geografickou polohu telekomunikačního zařízení uživatele veřejné komunikační služby, v případě pevného komunikačního zařízení se údaji o poloze rozumí adresa zařízení;
e. „identifikace polohy“ identifikace buňky, prostřednictvím které je uskutečňováno mobilní telefonní spojení (Cell-ID);
f. "zpráva" každá informace, která je vyměněna nebo předána mezi konečným počtem účastníků prostřednictvím komunikační služby. To nezahrnuje informace, které jsou prostřednictvím komunikační sítě předávány veřejnosti

jako součást rozhlasové služby, pokud tyto informace nelze spojit s identifikovatelným účastníkem nebo uživatelem.;

g. „neúspěšný pokus o hovor“ telefonát, při kterém bylo úspěšně navázáno spojení, na který však nebylo odpovězeno nebo při kterém zasáhl management sítě;
h. "služba s dodatečným užitkem " každá služba, kdy zpracování provozních údajů nebo jiných údajů o poloze jako provozních údajů je v určitém rozsahu vyžadováno, aby na základě přenosu zprávy nebo na základě fakturace tohoto procesu nebyla překročena určitá míra přiměřenosti;
i. "elektronická pošta" každá textová, hlasová, zvuková nebo obrazová zpráva, kterou lze uložit v síti nebo v koncovém přístroji uživatele do doby, než si ji uživatel vyvolá;
j. „elektronická poštovní schránka“ elektronický úložný systém, který je uživateli přidělen službou E-mail;
k. „E-Mail“ elektronická pošta, která je prostřednictvím internetu zasílána na základě „Simple Mail Transfer Protocol“ (SMTP);
l. „internetová-telefonická služba“ veřejná telefonická služba ve smyslu § 3 bod 16, spočívající na přenosu zpráv prostřednictvím internetového protokolu formou ucelených souborů;
m. „internetová přístupová služba“ komunikační služba ve smyslu § 3 bod 9, která spočívá v připravenosti zařízení nebo služeb k zajištění přístupu k internetu;
n. „služba E-mail“ komunikační služba ve smyslu § 3 bod 9, která zahrnuje odesílání a přijímání E-mailů na základě „Simple Mail Transfer Protocol“ (SMTP);
o. „veřejná IP-adresa“ jediná numerická adresa z adresního bloku, která byla přidělena prostřednictvím Internet Assigned Numbers Authority (IANA) anebo prostřednictvím regionálního zadávacího místa (Regional Internet Registries) poskytovateli přístupu k internetu, aby ji poskytovatel mohl přidělovat svým zákazníkům, na základě které je počítač připojený k internetu jednoznačně identifikovatelný a může být v internetu lze určit jeho polohu. Veřejné IP-adresy jsou přístupovými daty ve smyslu § 92 odst. 3 bod 4a. Je-li účastníku přidělena konkrétní veřejná IP-adresa k tomu, aby ji tento účastník

používal výlučně po dobu trvání smlouvy, jedná se současně o kmenový údaj ve smyslu § 92 odst. 3 bod 3;

p. "porušení ochrany osobních údajů" každé porušení bezpečnosti, které vede ke ztrátě, ke změně nebo neoprávněnému předání resp. k neoprávněnému přístupu k osobním údajům ať již omylem nebo protiprávně, kdy tato data jsou přenášena, ukládána do paměti nebo jiným způsobem zpracovávána v souvislosti s funkcí veřejných komunikačních služeb ve společnosti;

Slovenská republika

Ve Slovenské republice je pohled na institut odposlechu a záznamu telekomunikačního provozu i právní úprava velmi podobná jako v České republice. Příkaz k nařízení odposlechu vydává ve Slovenské republice předseda senátu před zahájením trestního stíhání nebo v přípravném řízení[23] na návrh prokurátora. Pokud však jde o záležitosti, které nesnesou odkladu, a příkaz soudce pro přípravné řízení není možné získat předem, může příkaz o nařízení odposlechu vydat prokurátor, pokud však odposlech a záznam telekomunikačního provozu není spojen se vstupem do obydlí, ten však musí nejpozději do 24 hodin od jeho vydání potvrdit soudce pro přípravné řízení, jinak ztrácí platnost a informace získané tímto způsobem nelze použít pro účely trestního řízení a z tohoto důvodu se musí předepsaným způsobem zničit.[24] Stejně tak jak je ustanoveno v našem trestním řádu, upravuje slovenský trestný poriadok odposlech mezi advokátem a obviněným. Pokud se při odposlechu či záznamu telekomunikačního provozu zjistí, že obviněný komunikuje se svým obhájcem, nemohou být informace, které jsou tímto institutem zjištěny, použity pro účely trestního řízení a musí se předepsaným způsobem zničit.

Příkaz k odposlechu a záznamu telekomunikačního provozu musí být dán písemnou formou, je nutné odůvodnit skutkové okolnosti, a to na každou účastnickou stanici nebo zařízení. Příkaz musí obsahovat určení účastnické stanice nebo zařízení,

[23] Dle použité terminologie by se mohlo zdát, že se jedná o druh zvláštního soudce, jedná se však o srovnatelný institut jako v České republice plní v přípravném řízení dosahový soudce(§26 tr.ř.) – srovnání s § 10 odst. 3 slovenského Trestného poriadku – soudce pro přípravné řízení je soudce soudu 1. stupně, který je soudem pověřený rozhodovat zejména o zásazích do lidských práv a svobod, a to jak před zahájením trestního řízení tak i v řízení přípravném, dále také o stížnostech proti rozhodnutí prokurátora a o případech, o kterých to stanoví tento zákon(př. §348/odst.1;§204/odst.1 Tr. por.)

[24] Zákon č. 301/2005 Z.z., trestný poriadok

dále údaje o osobě, které se odposlech a záznam telekomunikačního provozu týká (pokud je známa) a dále čas, po který bude odposlech a záznam telekomunikačního provozu prováděn. Doba odposlechu a záznamu telekomunikačního provozu je stanovena nejdéle na 6 měsíců. Tato doba se dá, a to i opakovaně, prodloužit vždy o 2 měsíce, tuto dobu může v přípravném řízení na návrh prokurátora prodloužit soudce. Odposlech a záznam telekomunikačního provozu provádí příslušný útvar Policejního sboru (§115/odst.3). Policista nebo příslušný útvar Policejního sboru je povinný soustavně zkoumat trvání důvodů, které vedly k vydání příkazu k odposlechu a záznamu telekomunikačního provozu. Pokud důvody pominuly, odposlech a záznam telekomunikačního provozu se musí ukončit, a to i před uplynutím lhůty. O této skutečnosti je nutné bezodkladně písemně obeznámit toho, kdo příkaz vydal a pokud se jedná o přípravné řízení, je třeba s touto skutečností seznámit i prokurátora.

Polsko

V polském trestním řádu je v §237/odst.1 zakotvena kontrola a záznam telefonických hovorů s cílem nalézt a získat nové důkazy už u probíhajícího trestního řízení nebo jako prevence k novým trestným činům. Po zahájení trestního řízení tuto činnost nařizuje soud a v případech, které nesnesou odkladu, může tento úkon nařídit prokurátor, který má povinnost se nejdéle do tří dnů obrátit se žádostí na soud, který mu musí příkaz potvrdit. Soud má lhůtu pěti dnů. V § 237/odst.3 polský trestní řád obsahuje výčet několika trestných činů, u kterých lze odposlech nařídit. Jsou jimi například: vražda, obecné ohrožení, obchod s lidmi, státní převrat, únos letadla nebo lodi či jiného dopravního prostředku, shromažďování výbušnin, zbraní a radioaktivních látek a dále také například trestná činnost spojená s padělaním peněz a platebních prostředků a jiných listin, výroba, držení, a obchod s drogami nebo také korupce, kuplířství a trestné činy obsažené v čl. 5- 8 Římského statutu. § 237/odst.4. Zabývá se dále otázkou, koho je možno odposlouchávat. Z dikce zákona vyplývá, že je možno odposlouchávat podezřelého, poškozeného nebo osoby, se kterými může obviněný navázat kontakt nebo ty osoby, které mohou mít s pachatelem nebo s hrozícím trestným činem nějaký užší vztah.

Polský trestní řád stejně tak jako trestní řád České republiky nebo trestný poriadok Slovenské republiky také omezuje dobu po kterou lze odposlech provádět. V § 238/odst.1 se omezuje doba na provedení odposlechu na 3 měsíce s možností prodloužení na 3 další měsíce. Pokud se zaměříme na odst. 2 totožného paragrafu, zde zákon přikazuje okamžité ukončení odposlechu, pokud však pominuly důvody, které k nařízení odposlechu vedly.[25]

6.1. Mezinárodně právní pomoc

Jednou z dalších možností, kdy může policejní orgán dle trestního řádu využít odposlechu, je tzv. **příhraniční odposlech**. Tento institut upravuje trestní řád v §437a:

(1) Umožňuje-li vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, aby byl z cizího státu prováděn odposlech telekomunikačního provozu na území České republiky bez její technické pomoci, je k rozhodování o udělení souhlasu s provedením odposlechu nebo s jeho pokračováním a k souvisejícím úkonům příslušný krajský soud v Praze; je-li v cizím státě provádějícím odposlech trestní řízení ve stadiu před podáním obžaloby, rozhodne na návrh státního zástupce krajského státního zastupitelství v Praze. Souhlas s provedením odposlechu nebo s jeho pokračováním lze udělit pouze při splnění podmínek uvedených v §88.

(2) Umožňuje-li vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, aby byl z České republiky prováděn odposlech telekomunikačního provozu na území cizího státu bez jeho technické pomoci, státní zástupce a po podání obžaloby soud informuje cizí stát o předpokládaném nebo prováděném odposlechu.[26]

Mezinárodní smlouvou, která toto umožňuje, je například 55/2006 Sb.m.s. Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie.

Toto ustanovení má široké pole působnosti právě v elektronických komunikacích po internetové síti, kdy jsou servery rozmístěny po celém světě a uživatelé těchto serverů mohou být rozmístěni v mnoha státech. Zde pak záleží pouze na

[25] Dragoun,R.:Zákonná úprava možnosti odposlechu a záznamu telekomunikačního provozu při postihu korupce-srovnání české úpravy s úpravou zahraniční. Státní zastupitelství,2011,č.10
[26] Zákon č. 141/1961Sb., trestní řád, ve znění pozdějších předpisů

technologické úrovni každého státu, zdali umí tyto komunikace zachytit a následně vyhodnotit.

6.2. Společný vyšetřovací tým

Právní úprava a její změny

Zakládání společných vyšetřovacích týmů vychází z legislativního základu *Amsterodamské smlouv*y. Tato smlouva objasňuje zakládání společných vyšetřovacích týmů v čl. 30 odst. 2, a to v souvislosti s rozšířením funkcí *EUROPOLU* na úseku vyšetřování a podpůrných operativních akcí.

Postup při zřizování společných vyšetřovacích týmů pro účely trestního vyšetřování spolu se základními funkčními aspekty jsou obsaženy v čl. 13 *Úmluvy o vzájemné pomoci ve věcech trestních mezi členskými státy EU* z 29. května 2000 (dále jen Úmluva o vzájemné pomoci), která dosud nevstoupila v platnost. Z důvodu celkového zpoždění procesu ratifikace této úmluvy a s přihlédnutím k potřebě urychlit zavádění společných vyšetřovacích týmů do praxe přijala Rada Evropy 13. června 2002 rámcové rozhodnutí o společných vyšetřovacích týmech, které recipuje (přebírá) čl. 13 Úmluvy o vzájemné pomoci. Současně bylo požadováno, aby členské státy přijaly opatření nezbytná pro dosažení souladu s tímto rámcovým rozhodnutím do 1. ledna 2003. Jednalo se o předběžný právně-legislativní krok s cílem zavést účinné formy přeshraničního vyšetřování případů terorismu, obchodu s drogami a s lidmi.

Podle čl. 13 Úmluvy o vzájemné pomoci mohou příslušné orgány dvou nebo více členských států Unie na základě vzájemné dohody zřídit společný vyšetřovací tým pro určitý účel a na určitou dobu s cílem vést trestní vyšetřování v jednom nebo více členských státech, které tým zřídily. Složení týmu se stanoví dohodou.

Společný vyšetřovací tým (SVT) se zřizuje zejména v případech, kdy

- „policejní“ SVT – sdílení operativních informací, koordinace postupu
- „justiční“ SVT – společné provádění dokazování v konkrétním trestním řízení - § 442 a 443 TŘ – možné pouze na základě MS (např. čl. 13 Úmluvy 2000, č. 55/2006 Sb.m.s.)

„Justiční“ SVT

- Skupina složená z OČTŘ dvou či více států zřízená
- z podnětu žádosti SZ o právní pomoc
- na základě dohody zúčastněných států
- na určitou dobu a pro určitý účel
- Koordinace vyšetřování v jednom či více státech
- Sdílení informací a důkazů bez nutnosti žádat v jednotlivých případech o právní pomoc

Účastníci SVT

- pouze orgány oprávněné provádět dokazování v trestním řízení
- OLAF, Europol – postavení konzultantů podle § 157/3 TŘ
- Eurojust – možnost financování SVT

Žádost o zřízení společného vyšetřovacího týmu může předložit kterýkoliv členský stát EU a podává ji dozorový státní zástupce prostřednictvím NSZ. Tým se zřizuje v tom státě, ve kterém má vyšetřování probíhat. Žádost musí obsahovat:

- označení trestní věci – popis skutku + právní kvalifikace,
- cíl SVT – které úkony bude třeba provést,
- se kterými státy by měla být uzavřena dohoda o SVT
- odůvodnění proč je SVT potřebný
- doba, na kterou má být SVT ustanoven
- které policejní orgány se za ČR budou SVT účastnit
- navrhovaný pracovní jazyk SVT
- navrhovaný způsob velení, komunikace a ochrany osobních dat

Dohoda o SVT uzavřená NSZ

nahrazuje:

- žádosti o právní pomoc mezi státy zúčastněnými na SVT v dané trestní věci
- Rozhodnutí o povolení účasti orgánu dožadujícího státu na úkonu dokazovaní v dožádaném státě

Společný vyšetřovací tým působí na území toho členského státu, který jej zřídil, za těchto obecných podmínek:

- vedoucím týmu je zástupce příslušného orgánu účastnícího se trestního vyšetřování z toho členského státu, ve kterém tým působí,
- tým postupuje v souladu s právem členského státu, ve kterém působí,
- členský stát, na jehož území tým působí, vytvoří pro jeho činnost příslušné organizační podmínky

Pravomoci vyslaných členů

Pod velením osoby služebně činné v policejním orgánu ČR se mohou účastnit (§ 443 TŘ):

a) výslechů osob, včetně konfrontace, rekognice – doplňující otázku mohou klást pouze se souhlasem orgánu ČR činným v trestním řízení, který provádí výslech
b) vydání a odnětí věci
c) domovní prohlídky a prohlídky jiných prostor a pozemků,
d) ohledání,
e) vyšetřovacího pokusu,
f) rekonstrukce,
g) prověrky na místě

Vyslaní členové společného vyšetřovacího týmu mají právo účastnit se vyšetřovacích úkonů v členském státě, ve kterém se vyšetřování provádí. Za určitých podmínek mohou být pověřeni vedoucím týmu k provedení určitých vyšetřovacích úkonů na území státu, kde tým působí.

<u>Informace získané zákonným způsobem mohou být využity:</u>

a) pro účely, pro které byl vyšetřovací tým zřízen,
b) pro odhalení, vyšetřování a stíhání jiných trestných činů na základě předchozího souhlasu členského státu, ve kterém byla informace k dispozici,
c) pro předcházení bezprostředního a závažného ohrožení veřejné bezpečnosti a následuje-li zahájení trestního vyšetřování

d) pro jiné účely, jejichž rozsah je dohodnut mezi členskými státy, které zřídily vyšetřovací tým.

e) Důkazy provedené kterýmkoli členem SVT jsou v ČR v trestním řízení přípustné (§ 442/5 TŘ), pokud byly provedeny:

- v jednom ze států zúčastněných na SVT
- v souladu s právním řádem států zúčastněných na SVT

Je-li třeba provést důkaz ve státě, který není na SVT zúčastněn, je třeba o něj požádat dožádáním (§ 442/6 TŘ).

Je možné dohodnout účast jiných osob než zástupců příslušných orgánů členských států zřizujících společný vyšetřovací tým na činnostech týmu. Společné vyšetřovací týmy mají jedinečný význam v rámci soudní spolupráce v trestních věcech hlavně v tomto smyslu, že dodatečná pomoc a expertízy mohou být zajištěny týmu příslušníky členských států nebo i ze strany mezinárodních organizací. Členové EUROJUSTU, EUROPOLU, *Evropské justiční sítě ve věcech trestních* nebo *OLAF* se mohou podílet na činnosti společných vyšetřovacích týmů tam, kde to stanoví dohoda, především podpůrně s poradní funkcí.

Zřízení těchto týmů předpokládá a zavazuje orgány různých států požadavkem na spolupráci, přičemž na úseku koordinace vyšetřování a trestního stíhání zde hraje EUROJUST hlavní roli.

• Eurojust byl zřízen rozhodnutím Rady 2002/187/SVV, ve znění rozhodnutí Rady 2009/426/SVV ze dne 16. prosince 2008.

Hlavním cílem Eurojustu je zlepšit efektivitu národních orgánů pověřených vyšetřováním závažné mezinárodní a organizované trestné činnosti a zabezpečit, aby pachatelé těchto činů byli urychleně postaveni před soud. Vizí Eurojustu je být klíčovým hráčem a odborným centrem justiční spolupráce v boji proti organizované mezinárodní trestné činnosti v EU.

Eurojust byl zřízen v roce 2002. Jeho úlohou je podporovat a zlepšovat spolupráci justičních orgánů členských států EU v boji proti závažné mezinárodní trestné činnosti v Evropské unii.

Do Eurojustu, který má sídlo v Haagu, jsou vysíláni zástupci z každého členského státu Evropské unie. Jedná se o zkušené státní zástupce, soudce či policisty s příslušnou kvalifikací.
Jejich úkolem je naplňovat cíle Eurojustu, tedy především koordinovat národní orgány v každém stádiu trestního řízení. Zabývají se rovněž dalšími problémy, které vyplývají z odlišností právních systémů jednotlivých členských zemí.

Na jednotlivých zastoupeních, společně s národními členy, působí také jejich zástupci, asistenti a vyslaní národní experti. Pokud Eurojust uzavřel s určitým státem mimo Evropskou unii dohodu o spolupráci, může v rámci Eurojustu pracovat i styčný zástupce daného státu. V současnosti jsou do Eurojustu vyslaní zástupci z Chorvatska, Norska a USA. Nová legislativa EU umožňuje Eurojustu vysílat své styčné zástupce i do nečlenských zemí EU.
Eurojust je také sídlem sekretariátu Evropské justiční sítě, Sítě kontaktních bodů proti genocidě ohledně osob odpovědných za genocidu, zločiny proti lidskosti a válečné zločiny a Sítě společných vyšetřovacích týmů.

Eurojust má přibližně 200 zaměstnanců, kteří zabezpečují rychlé vyřízení žádostí o právní pomoc národních orgánů a dalších evropských institucí.

Činnost Eurojustu

Eurojust ročně eviduje téměř 1400 případů a uspořádá přibližně 140 koordinačních schůzek. Těchto koordinačních se účastní zástupci orgánů činných v trestním řízení jednotlivých členských zemí, a pokud to daný případ vyžaduje, mohou se jich účastnit i zástupci třetích zemí. Na těchto schůzkách se projednávají konkrétní případy a plánují se operativní akce jako například souběžné zatýkání či domovní prohlídky.

Koordinační schůzky se zaměřují na případy spadající do prioritních oblastí trestné činnosti vymezených Radou EU: terorismus, obchod s drogami, obchod s lidmi, podvody, korupce, počítačová kriminalita, praní špinavých peněz a ostatní činnosti spojené s přítomností organizovaných zločineckých skupin v ekonomice.

Eurojust má několik klíčových úloh a pravomocí vyplývajících z Rozhodnutí o Eurojustu. Kromě jiného poskytuje národním orgánům členských zemí součinnost při

žádostech o právní pomoc, může také požádat členské země o zahájení trestního řízení pro konkrétní trestné jednání.

Eurojust také pomáhá řešit spory o příslušnost v případech, kdy může více národních orgánů vést trestní řízení v dané věci. Eurojust je nápomocen také v případě dalších mezinárodních justičních nástrojů, jako např. při aplikaci evropského zatýkacího rozkazu. Eurojustem jsou rovněž poskytovány prostředky na založení a provozní potřeby společných vyšetřovacích týmů.

Partneři Eurojustu

Práce Eurojustu je založena na úzké spolupráci s jeho partnery. Jedná se jak o národní, tak i o orgány EU jako jsou např. Evropská justiční síť, Europol, OLAF (v případech kriminální činnosti ovlivňující finanční zájmy Evropské unie), Frontex, Sitcen, CEPOL, Evropská justiční vzdělávací síť a další subjekty.

Povinností Eurojustu je zajistit, aby se tato partnerství v boji proti mezinárodní kriminalitě dále rozvíjela (přičemž výměna informací mezi příslušnými orgány zde hraje významnou roli) a poskytovala tak nejlepší možnou koordinaci a spolupráci v oblasti ochrany svobody, bezpečnosti a spravedlnosti všech občanů EU.

7. Zajištění ochrany osobních údajů v rámci § 8 a 8a - kontrola použití odposlechů

„Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života“[27]

Toto je jedna z nejzákladnějších zásad demokratické společnosti a jejích občanů. Vychází z Listiny základních lidských práv a svobod (dále také jen Listina) jakožto součásti Ústavního pořádku České republiky. Výše uvedená citace je de facto výňatek z čl. 10 odst. 2 Listiny základních práv a svobod (zákon č. 2/19993 Sb.), ve znění zákona č. 162/1998 Sb., kterým se mění Listina základních lidských práv a svobod. Tato listina rozlišuje dvě lidská práva. Právo na ochranu soukromí a právo na informační sebeurčení (čl. 17). Ochrana osobních údajů je zakotvena v § 10:

[27] http://www.echr.coe.int/NR/rdonlyres/82E3CE7F-5D3D-46EB-8C13-4F3262F9E20B/0/CzechTch%C3%A8que.pdf, 27.2.2013 (PDF)

"Při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů".

Další ochranou soukromí uvedeného v Listině je formulováno v čl. 13 kdy:

„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon".

V neposlední řadě jsou to články 7 a 8, které garantují nedotknutelnost soukromí, právo na ochranu zpráv, které jsou podávány telefonním či jiným zařízením.

„Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence."

Právě tyto konkrétní články jsou v konfliktu s ustanoveními paragrafu 88 a paragrafu 88a, ale toto je ošetřeno výjimkou případů a způsoby, které stanoví zákon. Tato výjimka je ukotvena v trestním řádu pod paragrafem 8a) až 8d), který pamatuje (a je v něm přesně stanoveno), za jakých podmínek se poskytují informace o trestním řízení a osobách na něm zúčastněných.

Ustanovení těchto paragrafů jsou závazná nejen pro orgány činné v trestním řízení, ale v dnešní době jsou závazná zejména pro mediální prostředky, které se vehementně dožadují informací o probíhajícím trestním řízení. Zejména média by měla dbát na to, aby svými mediálními výstupy nenarušila vlastní trestní řízení nebo neporušila významná základní lidská práva a svobody, které mají i účastníci trestního řízení. V dnešní době se setkáváme s mnoha excesy, které se týkají porušování základních lidských práv a svobod ze strany médií. V těchto případech se nejedná pouze o zveřejňování jmen, fotografií pachatelů či svědků, ale setkáváme se s případy, kdy média ve svých reportážích ukazují příliš podrobně způsob provedení spáchaného trestného činu a de facto svou reportáží „navádějí" případné a potencionální pachatele. Existují případy, že média za honbou zveřejnění senzací naruší vlastní trestní řízení, a to tím, že zprávy získané nikoliv od orgánů činných v trestním řízení předčasně zveřejní,

čímž umožní ostatním spolupachatelům přijmout taková opatření, která nezvratně naruší vlastní průběh trestního řízení.

Narušení ochrany osobních údajů je v současné době řešeno pouze v rámci občanskoprávního sporu a porušení těchto práv v oblasti trestního práva je řešeno velmi zřídka.

Dovolím si konstatovat, že mi není znám případ, kdy by média, která svými reportážemi narušila zvlášť závažným způsobem vyšetřování, byla brána k trestní odpovědnosti, byť na tuto možnost reaguje § 180 trestního zákoníku (neoprávněné nakládání s osobními údaji).

Pokud se konkrétní skutečnosti nebo výsledky trestního řízení předčasně zveřejní, může to mít za následek ztížení nebo dokonce zmaření objasnění dané skutečnosti a usvědčení pachatele. Proto musí orgány činné v trestním řízení zvažovat, které informace a v jakém rozsahu použijí pro zveřejnění. V §8a odst. 1 je uvedeno, že se nesmějí zveřejňovat údaje o osobách, které se účastní trestního řízení ani údaje, které přímo nesouvisejí s trestnou činností. Tento institut ochrany osobnosti upravuje i Listina základních práv a svobod, a to konkrétně v čl. 10, kde je ustanoveno, že každý má právo na ochranu před neoprávněným zasahováním do rodinného či soukromého práva a dále také právo na ochranu před neoprávněným zveřejňováním nebo jiným zneužíváním údajů o své osobě. Z tohoto důvodu je třeba zaměřit se na podstatné informace, které se týkají dané věci a které jsou dostatečně prokázány. Poskytnutí některých informací je nutné odepřít také z důvodu, kdy by mohlo dojít k porušení zásady presumpce neviny. Orgány činné v trestním řízení v přípravném řízení pečlivě zvažují poskytnutí informací sdělovacím prostředkům, aby nedošlo například k nactiutrhání. Obdobné postupy se vyskytují i během trestního stíhání, kdy orgány činné v trestním řízení velmi obezřetně přistupují ke zveřejňování informací o průběhu vyšetřování i informací o obviněné osobě.

V praxi se občas vyskytují situace, které jsou v rozporu s §8a trestního řádu, a to v souvislosti se zveřejňováním odposlechů telekomunikačního provozu, které ale neposkytly ke zveřejnění orgány činné v trestním řízení. V těchto situacích je veřejnost do posledního detailu informována o obsahu trestní věci, o obviněném či podezřelém v plném rozsahu z telefonních hovorů či jiných forem telekomunikačního provozu. Tím, kdo tyto informace nejčastěji poskytuje, jsou sdělovací prostředky, které velmi často

odmítají prozradit svůj zdroj informací. Mylně se domnívají, že pokud soud nebo v přípravném řízení soudce povolil odposlech, mohou ho zveřejnit, jindy jsou si však svého nezákonného postupu vědomy a velmi často nechtějí zveřejnit svůj zdroj.

Zveřejňování odposlechů a záznamů telekomunikačního provozu ve sdělovacích prostředcích se stává velmi atraktivní záležitostí- je velmi žádaným „zbožím“, zvyšuje sledovanost a je žádané veřejností. I když informace o odposleších má k dispozici pouze omezený okruh osob, který je přesně vymezen, je vyšetřování úniku informací vždy složité a většinou nedojde k vypátrání osoby, která tyto informace „vynáší“ na veřejnost. Osoby, které záznamy odposlechu dodávají do tisku, televize anebo je umisťují na různé internetové servery, zůstávají neodhaleny a nikterak trestně nepostihnuty. Z tohoto důvodu problém týkající se úniku informací na veřejnost přetrvává.

Je nutné podotknout, že hromadné sdělovací prostředky nepovažují za podstatné, že přípravné řízení je neveřejné a že zveřejnění nahrávek odposlechů či jejich záznamu zcela zásadním způsobem narušuje trestní řízení a ohrožuje účel legálně povolených odposlechů, jímž je usvědčení pachatelů prostředky, jež povoluje trestní řád.“[28] Důležité je také zmínit, že k legálnímu zveřejnění obsahu odposlechu a záznamu telekomunikačního provozu může dojít pouze tehdy a v případech, kdy obsah např. telefonního rozhovoru bude zveřejněn jako důkaz před soudem.

V souvislosti se zveřejňováním odposlechů a záznamu telekomunikačního provozu je třeba postihnout ty, kteří tyto informace zveřejňují v masmédiích. Jejich jednání může mít trestněprávní dopady- mohou se dopustit trestného činu pomluvy (§ 184 trestního zákona) nebo trestného činu křivého obvinění (§ 345 trestního zákona). Poškozená osoba se většinou obrátí na orgány činné v trestním řízení, a to cestou trestního oznámení, které mají povinnost z úřední povinnosti konat. Trestní řízení s osobou, která některým z již výše zmiňovaných trestných činů způsobila újmu osobě poškozené, může skončit odsouzením na 2 roky případně až na 3 roky u trestného činu křivého obvinění nebo zákazem činnosti. Trestní odpovědnost mohou mít pouze fyzické osoby, kterými jsou konkrétní pracovníci např. autor článku, šéfredaktor, aj.

V oblasti autorského práva by se novinář mohl zveřejněním odposlechu dopustit trestného činu porušování autorského práva a práv souvisejících s právem autorským.

[28] Vantuch,P.:Zveřejňování odposlechů v mediích. Právní rádce,2008,č.5

Policisté a zaměstnanci policie zařazeni v oprávněném subjektu a ve specializovaném pracovišti odpovídají za ochranu informací získaných prováděným úkonem a dalších souvisejících informací před vyzrazením a zneužitím. Při zpracování informací postupují v souladu s právními předpisy a interními akty řízení upravujícími ochranu osobních údajů a v souladu s právními předpisy a interními akty řízení upravujícími ochranu utajovaných informací.

Při doručení žádosti a příkazu o nařízení odposlechů určený policista útvaru zvláštních činností stanoví způsob provedení a zajištění odposlechu. Policejní orgán ve spolupráci s určeným policistou určí, kdo a jakým způsobem je oprávněn získané informace od specializovaného pracoviště přebírat, uvedené skutečnosti potvrdí svým podpisem v pověření. Oprávněný subjekt se podílí na přípravě, provádění i ukončení odposlechu a zajišťování podmínek nezbytně nutných pro jeho provádění. Na vyžádání specializovaného pracoviště policejní orgán zpracuje písemný plán zajištění odposlechu s určením osob odpovědných za plnění jeho jednotlivých fází a je povinen spolupracovat se specializovaným pracovištěm při všech mimořádných situacích. Policejní orgán a specializované pracoviště se vzájemně informují o všech změnách situace související s odposlechem, zejména pominou-li důvody jeho provádění. V případě změny údajů uvedených v příkazu nebo v písemném souhlasu uživatele, je policejní orgán povinen bezodkladně požádat soudce nebo uživatele, který souhlas udělil, o opravu a doplnění. Další technicky – organizační opatření jsou shrnuta v následujících bodech:

• editovat požadavek lze pouze z pracoviště útvaru zvláštních činností, na kterém je veden spisový materiál ke konkrétnímu odposlechu,

• přistupovat do systému může pouze oprávněná osoba po své individuální identifikaci („zalogování“),

• „logy“ všech přístupů jsou archivovány a centrálně dostupné v technologii útvaru zvláštních činností,

• aktivaci odposlechu vůči telekomunikačním operátorům provádí oddělení útvaru zvláštních činností - Centrum informačních systémů, toto pracoviště nemá možnost požadavek editovat a nemá přístup k záznamům,

• informace o provádění každého odposlechu je z technologických důvodů přítomna ve všech částech systému (na všech pracovištích útvaru zvláštních činností). Jednotlivé

části technologie mají různé správce, kteří by se automaticky dozvěděli o nekorektním nasazení odposlechu,
• záznamy jsou zpracovány automaticky na tom pracovišti, na které jsou směrovány technologií operátora,
• operátoři jsou povinni uchovávat veškeré údaje o aktivaci a deaktivaci odposlechu pro potřeby kontrolního orgánu Poslanecké sněmovny Parlamentu ČR.

Centrum informačních systémů útvaru zvláštních činností:

• přijímá požadavky výhradně z pracovišť útvaru zvláštních činností a posílá je dále příslušnému operátorovi, • nemá přímý kontakt s jinými součástmi Policie ČR nebo jinými oprávněnými subjekty dle ustanovení § 12 tr. ř.,
• dohlíží na řádný průběh aktivace a deaktivace žádaných čísel,
• nemá oprávnění samostatně editovat požadavky,
• nemá přístup k výstupním informacím,
• zprostředkovává další informace od telekomunikačních operátorů (§ 88a tr. ř., §§ 66, 68, 71 zákona č. 273/2008 Sb., o Policii ČR),
• všichni pracovníci útvaru zvláštních činností jsou určeni ke styku s utajovanými informacemi podle zákona č. 412/2005 Sb., ve znění pozdějších předpisů,
• pracovníci útvaru zvláštních činností, kteří mají přístup k technologii zabezpečující odposlechy, mají povinnost zachování naprosté mlčenlivosti zdůrazněnou i ve svých pracovních náplních,
• při jakékoli manipulaci s písemnostmi, jež se týkají odposlechů, jsou důsledně dodržována pravidla administrativní bezpečnosti podle zákona č. 412/2005 Sb. ve znění pozdějších předpisů, a vyhlášky Národního bezpečnostního úřadu č. 529/2005 Sb., ve znění pozdějších předpisů. Se záznamy na přenosném paměťovém médiu je důsledně nakládáno v souladu se spisovým řádem Ministerstva vnitra ČR jako s evidovanými přílohami písemností. Zařízení pro pořizování záznamu telekomunikačního provozu je konstruováno tak, že z praktického hlediska je téměř nemožné realizovat odposlech bez splnění zákonem definovaných podmínek. Je toho docíleno tím, že systém pro pořizování záznamů obsahuje prvky jasně definované osobní odpovědnosti za vkládané nebo doplňované údaje a historie všech takových zásahů je archivována. Kromě toho musí mít každý úkon odraz ve spisovém materiálu, který je veden k trestní věci, nejen

na útvaru zvláštních činností, ale i na příslušném pracovišti SKPV, státním zastupitelství a soudu. K zajištění ochrany a bezpečnosti informací při využití institutu odposlechu a záznamu telekomunikačního provozu napomáhá i skutečnost, že pořízené záznamy existují ve dvojí podobě. V původním formátu se všechny zaznamenané hovory uchovávají v datovém úložišti technologie do doby ukončení odposlechu konkrétního zájmového čísla. Potom jsou záznamy automaticky vypáleny na „archivní CD“. Jedná se o nepřepisovatelný nosič se speciálním potiskem, označený pro pozdější identifikaci kontrolním součtem. Tato CD jsou protokolárně předána vyžadujícímu oprávněnému subjektu k založení do trestního spisu. Je-li později rozhodnuto o použití záznamu nebo jeho části v řízení před soudem, pořídí příslušné pracoviště útvaru zvláštních činností kopii vybraných pasáží z „archivních“ nosičů na jiné, stejně zabezpečené CD a spolu s protokolem podle trestního řádu jej předá orgánu činnému v trestním řízení. Ve všech fázích tohoto procesu je jasně definována odpovědnost za manipulaci s tímto druhem záznamů při současném zachování jejich kompletnosti a prokazatelné autenticity. Technicko-organizační opatření vedoucí k zásadnímu zvýšení individuální odpovědnosti za jakoukoli manipulaci se záznamy pro operativní použití:

1) záznamy nejsou odeslány na komunikační počítač pracoviště SKPV, ale ukládají se na databázovém serveru v zašifrovaném tvaru,
2) přístup k nim a jakákoli manipulace s nimi je možná pouze prostřednictvím hardwarového klíče s naprogramovanými přístupovými právy ke konkrétnímu odposlechu; každý pracovník SKPV se jednoznačně identifikuje svým vlastním klíčem a je osobně odpovědný za jeho používání,
3) veškerá manipulace s jakýmkoli záznamem je evidována a kdykoli kontrolovatelná,
4) záznamy jsou srozumitelně reprodukovatelné pouze speciálním softwarovým nástrojem, který je možné použít rovněž pouze prostřednictvím hardwarového klíče,
5) v případě, že je nezbytné pořídit z jakéhokoli důvodu kopii záznamu, je zřejmé, kdo konkrétně kopii vytvořil a je na něm, jak doloží důvod tohoto kroku a způsob, kterým kopii zabezpečil proti zneužití,
6) takto vytvořená kopie je srozumitelně reprodukovatelná pouze přímo z CD, na kterém byla předána; každá eventuální další kopie ponese identifikační znaky té původní,

7) v případě jakéhokoli zásahu do struktury dat uložených na předané kopii (zašifrovaný záznam, speciální přehrávací software a identifikační kódy) se záznam stane nesrozumitelným. Popsaný postup technicko organizačních opatření spolu s úpravou interních aktů řízení a odpovídajícím proškolováním oprávněných policistů vytváří podmínky pro stanovení vymahatelné individuální osobní zodpovědnosti za ochranu dat z odposlechů. Přestože Policie ČR přijímá na ochranu údajů z odposlechu a záznamu telekomunikačního provozu stále nová opatření, je třeba i nadále počítat s rizikem nezákonného použití a zneužití získaných údajů mimo působnost Policie ČR. Jako velmi reálné se jeví nebezpečí zneužití údajů z odposlechu a záznamu telekomunikačního provozu ze strany „třetích osob". Osobami, které můžou tyto osobní údaje zneužít, jsou velmi často zaměstnanci společností nebo státních orgánů, které údaje zpracovávají, ale i další osoby. Zcela důvodně se lze domnívat, že také někteří účastníci trestního řízení zcela přehlížejí skutečnost, že informace byly získány pro účel trestního řízení a jejich použití k jinému účelu je nepřípustné. Jedním z opatření, částečně eliminujících tuto nevyhovující situaci, bylo přijetí zákona č. 52/2009 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů a některé další zákony, s účinností od 1. 4. 2009. Tato novela trestního řádu důsledněji vymezuje podmínky, za kterých lze poskytovat informace o trestním řízení a osobách na něm zúčastněných. Zpřísňuje podmínky, za kterých mohou orgány činné v trestním řízení poskytovat informace o své činnosti veřejnosti. Do trestního řádu byl vložen § 8b, kde je stanoveno, že osoby, kterým byly orgány činnými v trestním řízení poskytnuty informace o osobách zúčastněných na trestním řízení, nesmějí tyto informace nikomu dále poskytnout, pokud jejich poskytnutí není nutné k uvedeným účelům. O tom musí být tyto osoby poučeny. Dalším aspektem v posílení ochrany informací a osobních údajů při využití institutu odposlechu a záznamu telekomunikačního provozu je nově také zákon č. 207/2011 Sb., ze dne 8. června 2011, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, který v § 8c nově zní:

„Nikdo nesmí bez souhlasu osoby, které se takové informace týkají, zveřejnit informace o nařízení či provedení odposlechu a záznamu telekomunikačního provozu podle § 88 nebo informace z něj získané, údaje o telekomunikačním provozu zjištěné na základě příkazu podle § 88a, nebo informace získané sledováním osob a věcí podle § 158d odst.

2 a 3, umožňují-li zjištění totožnosti této osoby a nebyly-li použity jako důkaz v řízení před soudem".

Lze předpokládat, že ve většině případů se postupuje v souladu se stanoviskem Vrchního státního zastupitelství v Olomouci ze dne 14. dubna 2005 (4 SPR 50/2005), podle kterého doslovný přepis zvukového záznamu do písemné podoby není nutné provádět, v protokolu se pouze vyznačí obsah rozhovoru, který je zachycen na zvukovém nosiči. V případě, pokud jsou přepisy pro věc nezbytné, měl by je zpracovávat policejní orgán, který vede trestní řízení, případně též státní zástupce, neboť jen oni jsou schopni posoudit, který ze záznamů obsahuje skutečnosti důležité z hlediska konkrétní trestní věci. Záznamy důležité pro trestní řízení se přenášejí na samostatný zvukový nosič, který se opatří protokolem, který sepíše zpravidla policejní orgán a založí do spisu (ostatní záznamy se spolehlivě uschovají odděleně od spisu) a v řízení před soudem se odposlech provádí jako důkaz zásadně poslechem záznamu na nosiči. Uvedený postup má zabránit shromažďování údajů a informací, které nemají význam pro trestní řízení a obsahují skutečnosti zasahující do soukromí občanů, nelze jej však považovat za absolutní. Nicméně, touto cestou lze významným způsobem úniky informací z odposlechu a záznamu telekomunikačního provozu omezit. V případech, kdy jsou nadále pro potřeby dozorových státních zástupců zvukové záznamy přepisovány do písemné podoby, je třeba vnímat riziko úniku informací z odposlechů v souvislosti s širokým okruhem osob, které mají ve smyslu § 65 odst. 1 tr. ř. právo nahlížet do trestních spisů. Výsledkem pak bývá nemožnost jednoznačně identifikovat a postihnout původce úniku. Účastníci trestního řízení si mohou být jisti, že v okamžiku, kdy byla v souladu se zákonem pořízena a předána kopie trestního spisu nebo jeho části, se odpovědnost za ochranu zde obsažených údajů rozmělnila a je nanejvýš nepravděpodobné, že se podaří zjistit eventuálního původce zneužití. Odpovědnost za provedení odposlechu a záznamu telekomunikačního provozu je svěřena zákonem Policii ČR. Přitom je nutné vycházet z presumpce správnosti postupu státního orgánu, pokud nebude zásadním a hodnověrným způsobem prokázán opak. Je třeba též vycházet ze současné úrovně technických možností při monitorování a záznamu telekomunikačního provozu, jakož i při nakládání s přenositelnými zvukovými médii jako nosiči dat a jejich dalším používáním. Proto přenášení či komprimace datových

souborů nelze považovat za nezákonnou manipulaci, která by zkreslovala, měnila či jiným způsobem ovlivňovala význam záznamu telekomunikačního provozu pro dokazování v trestním řízení. Mimo to, technická opatření Policie ČR nezákonné pozměňování, doplňování či úpravu záznamů de facto neumožňují. Legislativní opatření přijatá Policií ČR v oblasti ochrany osobních údajů a informací získaných z odposlechu a záznamu telekomunikačního provozu jsou popsána v následující kapitole věnované kontrolním mechanismům.[29]

Jak bylo uvedeno již v předchozí kapitole, použití odposlechů zasahuje vážnou měrou do základních lidských práv a svobod. Proto jejich provádění musí být velmi striktně kontrolováno, a to i ve více úrovních. Občané musejí mít jistotu, že tento institut není zneužíván, že jsou dodrženy všechny formální náležitosti odposlechů a informace z nich získané jsou použity výhradně k zákonem stanoveným účelům. V této kapitole se budu snažit popsat kontrolní mechanismy, které by měly výše uvedené dostatečně zajistit.

Kontrolní mechanismy

Při využívání úkonů odposlechu a záznamu telekomunikačního provozu je uplatňován třístupňový kontrolní systém, který vylučuje – bez selhání lidského faktoru v některé z jeho fází – aby byl realizován úkon, který by

a) nebyl posouzen služebními funkcionáři Policie ČR z hlediska jeho opodstatněnosti pro probíhající trestní řízení,
b) nebyl následně posouzen justičními orgány ze stejného hlediska a navíc i z hlediska dodržení požadavků přiměřenosti, zdrženlivosti a subsidiarity,
c) nebyl kontrolovatelný Stálou komisí pro kontrolu použití operativní techniky Policie ČR Poslanecké sněmovny Parlamentu ČR.

Kontrolní mechanismy realizované justičními a parlamentními orgány lze označit jako kontrolní mechanismy vnější, kontrolní činnost v rámci Policie ČR pak jako kontrolní mechanismy vnitřní.

[29] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011 –zpracoval Odbor analýz PP PČR

Vnitřní kontrolní mechanismy lze rozdělit na kontrolní mechanismy technického charakteru a organizačního charakteru.

Vnitřní kontrolní mechanismy organizačního charakteru spočívají především v uplatňování principu podřízenosti a nadřízenosti a předkládání a schvalování písemností vyhotovených v souvislosti s odposlechem a záznamem telekomunikačního provozu v rámci organizačního článku Policie ČR. Vnitřní kontrolní mechanismy organizačního charakteru představují mimo jiné proces zpracování žádosti o povolení odposlechu a záznamu telekomunikačního provozu před jejím předložením státnímu zástupci, jehož nedílnou součástí je její schválení služebním funkcionářem. Princip podřízenosti a předkládání žádostí ke schválení cestou přímého nadřízeného (vedoucího organizačního článku konkrétního útvaru SKPV) je zakotven v interních aktech řízení a odpovídá hierarchické struktuře a působnosti dané organizačním řádem útvaru. Organizační řád stanoví pravomoc a odpovědnost vedoucích funkcionářů a zároveň rozlišuje jednotlivé úrovně řízení a rozsah svěřené působnosti. Nejedná se tedy o pouhou formalitu, tento postup je uplatňován vždy bez výjimek. Popsaný princip schvalování žádostí a kontrolní činnost vedoucích služebních funkcionářů není v Policii ČR žádnou novinkou, ale je v praxi uplatňován dlouhodobě. Tento princip se uplatňuje po celou dobu realizace úkonu i při vyhodnocování po jeho ukončení. Vždy tedy platí, jak bylo uvedeno výše, že bez schválení vedoucího služebního funkcionáře a bez doporučení přímého nadřízeného nelze žádost o odposlech a záznam telekomunikačního provozu státnímu zástupci předložit.

Kontrola v rámci Policie ČR, včetně nahodilých kontrolních akcí specializovaným kontrolním orgánem, je upravena zejména závazným pokynem policejního prezidenta č. 110/2006, o obecné kontrole v Policii ČR. Tento interní akt řízení vymezuje kontrolní útvary, skupiny a pracoviště Policie ČR, které jsou zmocněny a pověřeny provádět kontrolní činnost. Interní kontrolní prvek v rámci trestního řízení je navíc posílen nutností periodických i namátkových kontrol, které jsou prováděny v závislosti na úrovni stupně řízení, a to od vedoucího oddělení přes vedoucího odboru až k nejvyššímu stupni řízení.

Za další kontrolní mechanismus se dá považovat skutečnost, že veškerá manipulace s písemnostmi a záznamy vzniklými v souvislosti s odposlechem

telekomunikačního provozu je prováděna v souladu s interními akty řízení vycházejícími z právních předpisů, které upravují nejen spisovou službu, ale např. i ochranu utajovaných informací, osobních údajů atd. Každý jednotlivý úkon je prokazatelný a tedy i kontrolovatelný.

Zpracovávání osobních údajů Policií ČR regulují dva základní zákony - zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a zákon č. 273/2008 Sb., o Policii ČR, který je k zákonu o ochraně osobních údajů ve vztahu speciality. [30] Spisová služba se projevuje i v rámci trestního řízení, kde se vedle norem trestního práva (trestní zákon a trestní řád) uplatňují další právní předpisy a interní akty řízení, zejména závazný pokyn policejního prezidenta č. 130/2007, kterým se upravuje postup Policie ČR při plnění úkolů v trestním řízení.

Zdůraznění ochrany osobních údajů vyjadřuje závazný pokyn policejního prezidenta č. 55/2007, kterým se stanoví jednotný postup Policie ČR při zpracovávání osobních údajů při plnění úkolů Policie ČR v souvislosti s trestním řízením. Tento závazný pokyn vymezuje základní pojmy, subjekty zpracování osobních údajů a jejich povinnosti, upravuje problematiku zpřístupňování osobních údajů, prokazování oprávněnosti a nutnosti přístupu, registr evidencí a zpřístupnění informací o prováděných zpracováních. S ohledem na jistou abstraktnost a složitost této problematiky jsou k závaznému pokynu průběžně vydávány další metodické materiály.

Ochrana skutečností, se kterými se policista seznámil při plnění úkolů Policie ČR (tím i zpracovávaných osobních údajů), je garantována povinností policistů zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění úkolů Policie ČR nebo v souvislosti s nimi, a které v zájmu zabezpečení úkolů Policie ČR nebo v zájmu jiných osob vyžadují, aby zůstaly utajeny před nepovolanými osobami.

V trestním řízení má k informacím o něm přístup pouze určený počet osob. V rámci Policie ČR je vždy několik fyzických osob, které jsou oprávněny zpracovávat informace, včetně osobních údajů (např. oprávněný žadatel, osoby plnící úkoly na specializovaném pracovišti, nadřízení služební funkcionáři oprávněného žadatele). K tomu je nutné konstatovat, že vedoucí pracovníci plní zejména úlohu schvalovací

[30] existuje-li v těchto zákonech rozdílná právní úprava ve stejné věci, použije se přednostně ustanovení speciálního zákona.

(směrem k podřízeným), úlohu navrhovací (směrem ke státním zastupitelstvím) a úlohu kontrolní (směrem k vykonaným postupům). Se samotným výstupem, tj. vlastním obsahem pořízených datových souborů, se v Policii ČR seznamuje většinou pouze oprávněný žadatel nebo osoba k tomu určená a schválená služebním funkcionářem. V rámci Policie ČR mohou úkony odposlechu a záznamu telekomunikačního provozu použít jen oprávněné policejní orgány, úřední osoby zařazené v policejním orgánu musí být zároveň držiteli „osvědčení fyzické osoby“ o právu seznamovat se s utajovaným informacemi ve stupni „Vyhrazené“, popř. vyšším. V praxi je dodržován princip zákona na ochranu utajovaných informací ve směru seznamování se s utajovanými informacemi u policejních orgánů, kteří je nezbytně nutně potřebují k výkonu své funkce.

Kromě výše popsaných kontrolních mechanismů uplatňovaných v rámci rezortu Policie ČR spadá do systému kontroly oblasti odposlechu a záznamu telekomunikačního provozu i činnost dalších subjektů mimo Policii ČR, kterou lze označit jako vnější kontrolní mechanismy. V první řadě se jedná o funkci státních zastupitelství, která vykonávají dozor v trestní věci. Ve vztahu k policejnímu orgánu je státní zástupce v rámci své dozorové funkce mimo jiné oprávněn dávat policejnímu orgánu závazné pokyny k vyšetřování trestných činů, vyžadovat od policejního orgánu spisy a další materiály za účelem prověrky, zda policejní orgán řádně postupuje v trestním řízení, vracet věc policejnímu orgánu se svými pokyny k doplnění, rušit nezákonná nebo neodůvodněná rozhodnutí a opatření policejního orgánu. Policejní orgán je pak povinen umožnit státnímu zástupci, aby mohl osobně a soustavně sledovat postup trestního řízení a být osobně přítomen kterémukoliv procesnímu úkonu. Policejní orgán plní pokyny státního zástupce, tyto pokyny, jsou-li v písemné podobě, jsou ukládány do spisu. O ústních pokynech jsou zpracovány úřední záznamy.

Ke kontrole využití odposlechu a záznamu telekomunikačního provozu je dále oprávněna na základě ustanovení § 98 zákona č. 273/2008 Sb., o Policii ČR, Stálá komise pro kontrolu použití operativní techniky Policie ČR Poslanecké sněmovny Parlamentu ČR.

Dalším subjektem, který může v rámci svých oprávnění provést kontrolu ochrany informací z odposlechu a záznamu telekomunikačního provozu, je Úřad na ochranu osobních údajů. [31]

[31]POLICEJNÍ PREZIDIUM, *Analýza odposlechů,* textový soubor, str. 26-30 [online] [cit 2011-04-05-2011]. Dostupné z: <www.mvcr.cz/soubor/analyza-odposlechu-2007-doc.aspx>.

8. ZÁVĚR

Odposlech a záznam telekomunikačního provozu je institutem trestního práva procesního a jako takový slouží orgánům činným v trestním řízení k dokazování trestných činů.

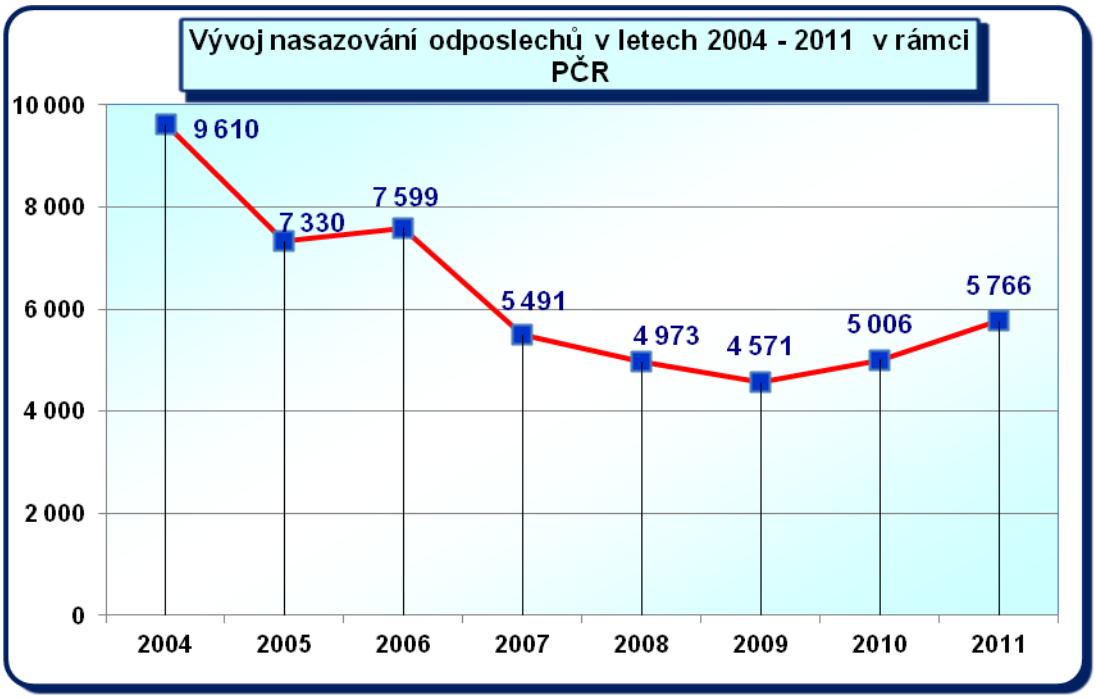
Právě z komunikace pachatelů trestných činů mají policejní orgány ty nejlepší zdroje informací, které napomáhají při odhalování jejich trestné činnosti. Zajímavé by bylo, pokud by bylo možné odposlouchávat veškerou komunikaci, která probíhá na území našeho státu. Systémy, které zachytávají velkou část komunikace přes elektronické přenosové soustavy, jsou některými státy vyvíjeny a provozovány (americký systém ECHELON). Monitorování telefonických hovorů a internetové komunikace, ale i provoz těchto systémů, provázely zpočátku velké protesty a nelze si dost dobře představit diskuze našich zákonodárců k tomuto tématu. Ovšem v některých zemích, zejména pak v USA, po teroristických útocích z 11. září 2001, byly tyto nesouhlasné hlasy umlčeny a v jakési podobě jsou využívány.

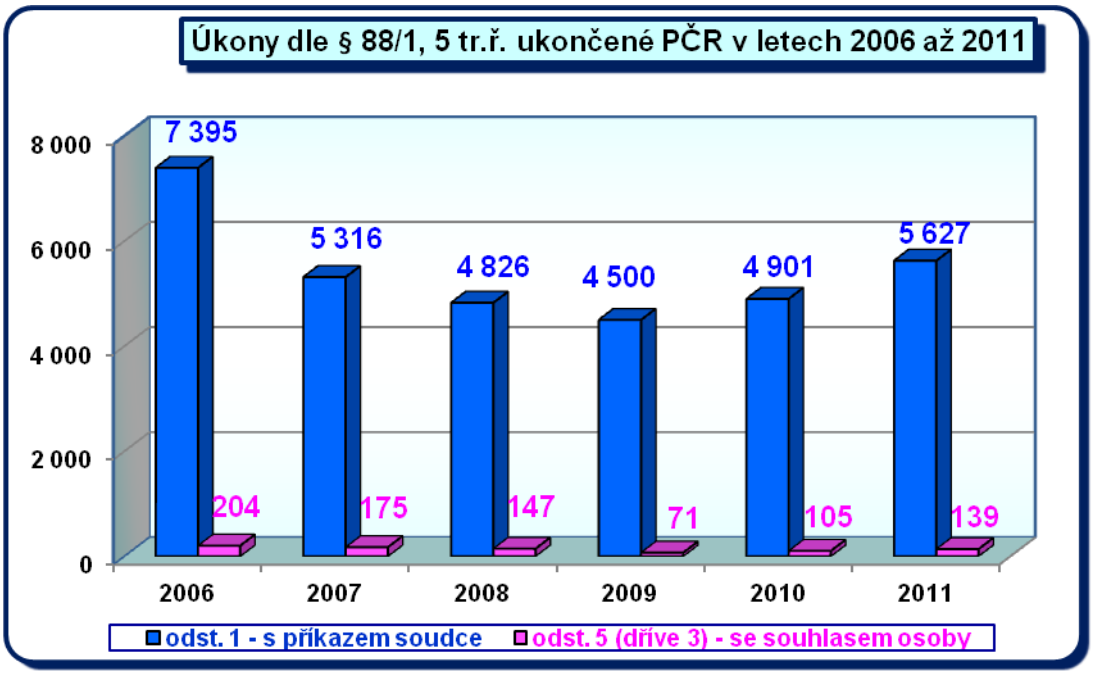
Takový rozsah odposlechu, který sleduje občana na každém kroku je v našem státě zcela nemožný. V ČR má každý občan dle Ústavy a Listiny právo na soukromí, které může být narušeno jen za zákonem daných podmínek. Právní rámec odposlechů je primárně zakotven v trestním řádu č. 141 /1961 Sb. v §88 a §88a.

Počátkem institutu odposlechů v rámci trestního řízení v ČR je novela trestního řádu 178/1990 Sb., která poprvé definovala zákonný rámec odposlechů pouze v §88 TŘ. Vývoj institutu odposlechů následně ovlivnila celá řada dalších novelizací snažících se spíše méně než více úspěšně respektovat překotný vývoj a rozvoj telekomunikační techniky. Zcela zřejmým příkladem stárnutí této právní úpravy je novela trestního řádu 178/1990 Sb., která na počátku umožňovala pouze odposlech telefonních přístrojů.

Nad každou právní normou vznikají ve společnosti diskuze. Problematikou odposlechů se zabývají mnohé rozsáhlé odborné práce i novinové články, ale v posledních deseti letech je problematika odposlechů také stálicí v diskuzích českých politiků. V těchto diskuzích se velmi často objevuje názor, že orgány činné v trestním řízení využívají odposlechů v nadměrné míře, kdy je každý den monitorováno tisíce „hovorů" (hovor,SMS, MMS, email atd.). Tento názor je však snadno vyvratitelný, a to

na základě statistického zkoumání počtu a struktury odposlechů nařízených orgány činných v trestním řízení za posledních osm let.

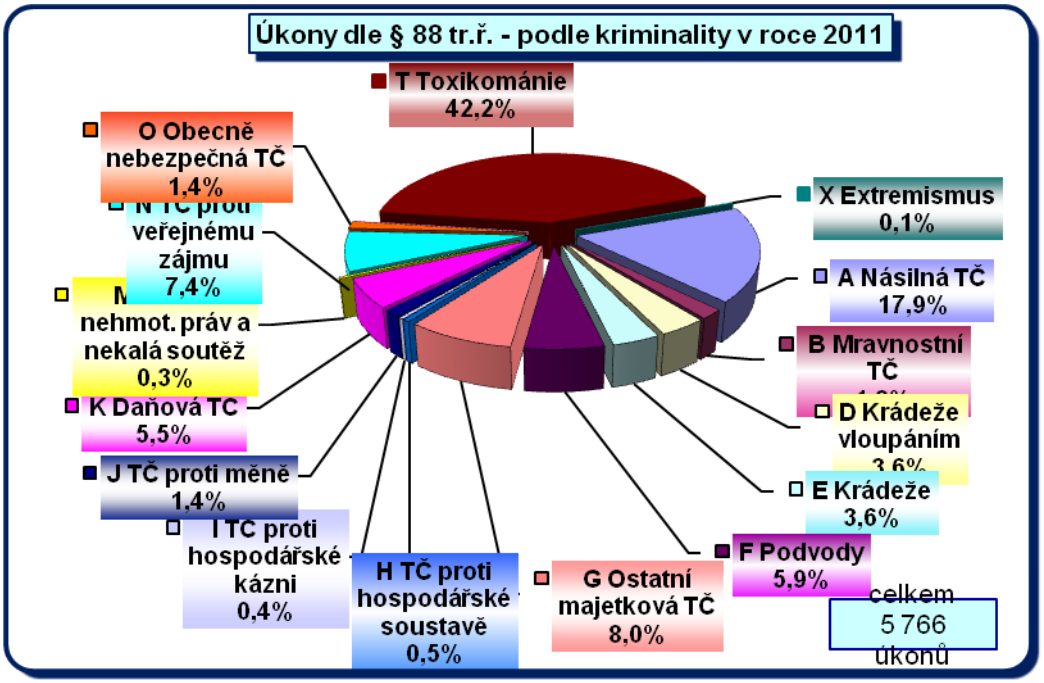


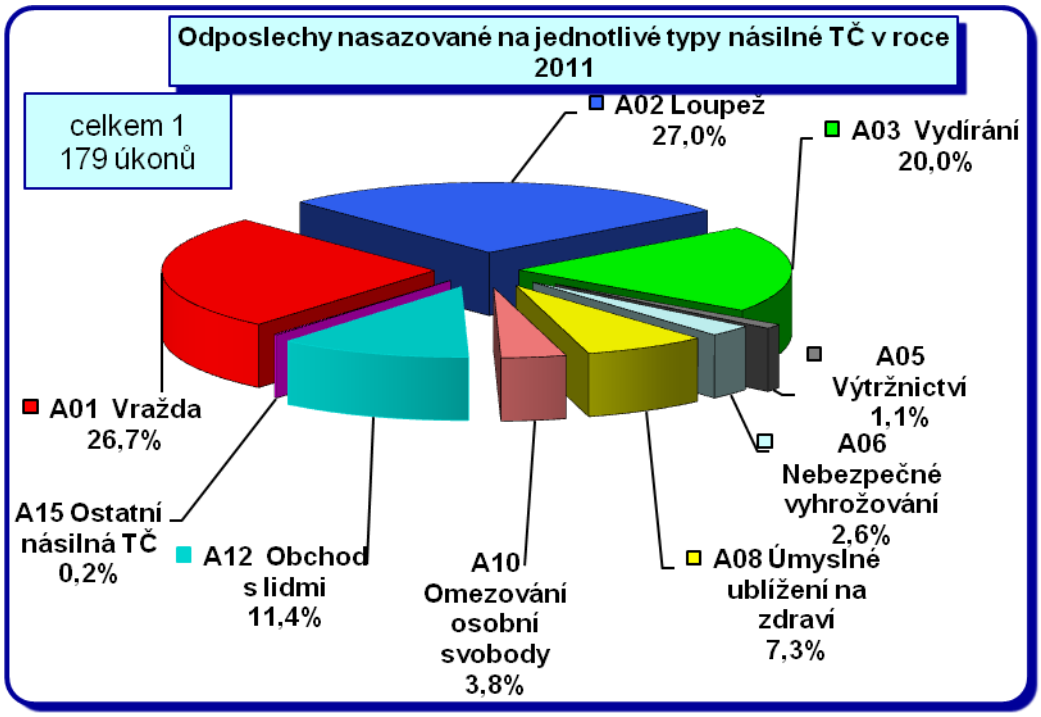


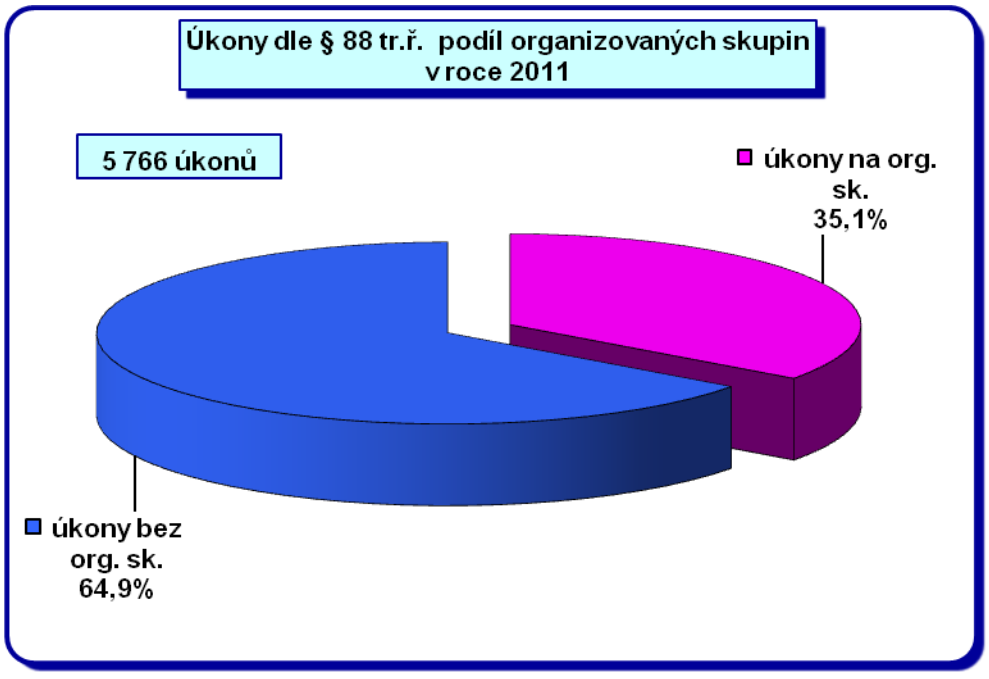
Ze shromážděných dat vyplývá, že k žádnému nadměrnému nasazování odposlechů nedochází, spíše naopak, počet nařízených odposlechů od roku 2004 trvale klesá a nekopíruje tedy několikanásobné navýšení počtu telekomunikační techniky, ke kterému od té doby došlo. Ukazatel tisíce „hovorů" však nejspíše pravdivý bude, ale

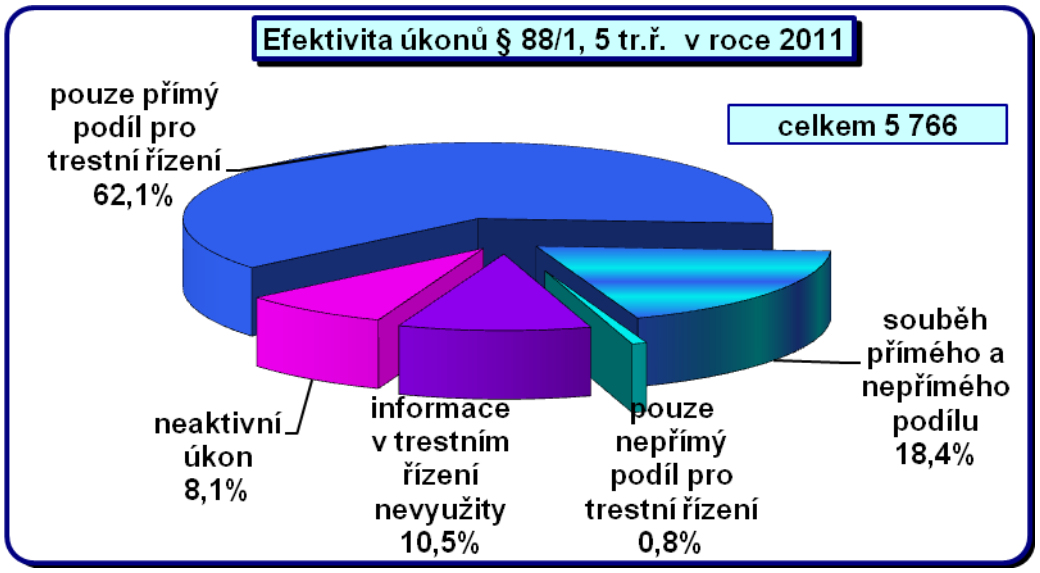
opět je nutno vzít v potaz několik faktů pro zvážení přiměřenosti počtu prováděných odposlechů. Především je třeba přihlédnout k současnému životnímu stylu, protože člověk může každý den běžně uskutečnit i několik desítek „hovorů". Pokud si uvědomíme, že nařízených odposlechů je cca 5000 ročně a samotný odposlech může trvat i několik měsíců, pak počet odposlouchávaných „hovorů" jdoucí do řádů tisíců za den není třeba považovat za nadměrný, ale spíše za přiměřený.

Při hodnocení samotného institutu odposlechů je důležité také vědět, že 72% nařízených odposlechů slouží k odhalování kriminality související s drogami, násilím, krádežemi a loupežemi i to, že 75% z celkového počtu nařízených odposlechů přináší důležité informace, které jsou významné pro trestní řízení.




Odposlechy nasazované na jednotlivé typy násilné TČ v roce 2011
celkem 1 179 úkonů
A02 Loupež 27,0%
A03 Vydírání 20,0%
A05 Výtržnictví 1,1%
A06 Nebezpečné vyhrožování 2,6%
A08 Úmyslné ublížení na zdraví 7,3%
A10 Omezování osobní svobody 3,8%
A12 Obchod s lidmi 11,4%
A15 Ostatní násilná TČ 0,2%
A01 Vražda 26,7%


Úkony dle § 88 tr.ř. podíl organizovaných skupin v roce 2011
5 766 úkonů
úkony na org. sk. 35,1%
úkony bez org. sk. 64,9%



Odposlechy jako takové jsou obrovským zásahem do soukromí občana a jsou „ospravedlněny“ právě pocitem klidu a bezpečí, který s sebou pokles kriminality přináší. Velká část občanů se totiž ve svém životě stala obětí trestného činu a přitom neexistuje člověk, který by se chtěl zcela dobrovolně stát obětí zločinu. Tento zásah do soukromí velkou měrou napomáhá v boji s kriminalitou a ten, kdo se chová dle práva a jedná ve svém životě čestně, se nemusí obávat, že při takovém vstupu do jeho soukromí bude krácen na svých právech. Diskuze na toto téma mne v posledních letech proto velmi překvapují. Od diskuze o přiměřenosti počtu odposlechů by se mělo zcela opustit a spíše než k současnému stavu by se měl pohled na tuto problematiku obrátit k budoucnosti, protože prostor ke změně právních mezí pro nasazení odposlechů je rozsáhlý. Především je nutné změnit současný stav tak, aby orgány činné v trestním řízení mohly držet krok s pachateli trestných činů, kteří ke svému kriminálnímu jednání stále častěji využívají nejmodernější telekomunikační technologie. Stále je totiž u nás patrný trend, kdy právní úprava příliš konkretizuje použití institutu odposlechů a brání nasazení modernějších technologií k získávání odposlechů. Současná právní úprava nepostihuje vývoj techniky a zaostává tak o 5-10 let. Jako nutnost se proto jeví dát větší prostor orgánům činným v trestním řízení při výběru technologie k získání odposlechu například tím, že bude obecně povolovat k získání odposlechu telekomunikačního provozu použití technologií, které jsou aktuálně dostupné. Příkladem by mohlo být sledování telekomunikačního provozu v datových sítích za použití „virů" přímo v počítači odposlouchávaných osob.

Další možnou změnou, která by mohla vést ke zlepšení situace týkající se efektivity odposlechů, je rozšíření působnosti §88 a §88a na všechny skutkové podstaty trestního zákona, neomezovat je hranicí trestní sazby. Při rozhodování o povolení takového odposlechu je třeba se řídit především tím, zda je možné odposlechem získat relevantní informace pro trestní řízení.

Je také důležité se zaměřit na přísný postih všech osob, které poruší velmi křehký institut odposlechů a upravit legislativu tak, aby bylo zabráněno nechtěným únikům obsahu odposlechů či neoprávněnému nasazení odposlechů a bude přísně a důsledně kontrolován přístup k samotným odposlechům v rámci seznamování s trestním spisem. Jako výhodné se také jeví vedení odposlechů odděleně od spisu. V případech, kdy je nutné s obsahem odposlechů seznámit účastníky trestního řízení, by mohlo být využito speciálních místností, kde by se oprávněné osoby mohly seznámit s obsahem odposlechů. Místnost by byla pod dohledem kamerového systému a nebylo by do ní možné vnést elektronické zařízení umožňující záznam zvuku či kopírování materiálů v listinné podobě. Přehrávaný odposlech by bylo možné dále doplnit o jedinečný „zvukový vodoznak" (a pokud by se jednalo o přepisy hovorů, byly by tyto na speciálních arších papíru), který by v případě úniku pomohl okamžitě identifikovat viníka.

Vývoj institutu odposlechů je nutný, neboť je zcela jisté, že trestná činnost pachatelů se bude v budoucnosti stále více sofistikovat a společnost se bude čím dál tím častěji setkávat se zločinci využívajícími nejmodernější techniku. Proto je nutné s pachateli trestné činnosti nejen držet krok, ale být naopak o krok dál. Začít je třeba právě v legislativní úpravě, která napomůže v práci orgánům činným v trestním řízení.

RESUMÉ

Thesis on "Legislation and evidence use wiretaps in criminal proceedings" deals with an issue that has recently sparked socio-political debate on certain paragrafových as amended Criminal Procedure Code and the Law on Electronic Communications.

Deleting these major sections (provisions) would very significantly complicate the operational work of the bodies active in criminal proceedings and in particular the Police of the Czech Republic.

Therefore, in this thesis, we discussed the various articulated amended by Act No. 127/2005 Coll. Electronic communications (§ 97 paragraph 3 and 4) of Act No. 141/1961 Coll. Criminal Procedure (§ 88, § 88a), compared the use of similar terms of operational resources in neighboring countries.

The thesis is justified by the rationale of § 88 and § 88a of the Criminal Procedure Code and § 97 paragraph 3 and 4 of Act No. 127/2005 Coll. Electronic communications. There are analyzed the particular case in which it is clear that without the use of the above sections would not be possible to demonstrate the perpetrators of crime.

Part of the work is devoted to the way it is with sensitive data, which interferes with the acquisition of personal rights of citizens by the police and treated at the same time pointed out the shortcomings regarding the protection of personal data obtained.

In this thesis points out the fact that the concerns of 51 deputies of the Parliament of the Czech Republic, whose interest was to prevent the retention of telecommunications traffic are unfounded, and their concerns about the proliferation of wiretaps deployed or increasing the frequency of requesting data on telecommunications traffic were unfounded.

SEZNAM POUŽITÉ LITERATURY

Prameny:

- ASPI [právní databáze]. Wolters Kluwer ČR, a. s.
- Zákon č. 1/1993 Sb., Ústava České republiky
- Zákon č. 2/1993 Sb., Listina základních práv a svobod
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
- Zákon č. 161/1961 Sb., trestní řád, ve znění pozdějších předpisů
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů
- Zákon č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů
- Rozsudek Ústavního soudu ze dne 23. května 2007, sp. zn. 615/06
- Rozsudek Ústavního soudu ze dne 27. září 2007, sp.zn. 789/06
- Rozsudek Nejvyššího soudu České republiky ze dne 14. dubna 2005, sp.zn. 7 Tz 196/2004
- Německý trestní řád, (Strafprozeβordung)
- Zákon č. 301/2005 Z.z., trestný poriadok
- Rakouský trestní řád, sbírka spolkových zákonů č. 631/1975 ve znění pozdějších předpisů
- Zákon o telekomunikacích, sbírka spolkových zákonů I č. 70/2003 ve znění pozdějších předpisů (Rakousko)

Literatura:

• Císařová, D., Fenyk, I., Kloučková, S.: *Trestní právo procesní,* 3. aktualizované a rozšířené vyd. Praha: Nakladatelství LINDE PRAHA a.s., 2004

• Šámal, P., a kol.: *Trestní řád, komentář*, 6. vyd. Praha: Nakladatelství C.H. Beck, rok. 2008.

Články:

• Dragoun, R.: Zákonná úprava možnosti odposlechu a záznamu telekomunikačního provozu při postihu korupce-srovnání české úpravy s úpravou zahraniční. Státní zastupitelství, 2011, č. 10

• Málek, P.: Odposlechy trochu jinak. Část 2., Bezpečnostní teorie a praxe, 2011, s. 104 – 105.

• Vantuch, P.: Zveřejňování odposlechů v mediích. Právní rádce, 2008, č.5

Ostatní:

• http://alex.onb.ac.at/cgi-content/alex?aid=rbo&datum=1873&size=45&page=417, 9.3. 2013

• Analýza odposlechů, Policejní prezidium PČR, www.mvcr.cz/soubor/analyza-odposlechu-2007-doc.aspx, 2. 3. 2013

• Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací, Policie ČR za rok 2011, zpracoval Odbor analýz Policejního prezidia PČR

• http://www.echr.coe.int/NR/rdonlyres/82E3CE7F-5D3D-46EB-8C13-4F3262F9E20B/0/CzechTch%C3%A8que.pdf, 27. 2. 2013