

PRÁVNICKÁ FAKULTA UNIVERZITY
KARLOVY V PRAZE

**Odposlech a záznam telekomunikačního
provozu**

Diplomová práce

Bc. Hana Valentová

prof. JUDr. Pavel Šámal, Ph.D.

říjen 2013

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.

V Praze.....

Podpis.....

Ráda bych tímto poděkovala panu prof. JUDr. Pavlu Šámalovi, Ph.D. za výborné vedení při psaní této diplomové práce.

Obsah

Obsah	4
Úvod.....	6
1. Historie právní úpravy odposlechu a záznamu telekomunikačního provozu podle § 88 trestního řádu a zjišťování údajů o telekomunikačním provozu podle § 88a trestního řádu.....	9
1.1 Historie právní úpravy odposlechu a záznamu telekomunikačního provozu podle § 88 trestního řádu.....	9
1.2 Historie právní úpravy zjišťování údajů o telekomunikačním provozu podle § 88a trestního řádu.....	13
2. Právní úprava odposlechu a záznamu telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu.....	20
2.1 Odposlech a záznam telekomunikačního provozu.....	20
2.1.1 <i>Podmínky pro nařízení odposlechu a záznamu telekomunikačního provozu</i> .	26
2.1.2 <i>Postup při nařízení odposlechu a záznamu telekomunikačního provozu a náležitosti příkazu</i>	30
2.1.3 <i>Provedení, průběh a ukončení odposlechu</i>	37
2.1.4 <i>Odposlech se souhlasem uživatele</i>	39
2.1.5 <i>Odposlech a záznam telekomunikačního provozu jako důkaz v trestním řízení</i>	43
2.1.6 <i>Zničení záznamu odposlechu telekomunikačního provozu</i>	48
2.1.7 <i>Informační povinnost</i>	49
2.1.8 <i>Řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu</i>	55
2.1.9 <i>Přeshraniční odposlech</i>	59
2.2 Zjišťování údajů o telekomunikačním provozu	61
2.2.1 <i>Podmínky pro nařízení zjišťování údajů o telekomunikačním provozu a náležitosti příkazu</i>	63
2.2.2 <i>Informační povinnost</i>	71

2.2.3 Řízení o přezkumu příkazu k zjištění údajů o telekomunikačním provozu	72
2.2.4 Zjišťování údajů o telekomunikačním provozu se souhlasem uživatele	74
3. Německá právní úprava	76
3.1 Monitorování telekomunikací podle § 100a a 100b StPO	76
3.2 Zjišťování provozních údajů podle § 100g StPO, opatření u mobilních telefonů podle § 100i StPO a zjišťování údajů podle § 100j StPO	86
3.3 Informační povinnost a právní ochrana.....	90
4. Odposlech a záznam telekomunikačního provozu jako zásah do zaručených práv a svobod a úniky odposlechlů	94
5. Úvahy de lege ferenda	102
Závěr	106
Seznam zkratk	110
Literatura.....	112
Interception and recording of the telecommunication operation	119
Resumé.....	119
Abstract.....	121
Klíčová slova v češtině a v angličtině.....	124

Úvod

Odposlech a záznam telekomunikačního provozu je celosvětově rozšířeným právním institutem běžně používaným při boji s kriminalitou. V českém právním řádu je upravený v zákoně č. 141/1961Sb., o trestním řízení soudním, ve znění pozdějších předpisů (dále „trestní řád“). Hlavním smyslem jeho použití je především efektivní potírání závažnějších forem kriminality, jejíž pachatelé využívají velmi sofistikované postupy pro páčání a následné zakrytí své činnosti. Je tedy jasné, že státní aparát by měl mít k dispozici srovnatelné prostředky, které by byly schopny vyrovnat se s neustálým technickým i právním vývojem a vedle toho by byly účinné při získávání informací a důkazů o takovéto ilegální činnosti.

V úzké návaznosti na odposlech a záznam telekomunikačního provozu pak existuje ještě institut zjišťování údajů o telekomunikačním provozu, který je rovněž upraven v trestním řádu a vztahují se na něj podobné podmínky jako na odposlech a záznam telekomunikačního provozu (dále „odposlech“).

Odposlech a záznam telekomunikačního provozu i zjišťování údajů o telekomunikačním provozu jsou často předmětem rozhodování soudů, které posuzují jejich soulad se základními právy a svobodami uvedenými v Listině základních práv a svobod (dále „Listina“) nebo v Úmluvě o ochraně lidských práv a základních svobod (dále „Úmluva“). Ústavní soud k tomu uvedl, že základním atributem ústavního konceptu právního státu a podmínkou jeho fungování je respekt k základním právům a svobodám jednotlivce, který je výslovně vyjádřen v čl. 1 odst. 1 ústavního zákona č. 1/1993Sb., Ústava České republiky, ve znění pozdějších předpisů (dále „Ústava“). Toto ustanovení je bází materiálně chápané právní státnosti, kterou charakterizuje respekt veřejné moci ke svobodné sféře jednotlivce vymezené základními právy a svobodami, a do této sféry veřejná moc zásadně nezasahuje, resp. zasahuje pouze v případech, které jsou odůvodněny kolizí s jinými základními právy, resp. ústavně aprobovaným a zákonem jednoznačně definovaným veřejným zájmem, a za předpokladu, že je zákonem předvídaný zásah proporcionální jak s ohledem na cíle, jichž má být dosaženo, tak s ohledem na míru krácení omezovaného základního práva či svobody. K omezení osobní integrity a soukromí osob tak ze strany veřejné moci může dojít jen zcela výjimečně, je-li to v demokratické společnosti nezbytné, nelze-li účelu sledovaného veřejným zájmem dosáhnout jinak a je-li to akceptovatelné z pohledu zákonné existence a

dodržení účinných a konkrétních záruk proti libovůli. Esenciální předpoklady spravedlivého procesu totiž vyžadují, aby byl jednotlivec vybaven dostatečnými garancemi a zárukami proti možnému zneužití pravomoci ze strany veřejné moci. Ony nezbytné záruky sestávají z odpovídající právní úpravy a z existence účinné kontroly jejich dodržování, kterou představuje především kontrola těch nejintenzivnějších zásahů do základních práv a svobod jednotlivců nezávislým a nestranným soudem.¹

Kvalitní právní úprava, s přesně a jasně stanovenými podmínkami, je vzhledem k represivní povaze těchto institutů tedy nezbytná pro jejich zavedení do právního řádu. Při úkonech s nimi spojených totiž téměř vždy dochází k zásahům do lidských práv, která jsou v České republice chráněna ústavním pořádkem a závazky vyplývajícími z mezinárodních smluv, jimiž je Česká republika vázána.² Článek 4 Listiny sice výslovně stanoví možnost omezení lidských práv a svobod, dodává k tomu však určitá kritéria. Tato omezení mohou být dána pouze zákonem, musí platit stejně pro všechny případy, které splňují stanovené podmínky, přičemž musí být šetřeno podstaty a smyslu práv a svobod, a nakonec nesmí být tato omezení zneužívána k jiným účelům, než pro které byla stanovena. A přesně v těchto intencích se musí pohybovat právní úprava odposlechu a záznamu telekomunikačního provozu i zjišťování údajů o telekomunikačním provozu.

Cílem této práce je komplexní rozbor zákonné právní úpravy, doplněný částečně podzákonnou právní úpravou obsaženou v interních normativních instrukcích (pokyny obecné povahy apod.) a judikaturou Ústavního a Nejvyššího soudu a Evropského soudu pro lidská práva, která má na vývoj těchto institutů značný vliv.

V první kapitole této práce se věnuji historii vývoje právní úpravy obou těchto institutů, zejména z pohledu těch nejdůležitějších zákonných novel a judikátů.

V druhé kapitole pak přistoupím již k samotnému rozboru právní úpravy, a to nejprve právní úpravy odposlechu a záznamu telekomunikačního provozu. Jednotlivě se věnuji podmínkám nařízení odposlechu, procesem vydávání příkazu k nařízení odposlechu a jeho náležitostmi, povinnostmi orgánů činných v trestním řízení při provádění odposlechu, možnostmi nařízení odposlechu i bez příkazu, použitím záznamu

¹ Srov. plenární náleží Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/2010, uveřejněný pod č. 52 ve svazku 60 Sbírký náleží a usnesení Ústavního soudu České republiky, vyhlášený pod č. 94/2011 Sb.

² Jedná se především o čl. 4 odst. 2, 3 a 4, čl. 7 odst. 1, čl. 10 odst. 2 a 3, čl. 12 odst. 3 a čl. 13 Listiny.

odposlechu jako důkazu v trestním řízení a ukládáním a likvidací těch záznamů, které jako důkaz v trestním řízení použity nejsou. Dále se zabývám i informační povinností orgánů činných v trestním řízení a výjimkami z ní, stejně jako řízením o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu, které na tuto informační povinnost navazuje. S tím souvisí i vyloučení soudce, který se účastnil takového řízení. Na závěr se krátce věnuji i ustanovení upravujícímu přeshraniční odposlech.

U institutu zjišťování údajů o telekomunikačním provozu, který navazuje na rozbor právní úpravy odposlechu, se rovněž zaměřím na podmínky jeho povolování, proces vydávání příkazu a jeho zákonné náležitosti, informační povinnost orgánů činných v trestním řízení, přezkumné řízení ohledně příkazu k zjišťování údajů o telekomunikačním provozu a nařízení zjišťování údajů o telekomunikačním provozu i bez příkazu.

Na českou právní úpravu navazuji v třetí kapitole rozбором základních aspektů právní úpravy německé, která je obsažena v německém trestním řádu.

Ve čtvrté kapitole se pak věnuji trochu obecnější tématice souladu institutu odposlechu s ochranou lidských práv. Tento institut je totiž často napadán právě kvůli tomu, že nepřiměřeným způsobem zasahuje do soukromé sféry jím dotčených osob. Při této příležitosti se krátce podívám i na problematiku úniků odposlechů.

V poslední, páté kapitole, pak navrhuji určité změny české právní úpravy, které by dle mého názoru vedly k jejímu zlepšení. Po této kapitole následuje závěr práce.

Základní fakta jsem zpracovávala na základě poznatků získaných zejména z odborné literatury (komentáře, učebnice trestního práva, odborné publikace) a časopiseckých článků. Problematické části právní úpravy jsem pak rozebírala na základě soudní judikatury a důvodových zpráv k jednotlivým novelám trestního řádu.

Při své práci jsem zůstala čistě na teoretické úrovni a nepoužívala jsem pro podložení svých tvrzení žádné statistické zprávy. Nejedná se tudíž o zhodnocení potřebnosti daného institutu, ale opravdu jenom o čistě právní rozbor, jehož cílem je zjistit, zdali česká právní úprava vyhovuje ústavním a evropským standardům.

Tato práce je zpracována podle právního stavu k 1. 9. 2013

1. Historie právní úpravy odposlechu a záznamu telekomunikačního provozu podle § 88 trestního řádu a zjišťování údajů o telekomunikačním provozu podle § 88a trestního řádu

Během více jak dvacetileté historie prošla úprava institutů obsažených v § 88 a 88a trestního řádu přesně deseti novelami. První novely měly za cíl zejména odstranit nedostatky prvotní právní úpravy. Dále pak reflektovaly zejména potřeby vyplývající z vývoje kriminality na našem území, praktické problémy a nakonec i vývoj české soudní judikatury a požadavky stanovené Evropským soudem pro lidská práva (dále „ESLP“). V této kapitole se chci detailněji zabírat především těmi nejdůležitějšími novelami a jejich přínosem pro zkvalitnění právní úpravy.³

1.1 Historie právní úpravy odposlechu a záznamu telekomunikačního provozu podle § 88 trestního řádu

Zpočátku byl tento institut upraven jako odposlech telefonních hovorů. Do trestního řádu jej zavedl zákon č. 178/1990 Sb., který nabyl účinnosti dne 1. 7. 1990. Podle důvodové zprávy k tomuto zákonu bylo nezbytné upravit podmínky odposlechu telefonních hovorů k účinnému postupu při odhalování a prokazování nejzávažnějších trestných činů, organizované zločinnosti přesahující rámec naší republiky, obchodu s narkotiky, spekulativního obchodu v mezinárodním měřítku, mezinárodního terorismu, jakož i pachatelů trestných činů ohrožujících ústavní základy republiky. Současně se takovou právní úpravou zajišťuje právní jistota občanů, že k odposlechu telefonních hovorů nebude docházet jen na základě volné úvahy orgánu činného v trestním řízení.⁴

Prvotní ustanovení § 88 trestního řádu obsahovalo čtyři odstavce. V prvním z nich byly vymezeny podmínky nařízení tohoto institutu. Odposlech telefonních hovorů mohl být nařízen po zahájení trestního stíhání:

- a) pro zvlášť závažný úmyslný trestný čin nebo

³ Vedle nich byly provedeny menší novely zákony č. 558/1991 Sb., č. 152/1995 Sb. a č. 41/2009 Sb.

⁴ Důvodová zpráva k návrhu zákona č. 178/1990 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Federální shromáždění Československé socialistické republiky, 1990.

b) pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva.

Nařídit jej mohl předseda senátu a v přípravném řízení prokurátor nebo s jeho souhlasem vyšetřovatel, pokud šlo důvodně předpokládat, že jím budou sděleny významné skutečnosti pro trestní řízení. Již tehdy však byl zakázán odposlech telefonních hovorů mezi obhájcem a obviněným.

Příkaz musel být vydán písemně a musel být odůvodněn. Vedle toho bylo nutnou náležitostí příkazu určení doby, po kterou byl odposlech telefonních hovorů prováděn.

Již v této prvotní úpravě bylo možné nařídit odposlech telefonních hovorů se souhlasem účastníka odposlouchávané telefonní stanice, bylo-li vedeno trestní stíhání pro jiný trestný čin, než který byl uveden v odstavci 1.

V případě použití záznamu telefonního hovoru jako důkazu bylo nutné připojit k němu protokol s uvedením údajů o místě, času, způsobu a obsahu provedeného záznamu, jakož i o osobě, která záznam pořídila. Odposlech zajišťoval orgán Sboru národní bezpečnosti.

Na základě současných poznatků je zřejmé, že toto znění neposkytovalo dostatečné záruky proti zneužití takového institutu, stejně jako nemohlo dostávat požadavkům trestního řízení, které bylo značně ovlivněno rychlým technologickým vývojem.

Zejména pak chybějící požadavek subsidiarity odposlechu telefonních hovorů uděloval orgánům činným v trestním řízení značně volné pole působnosti. V kombinaci s odstavcem 3 bylo možno odposlech dokonce použít pro jakýkoli trestný čin, což dle mého názoru mohlo vést k nadměrnému používání, až zneužívání odposlechů v trestním stíhání.

Na druhou stranu však nebylo podle tohoto znění možné využít tento institut před zahájením trestního stíhání a výsledky takto získané použít jako důkaz.⁵ Stejně tak

⁵ Pro dobu před zahájením trestního stíhání připouštěl odposlech zákon č. 283/1991 Sb., o Policii ČR, ve znění pozdějších předpisů. Soudní judikatura však vyloučila možnost použití odposlechů získaných na základě tohoto zákona jakožto důkazů v trestním řízení. Srov. *Sokol, T.* Odposlech. Státní zastupitelství, 2008, č. 3, s. 16.

nebylo možné odposlechy použít i pro jiné typy komunikací, např. fax, protože zákon stanovil možnost pouze telefonního odposlechu.

V neposlední řadě tato úprava naprosto vynechávala postup při úschově a zničení provedených záznamů.

Je tedy nasnadě, že na základě těchto nedostatků museli zákonodárci přistoupit k novelizacím, které reflektovaly jak rychlý společenský vývoj 90. let, tak i praktické problémy, které společně s používáním tohoto institutu v praxi nečekaně vyvstaly.

První větší novela byla provedena zákonem č. 292/1993 Sb., který změnil odposlech telefonních hovorů na odposlech a záznam telekomunikačního provozu, čímž byla úprava rozšířena i na obdobné případy používání telekomunikačního provozu. Rovněž, s ohledem na závažnost zásahu do osobních práv dotčených osob, svěřila tato novela rozhodování o nařízení odposlechu a záznamu telekomunikačního provozu do výlučné pravomoci soudu. Odposlech je oproti předešlé úpravě možné používat ve všech stádiích trestního řízení a byla zavedena i možnost jej uplatnit v jiné trestní věci, než byla ta, v níž byl proveden. Rovněž byl rozšířen okruh skutkových podstat, u kterých bylo možné jej uplatnit se souhlasem účastníka odposlouchávané stanice. Zákon také stanovil časové omezení provádění odposlechu na maximální dobu šesti měsíců s možností opakovaného prodloužení. Tento zákon rovněž již upravil ukládání záznamů a zničení záznamů, kterými nebyly zjištěny skutečnosti významné pro trestní řízení.

V téměř nezměněné podobě pak tato úprava vydržela až do 1. 7. 2008, kdy v účinnost vstoupila zatím nejrozsáhlejší novela provedená zákonem č. 177/2008 Sb. Jejím cílem bylo, aby odposlech nemohl být využíván jako běžný způsob získávání informací v trestním řízení na základě zavádějících informací. Podle důvodové zprávy k tomuto zákonu byla hlavním důvodem potřeba upřesnit podmínky pro povolování odposlechu dalším zvýrazněním zásady přiměřenosti a zdrženlivosti.⁶ U předešlé úpravy bylo totiž problematické, že návrhy státního zástupce bývaly nedostatečně odůvodněné, nezřídka mechanicky přejímané od policejních orgánů, a soudce při povolení odposlechu postupoval formálně, aniž by zjišťoval, zda v konkrétním případě jsou splněny zákonné předpoklady pro povolení odposlechu. Nová úprava § 88 trestního řádu tak měla přimět policejní orgány i státní zástupce ke kvalitnějšímu odůvodňování

⁶ Důvodová zpráva k návrhu zákona č. 177/2008 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Poslanecká sněmovna, 2007.

návrhů na provedení odposlechu a soudy k pečlivému zjišťování, zda návrhy jsou potřebné a důvodné a zda odposlechy doplňují již zjištěné důkazy.⁷

Další důležitou změnou oproti tehdejší úpravě bylo zavedení institutu informační povinnosti vůči osobě, u které byl nařízen odposlech její telefonní stanice s tím, že tato novela umožnila rovněž přezkoumání zákonnosti odposlechu a záznamu telekomunikačního provozu Nejvyšším soudem podle § 314l až 314n trestního řádu. Vedle toho rovněž upravila zejména vyloučení soudce z řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu, upřesnila náležitosti odůvodnění návrhu na vydání příkazu, pozměnila postup při nahrávání rozhovoru mezi obhájcem a obviněným, zkrátila dobu trvání nařízení odposlechu ze šesti měsíců na čtyři, zavedla povinnost průběžně vyhodnocovat, zda i nadále trvají důvody, které vedly k vydání příkazu, a pokud již tyto důvody netrvají a odposlech je ukončen dříve, povinnost policejního orgánu tuto skutečnost písemně oznámit předsedovi senátu, který příkaz vydal, v přípravném řízení pak soudci a státnímu zástupci. Rovněž tato novela změnila oprávněnou osobu, která může dát souhlas k odposlechu své stanice, z účastníka na uživatele. Nakonec upravila postup při zničení získaných záznamů, kterými nebyly zjištěny skutečnosti významné pro trestní řízení.

Zatím poslední větší novelu provedl zákon č. 459/2011 Sb. Tato novela navazuje především na vydání zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů (dále „trestní zákoník“), který nepřímo novelizoval i trestní řád (novela trestního řádu zákonem č. 41/2009 Sb.). Trestní zákoník totiž v § 14 odst. 3 stanovuje za zvlášť závažné zločiny ty trestné činy, které jsou úmyslné a na které trestní zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně deset let. Tato nepřímá novela tak zpřísnila podmínku pro uplatnění odposlechu, která byla až do té doby stanovena na zvlášť závažný úmyslný trestný čin. Tím byly podle § 41 odst. 2 zákona č. 140/1961 Sb., trestního zákona, ve znění pozdějších předpisů, trestné činy uvedené v § 62 tohoto zákona a ty úmyslné trestné činy, na něž zákon stanovil trest odnětí svobody s horní hranicí trestní sazby nejméně osm let.⁸

⁷ Srov. *Vantuch, P.* Nová úprava odposlechu v trestním řádu od 1. 7. 2008. *Bulletin advokacie*, 2008, č. 10, s. 29.

⁸ Původní návrh trestního zákoníku ve znění schváleném vládou vymezoval zvlášť závažné zločiny jako úmyslné trestné činy, na něž zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm

Touto změnou byl odposlech a záznam telekomunikačního provozu výrazně dotčen. Oproti předchozí právní úpravě totiž došlo k omezení počtu trestných činů, u kterých lze odposlechy nařídit a u nichž je využití odposlechů mnohdy klíčové k jejich odhalení. Zcela markantně se to projevilo zejména v okruhu trestných činů páchaných organizovaně a dále pak u majetkových deliktů, přičemž ztížení možnosti odhalovat trestné činy spojené s organizovaným zločinem se negativně projevilo i v oblasti odhalování korupčních praktik.⁹

Touto novelou se rovněž rozšířil okruh trestných činů, u nichž je možné odposlech a záznam telekomunikačního provozu využít, o taxativní výčet trestných činů, u kterých by to jinak nebylo možné, ale v rámci protikorupčního boje se jedná o významný nástroj pro odhalování korupce.

Vedle toho provedla tato novela ještě několik menších doplnění, která měla za účel odstranit nedostatky způsobené zákonem č. 177/2008 Sb. Od této doby nezaznamenala právní úprava odposlechu a záznamu telekomunikačního provozu již dalších změn.

1.2 Historie právní úpravy zjišťování údajů o telekomunikačním provozu podle § 88a trestního řádu

Tento institut byl do trestního řádu zaveden o něco později než odposlech a záznam telekomunikačního provozu. Stalo se tak zákonem č. 265/2001 Sb., který reagoval na nálezy Ústavního soudu České republiky (dále „Ústavní soud“) vydané v roce 2001 pod sp. zn. II. ÚS 502/2000, IV. ÚS 536/2000 a IV. ÚS 78/2001. Do vydání těchto nálezů se v praxi trestního řízení informace o skutečnostech, které jsou předmětem telekomunikačního tajemství nebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, vyžadovaly postupem podle § 8 odst. 1 trestního řádu s odkazem na ustanovení § 86 odst. 1 zákona č. 151/2000 Sb., o telekomunikacích a o změně

let. V Poslanecké sněmovně Parlamentu ČR však došlo ke změně vymezení zvlášť závažných zločinů v návaznosti na nové vymezení přečinů tak, že hranice trestní sazby byla u zvlášť závažných zločinů posunuta z osmi na deset let. Důvodová zpráva k návrhu zákona č. 459/2011 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Poslanecká sněmovna, 2007.

⁹ Důvodová zpráva k návrhu zákona č. 459/2011 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Poslanecká sněmovna, 2007.

dalších zákonů, ve znění pozdějších předpisů (dále „zákon o telekomunikacích“), tj. bez souhlasu soudce. Bylo vycházeno z názoru, že při získávání údajů o uskutečněném telekomunikačním provozu nelze postupovat podle ustanovení § 88 trestního řádu, které upravuje odposlech a záznam telekomunikačního provozu, neboť takovýto postup je prostředkem k získání obsahu takto dopravovaných zpráv, nikoli k získání údajů o uživatelích telekomunikačních služeb ve smyslu § 86 odst. 1 zákona o telekomunikacích.¹⁰ Výše zmiňované nálezy tak tuto praxi změnily a stanovily, že orgány činné v trestním řízení, resp. policejní orgány před zahájením trestního stíhání, jsou v případě pořizování či získávání evidence telekomunikačního provozu povinny postupovat přiměřeně podle § 88 trestního řádu, resp. podle § 36 zákona č. 283/1991 Sb., o Policii ČR, ve znění pozdějších předpisů, s tím, že pojem „záznam“ se vztahuje také na údaje získané evidováním telekomunikačního provozu ve vztahu ke konkrétní osobě nebo osobám.¹¹

Tyto nálezy vycházely z toho, že čl. 13 Listiny nezakládá pouze ochranu tajemství vlastního obsahu zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením, ale i dalších údajů evidovaných při registraci telekomunikačního provozu ve vztahu ke konkrétním osobám.¹² Takovými údaji jsou volaná čísla, datum a čas hovoru, doba trvání hovoru a v případě mobilní telefonie údaj o základových stanicích zajišťujících hovor. V nálezu sp. zn. II. ÚS 502/2000 pak Ústavní soud vyjádřil názor, že pokud jsou stanovena pravidla pro odposlech a záznam telekomunikačního provozu ze strany státních orgánů, která umožňují kromě dalších údajů pořídit především obsah telefonické zprávy, je možné postupovat podle těchto pravidel i při pořizování či získávání těchto „dalších“ údajů. Touto ústavně konformní interpretací lze dosáhnout účinné kontroly před neoprávněnými zásahy do daného základního práva ze strany státních orgánů a současně nebude vyloučena pro tyto orgány možnost pořizovat nepochybně často nezbytný typ důkazů pro plnění svých

¹⁰ Usnesení Ústavního soudu ze dne 18. 12. 2002, sp. zn. II. ÚS 616/01.

¹¹ Nález Ústavního soudu ze dne 13. 2. 2001, sp. zn. IV. ÚS 536/2000, uveřejněný pod č. 29 ve svazku 21 Sbírký nálezů a usnesení Ústavního soudu České republiky.

¹² Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1224.

funkcí, a to případně do doby přijetí specifické právní úpravy ohledně pořizování těchto údajů.¹³

Následně byl tedy zaveden § 88a trestního řádu, nazvaný poskytování údajů o uskutečněném telekomunikačním provozu, který stanovil povinnost právnické nebo fyzické osoby, která vykonává telekomunikační činnost, aby na příkaz předsedy senátu nebo v přípravném řízení soudce sdělila údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat.

Úprava v tomto znění vydržela více jak desetiletí až do roku 2011, kdy byly vydány další dva zásadní nálezy Ústavního soudu pod sp. zn. Pl. ÚS 24/2010 a Pl. ÚS 24/2011.

První zmiňovaný náleze se nezaměřoval přímo na trestní řád, ale na úpravu ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále „zákon o elektronických komunikacích“), a na vyhlášku č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, přičemž oba tyto právní předpisy byly tímto náleze zrušeny. Podstatou námitek proti těmto právním předpisům bylo, 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.¹⁴

Navíc jsou tyto údaje uchovávány bez existence konkrétního podezření. Optikou napadených ustanovení je tak každá osoba považována za podezřelou bez existence konkrétních okolností, které by toto podezření odůvodňovaly. Ve vztahu k § 88a

¹³ Srov. náleze Ústavního soudu ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000, uveřejněný pod č. 11 ve svazku 21 Sbirky nálezů a usnesení Ústavního soudu České republiky.

¹⁴ Srov. plenární náleze Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/2010, uveřejněný pod č. 52 ve svazku 60 Sbirky nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 94/2011 Sb.

trestního řádu pak Ústavní soud uvedl, že sběr a uchovávání lokalizačních a provozních údajů tak rovněž představuje významný zásah do práva na soukromí, a z toho důvodu je nezbytné pod rozsah ochrany základního práva na respektování soukromého života v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny) zahrnout nejen ochranu vlastního obsahu zpráv podávaných prostřednictvím telefonní komunikace či komunikace prostřednictvím tzv. veřejných sítí, ale i provozní a lokalizační údaje o nich. Zejména pak citované ustanovení § 88a trestního řádu upravující podmínky použití uchovávaných údajů o uskutečněném telekomunikačním provozu pro účely trestního řízení dle názoru Ústavního soudu výše předestřené ústavněprávní limity a požadavky zdaleka nerespektuje.¹⁵

Ústavní soud na závěr svého nálezu apeloval na zákonodárce, aby změnil § 88a trestního řádu, ten tomu tak ale neučinil, což vedlo k vydání druhého zmiňovaného nálezu Pl. ÚS 24/2011, kterým bylo toto ustanovení zrušeno ke dni 30. září 2012.

V tomto nálezu podal návrh na zrušení § 88a trestního řádu Obvodní soud pro Prahu 6. Argumentoval tím, že toto ustanovení neobsahuje dostatečné garance práv uživatelů služeb elektronických komunikací, jež by byly srovnatelné s těmi, které pro případ nařízení odposlechu a záznamu telekomunikačního provozu předpokládá § 88 trestního řádu. Konkrétně pak Ústavní soud v nálezu zdůrazňuje, že přístup orgánu veřejné moci k těmto údajům bez souhlasu uživatelů těchto služeb se vzhledem k možnosti dovést z nich informace o místě, čase, účastnících a způsobu jejich komunikace bezprostředně a citelně dotýká jejich práva na informační sebeurčení, neboť je v tomto rozsahu zbavuje možnosti, aby sami rozhodli, zda tyto informace zpřístupní jiným osobám. Tato skutečnost sice nevylučuje přípustnost takového zásahu, musí však pro něj být splněny podmínky vyplývající z ústavního pořádku. Jde tedy o to, zda napadené ustanovení poskytuje z hlediska základního práva na informační sebeurčení dostatečné garance proti zneužití předmětných údajů během celého trvání trestního řízení. Těmito garancemi je přitom třeba rozumět jak stanovení podmínek, za nichž mají mít příslušné orgány přístup k údajům o uskutečněném telekomunikačním

¹⁵ Srov. plenární nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/2010, uveřejněný pod č. 52 ve svazku 60 Sbirky nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 94/2011 Sb.

provozu, tak i existenci účinné kontroly jejich dodržování.¹⁶

A právě nedostatečnost takovýchto garancí byla napadené úpravě vytýkána. Jedinou podmínkou pro nařízení sdělení údajů o uskutečněném telekomunikačním provozu v tehdejší úpravě bylo, že takovéto opatření musí sledovat účel „*objasnění skutečností důležitých pro trestní řízení*“. Ústavní soud měl za to, že tímto způsobem upravené meze základního práva na informační sebeurčení jsou formulovány velmi široce a neurčitě a ve své podstatě umožňují vyžádání a použití předmětných údajů ze strany orgánu činného v trestním řízení pokaždé, je-li jim možné přiznat nějakou souvislost s probíhajícím trestním řízením. Zároveň upozorňuje na to, že podle takové úpravy je sice možné korigovat sdělení údajů o uskutečněném telekomunikačním provozu na úrovni orgánů činných v trestním řízení, které mají povinnost aplikovat podústavní právní předpisy v souladu s ústavním pořádkem, a tudíž i s ohledem na dodržování práv zaručených v Listině, zároveň ale dodává, že takový postup není v souladu ani s čl. 4 odst. 2 Listiny, podle něhož lze meze základních práv a svobod stanovit pouze zákonem, ani s požadavkem právní jistoty. Podle Ústavního soudu nemůže být oprávnění orgánů činných v trestním řízení zjistit údaje o tom, s kým a jak často určitá osoba komunikuje a z jakého místa a jakými prostředky tak činí, vzhledem k intenzitě, se kterou zasahuje do tohoto základního práva, považována za obvyklý nebo rutinní prostředek prevence a odhalování trestné činnosti, nýbrž k jejímu užití může dojít pouze tehdy, pokud pro dosažení tohoto účelu nebude existovat jiný a ve vztahu k tomuto základnímu právu šetrnější postup. Vedle toho byla napadené úpravě rovněž vytýkána naprostá absence úpravy dalšího nakládání s těmito údaji ze strany orgánů činných v trestním řízení, která by zahrnovala minimální požadavky na zabezpečení uchovávaných údajů, které by zaručovaly, že nedojde k jejich využití k jiným než zákonem stanoveným účelům (zamezení přístupu třetích osob, stanovení ochrany celistvosti a důvěrnosti těchto údajů, stanovení procedury jejich ničení). Rovněž byla napadena absence povinnosti dodatečně informovat osobu uživatele služeb elektronické komunikace o tom, že jí týkající se provozní a lokalizační údaje byly sděleny orgánům

¹⁶ Srov. plenární náleží Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/2011, uveřejněný pod č. 217 ve svazku 63 Sbírký náleží a usnesení Ústavního soudu České republiky, vyhlášený pod č. 43/2012 Sb.

činným v trestním řízení, a absence právního prostředku, který by umožňoval soudní přezkum postupu při získávání a nakládání s předmětnými údaji. Ústavní soud rovněž navrhl upravit podrobnější pravidla pro obsah příkazu ke sdělení údajů o uskutečněném telekomunikačním provozu a formální náležitosti pro samotnou žádost orgánu činného v trestním řízení. Jejich smyslem by bylo přitom zabezpečit, že soudce bude při svém rozhodování disponovat všemi potřebnými informacemi. V neposlední řadě rovněž Ústavní soud dané úpravě vytýká, že v ní není určeno, při stíhání kterých trestných činů je možné sdělení údajů o telekomunikačním provozu nařídit, z čehož vyplývá, že je to možné pro všechny trestné činy bez ohledu na požadavek proporcionality zásahu do základního práva s ohledem na sledovaný účel.¹⁷

Za zmínku stojí ještě odlišné stanovisko soudkyně Ivany Janů, která upozorňuje na fakt, že Ústavní soud se ve své rozhodovací praxi řídí dlouhodobě zásadou priority ústavně konformní interpretace před derogací. Ustanovení § 88a trestního řádu je pak podle ní nutné aplikovat v souladu s omezeními stanovenými v § 88 trestního řádu. Soudkyně mimo jiné uvádí, že hodnocení provedené plénem není provedeno abstraktně – v rovině objektivní možnosti či nemožnosti ústavně konformní interpretace -, nýbrž ve světle konkrétních (statistických) indicií rekapitulovaných v nálezu sp. zn. Pl. ÚS 24/2010; ty však nevyplývají z právní nemožnosti ústavně konformní interpretace napadeného ustanovení, nýbrž z „nevůle“ orgánů činných v trestním řízení, včetně obecných soudů, Ústavním soudem předložený ústavně konformní výklad respektovat.¹⁸ Derogace ustanovení § 88a trestního řádu tak podle ní nahrazuje správnou aplikaci tohoto ustanovení orgány činnými v trestním řízení a do budoucna nezamezí nadužívání tohoto institutu v rutinní praxi těchto orgánů.

Pro úplnost je rovněž nutné dodat, že Ústavní soud současně s § 88a odst. 1 trestního řádu zrušil i odstavec 2, který by se jinak stal obsoletním.

V návaznosti na tato rozhodnutí došlo k zatím poslední novele tohoto institutu,

¹⁷ Srov. plenární nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/2011, uveřejněný pod č. 217 ve svazku 63 Sbírký nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 43/2012 Sb.

¹⁸ Plenární nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/2011, uveřejněný pod č. 217 ve svazku 63 Sbírký nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 43/2012 Sb.

která byla provedena zákonem č. 273/2012 Sb. s účinností od 1. 10. 2012. Tato novela zavedla do trestního řádu úplně nový § 88a, jehož podmínky jsou oproti předchozí úpravě stanoveny značně restriktivně. Toto ustanovení zároveň zavedlo nově informační povinnost orgánů činných v trestním řízení a na ní navazující možnost zahájení přezkumného řízení k příkazu ke zjištění údajů o telekomunikačním provozu.

2. Právní úprava odposlechu a záznamu telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu

Instituty odposlechu a záznamu telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu jsou upraveny v části první „*Společná ustanovení*“, hlavě čtvrté „*Zajištění osob, věcí a jiných majetkových hodnot*“, oddílu šestém trestního řádu, čímž systematicky spadají mezi zajišťovací instituty.¹⁹

2.1 Odposlech a záznam telekomunikačního provozu

Úprava odposlechu a záznamu telekomunikačního provozu v současné době čítá devět obsáhlých odstavců, přičemž je možné, že v budoucnu bude následovat ještě jejich rozšíření.

Podle definice je odposlech záměrné a utajené a současné vnímání obsahu komunikace zprostředkované telekomunikačními zařízeními nebo sítěmi prostřednictvím k tomu určených zařízení. Záznamem pak je souběžné zachycení obsahu komunikace na nosičích záznamu umožňujících jejich uchování a reprodukci. Odposlech a záznam telekomunikačního provozu se provádí připojením zařízení pro odposlouchávání a zaznamenávání telekomunikačního provozu v určených bodech telekomunikační sítě.²⁰

Z této definice tak vyplývá, že odposlech se týká především zjišťování vlastního obsahu zpráv, přičemž je zaměřen na telekomunikační provoz, který aktuálně probíhá nebo bude probíhat v budoucnosti. Navíc z něj však lze i zjistit informaci o tom, které účastnické stanice mezi sebou komunikují, a umožňuje identifikaci komunikujících

¹⁹ Odposlech a záznam telekomunikačního provozu mimo podmínky stanovené trestním řádem je možný podle zákona č. 154/1994 Sb., o Bezpečnostní informační službě, podle zákona č. 289/2005 Sb., o Vojenském zpravodajství nebo podle zákona č. 169/1999 Sb., o výkonu trestu odnětí svobody, pokud se týká odposlechu odsouzených ve výkonu trestu odnětí svobody. Ve všech těchto případech je odposlech operativně pátrací metodou provedenou podle jiného předpisu než trestního řádu. Záznam o odposlechu v takových případech však nelze použít jako důkaz v trestním řízení. Takový záznam má pouze operativní hodnotu a může případně sloužit pouze jako východisko pro další šetření. *Jelínek, J. a kol. Trestní zákoník a trestní řád s poznámkami a judikaturou. 2. aktualiz. vyd. podle stavu k 1. 12. 2011. Praha: Leges, 2011, s. 662.*

²⁰ *Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007, s. 363.*

osob a údajů o době a délce odposlouchávaného a zaznamenávaného spojení.²¹ Umožňuje tak získávání jak informací operativního rázu, nutných pro další postup v trestním řízení, tak i nezbytných důkazů použitelných při samotném jednání před soudem.

Zákon o elektronických komunikacích v § 136 odst. 20 písm. a) definuje telekomunikační provoz jako přenášenou zprávu podle tohoto zákona. Zprávou se rozumí jakákoli informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné služby elektronických komunikací (srov. § 89 odst. 2 zákona o elektronických komunikacích). K přenosu zprávy může dojít pomocí telefonu, telefaxu, dálnopisu, mobilního telefonu, vysílačky, elektronickými prostředky telekomunikace a jinými telekomunikačními zařízeními, včetně zasílání zpráv elektronickou poštou.²² Sporné je, jak pohlížet na e-mailovou zprávu po jejím vytištění prostřednictvím tiskárny připojené k počítači. Podle některých názorů jde v tomto případě o zásilku ve smyslu § 87c trestního řádu, avšak podle názoru uvedeného v komentáři trestního řádu se jedná podobně jako u vytištěné faxové zprávy o součást telekomunikačního provozu, jehož výsledek zachycený v listinné podobě, jde-li o věc důležitou pro trestní řízení, lze vyžádat podle § 78 trestního řádu nebo jde odejmout podle § 79 trestního řádu, podobně jako doručený dopis, balík či jinou zásilku.²³

Podle zákona je možné odposlech použít „*je-li vedeno trestní řízení*“, přičemž trestním řízením je podle § 12 odst. 10 trestního řádu jakékoli řízení podle trestního řádu, takže není omezeno na konkrétní stádium trestního řízení. Toto ustanovení se rovněž uplatňuje v řízení v trestních věcech mladistvých, neboť zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů, ve znění pozdějších předpisů (dále „zákon o soudnictví ve věcech mládeže“), nemá speciální ustanovení, které by použití tohoto institutu upravovalo. Stejně tak se aplikuje v trestním řízení proti právnickým osobám, přičemž

²¹ Srov. Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007, s. 364.

²² Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007, s. 362.

²³ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1198.

skutkové podstaty příslušných trestných činů, o které se má v konkrétní věci jednat, musí spadat pod vymezení jak v § 88 odst. 1 a 5 trestního řádu, tak i v § 7 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů (dále „zákon o trestní odpovědnosti právnických osob“).

Přesto se odposlech v praxi používá převážně v přípravném řízení. Nakládání s odposlechem a záznamem telekomunikačního provozu v tomto stádiu trestního řízení se realizuje zpravidla ve třech fázích:

- 1) první fáze zahrnuje přípravu úkonu, podání návrhu soudci, eventuální vydání příkazu a jeho bezprostřední provedení (započetí realizace odposlechu příslušným policejním útvarem), přičemž v této fázi se s odposlechem nakládá jako s utajovanou informací, stupně utajení „Vyhrazené“ nebo „Důvěrné“,
- 2) ve druhé fázi dochází k samotnému provádění odposlechu až do jeho skončení včetně průběžného vyhodnocování jeho výsledků (i v této fázi může odposlech podléhat utajení, utajena zůstává sama o sobě skutečnost, že je prováděn),
- 3) třetí fáze se týká konečného vyhodnocení výsledků a rozhodování o dalším postupu z hlediska jeho využitelnosti (v této fázi již většinou obsah tohoto úkonu není utajován).^{24, 25}

Podle definice uvedené v § 12 odst. 10 trestního řádu je přípravné řízení zahájeno sepsáním záznamu o zahájení úkonů trestního řízení, provedením neodkladných a neopakovatelných úkonů nebo zahájením trestního stíhání.

Za určitých podmínek může být právě i odposlech a záznam telekomunikačního provozu proveden jako neodkladný úkon podle § 160 odst. 4 trestního řádu, což je úkon, který vzhledem k nebezpečí jeho zmaření, zničení nebo ztráty důkazu nesnese z hlediska účelu trestního řízení odkladu na dobu, než bude zahájeno trestní stíhání.

²⁴ V první fázi nepřichází v úvahu, že by se obhajoba mohla s výsledkem úkonu podrobněji seznámit, ve druhé fázi (vyšetřování) není zcela vyloučeno, že obviněnému je předložena část záznamu k vyjádření. Ve třetí fázi, zejména bylo-li již vyšetřování uznáno za skončené a probíhá prostudování spisu podle § 166 trestního řádu, má obviněný a jeho obhájce právo seznámit se s obsahem tohoto úkonu, který má sloužit jako důkaz, a vyjádřit se k němu. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1199.

²⁵ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1198-1199.

Pokud by totiž takový úkon byl proveden jako běžný, jednalo by se o vybočení z mezí ústavnosti. V protokolu o provedení tohoto úkonu je třeba uvést, na základě jakých skutečností byl úkon za neodkladný považován.²⁶ Obsah tohoto úkonu je možné použít rovněž jako důkaz v trestním řízení.²⁷ Nelze jej však považovat za neodkladný úkon, kterým by bylo možné zahájit trestní řízení, neboť trestní řízení musí být již zahájeno. Proto nelze povolit odposlech a záznam telekomunikačního provozu s odůvodněním, že teprve odposlechem budou zjištěny skutečnosti nasvědčující tomu, že byl spáchán trestný čin.²⁸

Odposlech lze rovněž nařídit, resp. prodloužit, i v řízení před soudem, což je možné uplatnit např. v řízení proti uprchlému.

Podle nově vydaného stanoviska Nejvyššího soudu je možné výjimečně nařídit a provést odposlech a záznam telekomunikačního provozu i ve vykonávacím řízení v souvislosti s pátráním po odsouzených, kteří mají nastoupit výkon trestu odnětí svobody uložený za některý z trestných činů uvedených v § 88 odst. 1 trestního řádu. To je ovšem přípustné jen za předpokladu, že zjištění pobytu odsouzeného a jeho dodání do výkonu trestu odnětí svobody není možno dosáhnout jinak nebo by to bylo jinak podstatně ztížené. Zákonnost příkazu k odposlechu a záznamu telekomunikačního provozu lze i v tomto případě přezkoumat postupem za analogického užití ustanovení § 88 odst. 8, 9 a § 314l až § 314n trestního řádu.²⁹

Nejvyšší soud tak vyřešil otázku, ve které jinak panovala nejednotná soudní praxe. V rámci připomínkového řízení však s tímto stanoviskem vyjádřily kromě Ministerstva spravedlnosti nesouhlas všechny z dotázaných institucí a jeho přijetí nedoporučily. Podle názoru těchto institucí (Vrchní soud v Praze, Krajský soud v Praze a Právnická fakulta Univerzity Karlovy v Praze) návrh nepřípustně rozšířil možnost zásahu do ústavně chráněných práv zejména osob, které se nijak nepodílejí na trestním řízení. Rovněž byl kritizován postup Nejvyššího soudu, který vycházel zejména z jazykového výkladu ustanovení § 88 odst. 1. Nakonec bylo vytčeno i nedostatečné

²⁶ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1206.

²⁷ Srov. Jelínek, J. a kol. Trestní zákoník a trestní řád s poznámkami a judikaturou. 2. aktualiz. vyd. podle stavu k 1. 12. 2011. Praha: Leges, 2011, s. 661.

²⁸ Souček, J. Odposlech a záznam telekomunikačního provozu. Státní zastupitelství, 2008, č. 3, s. 26.

²⁹ Stanovisko Nejvyššího soudu ze dne 5. 6. 2013, sp. zn. Tpjn 304/2012.

zahrnutí podmínek, které stanoví zákon pro povolení a provádění odposlechu do stanoviska.³⁰

Nejvyšší soud naproti tomu argumentoval zejména výše zmíněným gramatickým výkladem ustanovení § 88 odst. 1 trestního řádu, které umožňuje použití odposlechu právě „*je-li vedeno trestní řízení*“, přičemž trestním řízením se rozumí i řízení vykonávací. Rovněž jeho účel spočívající v tom, že lze důvodně předpokládat, že jím budou získány skutečnosti významné pro trestní řízení, je podle něj zachován, protože skutečnostmi významnými pro trestní řízení v uvedeném smyslu mohou být jakékoli skutečnosti, které jsou nezbytné k zajištění řádného průběhu celého trestního řízení podle zákona a k dosažení jeho účelu. Ve smyslu § 1 odst. 1 trestního řádu je pak účelem trestního řízení nepochybně i včasný výkon uložených trestů.³¹

Navíc podle Nejvyššího soudu nedojde ke zneužívání tohoto institutu, protože u většiny soudů není odposlech a záznam telekomunikačního provozu ve vykonávacím řízení využíván vůbec, a pokud dojde k jeho nařízení, jedná se o zcela výjimečné opatření, které se používá pouze v ojedinělých případech. Ostatně ve stanovisku je uvedeno, že odposlech je možné nařídit podle § 88 odst. 1 a 2, tudíž jsou zachovány zákonné podmínky pro jeho nařízení, a tato procedura se tudíž neliší od jakéhokoliv jiného použití tohoto institutu v jiném stádiu trestního řízení. I ve vykonávacím řízení tak může vydat příkaz k odposlechu a záznamu telekomunikačního provozu jen předseda senátu soudu prvního stupně, který je příslušný k výkonu rozhodnutí, jímž byl uložen trest odnětí svobody (§ 315 odst. 1, 3 trestního řádu), jde-li o výkon trestu odnětí svobody uloženého za některý z trestných činů vyjmenovaných v ustanovení § 88 odst. 1 trestního řádu, byť se popřípadě jedná o úhrnný nebo souhrnný trest. Zároveň musí být dodržena subsidiární povaha tohoto institutu, proto dříve než případně dojde k nařízení odposlechu a záznamu telekomunikačního provozu, je nezbytné využít všechny ostatní obvyklé a dostupné možnosti k vypátrání pobytu odsouzeného a k jeho dodání do výkonu uloženého trestu odnětí svobody. Rovněž je třeba omezit trvání odposlechu a záznamu telekomunikačního provozu jen na nezbytně nutnou dobu, tj. nejpozději do zjištění pobytu odsouzeného, neodpadne-li jeho důvod již dříve (např. po dodatečném prominutí trestu odnětí svobody, po zrušení výroku o jeho uložení v řízení o

³⁰ Srov. stanovisko Nejvyššího soudu ze dne 5. 6. 2013, sp. zn. Tpjn 304/2012.

³¹ Srov. stanovisko Nejvyššího soudu ze dne 5. 6. 2013, sp. zn. Tpjn 304/2012.

mimořádném opravném prostředku apod.). Samozřejmě se zde uplatní i ostatní obecná pravidla stanovená pro nařízení a provádění odposlechu podle § 88 trestního řádu včetně vydání písemného a náležitě odůvodněného příkazu, respektování zákazu odposlechu a záznamu komunikace mezi odsouzeným a jeho obhájcem, časového limitu odposlechu, možnosti jeho prodloužení a povinností policejního orgánu průběžně vyhodnocovat důvody jeho trvání.³²

Stejně tak je zachována i přezkumná činnost Nejvyššího soudu, přestože ustanovení § 88 odst. 8 trestního řádu předpokládá, že informaci o nařízeném odposlechu a záznamu telekomunikačního provozu podá předseda senátu soudu prvního stupně „*po pravomocném skončení věci*“. V případě jeho nařízení v situacích řešených tímto stanoviskem by se tak stalo po dosažení účelu odposlechu a záznamu telekomunikačního provozu, tedy zpravidla poté, co odsouzený nastoupil k výkonu trestu odnětí svobody, resp. byl do něj dodán, pokud by z jiných důvodů nebylo třeba informovat o odposlechu a záznamu telekomunikačního provozu v odlišnou dobu (např. po dodatečném prominutí trestu odnětí svobody, po zrušení výroku o jeho uložení v řízení o mimořádném opravném prostředku apod.).³³

Toto stanovisko mi nepřipadá jako nepřipustný extenzivní výklad § 88 trestního řádu. Právě naopak nevidím problém v tom, že by měl být odposlech použit i v rámci vykonávacího řízení. Vždyť intenzita zásahu do práv a svobod je stejná bez ohledu na to, ve které fázi trestního řízení je odposlech prováděn.

Nedostatečné zahrnutí podmínek pro povolení a provádění odposlechu, které bylo stanovisku vytýkáno v rámci připomínkového řízení, pak vyplývá z povahy samotného stanoviska. Jeho účelem je totiž zodpovědět stanovenou otázku, nikoli podávat komplexní právní výklad. Vzhledem k tomu, že otázka směřovala na možnost vydání příkazu ve vykonávacím řízení podle § 88 odst. 1 a 2 trestního řádu, bylo by zahrnutí ostatních podmínek do stanoviska jeho nepřipustným rozšířením. Nelze tudíž Nejvyššímu soudu vytýkat, že tyto podmínky do stanoviska nezahrnul. Proto i v tomto ohledu mi přijde stanovisko jako dostatečné.

³² Srov. stanovisko Nejvyššího soudu ze dne 5. 6. 2013, sp. zn. Tpjn 304/2012.

³³ Srov. stanovisko Nejvyššího soudu ze dne 5. 6. 2013, sp. zn. Tpjn 304/2012.

2.1.1 Podmínky pro nařízení odposlechu a záznamu telekomunikačního provozu

Podmínky pro nařízení odposlechu a záznamu telekomunikačního provozu jsou upraveny v § 88 odst. 1 trestního řádu.

Podle tohoto ustanovení je odposlech a záznam telekomunikačního provozu možno použít, je-li vedeno trestní řízení pro:

- a) zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, nebo
- b) pro trestný čin pletichy v insolvenčním řízení podle § 226 trestního zákoníku, porušení předpisů o pravidlech hospodářské soutěže podle § 248 odst. 1 písm. e) a odst. 2 až 4 trestního zákoníku, sjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě podle § 256 trestního zákoníku, pletichy při zadání veřejné zakázky a při veřejné soutěži podle § 257 trestního zákoníku, pletichy při veřejné dražbě podle § 258 trestního zákoníku, zneužití pravomoci úřední osoby podle § 329 trestního zákoníku, nebo
- c) pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva.

Ad a) Vymezení pojmu zločin je nutno vykládat podle ustanovení § 14 odst. 3 věty před středníkem trestního zákoníku v návaznosti na konkrétní sazby trestu odnětí svobody stanovené na určitý trestný čin. Tato podmínka se uplatní i v případech, kdy je konáno společné řízení o fyzické a právnické osobě.

Ad b) Tento taxativní výčet uvádí trestné činy, které spadají pod vymezení korupce (viz výše).³⁴

Ad c) Je nepochybné, že první dva body splňují kritéria přesnosti a jasnosti právní úpravy, u třetího bodu již tomu tak ale není. Vzhledem k neustále narůstajícímu počtu mezinárodních smluv totiž vede takovéto znění k neurčitosti. Není totiž přesně možné stanovit, které trestné činy mohou být

³⁴ Trestné činy přijetí úplatku (§ 331 trestního zákoníku), podplácení (§ 332 trestního zákoníku) a nepřímého úplatkářství (§ 333 trestního zákoníku) ve výčtu zahrnutý nejsou, protože tyto trestné činy obvykle spadají pod bod a) nebo c).

takovouto mezinárodní smlouvou zahrnutý. Pojem jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, totiž nemůže být vykládán tak, že jde jen o trestné činy, u kterých ke stíhání zavazuje přímo či bezprostředně vyhlášená mezinárodní smlouva, neboť v takovém případě by byl jejich okruh jen velmi omezený. Nepochybně jde totiž i o všechny trestné činy, které mají podklad v mezinárodních smlouvách, popř. na takové mezinárodní smlouvy navazují, jež obsahují závazek pro státy, jako jejich smluvní strany, stíhat nebo postihovat některá jednání ve skutkových podstatách těchto trestných činů popsaných, i když konkrétní vnitrostátní postih se zásadně provádí podle skutkových podstat trestných činů, které jsou součástí našeho právního řádu.³⁵

Toto ustanovení se vztahuje na celý průběh trestního řízení (nikoli pouze k okamžiku např. zahájení trestního řízení), tudíž pokud v kterékoli fázi trestního řízení vznikne podezření, že byl spáchán jeden z uvedených trestných činů a je tedy nutno mít za to, že pro takový čin bylo řízení vedeno, mohou orgány činné v trestním řízení odposlech nařídit. Na této skutečnosti nic nemění ani okolnost, že spáchání takového činu se v procesu dokazování neprokázalo a v dalším průběhu řízení byla použita mírnější právní kvalifikace trestného činu.³⁶

Další podmínkou, kterou zákon vymezil, kdy a za jakým účelem je možno odposlech použít, je uplatnění zásady subsidiarity, která má zajistit, aby docházelo k co nejmenším zásahům do garantovaných práv a svobod. Odposlech lze tedy použít *„pokud lze důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztíženo“*, čímž je tento institut zároveň v souladu se zásadou přiměřenosti a zdrženlivost vymezenou v § 2 odst. 4 trestního řádu. Při nařízení odposlechu a záznamu telekomunikačního provozu a jeho vlastním provádění tedy musí být zváženo, zda získání konkrétních významných skutečností pro trestní řízení nelze zajistit a posléze dokazovat i jinými důkazními prostředky uvedenými v trestním řádu.³⁷

³⁵ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1200-1201.

³⁶ Srov. usnesení Nejvyššího soudu ze dne 13. 4. 2011, sp. zn. 4 Pzo 2/2010.

³⁷ Výslech obviněného nebo svědka apod.

Z tohoto hlediska bude potřebné vycházet i ze zásady rychlosti trestního řízení (§ 2 odst. 4 trestního řádu) a hospodárnosti i efektivnosti provádění úkonů v trestním řízení.³⁸ Skutečnostmi významnými pro trestní řízení jsou zpravidla především skutečnosti naznačené v § 89 odst. 1 písm. a) až c) trestního řádu, za podmínky, že jsou pro trestní řízení závažné. Podstatné okolnosti umožňující stanovení následku a výše škody způsobené trestným činem [§ 89 odst. 1 písm. e) trestního řádu] budou významnými skutečnostmi ve smyslu tohoto ustanovení u těch trestných činů, kde následek, resp. účinek, nebo výše způsobené škody jsou znakem konkrétní skutkové podstaty trestného činu nebo okolností podmiňujících použití vyšší trestní sazby.³⁹

Důvodný předpoklad dosažení účelu odposlechu je pak možno vyvodit např. z povahy trestné činnosti, která vyžaduje častou komunikaci pachatele, ale i ze samotného faktu, že podezřelý velmi často komunikuje s dalšími podezřelými osobami.⁴⁰

Provedení odposlechu má však i zákonná omezení ohledně odposlouchávaných osob. Podle třetí věty odstavce 1 je odposlech nepřipustný na stanici obhájce ve vztahu k obviněnému, kterého obhájí. Nemůže být proto ani nařízen (jestliže by byl státním zástupcem podán návrh na takový odposlech, musí být soudcem zamítnut). Pokud je odposloucháván telekomunikační provoz na stanici obviněného a je policejním orgánem zjištěno, že je nebo byl zaznamenáván rozhovor s jeho obhájcem, je povinností tohoto orgánu záznam o odposlechu bezodkladně (tedy ihned) zničit. Přitom je nepřipustné informace, které se v této souvislosti dozvěděl, použít v jakémkoliv směru a k jakémukoliv účelu.⁴¹ Takový záznam pak nelze použít jako důkaz, neboť by se jednalo o důkaz nezákonný a absolutně neúčinný.⁴² O zničení záznamu odposlechu telekomunikačního provozu mezi obhájcem a obviněným je třeba sepsat protokol, který

³⁸ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1205.

³⁹ Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 1224.

⁴⁰ Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007, s. 364.

⁴¹ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1206.

⁴² Srov. Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007, s. 365.

se zakládá do trestního spisu.⁴³ Podle přesvědčení Ústavního soudu smysl současné právní úpravy spočívá v tom, aby orgány činné v trestním řízení nebyly protiprávně získanými informacemi, které přirozeně nemají a nemohou mít povahu ani podpůrného důkazu, procesně nepřipustným způsobem ovlivňovány. Jinak řečeno při střetu dvou zájmů, a to ústavně chráněného tajemství dopravovaných zpráv a veřejného zájmu na potírání trestné činnosti, je třeba dát přednost prvně zmíněnému před účelem trestního řízení. Důsledkem toho ovšem je, že jakýkoli záznam, dotýkající se ústavně chráněného tajemství, nesmí být prováděn nebo protokolárně podchycen (§ 88 odst. 6 trestního řádu), a to ani pouhým sdělením, že k ústavně chráněné komunikaci vůbec došlo. Proto také zařazení magnetofonových nahrávek nebo písemných sdělení o nich (bez ohledu na jejich formu nebo obsah) do trestního spisu je nejen zákonně, ale i ústavně zcela nepřipustné. Jestliže takovýto protizákonný a protiústavní stav soud trpí, a to bez ohledu na fakt, že k informacím získaným protiprávním odposlechem nezamýšlí ve svém dalším procesním postupu jakkoli přihlídnout, jedná se podle Ústavního soudu o jiný zásah veřejné moci.⁴⁴

Naproti tomu se však tento zákaz nevztahuje na komunikaci obviněného s obhájcem jiného obviněného, protože se již nejedná o důvěrný vztah mezi klientem a advokátem,⁴⁵ nebo na komunikaci obhájce, pokud tento je sledován jako podezřelý.

Tato právní úprava je však kritizována. Na rozdíl od znění před novelou provedenou zákonem č. 177/2008 Sb., které upravovalo povinnost policejního orgánu ihned přerušit odposlech hovoru mezi obhájcem a obviněným, má totiž policejní orgán možnost se s obsahem rozhovoru seznámit, a ačkoli nesmí takto získané informace nijak použít, nelze vyloučit, že jej tyto informace mohou přivést k dalším poznatkům, které by jinak nezískal, a tím ovlivnit průběh vyšetřování. To je v rozporu se zásadou, že každá procesní strana musí mít stejnou možnost hájit své zájmy a žádná nesmí mít

⁴³ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1206.

⁴⁴ Srov. náleží Ústavního soudu ze dne 30. 11. 1995, sp. zn. III. ÚS 62/95, uveřejněný pod č. 78 ve svazku 4 Sbírkou nálezů a usnesení Ústavního soudu České republiky.

⁴⁵ Srov. Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 1225.

podstatnou výhodu vůči protistraně.⁴⁶

V tomto směru však nelze vinit zákonodárce, že přehlédl mezeru v zákoně. Tento stav totiž vznikl samotným procesem získávání záznamů, který obstarává automatické nahrávací zařízení. To totiž neumožňuje poznat, s kým odposlouchávaná osoba hovoří. Identita osob je tak zjištěna až a posteriori ze záznamu obsahu odposlechnů. Není tak možné se vyhnout zjištění obsahu takového hovoru, protože pouze na jeho základě lze vyvodit identitu odposlouchávaných osob. To je samozřejmě nevýhodou takového zařízení. Nabízí se tudíž, že tento problém by odpadl, kdyby samotný odposlech byl zároveň kontrolován odpovědnou osobou. Při množství prováděných odposlechnů to ale vidím jako téměř nerealizovatelné. Takové opatření by totiž mělo vysoké požadavky na počet zaměstnanců, a tím by podstatně zvýšilo náklady prováděných odposlechnů. Z odposlechu by se tak pravděpodobně stal málo využívaný institut a nebylo by možné využít jeho potenciál. Nezbyvá tedy než konstatovat, že tento zásah je nutnou daní, která je na základě proporcionality mezi zásahem do svobody a požadovaným výsledkem ospravedlnitelná i přijatelná.

2.1.2 Postup při nařízení odposlechu a záznamu telekomunikačního provozu a náležitosti příkazu

Tento postup je upraven v odstavcích 2 až 4. Vzhledem k tomu, že nejenom podmínky nařízení odposlechu musí být stanoveny jasně a přesně, ale i způsob jeho provedení, včetně příkazu k jeho provedení, jedná se o poměrně podrobnou právní úpravu.

Nařízení odposlechu a záznamu telekomunikačního provozu se provádí příkazem k odposlechu a záznamu telekomunikačního provozu podle § 88 odst. 2 trestního řádu. Tento příkaz má povahu rozhodnutí sui generis.⁴⁷ Podle zákona musí být

⁴⁶ Vantuch, P. Nová úprava odposlechu v trestním řádu od 1. 7. 2008. Bulletin advokacie, 2008, č. 10, s. 29.

⁴⁷ Rozhodnutí sui generis je rozhodnutí orgánu činného v trestním řízení, které má zvláštní formu a uplatňuje se v určitých případech předvídaných trestním řádem (viz v § 119 odst. 1 trestního řádu slova „jestliže zákon nestanoví něco jiného“) tam, kde se vyžaduje, aby bylo rozhodnuto bez zbytečného prodlení, protože jde o zásah do práv a svobod občanů a hrozí, že jinak bude ohrožen účel trestního řízení. Proto jsou u těchto rozhodnutí svého druhu kromě zvláštních podmínek pro jejich vydání zpravidla stanoveny obsahové náležitosti a okruh osob, jimž se tato rozhodnutí doručují, popř. které jsou o těchto

vydán písemně a musí být odůvodněn. V řízení před soudem jej vydává předseda senátu (i odvolacího soudu) nebo samosoudce. V přípravném řízení pak na návrh státního zástupce soudce.⁴⁸

Státní zástupce musí před podáním návrhu ověřit, zda je trestní řízení vedeno pro trestný čin, pro který lze tento úkon nařídít. Učiní tak zejména posouzením, zda užitá právní kvalifikace odpovídá skutku popsanému v záznamu o zahájení úkonů trestního řízení nebo v usnesení o zahájení trestního stíhání. Zároveň musí vycházet z konkrétních skutkových okolností věci v době, kdy má být takový návrh podán. Dále musí prověřit, zda odposlechem mohou být zjištěny významné skutečnosti pro trestní řízení a zda sledovaného účelu nelze dosáhnout jinak nebo by jeho dosažení jinak bylo podstatně ztíženo.

Návrh státního zástupce na vydání příkazu k odposlechu a záznamu telekomunikačního provozu tak musí obsahovat zejména (tyto náležitosti se vztahují i na návrh na prodloužení doby odposlechu):⁴⁹

- a) uživatelskou adresu či zařízení a osobu uživatele, pokud je její totožnost známa,
- b) konkrétní skutkové okolnosti, které vydání příkazu, včetně doby jeho trvání, odůvodňují,

rozhodnutích vyrozumívány. Navíc je u nich zpravidla stanovena i písemná forma. V zájmu zajištění účelu trestního řízení proti nim zákon nepřipouští opravný prostředek a nabývají tak ihned po vydání právní moci a jsou vykonatelná. Rozhodnutí vydává soudce operativně bez jednání. Srov. Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 80-81.

⁴⁸ Příslušnost soudce v přípravném řízení je upravena v § 26 trestního řádu. V řízení před soudem se uplatní obecná ustanovení o příslušnosti § 16 a násl. trestního řádu.

⁴⁹ Podle čl. 67 odst. 1 a 2 závazného pokynu policejního prezidenta č. 30/2009 Sb., o plnění úkolů v trestním řízení, ve znění pozdějších předpisů (dále „ZPPP“), může policejní orgán navrhnout odposlech státnímu zástupci. V takovém návrhu pak musí stručně vyhodnotit skutkový stav trestní věci a odůvodnit provedení odposlechu (zejména uvedením, které skutečnosti významné pro trestní řízení v záznamech očekává a proč se domnívá, že v záznamech budou obsaženy). Dále uvede údaje k identifikaci uživatelské stanice (číslo, adresu a jméno nebo název uživatele, je-li jeho totožnost známa) a dobu, po kterou bude odposlech prováděn. Návrh podá až po předběžné konzultaci o technických možnostech provedení úkonu s útvarem zvláštních činností. Písemnost obsahující návrh nakonec označí příslušným stupněm utajení.

- c) je-li trestní řízení vedeno pro jiný úmyslný trestný čin, k jehož stíhání zavazuje mezinárodní smlouva, odkaz na tuto smlouvu,
- d) popis skutkových okolností nebo skutku, o který se jedná a v němž je spatřován trestný čin, a jeho právní kvalifikace,
- e) vyhodnocení dosavadního průběhu odposlechu a důvody k navrhované době prodloužení, jde-li o návrh na prodloužení doby jeho trvání,
- f) přehled již nařízených odposlechů u téhož účastníka telekomunikační služby, uživatele telefonní nebo jiné stanice, v téže věci s uvedením spisových značek soudu,
- g) vlastní návrh na vydání příkazu soudce či na prodloužení doby jeho provádění, včetně doby, po kterou má odposlech trvat.

Podrobnější postup upravuje pak instrukce Ministerstva spravedlnosti č. j. 505/2001-Org, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy (dále „soudní kancelářský řád“). V ustanovení § 32 tento předpis uvádí, že na základě telefonického nebo osobního sdělení v době dosažitelnosti příslušný soudce domluví způsob a přesný čas podání návrhu na nařízení odposlechu se státním zástupcem, zaměstnancem kanceláře státního zastupitelství nebo policejním orgánem. Na návrhu a jeho stejnopisu potvrdí datum a přesný čas jeho doručení. O návrhu státního zástupce podle § 88 odst. 2 trestního řádu rozhodne soudce bez zbytečného odkladu, případně ve lhůtě dohodnuté se státním zástupcem. Pokud je návrh státního zástupce na odposlech a záznam telekomunikačního provozu nebo jeho prodloužení označen příslušným stupněm utajení, podléhá řízení i spisová manipulace u soudu režimu utajení stejného stupně.

Náležitosti příkazu k nařízení jsou v hrubých rysech stanoveny v odstavci 2. Co se týče detailní úpravy, tou se zabýval Ústavní soud. Podle něj, aby byl záznam odposlechu telekomunikačního provozu v souladu s ústavním pořádkem (a tudíž byl procesně použitelným důkazem v trestním řízení), musí být příkaz k odposlechu podložen relevantními indiciemi, z nichž lze dovodit důvodné podezření ze spáchání trestného činu. Pouhé trestní oznámení samo o sobě nepostačuje k nařízení odposlechu, neboť nepostačuje ani k zahájení řízení k objasnění a prověřování skutečností důvodně

nasvědčujících tomu, že byl spáchán trestný čin podle § 158 trestního řádu.⁵⁰

Vedle toho musí být příkaz rovněž individualizován ve vztahu ke konkrétní osobě, která je uživatelem telefonní stanice. Pokud tato skutečnost nevyplývá ze zjištění, že se jedná o majitele telefonní stanice, musí být zdůvodněno, na základě jakých zjištění je dovozováno, že ji má v držení a že ji skutečně používá.⁵¹ Z příslušných opatření musí rovněž vyplývat, na základě jakých konkrétních indicií je dán vztah mezi sledovanou osobou (jí užívaným telefonním číslem nebo jí užívaným prostorem) a podezřením ze spáchání určité trestné činnosti.⁵² Konečně příkaz musí alespoň v minimální míře konkrétně uvést, jaké skutečnosti významné pro trestní řízení mají být takto zjištěny a z čeho je tak vyvozováno.⁵³

Ústavní soud rovněž kritizuje praxi, která setrvává stroze na formálních náležitostech a zcela rezignuje na posouzení materiálních podmínek pro nařízení odposlechu a záznamu telekomunikačního provozu. Posouzení těchto podmínek musí být rovněž patrné v odůvodnění příkazu, aby tak byl zcela zřejmý ústavně souladný postup soudu. Obecný soud, který rozhodne o vině především na základě záznamu odposlechu telekomunikačního provozu, aniž by návrh na příkaz k odposlechu byl soudem efektivně přezkoumán a aniž by byly zaznamenány ve spise všechny relevantní skutečnosti odůvodňující jeho vydání, porušuje podle Ústavního soudu ústavně garantovaná práva a svobody zakotvená v čl. 2 odst. 3, čl. 4 a čl. 90 Ústavy a čl. 8 odst. 2 a čl. 13 Listiny.^{54, 55}

⁵⁰ Srov. náleží Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06, uveřejněný pod č. 88 ve svazku 45 Sbírký nálezů a usnesení Ústavního soudu České republiky.

⁵¹ Srov. náleží Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06, uveřejněný pod č. 88 ve svazku 45 Sbírký nálezů a usnesení Ústavního soudu České republiky.

⁵² Nález Ústavního soudu ze dne 27. 1. 2010, sp. zn. II. ÚS 2806/2008, uveřejněný pod č. 15 ve svazku 56 Sbírký nálezů a usnesení Ústavního soudu České republiky.

⁵³ Srov. náleží Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06, uveřejněný pod č. 88 ve svazku 45 Sbírký nálezů a usnesení Ústavního soudu České republiky.

⁵⁴ Srov. náleží Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06, uveřejněný pod č. 88 ve svazku 45 Sbírký nálezů a usnesení Ústavního soudu České republiky.

⁵⁵ Nakonec je nutno zmínit, že těmto požadavkům musí dostát i návrh státního zástupce na vydání soudního příkazu (resp. i podnět policejního orgánu k němu) a musí k němu být přiloženy odpovídající důkazy. V opačném případě je nutno takový návrh zamítnout. Nález Ústavního soudu ze dne 23. 5. 2007,

Náležitostmi příkazu jsou pak podle výše uvedených skutečností (mimo obecných náležitostí):

- a) uložení provedení odposlechu a záznamu příslušného druhu telekomunikačního provozu,
- b) uživatelská adresa či zařízení (včetně telefonního čísla),
- c) osoba uživatele, pokud je její totožnost známa (uvedením jména a příjmení, adresy, příp. i zaměstnání a dalších potřebných identifikačních údajů),
- d) trestný čin naznačený v odstavci 1 (v případě trestního řízení pro úmyslný trestný čin, k jehož stíhání zavazuje mezinárodní smlouva, konkrétní odkaz na tuto vyhlášenou mezinárodní smlouvu),
- e) doba, po kterou bude odposlech a záznam telekomunikačního provozu prováděn a která nesmí být delší než čtyři měsíce.⁵⁶

V odůvodnění příkazu pak musí být uvedeny:

- a) konkrétní skutkové okolnosti, které vydání tohoto příkazu, včetně doby jeho trvání, odůvodňují,
- b) účel odposlechu a záznamu telekomunikačního provozu,
- c) vysvětlení důvodů, proč nelze sledovaného účelu dosáhnout jinak nebo proč by bylo jinak jeho dosažení podstatně ztíženo.⁵⁷

Co se týče osoby uživatele, tou je podle § 2 písm. b) zákona o elektronických komunikacích každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací. Není rozhodné, zdali se jedná o podezřelého, obviněného či jinou osobu. Takové konkrétní vymezení by totiž vedlo k nemožnosti využití tohoto institutu v mnohých případech, kdy by to bylo jinak opodstatněné. V současné době totiž pachatelé trestných činů často využívají krátkodobého či jednorázového použití telefonních čísel, která trvale užívá jiná osoba (nebo tzv. jednorázových SIM karet), takže soudce při povolování odposlechů není schopen zjistit a ověřit konkrétního

sp. zn. II. ÚS 615/06, uveřejněný pod č. 88 ve svazku 45 Sbírký nálezů a usnesení Ústavního soudu České republiky.

⁵⁶ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1207.

⁵⁷ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1207.

uživatele telefonního čísla.⁵⁸

V této souvislosti je nutné ještě zmínit, jak je to s podjatostí soudce, který tento příkaz vydává. Zajímavé je v tomto ohledu rozhodnutí Nejvyššího soudu sp. zn. 7 Tdo 630/2005. Dovolatel v tomto případě tvrdil, že bylo porušeno jeho právo na nestranného a nezávislého soudce, kdy ve věci o vině a trestu rozhodoval tentýž soudce, který rozhodoval o příkazu k odposlechu. Tento postup byl podle něj v rozporu s čl. 36 odst. 1 Listiny, resp. čl. 6 odst. 1 Úmluvy, protože skutečnost, že soudce před rozhodnutím o vydání příkazu k odposlechu dostává podklady pro posouzení návrhu a seznamuje se se skutečnostmi, které následně vedou ke sdělení obvinění a podání obžaloby, zpochybňuje jeho nestrannost a vylučuje jej ve smyslu § 30 odst. 2 trestního řádu z projednávání věci v otázce viny a trestu po podání obžaloby, přičemž intenzitu zásahu odposlechu do práv a svobod považoval za srovnatelnou s intenzitou takového zásahu při vzetí do vazby.⁵⁹

Nejvyšší soud však s tímto názorem nesouhlasil. Podle něj nařízení odposlechu nevyžaduje na rozdíl od rozhodnutí o vazbě, aby soudce v rámci rozhodování zaujímal tak konkrétní stanovisko k otázce možné viny obviněného, a tudíž nelze vyvozovat, že jeho rozhodnutí v uvedených případech v přípravném řízení by výrazněji ovlivnilo jeho postoj při rozhodování po podání obžaloby.⁶⁰

S tímto postojem Nejvyššího soudu, na základě jeho argumentace, se ztotožňuji. Případná podjatost soudce je dle mého názoru dostatečně kryta ustanovením § 30 odst. 1 trestního řádu, zejména s přihlédnutím k faktu, že odposlech nemusí být nařízen pouze u podezřelého (obviněného), ale i u jiné osoby, u které je předpokládán kontakt s podezřelým. V takovém případě by bylo naprosto neopodstatněné, aby daný soudce nemohl rozhodovat i ve věci samotné. Navíc, jak Nejvyšší soud správně podotknul,

⁵⁸ Srov. usnesení Nejvyššího soudu ze dne 26. 7. 2011, sp. zn. 4 Pzo 2/2011.

⁵⁹ Srov. usnesení Nejvyššího soudu ze dne 8. 6. 2005, sp. zn. 7 Tdo 630/2005.

⁶⁰ V této souvislosti nutno upozornit na ustanovení § 30 odst. 1 trestního řádu, které stanoví možnost vyloučení soudce pro (mimo jiné) poměr k projednávané věci. Lze proto připustit, že při rozhodnutích v konkrétních případech dojde k řešení otázky viny obviněného soudcem v takové míře, že to bude vzbuzovat pochybnosti o nestrannosti takového soudce pro rozhodování po podání obžaloby, takže buď z iniciativy samotného soudce nebo z podnětu některé ze stran řízení bude rozhodnuto o jeho vyloučení z vykonávání dalších úkonů v tomto trestním řízení podle § 30 odst. 1 trestního řádu. Usnesení Nejvyššího soudu ze dne 8. 6. 2005, sp. zn. 7 Tdo 630/2005.

obsahuje ustanovení § 30 odst. 2 věta druhá trestního řádu taxativní výčet případů, kdy je soudce paušálně vyloučen z rozhodování po podání obžaloby. Takovýto výčet tak není možné svévolně rozšiřovat na další instituty pouze na základě výkladu zákona. To by bylo možné pouze zákonnou novelou.⁶¹

Opis příkazu k odposlechu a záznamu telekomunikačního provozu je třeba jak v přípravném řízení, tak i v řízení před soudem bezodkladně doručit policejnímu orgánu, který podle odstavce 1 věty druhé vždy provádí odposlech a záznam telekomunikačního provozu. V přípravném řízení je soudce povinen doručit opis příkazu k odposlechu a záznamu telekomunikačního provozu i státnímu zástupci. Musí tak učinit bez odkladu, tedy ihned. Smyslem je informovat o tomto úkonu státního zástupce, aby mohl vykonávat dozor v přípravném řízení i nad prováděním odposlechu a záznamu telekomunikačního provozu.^{62, 63}

Rozsah povolení vychází u každé konkrétní trestní věci z individuálních podmínek. Co se týká časového rozsahu povolení, vždy musí být dbáno na přiměřenost této doby; jde tedy o dobu nezbytně nutnou, po kterou má být zasahováno do práv osob.⁶⁴ Zákon v tomto případě pouze stanovil hranici čtyř měsíců, která nesmí být překročena. Běh této čtyřměsíční lhůty, popřípadě kratší lhůty stanovené v příkazu, je počítán podle § 60 odst. 2 a 3 trestního řádu.

Tuto lhůtu může soudce soudu vyššího stupně, v přípravném řízení na návrh státního zástupce soudce krajského soudu, i opakovaně prodloužit, vždy však nejdéle na dobu dalších čtyř měsíců.⁶⁵ Rozhodnutí o prodloužení je vydáno na základě vyhodnocení dosavadního průběhu odposlechu, které předkládá policejní orgán v řízení před soudem předsedovi senátu a v přípravném řízení soudci prostřednictvím státního

⁶¹ Srov. usnesení Nejvyššího soudu ze dne 8. 6. 2005, sp. zn. 7 Tdo 630/2005.

⁶² Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1208.

⁶³ Podle ZPPP předá policejní orgán příkaz soudce (nebo vlastní příkaz spolu se souhlasem uživatele) s žádostí o provedení příslušnému pracovišti útvaru zvláštních činností, kde projedná způsob zpracování a předávání záznamů. V žádosti uvede číslo jednací trestního spisu.

⁶⁴ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1197.

⁶⁵ Soudem vyššího stupně je soud bezprostředně nadřízený soudu, jehož předseda senátu odposlech a záznam nařídil. Krajským soudem se rozumí krajský soud, který je nadřízen soudu, jehož soudce nařídil odposlech v přípravném řízení. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1210.

zástupce tak, aby ho rozhodující orgán měl včas pro své rozhodnutí k dispozici a mohl z něj vycházet.⁶⁶ Je nezbytné, aby na základě prodloužení odposlechu trvalo nebo bylo posilováno podezření existence souvislosti mezi sledovanou osobou a trestnou činností.⁶⁷

K náležitostem návrhu státního zástupce viz výše.

O návrhu státního zástupce na prodloužení doby trvání odposlechu v přípravném řízení rozhodne soudce krajského soudu nejpozději poslední pracovní den před vypršením doby, na kterou byl odposlech v příkazu povolen nebo prodloužen, jestliže ho státní zástupce podal alespoň tři pracovní dny před skončením uvedené lhůty. I toto rozhodnutí o prodloužení doby má povahu rozhodnutí sui generis.

Vedle časového rozsahu je ještě nutné vymezit i rozsah co do počtu odposlouchávaných stanic. Při splnění zákonných podmínek se odposlech využívá u všech telefonních čísel podezřelé osoby. Jinak je počet odposlouchávaných účastnických telefonních stanic, popř. jiných technických prostředků, stanoven rovněž na nezbytnou míru, přičemž ohledně každé takto odposlouchávané účastnické stanice musí existovat zcela konkrétní důvod, který je specifikován ve spisovém materiálu předkládaném státním zástupcem soudu.⁶⁸

2.1.3 Provedení, průběh a ukončení odposlechu

Odposlech provádí pro potřeby všech orgánů činných v trestním řízení Policie České republiky. Na celém území České republiky je oprávněn provádět tento úkon pouze Útvar zvláštních činností služby kriminální policie a vyšetřování (dále „útvar zvláštních činností“), který zajišťuje komunikaci s operátory, včetně hrazení nákladů operátorům vzniklých.

Podle odst. 3 je povinností policejního orgánu to, aby:

- vyhodnocoval průběh odposlechu a záznamu telekomunikačního provozu a na základě tohoto vyhodnocení, jakmile pominuly důvody vedoucí k jeho nařízení, aby

⁶⁶ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1210.

⁶⁷ Nález Ústavního soudu ze dne 27. 1. 2010, sp. zn. II. ÚS 2806/2008, uveřejněný pod č. 15 ve svazku 56 Sbírký nálezů a usnesení Ústavního soudu České republiky.

⁶⁸ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1197.

- ihned ukončil provádění odposlechu a záznamu telekomunikačního provozu, a to i před skončením doby uvedené v příkazu podle odstavce 2.⁶⁹

Vyhodnocování průběhu odposlechu a záznamu telekomunikačního provozu provádí policejní orgán z hlediska:

- a) konkrétních skutkových okolností, které byly uvedeny v odůvodnění příkazu, jímž byl odposlech nařízen,
- b) zda by nebylo možno sledovaného účelu dosáhnout jinak, popř. zda by dosažení sledovaného účelu již nadále nebylo podstatně ztíženo.⁷⁰

Jakmile byly již zjištěny skutečnosti významné pro trestní řízení, které se měly podle předpokladu příslušného orgánu činného v trestním řízení získat, anebo bylo naopak zjištěno, že uvedený předpoklad se nepotvrdil, je povinností policejního orgánu ihned provádění odposlechu a záznamu telekomunikačního provozu ukončit, a to bez ohledu na dobu vymezenou v příkazu (princip minimalizace zásahů do ústavních práv). To se týká i případu, že uživatel telefonní nebo jiné stanice zjistil, že je odposloucháván.⁷¹ Stejně musí policejní orgán postupovat, jestliže na základě vyhodnocení výsledků dosud provedeného odposlechu usoudí, že další odposlech již není třeba, poněvadž další skutečnosti významné pro trestní řízení je možno získat jinými důkazními prostředky⁷² nebo se změnil uživatel telefonní nebo jiné stanice.

K ukončení odposlechu před uplynutím lhůty, na kterou byl povolen, nepotřebuje policejní orgán souhlas soudu. Pokud pomine důvod, pro který byl nařízen, ukončí jej faktickým postupem, učiní o tom příslušný záznam a informuje státního zástupce, který ve věci vykonává dozor.⁷³

Ukončení odposlechu a záznamu telekomunikačního provozu policejní orgán bezodkladně písemně oznámí:

⁶⁹ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1209.

⁷⁰ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1209.

⁷¹ V těchto dvou případech může být odposlech ukončen i na pokyn státního zástupce.

⁷² Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1209.

⁷³ Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 455.

- v řízení před soudem předsedovi senátu, který příkaz k odposlechu vydal,
- v přípravném řízení soudci, který příkaz k odposlechu vydal, a státnímu zástupci, který vykonává dozor nad zachováváním zákonnosti v předmětné trestní věci.

Tímto postupem je dosahováno zpětné informovanosti mezi tím, kdo příkaz k odposlechu vydal, a orgánem, který sledování odposlechu zajišťuje. V případě nového návrhu na povolení odposlechu téže osoby mohou pak tyto orgány náležitě přihlídnout k tomuto faktu a posoudit důvodnost nové žádosti.⁷⁴

Po ukončení odposlechu policejní orgán jeho výsledek vyhodnotí a výsledek zanesou do k tomu určeného informačního systému. Bude-li některý záznam obsahovat skutečnosti významné pro trestní řízení, převezme do dvaceti dnů na útvaru zvláštních činností všechny pořízené záznamy.

2.1.4 Odposlech se souhlasem uživatele

Vzhledem k tomu, že mohou v rámci trestního řízení nastat i situace, kdy je nutné nařídit odposlech a zároveň zde existuje vysoké riziko, že při běžném postupu by mohlo dojít ke zmaření dosažení účelu trestního řízení, zavedl zákonodárce v odstavci 5 možnost provedení odposlechu i bez příkazu, pouze se souhlasem uživatele odposlouchávané telefonní stanice. Před novelou provedenou zákonem č. 177/2008 Sb. uděloval takovýto souhlas účastník odposlouchávané stanice, což je podle § 2 písm. a) zákona o elektronických komunikacích každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb. Nová úprava tak dala možnost udělit souhlas i osobám, které ačkoli nejsou stranou takovéto smlouvy, odposlouchávanou telefonní stanicí využívají (např. rodinní příslušníci).⁷⁵

Jedná se o zvláštní postup, existující paralelně s postupem běžným, na který se vztahují specifické podmínky povolování a který umožňuje získat cenné informace i v situacích časové tísně (např. únosy).

Tento odposlech je nařízen bez příkazu předsedy senátu (samosoudce),

⁷⁴ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1209.

⁷⁵ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1211.

v přípravném řízení soudce, přičemž provedení odposlechu nařídí, popřípadě provede,⁷⁶ sám příslušný orgán činný v trestním řízení, tj. státní zástupce nebo policejní orgán v přípravném řízení a předseda senátu (samosoudce) ve stádiu řízení před soudem.⁷⁷ Tento orgán vyhotoví nařízení odposlechu a záznamu telekomunikačního provozu, jehož obsahové náležitosti jsou obdobné jako v případě příkazu podle odstavce 2. Pouhý úřední záznam ve spise z tohoto hlediska nepostačuje, a to s ohledem na možnost použití záznamu telekomunikačního provozu jako důkazu. Nařízení má v tomto případě formu opatření, které proto postačí zaznamenat v protokole o úkonu.⁷⁸

Výčet trestných činů, u kterých je možno tento zvláštní režim nařídit, je v tomto případě značně omezený, přičemž se na něj nevztahují podmínky ohledně trestných činů uvedených v odstavci 1. Příslušnými trestnými činy podle zákona tedy jsou:

- obchodování s lidmi podle § 168 trestního zákoníku,
- svěření dítěte do moci jiného podle § 169 trestního zákoníku,
- omezování osobní svobody podle § 171 trestního zákoníku,
- vydírání podle § 175 trestního zákoníku,
- únos dítěte a osoby stížené duševní poruchou podle § 200 trestního zákoníku,
- násilí proti skupině obyvatel a proti jednotlivci podle § 352 trestního zákoníku,
- nebezpečné vyhrožování podle § 353 trestního zákoníku a
- nebezpečné pronásledování podle § 354 trestního zákoníku.

Souhlas je dán uživatelem odposlouchávané stanice (u organizace statutárním zástupcem), přičemž tato skutečnost se zaznamená pouze do protokolu o nařízení úkonu. Samostatné písemné formy se pak zpravidla použije jen tehdy, bude-li třeba o součinnost požádat provozovatele telekomunikační sítě.^{79, 80} Při absenci souhlasu je nerozhodné, zda uživatel souhlas výslovně odepřel nebo zda se k němu vůbec

⁷⁶ V praxi však provádí odposlech vždy útvar zvláštních činností.

⁷⁷ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1211.

⁷⁸ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1211.

⁷⁹ Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C.H. Beck, 2007, s. 366.

⁸⁰ Podle čl. 67 odst. 3 ZPPP musí být souhlas opatřen ještě před vydáním příkazu orgánu činného v trestním řízení, a to v písemné formě, aby mohl být založen do originálu i do stejnopisu trestního spisu.

nevyjádřil.⁸¹ V zákoně však není stanoven postup, pokud uživatel svůj souhlas odvolá. Obecně ale platí, že v takovém případě musí dojít k okamžitému ukončení odposlechu, protože by jinak tento úkon byl prováděn bez jakéhokoli zákonného oprávnění, přičemž o možnosti souhlas odvolat by měl být uživatel poučen ještě před započítím odposlechu. Z toho se zároveň vychází i při určení časového období, na které je odposlech nařízen, které není v § 88 odst. 5 stanoveno. Odposlech by tak měl trvat jen po dobu potřebnou k dosažení účelu, maximálně po dobu trvání souhlasu uživatele.^{82, 83}

Odposlech a záznam telekomunikačního provozu se souhlasem uživatele je značně kritizovanou částí české právní úpravy. Zejména je problematický zásah do práv a svobod osob, které jsou v rámci telekomunikačního provozu odposlouchávány, ale nejsou osobou, která udělila souhlas k odposlechu. Zatímco při běžném postupu je totiž zásah do jejich práv a svobod odůvodněn na základě řádného příkazu soudu, který má za úkol posoudit veškeré náležitosti případu a zvážit, zdali existuje odůvodněné podezření pro provedení odposlechu, u tohoto institutu tento postup není zákonem stanoven. Přesto však není zcela přeskočen. Právní úprava totiž i v tomto ohledu existuje, a to v pokynu obecné povahy nejvyšší státní zástupkyně č. 8/2009, o trestním řízení, ve znění pozdějších předpisů. Ten v článku 45 upravuje povinnost policejního orgánu, který provedení odposlechu podle § 88 odst. 5 nařídil, o tomto úkonu neprodleně informovat státního zástupce. Státní zástupce pak přezkoumá, zda byl odposlech nařízen v řízení vedeném pro trestný čin, pro který je možno tento úkon provést, a zda po celou dobu prováděného odposlechu je použití této právní kvalifikace odůvodněno. Má-li státní zástupce za to, že odposlechem nemohou být sděleny významné skutečnosti pro trestní řízení nebo zjistí-li přezkoumáním postupu policejního orgánu, že souhlas účastníka odposlouchávané stanice nebyl platně učiněn nebo byl vzat zpět anebo že je odposlech prováděn v řízení vedeném pro jiný než zákonem vymezený trestný čin, uloží policejnímu orgánu, aby ihned provádění odposlechu ukončil a

⁸¹ Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 1219.

⁸² Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C.H. Beck, 2007, s. 366.

⁸³ Ale například v čl. 67 odst. 3 ZPPP je uvedeno, že již ve vlastním příkazu musí být uvedena doba, po kterou má být odposlech prováděn.

záznamy zničil. Zjištěné informace pak nelze v dalším řízení použít. Nařídí-li provedení odposlechu státní zástupce, přiměřeně se užití ustanovení o odposlechu nařízeném soudcem.⁸⁴

Tato úprava v interním předpisu se může zdát dostatečná. Přesto si však myslím, že i v zákoně by mělo být uvedeno, že takové dodatečné povolovací řízení má být uplatněno a měla by být stanovena lhůta, do kdy má být požadované rozhodnutí vydáno. Ačkoli totiž není pochyb o tom, že tento institut má jistě své opodstatnění, nedá se podle mě říci, že všechny výše uvedené trestné činy ospravedlňují bez dalšího použití odposlechu pouze se souhlasem uživatele. Zákon totiž naprosto vynechává zásadu subsidiarity takového opatření a odposlech pak může být použit i v případech, kdy jeho využití není nezbytně nutné.

Zároveň bych v této souvislosti ještě ale zmínila nedostatek právní úpravy, který dle mého názoru může opravdu podstatně ovlivnit v určitých případech výsledek vyšetřování. Odposlech a záznam telekomunikačního provozu je možné nařídit buď „tradiční“ cestou, kdy je nejprve nutné získat soudní příkaz, nebo bez příkazu se souhlasem uživatele. Co ale dělat, pokud jsou splněny podmínky pro vydání příkazu, nikoli však pro nařízení odposlechu pouze se souhlasem uživatele, ale situace ve vyšetřování je taková, že čekáním na jeho získání by mohlo dojít k ztrátě důležitých stop a ohrožení účelu trestního řízení? Podíváme-li se na jiné instituty trestního řádu, které do práv a svobod osob zasahují obdobně, zjistíme zde zásadní rozdíl. Pro srovnání můžeme vzít institut sledování osob a věcí podle § 158d trestního řádu, který v odst. 5 stanoví, že sledování osob a věcí je možné zahájit i bez povolení, nesnese-li věc odkladu, ale policejní orgán musí o povolení bezodkladně dodatečně požádat, a pokud povolení do 48 hodin neobdrží, je povinen sledování ukončit a případný záznam zničit, čímž je dodatečně potvrzena i zákonnost takového rozhodnutí.

Není pochyb, že uplatnění takového postupu i při nařizování odposlechu by ve výše zmíněné situaci mohlo vést k získání důležitých informací o pachateli, které by nakonec vedly i k jeho dopadení. Rovněž si myslím, že by takováto úprava mohla pohodlně i nahradit použití odposlechu se souhlasem uživatele odposlouchávané telekomunikační stanice, protože by takové opatření zajistilo i v těchto případech

⁸⁴ Podle čl. 63 odst. 2 ZPPP musí policejní orgán rovněž uvést, jaké skutečnosti významné pro trestní řízení v záznamech očekává a proč se domnívá, že v záznamech budou obsaženy.

nutnost rychlého postupu orgánů činných v trestním řízení. Přesto by však v případě této úpravy bylo nutné zvážit rovněž riziko, že tento institut by mohl být policejními orgány zneužíván pro získávání informací operativního rázu.

Nutno bohužel podotknout, že obdobná úprava schází i u institutu zjišťování údajů o telekomunikačním provozu, kde by jeho využití mělo ještě větší význam než u odposlechu.⁸⁵

2.1.5 Odposlech a záznam telekomunikačního provozu jako důkaz v trestním řízení

Použití institutu odposlechu a záznamu telekomunikačního provozu má za cíl získání informací, které doplňují podezření na trestnou činnost konkrétní osoby. Z toho vyplývá nutnost, aby tento institut bylo možno použít v trestním řízení jako důkaz. To je přípustné za splnění podmínek uvedených v § 88 odst. 6 trestního řádu. Pro tento účel však musí být vyhotoven protokol o odposlechu, jehož význam spočívá zejména v tom, že uvedenými údaji lze zpětně prověřit autentičnost a neporušenost takového záznamu.⁸⁶

Nejprve je však nutno rozlišit funkci záznamu o odposlechu a funkci protokolu o odposlechu. Zatímco záznam o odposlechu telekomunikačního provozu je určen k posouzení zákonnosti postupu při rozhodování o vině obviněného, jinak řečeno je to důkazní prostředek, který slouží k objasnění skutečností důležitých pro trestní řízení, slouží protokol k posouzení zákonnosti postupu při provádění odposlechu a záznamu telekomunikačního provozu, přičemž na jeho základě posuzuje soud přípustnost záznamu jakožto důkazu, pokud je namítána jeho nezákonnost.⁸⁷

Tento protokol kromě obecných náležitostí podle § 55 a násl. trestního řádu musí obsahovat ještě další obligatorní náležitosti uvedené v § 88 odst. 6 trestního řádu. Těmito náležitostmi jsou:

⁸⁵ Taková úprava by se však nevztahovala např. na údaje uložené v nalezeném telefonu (zprávy a lokalizační údaje), které byly doručeny volanému předtím, než telefon získaly orgány činné v trestním řízení. Ty lze totiž zjišťovat i bez příkazu ke zjišťování údajů o telekomunikačním provozu.

⁸⁶ Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C.H. Beck, 2007, s. 367.

⁸⁷ Srov. Jelínek, J. a kol. Trestní zákoník a trestní řád s poznámkami a judikaturou. 2. aktualiz. vyd. podle stavu k 1. 12. 2011. Praha: Leges, 2011, s. 662.

- a) údaje o místě, času, způsobu a obsahu provedeného záznamu,
- b) jakož i o orgánu, který záznam pořídil.⁸⁸

Výše uvedené náležitosti jsou obligatorní, a pokud by v protokole nebyly uvedeny, použití záznamu jako důkazu by bylo vyloučeno.⁸⁹ Na druhou stranu však jejich nedostatek lze odstranit (i v řízení před soudem), a to stejným způsobem jako v případě odstranění formálních nedostatků protokolu sepsaného o jakémkoliv jiném úkonu trestního řízení, např. výsledkem osob, které se provedení úkonu zúčastnily, popř. jej provedly. Takový postup nelze považovat za nepřípustnou manipulaci se záznamy telekomunikačního provozu a nevymyká se ani možnostem soudu, takže věc nevyžaduje další šetření ve smyslu ustanovení § 221 trestního řádu o vrácení věci státnímu zástupci k došetření.⁹⁰ Ne všichni autoři však s tímto názorem souhlasí, zejména ohledně přepisů obsahu odposlechů. Podle nich je totiž výstižné a podstatné (nikoli doslovné) zachycení obsahu zpětně nekonvalidovatelnou obsahovou náležitostí záznamu, garantující jeho autentičnost ve smyslu podmínek použitelnosti záznamu jako důkazu.⁹¹

Ohledně přepisů odposlechů však panoval nejednotný názor i co se týče rozsahu, kterým má být v protokolu zachycen obsah takového odposlechu.⁹² Zákon totiž nijak nevymezuje, zdali to má být doslovný přepis jednotlivých hovorů nebo pouze uvedení některých údajů. Soudní judikatura se tak nakonec ustálila na názoru, že zákon nestanoví jako podstatnou náležitost předmětného protokolu přepis jednotlivých hovorů na provedeném záznamu a pro splnění této podmínky postačuje uvedení údajů o čase jednotlivých hovorů, telefonních číslech a osobách uživatelů účastnických stanic, tedy

⁸⁸ Srov. Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 455.

⁸⁹ Srov. Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 455.

⁹⁰ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. Praha: C. H. Beck, 2013, s. 1212.

⁹¹ Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C.H. Beck, 2007, s. 367.

⁹² Rovněž panovaly neshody ohledně uvedení osoby, která záznam prováděla, protože v praxi jsou odposlechy nahrávány automaticky a není možné určit konkrétní odpovědnou osobu. Tento problém byl avšak odstraněn novelou č. 177/2008 Sb., která osobu zaměnila za orgán, proto se jím nebudu v této práci více zabývat.

osobách volajících a volaných.⁹³

Zákon se rovněž vůbec nezmiňuje o osobě (orgánu), která má tento protokol vyhotovit. Z použití systematického výkladu a rovněž i průběhu tohoto procesu v praxi však vyplývá, že odpovědným orgánem bude policejní orgán. Konkrétní určení je pak obsaženo v čl. 67 odst. 7 ZPPP, který říká, že protokol vyhotoví ten, kdo záznam pořídil.

Důkaz záznamem o telekomunikačním provozu se provede přehráním záznamu z nosiče, na kterém byl zachycen. Je-li telekomunikační provoz veden v cizím jazyce, což je obvyklé, potom se záznam přehraje za přítomnosti tlumočnicka.⁹⁴ K důkazu se zpravidla přitom přehrají pouze ty záznamy, které obsahují skutečnosti důležité pro trestní řízení, popř. takové jejich části, pokud tomuto postupu nebudou bránit námitky procesních stran domáhajících se přehrání záznamů v jejich úplnosti.⁹⁵

Protokol o odposlechu telekomunikačního provozu je oproti tomu listinným důkazem, který se předloží stranám k nahlédnutí, a pokud kterákoli z nich navrhne jeho přečtení, je soud povinen jej přečíst.

Nejvyšší soud k této otázce uvedl, že pokud nevznikají pochybnosti o pravosti odposlechu a záznamu telekomunikačního provozu a o správnosti přepisu jeho obsahu, není vyloučeno, aby byl důkaz proveden jen čtením⁹⁶ přepisů telefonických hovorů, zejména když žádná ze stran řízení netrvala na poslechu pořízeného záznamu. V takovém případě je nezbytné, aby byl přepis zachycen v objektivně vnímatelné podobě, která umožňuje jeho přečtení. Má-li soud k dispozici jak odposlech a záznam telekomunikačního provozu, tak i jejich přepis, závisí pouze na úvaze soudu, zda provede tento důkaz jeho přehráním na technickém zařízení nebo přečte jeho přepis.⁹⁷

Samotné faktické nakládání se záznamem pak nemůže mít samo o sobě vliv na procesní použitelnost takového důkazu (například komprimace obsahu důkazu na CD

⁹³ Srov. Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 455.

⁹⁴ Jelínek, J. a kol. Trestní zákoník a trestní řád s poznámkami a judikaturou. 2. aktualiz. vyd. podle stavu k 1. 12. 2011. Praha: Leges, 2011, s. 662.

⁹⁵ Rozsudek Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006.

⁹⁶ Vzhledem k nové právní úpravě § 213 trestního řádu je to v současnosti prováděno předložením přepisu k nahlédnutí.

⁹⁷ Usnesení Nejvyššího soudu ze dne 24. 6. 2009, sp. zn. 5 Tdo 572/2009.

nosiči), ledaže by došlo ke zjevnému znehodnocení důkazu (důkazního prostředku), k jeho ztrátě či k podstatnému snížení jeho vypovídací hodnoty. Opačný názor by vedl k neodůvodněnému zpochybňování úlohy orgánů činných v trestním řízení.⁹⁸

Ostatní záznamy, u nichž se nepředpokládá, že budou použity jako důkaz v trestním řízení, je povinen policejní orgán označit, spolehlivě uschovat tak, aby byla zajištěna ochrana před neoprávněným zneužitím záznamu, a v protokolu založeném do spisu poznamenat, kde jsou uloženy.

Za splnění zákonných podmínek je možno záznam telekomunikačního provozu užit jako důkaz i v jiné trestní věci, než v níž byl předmětný odposlech proveden. K této problematice vydal rozhodnutí i Ústavní soud. Ten uvedl, že pokud byl původní odposlech proveden zákonně a byl-li takto legálně získaný záznam použit jako listinný důkaz, aniž byly dodrženy podmínky § 88 trestního řádu, neznamená to porušení zákona, neboť na listinné důkazy se ustanovení § 88 trestního řádu nevztahuje.⁹⁹ Toto rozhodnutí však bylo nepřesné již v době jeho vydání, protože i před novelou trestního řádu provedenou zákonem č. 292/1993 Sb. znamenalo obcházení zákona a bylo v rozporu s čl. 13 Listiny a čl. 8 Úmluvy. V současné době je tento nálezn již překonán, protože současné ustanovení § 88 odst. 6 trestního řádu již podrobně upravuje podmínky použití záznamu telekomunikačního provozu jako důkazu, popřípadě použití záznamu jako důkazu i v jiné trestní věci, než ve které byl odposlech nařízen a proveden.¹⁰⁰

Použití záznamu odposlechu telekomunikačního provozu jako důkazu v jiné trestní věci, než ve které byl nařízen, je tedy možné za splnění dvou alternativně stanovených podmínek, a to:

- je-li vedeno trestní stíhání pro trestný čin uvedený v odstavci 1, nebo
- souhlasí-li s tím účastník odposlouchávané stanice.¹⁰¹

⁹⁸ Usnesení Nejvyššího soudu ze dne 24. 6. 2009, sp. zn. 5 Tdo 572/2009.

⁹⁹ Nález Ústavního soudu ze dne 27. 4. 1994, sp. zn. II. ÚS 6/93, uveřejněný pod č. 22 ve svazku 1 Sbírký nálezů a usnesení Ústavního soudu České republiky.

¹⁰⁰ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1220.

¹⁰¹ Srov. Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007, s. 367.

Použití záznamu v těchto případech nevyžaduje ani současnost, ani souběžnost, ani věcnou souvislost probíhajících trestních řízení. Postačuje pouze potřeba tohoto důkazu ve více řízeních.¹⁰² Souhlas účastníka se však i v tomto případě vztahuje pouze na trestné činy vyjmenované v odstavci 5. U všech ostatních trestných činů musí být dodržena podmínka uvedená v § 88 odst. 1 trestního řádu, jinak by mohlo docházet k obcházení restriktivního omezení provádění odposlechu.¹⁰³

Zbývá ještě vyřešit, jak je to s použitím záznamů odposlechnů telekomunikačního provozu opatřených mimo území České republiky pro účely trestního stíhání v zahraničí. Touto problematikou se zabýval Nejvyšší soud v rozsudku sp. zn. 11 Tz 129/2006. V posuzované věci byly použity již dříve pořízené záznamy odposlechu telekomunikačního provozu opatřené mimo území České republiky, a to výlučně pro účely trestního stíhání v Itálii a ve vztahu k jiným osobám stíhaným v Itálii. Tyto záznamy pak byly na základě žádosti českých orgánů o právní pomoc poskytnuty k trestnímu řízení vůči obviněnému. Z hlediska formálního tak šlo o odposlechy pořízené jinak než postupem podle § 88 odst. 1, 2 trestního řádu a v jiné trestní věci.¹⁰⁴

Podle názoru Nejvyššího soudu však neexistuje důvod pokládat za záznamy opatřené v jiné než v posuzované trestní věci pouze ty z nich, které byly pořízeny v rámci trestního řízení konaného na území České republiky příslušnými českými orgány trestního řízení.¹⁰⁵ Z toho vyplývá závěr, že v případě právního styku s cizinou v trestní věci, ve které by jinak byly splněny formální vnitrostátní předpoklady pro nařízení odposlechu, není vyloučeno použití v České republice jako důkazní prostředek záznam opatřený v cizině i v jiné trestní věci. Použitelnost takového záznamu je však nutno posuzovat též z toho hlediska, zda zásah do soukromí je dostatečně podložen takovým zájmem, který činí průlom do práva na soukromí věcně odůvodnitelným, a zda i v cizině k němu došlo způsobem srovnatelným se zákonnými podmínkami

¹⁰² Musil, J., Kratochvíl, V., Šámal, P. a kol. Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007, s. 367.

¹⁰³ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1213.

¹⁰⁴ Rozsudek Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006.

¹⁰⁵ Srov. rozsudek Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006.

stanovenými českou právní úpravou. Ne každý odposlech uskutečněný v cizině lze tedy použít v trestním řízení v České republice jako důkaz.¹⁰⁶

K důkazní použitelnosti takto opatřených záznamů lze též připomenout, že v rámci mezinárodní právní pomoci může být vyžadováno provádění odposlechů v cizině, resp. jejich nařízení, a pak lze nepochybně záznamy takto opatřené použít i na území České republiky jako důkazní prostředek.¹⁰⁷

2.1.6 Zničení záznamu odposlechu telekomunikačního provozu

Zničení získaných záznamů je upraveno v odstavci 7, který říká, že pokud nebyly zjištěny skutečnosti významné pro trestní řízení¹⁰⁸, je policejní orgán povinen záznam bezodkladně zničit, a to

- po souhlasu soudu (v přípravném řízení státního zástupce) a
- po uplynutí tří let od pravomocného skončení věci.

Lhůta tří let je stanovena s ohledem na možnost podání mimořádného opravného prostředku, protože pokud ten byl podán ve lhůtě tří let od pravomocného skončení věci, příslušný soud vyrozumí o této skutečnosti příslušný policejní orgán, který provedl úschovu záznamu. V takovém případě policejní orgán nemůže záznam odposlechu zničit, byť by skončila tříletá lhůta po pravomocném skončení věci, poněvadž obhajoba by mohla požadovat využití i těchto záznamů, a proto by nebylo v zájmu spravedlivého procesu tyto záznamy zničit dříve. Policejní orgán proto vyčká rozhodnutí soudu o mimořádném opravném prostředku a podle jeho výsledku buď záznamy odposlechu bezodkladně zničí, nebo je i nadále ponechá v úschově až do nového pravomocného skončení věci a teprve poté postupuje podle tohoto ustanovení.¹⁰⁹

Současně policejní orgán požádá útvar zvláštních činností, aby obdobně zničil i záznamy dosud nepředané a protokol o jejich zničení mu zaslal.

¹⁰⁶ Rozsudek Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006.

¹⁰⁷ Rozsudek Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006.

¹⁰⁸ To se týká i odposlechů, které nebyly provedeny v souladu s podmínkami ustanovení § 88 trestního řádu, tudíž orgány veřejné moci nedisponují oprávněním s nimi nakládat a nelze je použít jako důkaz v trestním řízení. Srov. náleží Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. 615/06, uveřejněný pod č. 88 ve svazku 45 Sbirky nálezů a usnesení Ústavního soudu České republiky.

¹⁰⁹ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1213.

Zničení se provádí nejčastěji smazáním, spálením apod. Vztahuje se nejen na vlastní záznamy (magnetofonové kazety či pásky, počítačové diskety apod.), ale i na přepisy těchto záznamů atd. O zničení je třeba sepsat protokol, ve kterém se uvede mimo obecných náležitostí i způsob zničení.¹¹⁰

Protokol o zničení záznamu nakonec zašle policejní orgán v přípravném řízení státnímu zástupci, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předsedovi senátu prvního stupně, k založení do spisu.

2.1.7 Informační povinnost

Povinnost orgánu činného v trestním řízení, u kterého byla věc pravomocně skončena, aby o nařízeném odposlechu a záznamu telekomunikačního provozu informoval odposlouchávanou osobu uvedenou v odstavci 2, pokud je známa, je upravena v ustanovení § 88 odst. 8 trestního řádu. Tento postup je v souladu s judikaturou ESLP navazující na čl. 8 Úmluvy, podle které vždy, když je to možné a kdy to nepopírá smysl tajného odposlechu, musí být osoba dodatečně seznámena s tím, že její rozhovory byly odposlouchávány, a musí mít k dispozici účinný opravný prostředek, jímž může namítat nezákonnost nebo bezdůvodnost odposlechu.¹¹¹

Osobou uvedenou v odstavci 2 je osoba uživatele odposlouchávané stanice (telekomunikačního zařízení), jejíž osobní údaje a uživatelská adresa by měly být uvedeny v příkazu k odposlechu, pokud byla samozřejmě tato osoba v té době známa. Jinak je možno tyto údaje zjistit i kdykoli později, zejména v průběhu trestního řízení.¹¹²

Informaci podá v řízení před soudem předseda senátu soudu prvního stupně, a to bezodkladně po pravomocném skončení věci, tj. v okamžiku, kdy již nemohou být ohroženy výsledky trestního řízení. V přípravném řízení má pak tuto povinnost státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena. Státní zástupce podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a trestního řádu a policejní orgán bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem podle § 174 odst. 2 písm. e) trestního řádu.

¹¹⁰ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1214.

¹¹¹ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1214.

¹¹² Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1214.

Podle zákona musí tedy informace obsahovat:

- a) označení soudu, který vydal příkaz k odposlechu a záznamu telekomunikačního provozu,
- b) délku trvání odposlechu,
- c) datum jeho ukončení,
- d) poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu.¹¹³

Podle judikatury Nejvyššího soudu je odpovědným předsedou senátu soudu prvního stupně ten předseda senátu soudu prvního stupně v tom konkrétním řízení, v jehož rámci k nařízení odposlechu a záznamu telekomunikačního provozu došlo. Informační povinnost orgánu činného v trestním řízení a s ní související právo podat návrh na přezkoumání nařízení odposlechu a záznamu telekomunikačního provozu tak vzniká pouze po pravomocném skončení té trestní věci, v jejímž rámci k příkazu odposlechu došlo, a je vyloučeno, aby taková informace byla podávána v jiných trestních věcech, byť rovněž pravomocně skončených.¹¹⁴

Tento názor považuji osobně za problematický. Bezprostředně se totiž dotýká užití odposlechu v jiných trestních věcech, než ve kterých došlo k jejich nařízení. Podívejme se pro ukázkou na případ, kterým se zabýval ESLP v rozsudku ve věci Lambert proti Francii. Pan Lambert byl obviněn z trestného činu zatajování těžké krádeže a vzat do vyšetřovací vazby na základě informací získaných odposlechem, který byl nařízen v rámci vyšetřování krádeží a nezákonného držení zbraní na lince jiné osoby. Tyto odposlechy pan Lambert napadl u odvolacího i kasačního soudu, přičemž kasační soud se vyjádřil tak, že pan Lambert není v postavení, které by mu dovolovalo kritizovat podmínky, za nichž bylo nařízeno prodloužení telefonního odposlechu linky přidělené třetí osobě, tudíž jsou takové právní prostředky nepřijatelné. S tím však ESLP nesohlasil. Podle jeho názoru se stěžovateli v tomto případě nedostalo „účinné kontroly“, kterou požaduje právní stát a která by byla způsobilá omezit inkriminované

¹¹³ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1215.

¹¹⁴ Usnesení Nejvyššího soudu ze dne 9. 2. 2012, sp. zn. 4 Pzo 1/2012.

zasahování na to, co je nezbytné v demokratické společnosti.¹¹⁵ Tento případ dle mého názoru vystihuje podstatu celého problému, kdy zatímco jedné osobě by byla přiznána práva na přezkum příkazu k odposlechu, jiné osobě, jejíž práva však byla takovým odposlechem zasažena naprosto stejně, je takové právo odepřeno. To dle mého názoru zakládá nerovnost těchto osob před zákonem.

Nutno bohužel podotknout, že tato nerovnost vzniká již na zákonné úrovni. Trestní řád totiž ukládá informační povinnost pouze vůči osobě uvedené v odstavci 2, tedy osobě uživatele. Výklad Nejvyššího soudu je tak v souladu se zákonem. Podle mého názoru však v tomto směru zákon odporuje čl. 1 odst. 1, čl. 10 odst. 2 a čl. 13 Listiny, stejně jako čl. 8 Úmluvy a judikatuře ESLP.

Samozřejmě jsem si vědoma toho, že takovýto výklad nahrává tvrzení, že odposlech a záznam telekomunikačního provozu nezasahuje pouze do práv uživatele, ale do práv všech osob, jejichž komunikace s uživatelem je zaznamenána, stejně jako do práv osob, které náhodou použijí zařízení, u kterého je takovýto odposlech nařízen. Dalo by se tedy říci, že odposlech by pak musel být nařízen ohledně všech těchto osob a všechny tyto osoby by pak měly být informovány. Taková opatření by však byla dle mého mínění nadbytečná, nehledě i na jejich obtížnou realizovatelnost, která by značně ztížila, ne-li přímo vyloučila provádění tohoto institutu v rámci trestního řízení. Zásah do práv těchto osob je totiž ospravedlnitelný veřejnou potřebou použití tohoto institutu při vyšetřování trestné činnosti na základě zásady proporcionality a subsidiarity a dostatečně podepřen příkazem k odposlechu a záznamu telekomunikačního provozu. Vzhledem k tomu, že těmto osobám nevyplývá z odposlechu žádná jiná újma, není nutné, aby takové osoby byly o odposlechu informovány.

Stejně tak jsem si vědoma toho, že pokud je odposlech použit jako důkaz, může se dotčená osoba domáhat jeho přezkumu již námitkami v rámci řízení, kterými se soud musí zabývat. Mohlo by se tedy zdát, že neposkytnutí informace takovým osobám je v podstatě pouze hypotetický problém, protože důkazy získané těmito odposlechy jsou přezkoumávány již v samotném řízení. Přesto však nelze vyloučit, že i k výše zmíněné situaci může dojít. Pokud je tedy výsledek odposlechu použit v rámci trestního řízení jako důkaz a dotčená osoba může být na jeho základě nebo s jeho přispěním odsouzena,

¹¹⁵ Rozsudek ESLP ze dne 24. 8. 1998, ve věci Lambert proti Francii, stížnost č. 23618/94.

jedná se o závažný zásah do procesních práv a svobod této osoby, a pokud zákon použití odposlechu v jiné trestní věci přípouští, měl by podle mého názoru rovněž uložit informační povinnosti vůči osobám, proti kterým je takové řízení v jiné trestní věci vedeno.

Na druhou stranu však existují i případy, kdy by podání informace podle odstavce 8 bylo krajně nežádoucí. Pro takové případy zákon stanovil v odstavci 9 výjimky, u kterých není nutné takovou informaci poskytnout. Toto omezení není ani v rozporu s judikaturou ESLP navazující na již shora zmíněný čl. 8 Úmluvy, která uvedla, že aktivita nebo nebezpečí, k jejichž potření sledovací opatření směřují, může přetrvávat léta či dokonce desetiletí poté, co bylo od těchto opatření upuštěno. Následné upozornění každé osoby dotčené opatřením by tak mohlo kompromitovat dlouhodobý cíl, kterým bylo původně nařízení sledování odůvodněno.¹¹⁶

Informaci o nařízeném odposlechu a záznamu telekomunikačního provozu tedy předseda senátu, státní zástupce nebo policejní orgán nepodá:

- a) v řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, spáchaném organizovanou skupinou,
- b) v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny,
- c) v řízení o trestném činu účasti na organizované zločinecké skupině (§ 361 trestního zákoníku),
- d) pokud se na spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno,
- e) pokud je proti osobě, již má být informace sdělena, vedeno trestní řízení,
- f) pokud by poskytnutím takové informace mohl být zmařen účel trestního řízení, včetně řízení uvedeného v odstavci 6, nebo
- g) pokud by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob.

Ad a) Pojmem zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, jsem se zabývala již výše. Definice

¹¹⁶ Rozsudek ESLP ze dne 8. 9. 1978, ve věci Klass a další proti Německu, stížnost č. 5029/71.

organizované skupiny je pak dána soudní judikaturou. Organizovanou skupinou se rozumí sdružení více osob (podle soudní praxe nejméně tři trestně odpovědných osob), v němž je provedena určitá dělba úkolů mezi jednotlivé členy sdružení a jehož činnost se v důsledku toho vyznačuje plánovitostí a koordinovaností, což zvyšuje pravděpodobnost úspěšného provedení trestného činu, a tím i jeho nebezpečnost pro společnost. Skupina nemusí mít trvalejší charakter a tímto způsobem lze spáchat i jen ojedinělý, jednorázový trestný čin. Rovněž se nevyžaduje výslovné přijetí za člena skupiny nebo výslovné přistoupení ke skupině. Postačí faktické včlenění se do skupiny a aktivní zapojení se do její činnosti.¹¹⁷

Ad b) Organizovaná zločinecká skupina je společenstvím více osob (nejméně tři trestně odpovědných osob) s vnitřní organizační strukturou, s rozdělením funkcí a dělbou činností, která je zaměřena na soustavné páchání úmyslné trestné činnosti. Na rozdíl od organizované skupiny se tak organizovaná zločinecká skupina vyznačuje stabilitou a trvalejším charakterem svojí existence a činnosti.¹¹⁸

Za pachatele trestného činu spáchaného ve prospěch organizované zločinecké skupiny se považuje pachatel, který spáchal úmyslný trestný čin jako člen organizované zločinecké skupiny, nebo pachatel, který takový čin spáchá vědomě se členem organizované zločinecké skupiny anebo v úmyslu organizované zločinecké skupině napomáhat (srov. §107 odst. 1 trestního zákoníku).

Ad c) Účast na organizované zločinecké skupině je trestným činem podle § 361 trestního zákoníku a může být spáchána buď založením organizované zločinecké skupiny nebo účastí na činnosti organizované zločinecké skupiny nebo podporou organizované zločinecké skupiny, přičemž tento trestný čin může být spáchán členem i nečlenem organizované zločinecké skupiny.

¹¹⁷ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1216.

¹¹⁸ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1216.

Ad d) Na trestném činu se podílí více osob v případě trestné součinnosti. Tou jsou případy, kdy se na trestném činu účastní více spolupachatelů, anebo když jiné osoby jako účastníci trestný čin pachatele nebo spolupachatelů organizují, úmyslně vyvolávají nebo takový čin umožňují nebo usnadňují (organizátor, návodce či pomocník). Dále pak mohou jiné osoby ukrývat, na sebe nebo na jiného převádět nebo užívat věc nebo jinou majetkovou hodnotu získanou trestným činem, popřípadě to, co za ní bylo opatřeno, nebo výnosy z trestného činu, anebo pachatelům či osobám na něm zúčastněným pomohou uniknout trestnímu stíhání nebo trestu, anebo se na něm podílejí dalšími či jinými formami (trestné činy schvalování, nepřekažení a neoznámení trestného činu). Proti takovýmto osobám nemusí být nutně vedeno společné trestní řízení.¹¹⁹

Ad e) Informace se také nepodává, pokud je proti osobě, jíž má být informace sdělena, vedeno trestní řízení, přičemž vzhledem k tomu, že se informace podává po pravomocném skončení věci, musí jít o jiné trestní řízení, než ve kterém byl nařízen odposlech a záznam telekomunikačního provozu. Nezáleží na tom, pro jaký trestný čin se toto další trestní řízení vede. Toto omezení platí do pravomocného skončení takového dalšího trestního řízení.¹²⁰

Tato podmínka je v trestním řádu zahrnuta zejména z důvodu, že pokud probíhá více trestních řízení najednou, není možné určit, ve kterém z nich vznikne potřeba využít výsledky získané odposlechem.

Ad f) Řízením, jehož účel by mohl být zmařen, se míní jak řízení, ve kterém byl odposlech nařízen, tak i jiné, zpravidla navazující řízení, včetně řízení podle odstavce 6.¹²¹

Ad g) Možnost ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob bude odpovědný orgán činný v trestním řízení zvažovat s ohledem na povahu trestného činu, konkrétních okolností případu, včetně skutečností zjištěných

¹¹⁹ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1216-1217.

¹²⁰ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1217.

¹²¹ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1217.

v průběhu odposlechu, a osobu pachatele trestného činu, a to s přihlédnutím k výsledkům řízení, v němž byl nařízen odposlech a záznam telekomunikačního provozu.¹²²

Na tomto místě bych se ráda zabývala dvěma drobnými odlišnostmi mezi ustanoveními § 88 odst. 9 a § 88a odst. 3 trestního řádu. První z nich je formulace „pokud by poskytnutím takové informace mohl být zmařen účel tohoto nebo jiného trestního řízení“, která je v § 88 formulována jako „pokud by poskytnutím takové informace mohl být zmařen účel trestního řízení, včetně řízení uvedeného v odstavci 6“. Vzhledem k ustanovení v § 88 odst. 9 se totiž nabízí výklad, že se jedná pouze o trestní řízení, ve kterém byl odposlech nařízen, popřípadě použit. To však není pravda. Malá záměna v § 88a odst. 3 je tak jasnějším a srozumitelnějším vyjádřením účelu tohoto ustanovení.

Druhou zajímavou odlišností je formulace „nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob“ v § 88 odst. 9, kdy v § 88a odst. 3 je spojka „a“ nahrazena spojkou „nebo“. Opět je zde totiž možné na základě gramatického výkladu vykládat obě ustanovení jinak. § 88 odst. 9 totiž nahrává výkladu, že všechny tyto podmínky musí být splněny kumulativně, tedy že musí najednou dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob. To samozřejmě značně omezuje uplatnění této zákonné výjimky na případy nejzávažnějšího rázu. Záměnu spojky „a“ za spojku „nebo“ v § 88a odst. 3 považuji v tomto případě opět za zdařilou. Je tak totiž zamezeno jakýmkoli spekulacím o možném výkladu a zákon jasně určuje, že se jedná o podmínku alternativní, nikoli kumulativní.

2.1.8 Řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu

Toto řízení je upraveno v části třetí „Řízení před soudem“, hlavě dvacáté „Zvláštní způsoby řízení“, oddílu sedmém, § 314l až 314n trestního řádu. Jedná se o garanci respektování práva na ochranu soukromí a práva na tajemství dopravovaných

¹²² Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1217.

zpráv ze strany orgánů činných v trestním řízení, resp. dodržování zákonných omezení pro využívání odposlechu a záznamu telekomunikačního provozu.¹²³

Řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu je druhem zvláštního řízení, jak tomu napovídá i systematické začlenění. Účelem tohoto řízení je posouzení zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu, přičemž k jeho provedení je příslušný Nejvyšší soud. Tato ustanovení se rovněž uplatňují i v řízení o trestních věcech mladistvých, vzhledem k tomu, že zákon o soudnictví ve věcech mladistvých neobsahuje žádnou samostatnou úpravu, a obdobně i v řízení proti právnickým osobám, poněvadž to není z povahy věci vyloučeno, zvláště když zákon o trestní odpovědnosti právnických osob nemá ohledně těchto příkazů žádné zvláštní ustanovení.¹²⁴ Údaje o tomto řízení jsou vedeny v rejstříku pro odposlechy, který eviduje Nejvyšší státní zastupitelství.

Navrhovatelem je zde osoba uvedená v § 88 odst. 8, jíž se rozumí osoba uživatele odposlouchávané stanice (telekomunikačního zařízení), která byla informována o nařízeném odposlechu a záznamu telekomunikačního provozu.¹²⁵

Předmětem řízení je pouze přezkum dodržení všech zákonných ustanovení o nařízeném odposlechu a záznamu telekomunikačního provozu a jeho provedení ve smyslu § 88 odst. 1 až 5 trestního řádu. Nejvyšší soud se nemůže zabývat přezkumem zákonnosti dokazování, kdy záznam byl použit jako důkaz v řízení, protože k tomu jsou určeny opravné prostředky navazující na konkrétní rozhodnutí ve věci.¹²⁶

Přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu provede Nejvyšší soud v neveřejném zasedání, v senátě složeném z předsedy senátu a dvou soudců.

Shledá-li Nejvyšší soud, že zákon byl porušen při vydání nebo při provedení, případně při vydání i provedení odposlechu a záznamu telekomunikačního provozu,

¹²³ *Jelínek, J. a kol.* Trestní právo procesní. 2. vyd. podle novelizované právní úpravy účinné od 1. 9. 2011. Praha: Leges, 2011, s. 731.

¹²⁴ *Šámal, P. a kol.* Trestní řád II. § 157 až 314s. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 3623, 3625 a 3628.

¹²⁵ *Šámal, P. a kol.* Trestní řád II. § 157 až 314s. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 3623.

¹²⁶ *Šámal, P. a kol.* Trestní řád II. § 157 až 314s. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 3625-3626.

vysloví podle § 314m trestního řádu usnesením porušení zákona.

Na druhou stranu, shledá-li Nejvyšší soud, že vydání a provedení příkazu k odposlechu a záznamu telekomunikačního provozu bylo v souladu s podmínkami uvedenými v § 88 odst. 1 trestního řádu, vysloví podle §314n usnesením, že zákon porušen nebyl.¹²⁷

Problematická je absence právní úpravy, která by stanovila, kdy (a jestli vůbec) je možno návrh odmítnout. Nejvyšší soud tak ve své judikatuře stanovil, že z ustanovení trestního řádu zcela jednoznačně vyplývá, že před pravomocným skončením věci, v níž byl vydán příkaz k odposlechu a záznamu telekomunikačního provozu, a bez následného zaslání informace předsedou senátu soudu prvního stupně, resp. státním zástupcem nebo policejním orgánem, osobě uvedené v § 88 odst. 2 trestního řádu, nelze návrh na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu k Nejvyššímu soudu podat.¹²⁸ Nejvyšší soud tak není oprávněn v těchto případech zahájit řízení ve smyslu ustanovení § 314l a učinit o podaných návrzích konečné rozhodnutí. Vzhledem k tomu aplikuje v těchto (a obdobných)¹²⁹ případech podle analogie legis ustanovení § 265i odst. 1 písm. a) trestního řádu a návrh odmítne.

Ve všech případech rozhoduje Nejvyšší soud formou usnesení, proti kterému není opravný prostředek přípustný, a to ani řádný, ani mimořádný.

Smyslem tohoto řízení je ochránit osoby, které se o provedení odposlechu nedozvěděli jinou cestou, protože odposlech nebyl v rámci řízení použit jako důkaz

¹²⁷ V tomto ustanovení narážíme na určitý nesoulad. Zatímco § 314l a 314m obecně odkazují na zákonnost příkazu, § 314n odkazuje již konkrétně na soulad s podmínkami § 88 odst. 1. To je však nepřesné. Odstavec 1 sice upravuje základní podmínky nařízení odposlechu a záznamu telekomunikačního provozu, procedury vydávání a provádění jsou však upraveny i v následujících odstavcích. Je nutno tudíž tuto normu vykládat v souladu se všemi odstavci, ve kterých je upraveno vydání a provádění odposlechu a záznamu telekomunikačního provozu. Vzhledem k vymezení rozsahu přezkumu při prohlášení porušení zákona však nemůže tento nesoulad v praxi způsobit, že by došlo k prohlášení souladu, přestože by byla porušena některá z podmínek v odstavcích 2 až 5. Srov. Šámal, P. a kol. Trestní řád II. § 157 až 314s. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 3628.

¹²⁸ Usnesení Nejvyššího soudu ze dne 14. 10. 2010, sp. zn. 4 Pzo 1/2010.

¹²⁹ Např. při podání návrhu na přezkoumání odposlechu a záznamu telekomunikačního provozu v případech trestních věcí pravomocně skončených před datem účinnosti novely provedené zákonem č. 177/2008 Sb., který vstoupil v účinnost dne 1. 7. 2008. Usnesení Nejvyššího soudu ze dne 30. 1. 2012, sp. zn. 4 Pzo 4/2011.

nebo protože proti nim nebylo zahájeno trestní stíhání, popřípadě nebyla podána obžaloba. Je tedy nutno si uvědomit, že samotné vyslovení porušení zákona má pouze deklaratorní charakter a nemá přímý vliv na rozhodnutí, jež bylo učiněno v samotném řízení, ve kterém byly odposlechy využity. Primárně lze tedy rozhodnutí použít jako právní titul pro nárok na finanční zadostiučinění za vzniklou nemajetkovou újmu. Toto rozhodnutí však může být rovněž impulsem k podání opravného prostředku některou z oprávněných osob. Vzhledem k tomu, že uživatel odposlouchávaného zařízení je o provedení odposlechu vyrozuměn až po pravomocném skončení věci, půjde zpravidla o opravné prostředky mimořádné (stížnost pro porušení zákona).¹³⁰ Stanovení přezkumu má mít i určitou preventivní roli v tom smyslu, že uvedená možnost přezkumu Nejvyšším soudem povede orgány činné v trestním řízení k maximální obezřetnosti při dodržování ustanovení o nařízení a provádění odposlechu a záznamu telekomunikačního provozu, a tím k naplňování nejen principu zákonnosti, ale i zdrženlivosti (přiměřenosti) vymezeného v § 2 odst. 4 trestního řádu.¹³¹ K tomuto řízení se vztahuje ještě § 30 odst. 4 trestního řádu, který stanoví ve větě první vyloučení z řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu toho soudce, který se zúčastnil rozhodování v předchozím řízení.

Předchozím řízením je z hlediska dikce ustanovení celé řízení, jež předcházelo řízení o přezkumu příkazu, protože v rámci celého předchozího řízení je zpravidla přezkoumávána mimo jiné i zákonnost provedeného odposlechu, což je rozhodující v otázce, zda bude jeho obsah v rámci navazujícího řízení použit jako důkaz. Vyloučeným soudcem tedy bude v tomto případě bezpochyby soudce, který nařídil odposlech a záznam telekomunikačního provozu, a dále pak soudci rozhodující o vině. Na druhou stranu jím nebude například soudce, který ustanovil obhájce nebo se zúčastnil neodkladného nebo neopakovatelného úkonu, protože takové řízení nenavazuje na příkaz o nařízení odposlechu a není tudíž předchozím řízením ve smyslu tohoto ustanovení.¹³²

Podle věty druhé tohoto paragrafu je pak rovněž vyloučen z rozhodování

¹³⁰ Srov. *Jelínek, J. a kol.* Trestní právo procesní. 2. vyd. podle novelizované právní úpravy účinné od 1. 9. 2011. Praha: Leges, 2011, s. 732.

¹³¹ *Šámal, P. a kol.* Trestní řád II. Komentář. 6. vyd. Praha: C. H. Beck, 2008, s. 2417.

¹³² Srov. *Šámal, P. a kol.* Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 381-382.

v dalším řízení ten soudce, který se účastnil rozhodování v řízení o přezkumu příkazu k odposlechu. Vylučujícím důvodem je zde pouze účast na rozhodování, nikoli jiná činnost. K vyloučení soudce Nejvyššího soudu tak může dojít, pokud po rozhodnutí o zákonnosti příkazu k nařízení odposlechu bude podán některý mimořádný opravný prostředek (a to i z důvodu, který nesouvisí s provedeným odposlechem a záznamem telekomunikačního provozu), v jehož důsledku bude zrušeno předchozí pravomocné rozhodnutí a věc bude přikázána soudu k novému projednání a rozhodnutí.¹³³

2.1.9 Přeshraniční odposlech

Jak jsem již naznačila výše, je odposlech a záznam telekomunikačního provozu využíván při vyšetřování té nejzávažnější kriminality. Ta se však mnohdy neomezuje pouze na území jednoho státu, ale má mezinárodní charakter. Proto je nutné, aby při jejím vyšetřování příslušné státní složky disponovaly prostředky umožňujícími efektivní spolupráci.

V rámci Evropské unie je tato problematika upravena Úmluvou o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie (dále „Úmluva o pomoci v trestních věcech“).

Na tuto úmluvu navazuje trestní řád v § 437a, který implementuje do české právní úpravy čl. 20 této úmluvy. Ten se vztahuje na použití odposlechu telekomunikačního provozu bez technické pomoci jiného členského státu. V této souvislosti je však nutno zmínit, že dne 30. 4. 2013 vstoupil v platnost zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, účinný od 1. 1. 2014. Tento zákon upravuje veškeré formy justiční spolupráce orgánů ČR se zahraničními orgány, tedy i přeshraniční odposlech, který je upraven v § 64 tohoto zákona. Zároveň tento zákon ruší celou hlavu dvacátou pátou trestního řádu, která až do teď justiční spolupráci upravovala.

Podstata přeshraničního odposlechu spočívá v tom, že příkaz k odposlechu je vydán v jednom členském státě, kde dotčená odposlouchávaná osoba využívá služeb svého telefonního operátora (dále „stát provádějící odposlech“), ovšem pohybuje se a je odposlouchávána v příhraničním území druhého, sousedního členského státu (dále „uvědomovaný stát“), aniž je z tohoto státu poskytována jakákoli technická podpora

¹³³ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 382-383.

k prováděnému odposlechu.¹³⁴

Podle této úmluvy musí stát provádějící odposlech uvědomit členský stát, na jehož území je nebo má být odposlech prováděn, aby tento mohl ve lhůtě 96 hodin rozhodnout, zda souhlasí s pokračováním nebo provedením odposlechu, či zda požaduje, aby byl ukončen nebo neproveden. Provedení odposlechu může uvědomovaný stát podmínit i splněním podmínek, které je třeba dodržet v obdobném vnitrostátním případě. K tomuto uvědomění musí dojít buď před odposlechem, nebo bezprostředně poté, co se stát provádějící odposlech dozví, že se odposlouchávaná osoba nachází na území uvědomovaného členského státu.¹³⁵ Uvědomovaný stát, pokud nedal souhlas s provedením odposlechu, se také musí vyjádřit, zda je záznam získaný v době, kdy se odposlouchávaná osoba nacházela na jeho území, možno použít jako důkaz v trestním řízení, popřípadě za jakých podmínek.¹³⁶ Uvědomovaný stát rovněž může požádat o prodloužení původní lhůty (nejvýše však o 8 dnů), aby mohly být provedeny potřebné postupy podle jeho vnitrostátních právních předpisů. Dokud uvědomovaný stát nepřijme jedno z výše uvedených rozhodnutí, smí stát provádějící odposlech v jeho provádění pokračovat, ale materiály získané odposlechem nesmí použít, ledaže se dotyčné státy dohodnou jinak nebo je třeba přijmout naléhavé opatření, aby se zabránilo bezprostřednímu a vážnému ohrožení veřejné bezpečnosti.

Toto ustanovení je sice přímo vykonatelné, vzhledem k jeho proveditelnosti však bylo nutné upravit příslušnost jednotlivých orgánů k postupu a podmínky takového postupu ve vnitrostátním právu. Ostatně čl. 20 odst. 4 písm. d) Úmluvy o pomoci v trestních věcech stanoví povinnost členských států přijmout nezbytná opatření, aby zajistily, že odpověď bude poskytnuta v 96hodinové lhůtě, a zřídit kontaktní místa s 24hodinovou denní pracovní dobou.

Podmínky uplatnění ustanovení § 437a trestního řádu tedy jsou:

¹³⁴ Šámal, P. a kol. Trestní řád III. § 315 až 471. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 4319.

¹³⁵ Vzhledem k automatickému provádění odposlechu je tato úprava problematická. ZPPP proto stanoví v čl. 67 odst. 5 povinnost policejního orgánu informovat státního zástupce, pokud zjistí, že část odposlechu byla provedena v době, kdy se odposlouchávaná stanice nacházela v cizím státě, přičemž k odposlechu nebylo třeba technické součinnosti tohoto státu. V takovém případě může uvědomovaný stát dát již pouze souhlas s použitím výsledku odposlechu.

¹³⁶ Srov. Šámal, P. a kol. Trestní řád III. § 315 až 471. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 4319.

- 1) vázanost na existenci vyhlášené mezinárodní smlouvy, kterou je Česká republika vázána, a
- 2) splnění podmínek uvedených v § 88 trestního řádu.¹³⁷

Udělení souhlasu s provedením přeshraničního odposlechu je koncentrováno u Krajského soudu v Praze. V případě, že odposlech je v cizím státě prováděn ve stádiu před podáním obžaloby, podává návrh krajskému soudu státní zástupce Krajského státního zastupitelství v Praze. Informace poskytované státem provádějícím odposlech budou do České republiky přicházet prostřednictvím Policejního prezidia.¹³⁸

Ustanovení rovněž upravuje případy, kdy Česká republika bude chtít provést přeshraniční odposlech v cizím státě. V takovém případě informuje cizozemský orgán ten justiční orgán, který v České republice trestní řízení vede, tj. státního zástupce v přípravném řízení nebo soud po podání obžaloby.¹³⁹

2.2 Zjišťování údajů o telekomunikačním provozu

Institut zjišťování údajů o telekomunikačním provozu upravený v § 88a trestního řádu slouží k získávání těch údajů, které vznikly v souvislosti s již uskutečněným telekomunikačním provozem a na něž se rovněž vztahuje ochrana zakotvená v čl. 13 Listiny.^{140, 141} Těmi jsou podle § 136 odst. 20 písm. b) zákona o

¹³⁷ Šámal, P. a kol. Trestní řád III. § 315 až 471. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 4319.

¹³⁸ Šámal, P. a kol. Trestní řád III. § 315 až 471. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 4319.

¹³⁹ Šámal, P. a kol. Trestní řád III. § 315 až 471. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 4319.

¹⁴⁰ K tomu se několikrát vyjádřil i Ústavní soud, dle jehož názoru je třeba považovat výše uvedené údaje, zvláště pak volaná čísla, za nedílnou součást komunikace uskutečněné prostřednictvím telefonu. Nález Ústavního soudu ze dne 22. 1. 2001, sp. zn. II.ÚS 502/2000, uveřejněný pod č. 11 ve svazku 21 Sbírký nálezů a usnesení Ústavního soudu České republiky.

¹⁴¹ Této ochrany však nepoživají ty „vedlejší“ údaje, které jsou nezbytné k uplatnění právních nároků provozovatele telekomunikačních služeb vůči osobě, jíž jsou tyto služby poskytovány. Pokud by totiž provozovatel telekomunikačních služeb nemohl tyto „vedlejší“ údaje nikomu poskytnout, ocitl by se v nerovném postavení, které by mu znemožňovalo dosáhnout svých práv. Ani orgány činné v trestním řízení nejsou v takových případech vázány podmínkami § 88a trestního řádu a mohou tyto „vedlejší“ údaje použít jako důkaz při stíhání trestných činů namířených proti majetkovým právům poškozených provozovatelů telekomunikačních služeb. Usnesení Ústavního soudu ze dne 29. 4. 2004, sp. zn. IV. ÚS 554/03, uveřejněné pod č. 27 svazku 33 Sbírký nálezů a usnesení Ústavního soudu České republiky.

elektronických komunikacích provozní a lokalizační údaje, kterými se podle § 97 odst. 4 zákona o elektronických komunikacích rozumí údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času způsobu a doby trvání komunikace (např. číslo volané stanice, datum a čas počátku hovoru, doba trvání hovoru, označení základové stanice, která zajišťovala hovor v okamžiku spojení, a označení základové stanice, která zajišťovala hovor v okamžiku jeho ukončení).¹⁴²

V průběhu trestního řízení bývají tyto údaje použity ke zjištění a zajištění důkazního prostředku, z něhož lze často dovodit naplnění základních znaků skutkových podstat jednotlivých trestných činů, dále prokázání opakovanosti a organizovanosti trestné činnosti, prověřování alibi jednotlivých procesních stran, zejména pachatelů, potenciálních spolupachatelů, svědků apod. Rovněž je takový důkazní prostředek nezbytný k prvotnímu určení možných pachatelů. Převážně jednotlivé dílčí útoky pokračujícího trestného činu je možné díky provozním a lokalizačním údajům vzájemně provázat do série. Na základě analýzy provozních a lokalizačních údajů lze efektivněji rozhodnout i o využití jiných úkonů trestního řízení. I o tzv. anonymních SIM kartách lze díky provozním a lokalizačním údajům zajistit řadu důkazů využitelných pro trestní řízení.¹⁴³

Tento institut však nemusí být uplatněn pouze samostatně, ale i v rámci provádění jiného úkonu podle trestního řádu (např. znalecký posudek). Pokud by totiž při získávání těchto údajů v rámci trestního řízení byl postup podle ustanovení § 88a vynechán, založilo by to nezákonnost takového úkonu, stejně jako nezákonnost takovýmto úkonem získaného důkazu.¹⁴⁴

¹⁴² Provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování. Lokalizačními údaji se pak rozumí jakékoli údaje, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací. Rozsah uchovávaných provozních a lokalizačních údajů, formu a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu a způsob jejich likvidace stanoví prováděcí právní předpis.

¹⁴³ Srov. důvodová zpráva k návrhu zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Poslanecká sněmovna, 2012.

¹⁴⁴ Vyžádání provozních a lokalizačních údajů od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací způsobem

Je tedy zřejmé, že se jedná o důležitý institut, bez jehož uplatnění v trestním řízení by bylo odhalování pachatelů trestné činnosti páchané pomocí mobilních telefonů či internetu značně ztíženo, a u některých typů trestné činnosti dokonce znemožněno.¹⁴⁵

2.2.1 Podmínky pro nařízení zjišťování údajů o telekomunikačním provozu a náležitosti příkazu

Podmínky pro nařízení zjišťování údajů o telekomunikačním provozu a náležitosti takového příkazu jsou uvedeny v ustanovení § 88a odst. 1 trestního řádu. Vyžádání údajů o telekomunikačním provozu je možno uplatnit, je-li trestní řízení vedeno:

- a) pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, nebo
- b) 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

umožňujícím dálkový a nepřetržitý přístup je možné i podle zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů, zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, zákona č. 15/1998, o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů a zákona č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, ve znění pozdějších předpisů. V trestním řízení je však možné postupovat pouze podle § 88a. Dalším podobným ustanovením je pak § 158d odst. 9 trestního řádu, vůči kterému je § 88a speciálním ustanovením. Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, 1228-1229.

¹⁴⁵ Srov. důvodová zpráva k návrhu zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Poslanecká sněmovna, 2012.

trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo

- c) pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána.

Ad a) Okruh trestných činů je navržen s ohledem na přiměřenost zásahu do lidských práv, přičemž hranice sazby je odvozena z možnosti vzetí do vazby pro neúmyslný trestný čin. Zákonodárce vycházel z faktu, že jestliže se pro trestné činy s uvedenou trestní sazbou umožňuje vzetí osoby do vazby, což je nejinvazivnější prostředek trestního práva vedoucí ke zbavení její osobní svobody, pak je na místě, aby u takové kategorie trestných činů bylo možné získávat provozní a lokalizační údaje podle § 88a trestního řádu.¹⁴⁶ Otázkou však je, proč zákonodárce tedy nestanovil tuto hranici na 2 roky, což je minimální hranice horní trestní sazby pro úmyslné trestné činy, pro které může být vzat obviněný do vazby. Vzhledem k tomu, že ustanovení § 88a mluví o vyšetřování úmyslných trestných činů, byla by podle mého názoru taková úprava, a to i vzhledem k uvedené argumentaci, vhodnější.

Ad b) Na základě zkušeností z praxe byly tyto trestné činy do výčtu zahrnuty, protože by bez provozních a lokalizačních údajů nemohly být vůbec objasněny nebo by bylo jejich objasnění značně ztíženo. Jedná se totiž o trestné činy, které jsou ve velké míře páčány prostřednictvím internetu nebo mobilních telefonů.¹⁴⁷

Ad c) Tato skupina je do výčtu zařazena, aby bylo efektivně zajištěno plnění mezinárodních závazků České republiky. V opačném případě by se totiž Česká republika vystavila kritice ze strany příslušných mezinárodních organizací, zejména Rady Evropy (více viz výše).¹⁴⁸

¹⁴⁶ Důvodová zpráva k návrhu zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Poslanecká sněmovna, 2012.

¹⁴⁷ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1231.

¹⁴⁸ Důvodová zpráva k návrhu zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Poslanecká sněmovna, 2012.

Tyto podmínky jsou ještě doplněny požadavkem, že sledovaného účelu nelze dosáhnout jinak nebo by bylo jeho dosažení podstatně ztíženo, čímž je vyjádřen požadavek subsidiarity zjišťování údajů o telekomunikačním provozu, který má omezit používání tohoto institutu na nejnútnejší případy.

Účelem uplatnění tohoto institutu je podle zákona zjištění údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat.

Předmět telekomunikačního tajemství je následně vymezen v § 88 a násl. zákona o elektronických komunikacích. Podle § 88 odst. 1 je mimo jiné podnikatel poskytující veřejně dostupnou službu elektronických komunikací povinen zajistit technicky a organizačně bezpečnost poskytované služby s ohledem na ochranu osobních údajů fyzických osob v souladu se zvláštním právním předpisem, ochranu provozních a lokalizačních údajů a důvěrnost komunikací fyzických a právnických osob při poskytování této služby.

Poskytování osobních a zprostředkovacích dat je pak upraveno v § 97 odst. 3 zákona o elektronických komunikacích. Toto ustanovení uvádí, že právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací (dále „osoba“) je povinna uchovávat po dobu šesti měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejich veřejných komunikačních sítí a při poskytování jejich veřejně dostupných služeb elektronických komunikací. Po uplynutí této doby je taková osoba povinna tyto údaje zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu. Naproti tomu provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je tato osoba povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je povinna zajistit, aby při plnění těchto povinností nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout mj. též orgánům činným v trestním řízení pro účely a za podmínek stanovených zvláštním právním předpisem, kterým je § 88a trestního řádu.

Vydání údajů o telekomunikačním provozu nařídí v řízení před soudem předseda senátu (i odvolacího soudu) nebo samosoudce a v přípravném řízení nařídí jejich vydání

státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce. Příkaz ke zjišťování údajů o telekomunikačním provozu musí být vydán písemně a musí být odůvodněn. Rovněž i tento příkaz je rozhodnutím sui generis a není proti němu přípustná stížnost.

Oproti předchozí úpravě je nyní již stanovena povinnost předkládat žádosti o vydání příkazu v přípravném řízení prostřednictvím státního zástupce, což má vést k větší odpovědnosti státního zástupce při podávání návrhu na vydání příkazu. Státní zástupce tento návrh podává zpravidla na základě písemného a odůvodněného návrhu (podnětu) policejního orgánu. Před podáním návrhu na vydání příkazu soudu státní zástupce ověří, zda je vedeno trestní řízení pro trestný čin, pro který lze tento úkon nařídit. Učiní tak zejména posouzením, zda užitá právní kvalifikace odpovídá skutku popsanému v záznamu o zahájení úkonů trestního řízení nebo v usnesení o zahájení trestního stíhání, přičemž musí vycházet z konkrétních skutkových okolností v době, kdy má být takový návrh podán. Rovněž musí prověřit, zdali vydání příkazu je nezbytné pro získání skutečností významných pro trestní řízení. Dále musí prověřit, že sledovaného účelu nelze dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztíženo a že informace, které jsou podkladem pro podání návrhu na vydání tohoto příkazu, umožňují náležité vymezení údajů, které mají být tímto postupem získány. Státní zástupce v návrhu též uvede rozsah vyžadovaných údajů a návrh náležitě odůvodní. Žádost musí být písemná a musí obsahovat odkaz na konkrétní mezinárodní smlouvu v případě, že je vedeno trestní řízení pro trestný čin, k jehož stíhání mezinárodní smlouva zavazuje. Dále by v ní měl být identifikován uživatel používající komunikační prostředky, pokud je jeho totožnost známa. Je jasné, že se totožnost uživatele komunikačních prostředků nebude uvádět ve všech případech, neboť v určitých situacích by to bylo naprosto nelogické, zatěžující a neefektivní, např. u základové stanice, jejíž provoz má být zjišťován.¹⁴⁹ Soudce v případě vydání příkazu na návrh státního zástupce rozhoduje bez zbytečného odkladu, případně ve lhůtě dohodnuté se státním zástupcem.

Obsah příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu

¹⁴⁹ Srov. důvodová zpráva k návrhu zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Poslanecká sněmovna, 2012.

vyplývá ze znění § 88a odst. 1 trestního řádu a z jeho povahy jako rozhodnutí sui generis, proto musí mimo obecných náležitostí obsahovat:

- a) sdělení konkrétních údajů o uskutečněném telekomunikačním provozu (s odkazem na ustanovení zákona o elektronických komunikacích),
- b) dobu, za kterou mají být tyto údaje sděleny (se zřetelem na omezení uvedená v § 97 odst. 3 zákona o elektronických komunikacích),
- c) vztahuje-li se žádost ke konkrétnímu uživateli, jeho totožnost, je-li známa,¹⁵⁰
- d) účel zjišťování těchto údajů ve formě zejména údajů o trestném činu, pro který se řízení vede nebo pro který bylo zahájeno trestní stíhání,
- e) odkaz na příslušnou mezinárodní smlouvu, je-li trestní řízení vedeno pro trestný čin, k jehož stíhání zavazuje tato mezinárodní smlouva,
- f) kterému orgánu mají být tyto informace v přípravném řízení sděleny a
- g) jakým způsobem mají být požadované údaje sděleny (např. v písemné zprávě nebo způsobem umožňujícím dálkový a nepřetržitý přístup atd.).¹⁵¹

Údaje o osobě uživatele mohou být zjištěny i kdykoli později, zejména v průběhu trestního řízení. V tomto směru je však třeba upozornit na okolnost, že právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat provozní a lokalizační údaje pouze po dobu šesti měsíců a po uplynutí této doby je tato osoba povinna tyto údaje zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání. To znamená, že mnohdy může vyplynout nutnost vyžádání těchto údajů v době, kdy tyto nejsou již k dispozici.

Opis příkazu se zašle bezodkladně státnímu zástupci, příp. policejnímu orgánu při online spojení, a právnické nebo fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací.¹⁵² V žádosti uvede policejní orgán číslo jednací trestního spisu, ke kterému mají být údaje vyžádány,

¹⁵⁰ Pokud policejní orgán nezná konkrétní údaje o uživateli, může být příkaz vydán na základě informací o tom, kdy a kde se uživatel pohyboval (tzv. výpisy na buňku).

¹⁵¹ Srov. Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1232.

¹⁵² Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J. Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003, s. 83.

a s příkazem soudce nebo souhlasem uživatele ji předá útvaru zvláštních činností. Nastane-li potřeba některé údaje použít v trestním řízení jako důkaz, vyžádá si policejní orgán prostřednictvím příslušného pracoviště útvaru zvláštních činností jejich autorizaci.

K obsahovým náležitostem příkazu a postupu soudu při jeho vydávání se vyjádřil i Ústavní soud, a to v nálezu sp. zn. II. ÚS 789/06. Stěžovatel v této věci napadl postup soudu při vydání příkazu podle § 88a odst. 1 trestního řádu, který obsahoval označení žádajícího policejního orgánu, označení jím vedeného trestního řízení, označení trestného činu, popis vytykaného skutku, označení telefonních stanic a jejich uživatele, sledované období a konečně závěr: „*Vzhledem k tomu, že jde o objasnění skutečností důležitých pro trestní řízení a vyhodnocením získaných informací by bylo možno zjistit tyto skutečnosti, soud návrhu vyhověl v rozsahu uvedeném shora.*“ Ústavní soud stěžovateli dal za pravdu a uvedl, že soudce se v tomto případě nezabýval ani otázkou, zda trestní řízení bylo řádně zahájeno, tedy o jaké indicie se opírá závěr o důvodnosti podezření, že se stěžovatel mohl dopustit trestného jednání, jak bylo vyloženo shora, ani tím, k čemu konkrétně je zjištění požadovaných informací v rámci trestního řízení třeba, ani proč je možné tento úkon provést jako „obyčejný“, a nikoliv jako neodkladný nebo neopakovatelný. Předmětnému příkazu tudíž schází smysluplné odůvodnění, resp. propojení s jakýmkoliv ústavně chráněným účelem.¹⁵³

Dále uvedl, že účel zjišťování údajů podle § 88a odst. 1 trestního řádu je nutno zkoumat s ohledem na to, zda se stal skutek, v němž je spatřován trestný čin, zda tento skutek spáchal obviněný, případně z jakých pohnutek jej spáchal, a to jako na podstatné okolnosti mající vliv na posouzení nebezpečnosti činu. Tato kritéria totiž předpokládají, že je dána legitimita zásahu do práva na respektování soukromého života, namísto aby se posuzovala přítomnost kritérií opodstatňujících tento zásah. Vždy je tedy nutné účel zjišťování údajů podle § 88a odst. 1 trestního řádu posuzovat s ohledem na to, zda se jedná o nezbytný zásah v legitimním veřejném zájmu a zda se jedná o zásah přiměřený sledovanému cíli.¹⁵⁴

¹⁵³ Nález Ústavního soudu ze dne 27. 9. 2007, sp. zn. II. ÚS 789/06, uveřejněný pod č. 150 ve svazku 46 Sbírký nálezů a usnesení Ústavního soudu České republiky.

¹⁵⁴ Nález Ústavního soudu ze dne 27. 9. 2007, sp. zn. II. ÚS 789/06, uveřejněný pod č. 150 ve svazku 46 Sbírký nálezů a usnesení Ústavního soudu České republiky.

I v řízení podle § 88a odst. 1 trestního řádu je tedy nutné zkoumat opodstatněnost vedení příslušného trestního řízení. Pokud je řízení vedeno pouze na základě důvodného podezření, že byl spáchán trestný čin, tj. pokud byly teprve zahájeny úkony trestního řízení, musí být v odůvodnění vyloženo, o jaké skutečnosti se takový závěr opírá. Pouhé trestní oznámení samo o sobě, není-li doloženo alespoň indiciemi, z nichž lze důvodné podezření dovozovat, a opírá se tudíž jen o spekulativní úvahu, nepostačuje k nařízení tohoto institutu.¹⁵⁵

Pokud se tedy soud před vydáním příkazu k odposlechu dle § 88 a 88a trestního řádu nezabývá ani důvodností trestního řízení, ani konkrétním účelem vyžadovaných informací, porušuje právo na ochranu listovního tajemství a jiných záznamů a zpráv podle čl. 13 Listiny a nesplňuje svoji povinnost poskytovat zákonem stanoveným způsobem ochranu právům podle čl. 90 věty první Ústavy.¹⁵⁶

Ústavní soud nakonec uvedl, že zásah do základních lidských práv a svobod je možný pouze tehdy, pokud jsou zákonem poskytnuty dostatečné záruky, které představuje především soudní kontrola (tedy nezbytnost soudního příkazu). V této souvislosti je nutno opětovně připomenout, že i v trestním řízení je úkolem soudů poskytovat zákonem stanoveným způsobem ochranu právům, a to i právům a svobodám zaručeným ústavním pořádkem, jak bylo uvedeno výše. Soudní kontrola přitom musí být důsledná a efektivní, zejména s ohledem na povahu daného řízení, které nepředpokládá účast protistrany před rozhodnutím soudu. V praktické podobě se pak efektivita soudní ochrany projevuje v odůvodnění soudního příkazu, které odpovídá jak požadavkům zákona, tak ústavním principům, z nichž zákonné ustanovení vychází.¹⁵⁷

Důkazem, který je možno použít i v řízení před soudem, je v případě použití zjišťování údajů o telekomunikačním provozu zpráva o zjištění údajů o telekomunikačním provozu, která může být poskytnuta v písemné podobě, ale i v elektronické podobě, způsobem umožňujícím dálkový a nepřetržitý přístup

¹⁵⁵ Nález Ústavního soudu ze dne 27. 9. 2007, sp. zn. II. ÚS 789/06, uveřejněný pod č. 150 ve svazku 46 Sbírký nálezů a usnesení Ústavního soudu České republiky.

¹⁵⁶ Srov. nález Ústavního soudu ze dne 27. 9. 2007, sp. zn. II. ÚS 789/06, uveřejněný pod č. 150 ve svazku 46 Sbírký nálezů a usnesení Ústavního soudu České republiky.

¹⁵⁷ Nález Ústavního soudu ze dne 27. 9. 2007, sp. zn. II. ÚS 789/06, uveřejněný pod č. 150 ve svazku 46 Sbírký nálezů a usnesení Ústavního soudu České republiky.

k vyžadování informací z databáze účastníků veřejné telekomunikační služby i předávání dat souvisejících s poskytováním telekomunikační služby, kdy však požadované údaje o uskutečněném telekomunikačním provozu musí být zachyceny způsobem, který umožňuje pozdější provedení důkazu v řízení před soudem (např. v listinné podobě po jejím vytištění a autorizování, nebo na elektronických médiích, která umožňují ověřit věrohodnost a správnost předaných údajů poskytovatelem telekomunikační služby).¹⁵⁸ Na rozdíl od odposlechu není u zjišťování údajů o telekomunikačním provozu tato možnost dána zákonem přímo v ustanovení § 88a trestního řádu, a je tudíž nutno vycházet z obecných ustanovení § 89 odst. 2 a § 112 trestního řádu. Tato úprava mi přijde jako dostatečná, protože výsledkem zjišťování je zde zpráva zachycená v listinné podobě nebo na technickém médiu a k jejímu provedení není zapotřebí vyhotovit doprovodný protokol.

Judikaturou Ústavního soudu však byla řešena otázka, jak je to se zprávou jako důkazem, která byla získána, aniž by byl vydán příkaz k jejímu poskytnutí, a to v nálezů sp. zn. IV. ÚS 1556/07. V daném případě poskytli mobilní operátoři orgánům Policie České republiky na základě blíže nespecifikované žádosti údaje o hovorech prováděných z odcizených mobilních telefonů, přičemž však u části těchto žádostí nebyl vydán příkaz k jejich poskytnutí. Ústavní soud k tomu uvedl, že při projednávání předmětného případu obecné soudy zásadně pochybily, když připustily, že část nezákonně pořízené evidence o telekomunikačním provozu byla do spisu nejen zařazena, ale také jako důkaz provedena a následně v rozhodnutích hodnocena.¹⁵⁹

Základním předpokladem řádného výkonu spravedlnosti dle čl. 36 Listiny v demokratickém právním státě je totiž dodržování nejen ústavních, ale i zákonných mezí pro pořizování a provádění důkazů. Proto také postup kteréhokoli orgánu činného v trestním řízení, vybočující z rámce procesních předpisů v tomto ohledu, je v rozporu s ústavností státu a ve svých důsledcích znehodnocuje i samotný účel trestního řízení. Provedení a hodnocení nezákonně pořízených důkazů soudy v rámci trestního řízení tak

¹⁵⁸ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1233.

¹⁵⁹ Nález Ústavního soudu ze dne 3. 8. 2010, sp. zn. IV. ÚS 1556/07, uveřejněný pod č. 152 svazku 58 Sbírký nálezů a usnesení Ústavního soudu České republiky.

zakládá porušení práva na spravedlivý proces dle čl. 36 odst. 1 Listiny.¹⁶⁰

Z toho vyplývá, že takový nedostatek je nekonvalidovatelný, a na rozdíl od nedostatků samotného příkazu, které je možné odstranit i v řízení před soudem, absence příkazu samotného je důvodem pro absolutní neplatnost důkazu takto získaného.

Jak jsem již uvedla výše, bylo původní ustanovení zrušeno nálezem Ústavního soudu sp. zn. Pl. ÚS 24/2011. Otázkou je, zdali nové ustanovení splňuje veškeré požadavky, jejichž nedostatek Ústavní soud v tomto nálezu původnímu ustanovení vytýkal. Zejména mám pochybnosti ohledně ustanovení, která regulují nakládání s těmito údaji ze strany orgánů činných v trestním řízení. Ta by měla obsahovat jasná a detailní pravidla obsahující minimální požadavky na uchovávání těchto záznamů, popřípadě ničení těch zpráv, které nejsou použity jako důkaz v trestním řízení. Jedná se zejména o to, že k těmto zprávám, a tudíž i těmto citlivým informacím, mohou mít přístup i třetí osoby.¹⁶¹ Vzhledem k tomu, že tato úprava v § 88a trestního řádu stále chybí, je nutné v souladu s judikaturou Ústavního soudu v těchto případech postupovat per analogiam podle ustanovení § 88 trestního řádu.

2.2.2 Informační povinnost

Stejně jako u odposlechu a záznamu telekomunikačního provozu byla i u zjištění údajů o telekomunikačním provozu zavedena v odstavci 2 informační povinnost, která je v souladu s požadavky stanovenými judikaturou ESLP. Vzhledem k tomu, že podrobně se touto úpravou zabývám již u odposlechu a obě ustanovení jsou téměř totožná, zopakují nyní pouze základní skutečnosti.

Tuto povinnost má v řízení před soudem předseda senátu soudu prvního stupně, který informaci podá bezodkladně po pravomocném skončení věci. V přípravném řízení pak státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně

¹⁶⁰ Nález Ústavního soudu ze dne 3. 8. 2010, sp. zn. IV. ÚS 1556/07, uveřejněný pod č. 152 svazku 58 Sbírký nálezů a usnesení Ústavního soudu České republiky.

¹⁶¹ Zároveň bych však chtěla ještě zdůraznit, že zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnosti způsobilosti, ve znění pozdějších předpisů, a nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, utajení těchto údajů naprosto opomíjejí, tudíž by byla vhodná i změna těchto právních předpisů.

skončena. Státní zástupce podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a trestního řádu a policejní orgán podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem podle § 174 odst. 2 písm. e) trestního řádu.

Informace je směřována vůči osobě uživatele veřejně dostupné služby elektronických komunikací podle odstavce 1, pokud je známa. Tou je osoba, jejíž osobní údaje a uživatelská adresa jsou uvedeny v příkazu ke zjišťování údajů o telekomunikačním provozu.

Zákonnými náležitostmi této informace jsou:

- a) označení soudu, který vydal příkaz,
- b) údaj o období, jehož se tento příkaz týkal, a
- c) 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.

Stejně jako u odposlechu i zde jsou stanoveny výjimky, kdy tato informační povinnost odpadá, a to 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, 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, již 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.

2.2.3 Řízení o přezkumu příkazu k zjištění údajů o telekomunikačním provozu

Rovněž toto řízení je obdobné jako řízení o přezkumu zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu, proto ohledně detailů odkazují na příslušnou kapitolu této práce.

Toto řízení je zahájeno na návrh osoby uvedené v § 88a odst. 2 trestního řádu, již se rozumí osoba uživatele telekomunikačního zařízení. Aby mohlo být řízení

zahájeno, musí být jednak pravomocně skončena trestní věc, v níž byl vydán daný příkaz, jednak musí být tato osoba informována o nařízení zjišťování údajů o telekomunikačním provozu. Pokud jedna z těchto podmínek není splněna, je takový návrh per analogiam odmítnut jako nepřijatelný podle § 265i odst. 1 písm. a) trestního řádu.

K řízení je příslušný Nejvyšší soud, který jej provede v neveřejném zasedání. Účelem řízení je přezkum zákonnosti příkazu k zjištění údajů o telekomunikačním provozu. To znamená, že soud se výhradně zabývá tím, zdali byly při vydávání dodrženy všechny podmínky stanovené trestním řádem a jeho provedení bylo v souladu s § 88a odst. 1 a 4 trestního řádu.

Soud může shledat, že příkaz:

- a) byl vydán nebo proveden v rozporu se zákonem,
- b) byl vydán a proveden v rozporu se zákonem nebo
- c) byl vydán a proveden v souladu s podmínkami § 88a odst. 1 trestního řádu.

V případě rozporu se zákonem soud vysloví porušení zákona, které však nemá žádný vliv na rozhodnutí ve věci samé. Může však sloužit jako důvod k podání mimořádného opravného prostředku nebo jako právní titul při vymáhání finančního zadostiučinění za vzniklou nemajetkovou újmu. V případě, že je příkaz v souladu s podmínkami § 88a odst. 1, soud vysloví, že zákon porušen nebyl.

Všechna tato rozhodnutí mají povahu usnesení, přičemž proti nim není přípustný opravný prostředek.

Tato úprava se plně uplatní i v řízení v trestních věcech mladistvých, neboť v tomto směru zákon o soudnictví ve věcech mládeže nemá speciální ustanovení. To platí i v řízení proti právnickým osobám, poněvadž to není z povahy věci vyloučeno a zákon o trestní odpovědnosti právnických osob neobsahuje žádné speciální ustanovení.¹⁶²

Vzhledem k tomu, že zákonodárce při novelizaci tohoto ustanovení opomenul novelizovat taktéž ustanovení § 30 odst. 4 trestního řádu, je nutno pro vyloučení soudce

¹⁶² Šámal, P. a kol. Trestní řád II. § 157 až 314s. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 3623, 3625 a 3628.

postupovat analogicky podle tohoto ustanovení ve vztahu k řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu.

2.2.4 Zjišťování údajů o telekomunikačním provozu se souhlasem uživatele

Ustanovení odstavce 4 upravuje případy, kdy k zjištění údajů o telekomunikačním provozu dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají tyto údaje vztahovat. Souhlas uživatele telekomunikačního zařízení zde nahrazuje příkaz předsedy senátu (samosoudce) a v přípravném řízení soudce, kterého pak není třeba, a zjištění údajů o telekomunikačním provozu může vyžádat příslušný orgán činný v trestním řízení, tj. státní zástupce nebo policejní orgán v přípravném řízení a předseda senátu (samosoudce) ve stádiu řízení před soudem.¹⁶³

Uživatelé je osoba, která sama osobně předmětnou komunikaci uskutečnila (definice viz výše). Je-li tedy více uživatelů jedné účastnické stanice, je třeba, aby souhlas za svou osobu dal vždy zvlášť každý uživatel, kterého se poskytnutí údajů týká.

Vyžádání se zde uskutečňuje opatřením, jehož obsahové náležitosti budou obdobné jako v případě příkazu podle odstavce 1; navíc se zde uvede, že uživatel telefonní stanice nebo jiného telekomunikačního zařízení k němu dal souhlas, který je třeba v písemné podobě připojit k opatření o vyžádání údajů o telekomunikačním provozu. Úřední záznam poznamenaný ve spise zde nepostačuje vzhledem k tomu, že opatření je třeba zaslat právnické nebo fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací.¹⁶⁴

Je otázkou, zdali daný uživatel může svůj souhlas odvolat a co se v takovém případě stane. Zatímco u odposlechu se totiž jedná o kontinuální proces, který je možno kdykoliv přerušit, v případě zjišťování údajů by bylo odvolání souhlasu dle mého názoru možné do okamžiku, než je poskytnuta výsledná zpráva o údajích o telekomunikačním provozu, tzn. dokud není žádost náležitě vyřízena. Následně by již odvolání souhlasu mohlo mít pouze ten následek, že by výsledek získaný takovou zprávou nemohl být nijak použit v trestním řízení, což je však podle mě v rozporu s účelem úpravy. Toto řešení totiž používá trestní řád v případech, kdy je důkazní prostředek získán v rozporu se zákonem (srov. § 88 odst. 1 trestního řádu). V tomto

¹⁶³ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1234.

¹⁶⁴ Šámal, P. a kol. Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013, s. 1235.

případě by však byl získán zákonným způsobem, protože souhlas v době jeho vyžádání a doručení trval. Tudiž bych se přikláběla k názoru, že odvolání souhlasu je v tomto ohledu možné, ale pouze do doby, než je taková zpráva o zjištění údajů o telekomunikačním provozu doručena příslušnému orgánu činnému v trestním řízení.

V případě zjišťování údajů u mobilního telefonu, který se dostal do moci třetí osoby jinak než s přivolením oprávněného uživatele, postačí pro účely přípravného řízení k průlomu do telekomunikačního tajemství i souhlas původního oprávněného uživatele telekomunikačních služeb.¹⁶⁵

K důkazu se zde používá výsledek, tedy zpráva o zjištění údajů o uskutečněném telekomunikačním provozu, která může být poskytnuta v písemné podobě, ale i v elektronické podobě, způsobem umožňujícím dálkový a nepřetržitý přístup, kdy však požadované údaje musí být zachyceny způsobem, který umožňuje pozdější provedení důkazu v řízení před soudem (např. v listinné podobě nebo na elektronických médiích).

¹⁶⁵ Srov. výkladové stanovisko č. 25/2002 Sb. v. S. NSZ. Nejvyšší státní zastupitelství, 2002.

3. Německá právní úprava

Německá právní úprava je obsažena v německém trestním řádu (dále „StPO“), který je v současnosti používán ve verzi publikované dne 7. 4. 1987.¹⁶⁶

Instituty odpovídající odposlechu a záznamu telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu jsou obsaženy v knize první „*Všeobecná ustanovení*“, oddělení osmém „*Zabavení věci, sledování telekomunikací, zátah, nasazení technických prostředků, nasazení utajeného vyšetřovatele a prohlídka*“. Konkrétně se pak jedná o ustanovení § 100a a 100b, která upravují institut monitorování telekomunikací a ustanovení § 100g, 100i a 100j, která upravují získání provozních údajů, opatření u mobilních telefonů a získání dat podle § 95 a 111 telekomunikačního zákona (dále „TKG“). Společně se k těmto ustanovením vztahuje ještě § 101 StPO, který upravuje informační povinnost a soudní kontrolu příkazů k vydání těchto institutů. Dalšími důležitými ustanoveními jsou pak § 477 odst. 2 věta druhá a třetí StPO, který upravuje použití výsledků v jiné trestní věci, a § 148 a 160a StPO ohledně monitorování komunikace mezi obhájcem a obviněným.

3.1 Monitorování telekomunikací podle § 100a a 100b StPO

Účelem tohoto institutu je zjišťování obsahu zpráv přenášených prostřednictvím telekomunikací, přičemž je možné jej použít bez vědomí dotčené osoby, jejíž komunikace je odposlouchávána. Ustanovení § 100a StPO upravuje všeobecné podmínky nařízení tohoto institutu, ustanovení § 100b StPO pak příslušnost orgánů, které vydávají příkaz a samotný proces jeho vydávání.

Pojem telekomunikací je podle § 3 č. 22 TKG definován jako technický postup odesílání, zprostředkovávání a obdržení signálů prostřednictvím telekomunikačních systémů. Tento pojem zahrnuje všechny způsoby zprostředkovávání zpráv, včetně SMS

¹⁶⁶ Stejně jako v české právní úpravě je i v té německé možné nařídit odposlech podle více zákonů. Tajná služba tak může učinit podle zákona k článku 10 Základního zákona, omezujícího listovní, poštovní a telekomunikační tajemství, ve znění pozdějších předpisů. Vedle toho je rovněž možné učinit preventivní policejní sledování i podle zemských policejních zákonů. Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 200.

zpráv, e-mailů, internetového chatu a internetové telefonie.¹⁶⁷ S e-mailem je to stejně jako v české právní úpravě nejasné. Německá teorie rozlišuje 3 fáze práce s e-mailem: odeslání zprávy, uložení zprávy ve schránce a přijetí zprávy adresátem. První a třetí fáze spadají bez pochyb pod režim § 100a StPO. U druhé fáze to již však tak jasné není, protože zde přicházejí v úvahu i instituty zabavení věci a zabavení pošty. Spolkový ústavní soud k tomu dodal, že pokud se jedná o neutajené použití opatření k získání takových zpráv, spadá takové opatření pod zabavení věci. V případě, že je toto opatření uskutečňováno tajně, spadá však již pod režim § 100a StPO. Tento názor ale není zcela přesvědčivý, protože povaha získávaných poznatků je u monitorování telekomunikací a zabavení věci rozdílná. Navíc je kritizováno i to, že v rámci jednoho komunikačního přenosu jsou používána různá opatření v závislosti na fázi daného přenosu. Proto převažuje názor, že jediný správný postup je použití režimu ustanovení § 100a StPO na celý proces, bez ohledu na to, je-li prováděn utajeně nebo ne.¹⁶⁸ Navíc podle judikatury spadají pod § 100a StPO rovněž údaje o pozici mobilního telefonu, který není zrovna používán.¹⁶⁹

Telekomunikace mohou být tedy sledovány a zaznamenány i bez vědomí dotčené osoby, pokud:

1. určité skutečnosti odůvodňují podezření, že někdo se dopustil jako pachatel nebo účastník těžkého trestného činu označeného v odstavci 2; v případech, kdy je trestný pokus takového trestného činu, se jej někdo jako pachatel nebo účastník pokusil spáchat nebo se někdo jako pachatel nebo účastník dopustil trestného činu při přípravě takového trestného činu,
2. takový trestný čin je v jednotlivých případech posouzen jako závažný a
3. objasnění skutkového stavu věci nebo vyšetřování místa pobytu obviněného by bylo jinak podstatně ztíženo nebo znemožněno.

¹⁶⁷ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 291-292.

¹⁶⁸ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 292-293.

¹⁶⁹ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 201.

Ad 1. Pojem těžkého trestného činu není v německém právu přesně stanoven. Podle judikatury Spolkového ústavního soudu se má vycházet z trestných činů s minimální hranicí horní trestní sazby pěti let, které jsou dostatečně závažné, a z podmínky, aby zásah způsobený takovým trestným činem citelně poškozoval právní jistoty obyvatel a rušil právní klid.¹⁷⁰

Účastenství se posuzuje v tomto případě na stejné úrovni jako pachatelství. Naproti tomu zvláštní formy účastenství jako nadřzování nebo napomáhání k trestnému činu dostačující nejsou. Co se týče pokusu trestného činu, jeho přípravy nebo účastenství na něm, může být toto opatření nařízeno pouze, pokud se jedná o samostatné trestné činy nebo pokud jsou trestné podle § 30 německého trestního zákoníku (dále „StGB“), který upravuje pokus účastenství u zločinů.¹⁷¹

Pokud se v průběhu vyšetřování změní kvalifikace trestného činu, nemá to na zákonnost příkazu k monitorování telekomunikací vliv, pokud byl takový příkaz vydán v souvislosti s trestným činem uvedeným v odstavci 2.¹⁷²

Ad 2. Pro posouzení závažnosti trestného činu v konkrétním případě postačí podezření, že se o závažný trestný čin jedná. Pouze pokud by tato vlastnost u trestného činu evidentně chyběla, bylo by monitorování telekomunikací vyloučeno.¹⁷³

Ad 3. I v německé právní úpravě je použití sledování telekomunikací omezeno zásadou subsidiarity. Pokud je tedy možné uplatnit i jiné postupy, je nutné vzájemně porovnat vyhlídky na úspěch použití tohoto a jiných opatření.¹⁷⁴

K znemožnění vyšetřování trestného činu by došlo tehdy, pokud by nebylo možné použít jiné postupy. Podstatné ztížení vyšetřování nastává pak tehdy, kdy použití jiných prostředků požaduje podstatně více času, a vedlo by

¹⁷⁰ Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 202.*

¹⁷¹ Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 203.*

¹⁷² Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 204.*

¹⁷³ Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 202-203.*

¹⁷⁴ Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 202.*

tak k zásadním průtahům ve vyšetřování, přičemž větší pracovní náklady ospravedlňují použití monitorování telekomunikací pouze, pokud by byly tak rozsáhlé, že by to převážilo účel trestního řízení. Naproti tomu náklady řízení nesmějí hrát žádnou rozhodující roli při rozhodování o výběru opatření.¹⁷⁵

Odstavec druhý § 100a StPO uvádí v souladu se zásadou proporcionality taxativní výčet trestných činů, u kterých je použití tohoto institutu možné. Příkaz může být vydán na základě podezření založeného na určitých skutečnostech, které bezprostředně, popř. jako indicie, takové podezření opodstatňují. K tomuto účelu musí být osobě vydávající příkaz poskytnut prostor pro uvážení.¹⁷⁶

Německá právní úprava je obsažena v mnoha zákonech, kdy základním kodexem je StGB, který upravuje základní skutkové podstaty trestných činů. Na něj pak navazuje mnoho specializovaných zákonů, zabývajících se již úzce vyhraněnou problematikou. Těžkými trestnými činy ve smyslu odstavce 1 tedy jsou trestné činy podle trestního zákoníku, daňového řádu, protidrogového zákona, zákona o azylovém řízení, zákona o pobytu osob, zákona o vnějších hospodářských vztazích, zákona o omamných látkách, zákona o kontrole základních surovin, zákona o kontrole válečných zbraní, zákona o mezinárodním právu trestním a zákona o zbraních.

Mezi tyto trestné činy patří např. trestný čin přípravy útočné války, trestný čin velezrady a ohrožení demokratického právního státu, trestný čin podplácení poslanců, trestné činy proti veřejnému pořádku, trestné činy padělání peněz a cenin, trestné činy proti sexuálnímu sebeurčení, trestné činy vraždy a zabití, trestné činy loupeže a vydírání, trestné činy podvodu a počítačového podvodu, trestné činy padělání listin, trestné činy proti hospodářské soutěži, obecně nebezpečné trestné činy, trestné činy úplatkářství a podplácení, genocida, zločiny proti lidskosti, válečné zločiny a další.

Je tedy zřejmé, že na rozdíl od české právní úpravy neexistují v německé právní úpravě pochybnosti ohledně vymezení trestných činů, u kterých může být tento institut nařízen. Na druhou stranu je však rozsah tohoto výčtu dost kritizován, protože u některých trestných činů již není zachována zásada proporcionality vzhledem k jejich závažnosti. Proto byla stanovena soudní judikaturou i výše zmíněná hranice pro těžké

¹⁷⁵ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 202.

¹⁷⁶ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 203.

trestné činy, která v praxi použití tohoto opatření na některé trestné činy v odstavci 2 vyloučila.¹⁷⁷

Nařízení monitorování telekomunikací musí směřovat vůči určité osobě, kterou je v první řadě obviněný, přičemž jeho identita nemusí být jistě určena. Dále je pak možné uplatnit tento institut i proti osobě, o které se dá na základě určitých skutečností předpokládat, že pro obviněného nebo od obviněného přijímá určitá sdělení nebo je dále zprostředkovává nebo obviněný používá její telekomunikační připojení. Tato osoba však nemusí nutně znát obsah a způsob sdělení ani jeho vztah k trestnému činu. Výše uvedené se vztahuje i na osoby, které v dobré víře nechávají obviněného nebo výše uvedenou osobu používat svoje připojení.¹⁷⁸

I v německé úpravě existují omezení monitorování telekomunikací a jimi sdělovaném obsahu. Jedná se zejména o případy, existují-li skutečnosti nasvědčující předpokladu, že takovým opatřením by byly získány výlučně poznatky z oblasti soukromého života. Tehdy je takové opatření podle § 100a odst. 4 StPO nepřipustné. Získané poznatky ze soukromého života nesmějí být v řízení využity a záznamy o nich jsou bezodkladně zničeny. O jejich získání a zničení musí být učiněn záznam do spisu. I toto ustanovení je však kritizováno, protože v praxi může být využito orgány trestního řízení k obcházení zákona. Obsah záznamu, který obsahuje pro obviněného polehčující informace, totiž může být smazán se záminkou, že se týká právě oblasti soukromého života.¹⁷⁹

V souvislosti s § 148 a 160a StPO rovněž nesmí být odposloucháván rozhovor obviněného s obhájcem. Takto získané informace nesmí být nijak použity a záznamy o nich musí být bez prodlení zničeny. O jejich získání a zničení se učiní záznam do spisu. To však neplatí pro právní zástupce, kteří nejsou zároveň obhájci, nebo pro hovor obhájce s jinými osobami. Naproti tomu obhájce může být odposloucháván, pokud je sám podezřelý z trestného činu, pro který je možno nařídit sledování. Nesmí být však

¹⁷⁷ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 293.

¹⁷⁸ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 203.

¹⁷⁹ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 295.

použity informace z hovorů, které s takovým trestným činem nijak nesouvisí.¹⁸⁰ Rovněž mohou být obhájcovy hovory monitorovány, pokud je podezřelý z podněcování trestného činu, nadřování nebo podílnictví.

Jak jsem již uvedla výše, je nutno podmínky stanovené v § 100a StPO vykládat v souvislosti s ustanovením § 100b StPO, které upravuje příslušnost pro vydání příkazu k monitorování telekomunikací.

Podle tohoto ustanovení smějí být tato opatření nařízena pouze soudem na návrh státního zastupitelství. K nařízení příkazu je příslušný vyšetřovací soudce podle § 162 a 169 StPO.¹⁸¹ Při nebezpečí prodlení pak může být příkaz přijat i státním zastupitelstvím, pokud však takové nařízení není do tří pracovních dnů potvrzeno soudem, stává se neúčinným. Lhůta začíná plynout vydáním příkazu a na její běh se použijí ustanovení § 42 a 43 odst. 2 StPO. Poznatky tímto opatřením získané jsou však použitelné i tehdy, kdy takový příkaz není soudem potvrzen.¹⁸² Stížnost proti příkazu je přípustná, v praxi však nebývá uskutečněna, protože postižený se o nařízení odposlechnů zpravidla nedozví. Rovněž i proti rozhodnutí státního zastupitelství podle § 100b odst. 1 věta druhá je možné obrátit se k soudu podle § 98 odst. 2 věta druhá StPO.¹⁸³

Na rozdíl od české právní úpravy tak není v té německé možnost uplatnění tohoto opatření bez vydání příkazu. Naopak musí být soudní příkaz vydán i v případech, kdy je osoba účastnicí se telekomunikace s odposlechem srozuměna.¹⁸⁴ Z mého pohledu je v tomto ohledu německá úprava propracovanější, protože umožňuje použití

¹⁸⁰ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 204.

¹⁸¹ V přípravném řízení je návrh předložen státním zastupitelstvím okresnímu soudu, v jehož obvodu má toto státní zastupitelství sídlo. Po podání obžaloby je příslušný soud, který je příslušný v řízení ve věci. Ve věcech, které spadají v 1. instanci podle § 120 německého zákona o organizaci soudů do pravomoci vrchního zemského soudu (např. velezrada, vražda, zabití apod.), mohou být věci zajišťované v přípravném řízení soudcem okresního soudu zajištěny rovněž vyšetřovacím soudcem vrchního zemského soudu. Pokud je vyšetřování vedeno generálním spolkovým zástupcem, je příslušným vyšetřovacím soudcem soudce Spolkového soudního dvora.

¹⁸² Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 208.

¹⁸³ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 209-210.

¹⁸⁴ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 294.

odposlechu i v případech, kdy jsou sice splněny podmínky pro vydání příkazu, ale není na tento postup dostatek času. Stejně tak jsou však pokryty i případy, na které naše úprava používá odposlech se souhlasem uživatele odposlouchávané stanice. S čím však nesouhlasím, je možnost použití výsledků získaných monitorováním telekomunikací, ačkoli toto opatření nebylo soudem dodatečně povoleno. V tomto případě se dle mého názoru jedná o použití informací získaných bez zákonného podkladu.

Doba monitorování telekomunikací může být maximálně tři měsíce, přičemž běh této lhůty začíná od vydání příkazu. Tuto lhůtu je rovněž možné opakovaně prodloužit, vždy však maximálně o další tři měsíce, pokud se zřetelem na získané výsledky vyšetřování trvají podmínky pro vydání příkazu.

Příkaz musí být písemný a musí v něm být uvedeno, kdo jej vydal. Dalšími obligatorními náležitostmi příkazu podle odstavce 2 jsou:

- a) pokud je to možné, tak jméno a adresa dotčené osoby, proti které je toto opatření nařízeno,
- b) telefonní číslo nebo jiná specifikace odposlouchávaného připojení nebo koncového zařízení, pokud není na základě určitých skutečností prokázáno, že tato specifikace zároveň náleží i jinému koncovému zařízení,
- c) způsob, rozsah a doba opatření s uvedením data ukončení odposlechu.

Přiměřeně se navíc použije i ustanovení § 100d odst. 2 StPO, které upravuje náležitosti příkazu při nařízení prostorového odposlechu. Vedle těchto zákonných náležitostí musí příkaz ještě obsahovat označení trestného činu, zákonný důvod odposlechu (zkoumání skutkového stavu věci nebo zjišťování místa pobytu), na základě čeho je vyvozováno podezření z uvedeného trestného činu a důkazní situaci. Zároveň je ještě nutno vysvětlit, proč je použití tohoto opatření nezbytné.¹⁸⁵

Stejně tak je upraveno, jestli a v jakém rozsahu mají být pořizeny záznamy hovorů, které z připojení má být odposloucháváno, a zdali tak bude prováděno průběžně nebo v určitou denní dobu.¹⁸⁶

¹⁸⁵ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 208.

¹⁸⁶ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 208-209.

Na základě tohoto příkazu má osoba poskytující telekomunikační službu povinnost umožnit soudu, státnímu zastupitelství a v policejní službě působícím vyšetřovatelům provedení opatření podle § 100a StPO za podmínek stanovených v § 110 TKG (tzv. povinnost součinnosti). Zároveň má tato osoba povinnost poskytnout bez prodlení potřebné informace. Zda a v jakém rozsahu jsou učiněna opatření sloužící tomuto účelu, je určeno v telekomunikačním zákoně a ve vyhlášce o monitorování telekomunikací. Pokud tato osoba odmítne poskytnutí součinnosti, mohou proti ní být podle § 95 odst. 2 StPO uplatněny pořádkové a donucovací prostředky. V případě, že účastník mobilní sítě má v rámci služby roaming přístup k síti více poskytovatelů, musí osoba poskytující telekomunikační službu o existenci takové smlouvy vyšetřovací úřady neprodleně informovat. V takovém případě je zapotřebí pouze jeden příkaz.¹⁸⁷

Provedení monitorování telekomunikací má na starost státní zástupce státního zastupitelství, které dalo podnět k vydání příkazu (§ 36 odst. 2 StPO),¹⁸⁸ přičemž trvá tak dlouho, dokud není možné bez něj pokračovat ve vyšetřování nebo dokud není zjištěno místo pobytu obviněného nebo dokud nezaniknou vyhlídky na jeho úspěch.

Pokud podmínky pro nařízení příkazu již zanikly, jsou opatření přijatá na základě příkazu bez prodlení ukončena. Konečné rozhodnutí o ukončení činí zpravidla státní zastupitelství. Podle zákona je nutné informovat soud o ukončení opatření. Rovněž je nutné ale informovat i o jeho průběhu a o výsledcích monitorování získaných. Tím je soudu umožněna kontrola úspěšnosti použití tohoto opatření. Vedle toho je informován o této skutečnosti i provozovatel telekomunikační služby. V případě, že se obnoví podmínky pro nařízení monitorování telekomunikací, může být obnoveno i toto opatření.¹⁸⁹

Nebude-li materiálů získaných monitorování telekomunikací více pro trestní řízení potřeba, jsou bez prodlení zničeny. V případě zvukových pásek stačí jejich vymazání a zničení protokolů o záznamech. Rozhodnutí o zničení vydává v přípravném řízení státní zastupitelství. Po podání obžaloby soud. Provedení náleží policii pod dohledem státního zastupitelství, přičemž toto zničení je zadokumentováno.¹⁹⁰

¹⁸⁷ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 209.

¹⁸⁸ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 209.

¹⁸⁹ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 209.

¹⁹⁰ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 209.

Výsledky monitorování mohou být použity proti obviněnému a proti všem osobám zúčastněným na trestném činu.¹⁹¹ Smí být rovněž použity i jako důkaz ohledně trestných činů, které nejsou uvedeny ve výčtu v odstavci 2, ale které s takovým trestným činem úzce souvisí (např. v jednočinném souběhu). Je-li výčet trestných činů v odst. 2 po provedení opatření podle § 100a rozšířen o další trestný čin, mohou být informace získané tímto opatřením vztahující se k takovému trestnému činu rovněž použity v rámci trestního řízení.¹⁹²

Při získání náhodných poznatků o trestném činu třetí osoby (§ 477 odst. 2 StPO), který patří do výčtu trestných činů podle odst. 2, mohou být tyto poznatky použity i bez svolení dotčené osoby k důkazním účelům v jiném trestním řízení za účelem objasnění takového trestného činu třetí osoby. Pokud se ale nejedná o trestný čin podle odst. 2, jejich použití je vyloučeno. Zprostředkovaně mohou být tyto poznatky uplatněny jako podklad pro zahájení trestního stíhání proti třetí osobě nebo ohledně trestného činu, který není ve výčtu podle odst. 2 uveden, nebo jako základ pro další vyšetřování osoby obviněného, které povede k získání nových důkazů.¹⁹³ Stejně tak poznatky ohledně trestných činů podněcování k trestnému činu, podílnictví a nadřování, které byly spáchány vzhledem k trestnému činu uvedenému v odstavci 2, mohou být použity pouze jako podklad pro zahájení vyšetřování.¹⁹⁴

Naproti tomu osobní data získaná jako náhodné poznatky při monitorování telekomunikací v rámci jiného řízení mohou být použita bez souhlasu dotčené osoby pouze za účelem odvrácení značného ohrožení veřejné bezpečnosti nebo pro účely, pro které je zprostředkování přípustné podle § 18 zákona o spolupráci spolku a zemí v záležitostech ústavní ochrany a o Spolkovém úřadu pro ústavní ochranu, jakož i podle pravidel stanovených v § 476 StPO, který upravuje zprostředkování osobních dat zjištěných za vědeckými účely.

¹⁹¹ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 204.

¹⁹² Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 296.

¹⁹³ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 294.

¹⁹⁴ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 205-206.

Ještě širší je výklad povolení monitorování telekomunikací u trestných činů podle § 129 a násl. StGB, týkajícího se založení zločinecké organizace. V takovém případě se mohou náhodně získané informace použít i na vyšetřování, která se vztahují na jiné trestné činy spáchané v rámci činnosti takové zločinecké organizace. Co však zachází již příliš daleko, je výklad, že takové výsledky jsou použitelné i tehdy, kdy zločinecká skupina ve skutečnosti neexistuje (jedná se o případy vykonstruovaných obvinění). Takováto praxe totiž umožňuje nařízení tohoto opatření i u těch trestných činů, které nejsou uvedeny v odstavci 2 a nemohou být jako takové důvodem pro nařízení monitorování telekomunikace.¹⁹⁵

Pokud bylo monitorování telekomunikací uskutečněno bez příkazu soudce nebo státního zástupce, čímž došlo k obejití § 100a StPO, nebo když byl příkaz vydán za vědomého překročení zákonné pravomoci, nejsou poznatky takto získané použitelné v trestním řízení.¹⁹⁶ Nepoužitelný materiál nesmí být uplatněn ani v hlavním líčení jako důkaz, ani jako námitka vůči osobě zúčastněné na telefonním hovoru. Vypovídal-li odposlouchávaný na základě námítky takového důkazního materiálu, je tato výpověď nepoužitelná. Doznání je naproti tomu použitelné; výsledky nepřipustného monitorování však na něj nesměly mít žádný vliv.¹⁹⁷

Zákon nezmiňuje, jakým způsobem jsou informace získané opatřením podle § 100a uplatněny. Podle judikatury Spolkového soudního dvora tak může být učiněno buď přehráním záznamu nebo použitím přepisu obsahu záznamu. Nepřípustné je však přehránění nebo přečtení pouhého výňatku z takového záznamu, popř. shrnutí jeho obsahu.¹⁹⁸

Na základě ustanovení § 100b odst. 5 a 6 StPO je nakonec stanovena povinnost zemského a spolkového generálního státního zástupce informovat Spolkový úřad pro spravedlnost o těchto opatřeních nařízených v oblasti jejich pravomoci, a to za každý

¹⁹⁵ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 296.

¹⁹⁶ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 206.

¹⁹⁷ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 297.

¹⁹⁸ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 294.

rok vždy do 30. června následujícího roku. Tento úřad pak vypracuje celostátní přehled nařízených opatření a zveřejní jej na internetu.

3.2 Zjišťování provozních údajů podle § 100g StPO, opatření u mobilních telefonů podle § 100i StPO a zjišťování údajů podle § 100j StPO

Instituty obdobné našemu zjišťování údajů o telekomunikačním provozu jsou upraveny v § 100g, 100i a 100j StPO.

První z nich, ustanovení § 100g, upravuje zjišťování provozních údajů, a to i bez vědomí dotčené osoby. Těmi jsou podle § 3 č. 30 TKG ve spojení s § 96 odst. 1 a § 113a TKG data, která jsou při poskytování telekomunikační služby získána, zpracována nebo použita. Konkrétně jimi jsou telefonní čísla, čísla karty, doba trvání rozhovoru a adresát hovoru, stanoviště mobilního telefonu, IP adresa počítače s internetovým připojením apod. Tato data spadají pod ochranu čl. 10 odst. 1 Základního zákona (dále „GG“), který zaručuje ochranu listovního, poštovního a telekomunikačního tajemství.¹⁹⁹

Pod toto ustanovení spadají rovněž opatření týkající se tzv. základových stanic, přes které je možné získat souborná data o mobilních telefonech. Tyto základové stanice totiž zprostředkovávají na určitém místě a v určitém čase přes mobilní síť komunikaci těchto zařízení. U takového opatření je však nutné klást zvláštní důraz na podmínku nutnosti takového opatření, protože jím je zasaženo do práv mnoha nezúčastněných osob, které zrovna té které základové stanice využívají pro své připojení.

Opatření podle § 100g StPO je tedy možné uskutečnit, zakládají-li určité skutečnosti podezření, že:

- a) někdo spáchal nebo se účastnil trestného činu, který splňuje v konkrétním případě podmínku podstatné závažnosti, obzvláště pak trestný čin uvedený v § 100a odst. 2 StPO; v případě, že je trestný pokus trestného činu, tak se někdo jako pachatel nebo účastník takový trestný čin pokusil spáchat, nebo někdo jako

¹⁹⁹ Na údaje, které se dají získat prostým přístupem k telekomunikačnímu zařízení (např. údaje o posledním volaném čísle apod.), se vztahují ustanovení o zabavení věci a prohlídce. Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 298.

pachatel nebo účastník spáchal jiný trestný čin při přípravě takového trestného činu nebo

- b) někdo jako pachatel nebo účastník spáchal trestný čin prostřednictvím telekomunikací.

Toto opatření je učiněno, pokud je to nutné pro zjišťování skutkového stavu věci nebo při pátrání po místě pobytu obviněného.²⁰⁰ Pokud se jedná o podezření na trestný čin spáchaný prostřednictvím telekomunikací, je opatření přípustné pouze tehdy, pokud by zjišťování skutkového stavu věci nebo pátrání po místě pobytu obviněného bylo jinak zmařeno a užití tohoto opatření splňuje podmínku přiměřenosti. Zjišťování údajů o stanovišti zařízení v reálném čase je pak přípustné pouze v případě trestných činů uvedených pod písmenem a).

Ráda bych zde upozornila na odlišnost mezi českou a německou právní úpravou. Ta německá totiž na tomto místě obsahuje demonstrativní výčet trestných činů, u kterých je možné takové opatření uplatnit. Navíc tento výčet je vymezen pouze na trestné činy značného významu, přičemž posouzení, zdali se jedná o trestný čin značného významu, ponechává na úvaze soudu. Podle mého názoru v tomto směru česká úprava daleko lépe splňuje požadavek přesnosti a předvídatelnosti. Konec konců právě nedostatek přesného vymezení trestných činů byl české právní úpravě vytýkán ve výše zmiňovaném nálezu Ústavního soudu sp. zn. Pl. ÚS 24/2011. Je však nutno podotknout, že i v německé právní úpravě jsou v tomto ohledu navrhovány změny, kterými by byl zaveden taxativní výčet trestných činů, při jejichž vyšetřování by bylo možné takové opatření uplatnit.

Na toto ustanovení se jinak obdobně použijí ustanovení § 100a odst. 3 StPO ohledně osoby, proti které je možné takové opatření nařídit, a ustanovení § 100b odst. 1 až 4 věta první StPO, která upravují vydání příkazu a jeho náležitosti, povinnost součinnosti provozovatele telekomunikačních služeb a nakonec povinnost ukončení opatření, pokud již nejsou dány podmínky pro jeho nařízení. Odchylně však od § 100 b

²⁰⁰ Až potud je však toto ustanovení neplatné, protože věta první odstavce 1 je v případě zjišťování údajů podle § 113a TKG neslučitelná s čl. 10 odst. 1 GG. Srov. nález Spolkového ústavního soudu ze dne 2. 3. 2010, BGBl. I s. 272.

odst. 2 věta druhá č. 2 StPO, který vyžaduje uvedení telefonního čísla nebo jiné specifikace sledovaného zařízení, stačí v případě trestného činu značného významu dostatečně prostorově i časově určené určité označení telekomunikace, pokud by bylo zjišťování skutkového stavu věci nebo pátrání po místě pobytu obviněného jiným způsobem zmařeno či podstatně ztíženo.

Obdobně jako u monitorování telekomunikací je i u těchto opatření každoročně vyhotoven Spolkovým úřadem pro spravedlnost přehled jejich použití.

Dalším ustanovením týkajícím se dat získaných v telekomunikačním provozu je § 100i StPO. Ten vytváří právní základ pro získání tzv. jiné specifikace koncového zařízení, jejíž uvedení patří mezi obligatorní náležitosti příkazu k monitorování telekomunikací. Rozdílná úprava je zde proto, že tato data nespádají pod ochranu čl. 10 odst. 1 GG.²⁰¹

Tato jiná specifikace koncového zařízení se týká dvou typů dat, a to tzv. IMSI a IMEI. Podle toho je rovněž tento institut někdy nazýván IMSI- nebo IMEI-Catcher.

IMSI (International Mobile Subscriber Identity) je identifikační číslo uživatele, které je uloženo na SIM kartě. Toto číslo je na celém světě přiděleno pouze jednomu uživateli a pomocí něj může být zjištěno telefonní číslo a jméno účastníka. Mimoto umožňuje lokalizaci zapnutého mobilního telefonu. Přitom může být dokonce určeno stanoviště mobilního telefonu v rámci jedné základové stanice.²⁰²

Naproti tomu IMEI (International Mobile Equipment Identity) je číslo přístroje. To umožňuje zachytit všechny používané SIM karty u stejného telefonního čísla, tudíž jeho uplatnění je na místě, pokud je na jednom mobilním telefonu používáno více SIM karet.²⁰³

Toto opatření se uplatní, zakládají-li určité skutečnosti podezření, že někdo spáchal nebo se účastnil trestného činu, který v konkrétním případě splňuje podmínku podstatné závažnosti, obzvláště pak trestný čin uvedený v § 100a odst. 2; v případě, že je trestný pokus trestného činu, tak se někdo jako pachatel nebo účastník takový trestný čin pokusil spáchat anebo někdo jako pachatel nebo účastník při přípravě takového

²⁰¹ Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 222.*

²⁰² Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 223.*

²⁰³ Srov. *Joecks, W. Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 223.*

trestného činu spáchal jiný trestný čin. Za splnění jedné z těchto podmínek smějí být technickými prostředky vyšetřovány:

1. číslo mobilního telefonu a číslo v něm používané karty, stejně jako
2. místo, kde se mobilní telefon právě nachází.

Rovněž i zde je však dáno omezení zásadou subsidiarity. Jeho použití je tudíž možné, pokud je to nutné pro zjištění skutkového stavu věci nebo při pátrání po místě pobytu obviněného.

Osobní data třetí osoby smějí být při příležitosti takového opatření získána pouze tehdy, když je to z technických důvodů nevyhnutelné k dosažení účelu podle odstavce 1. Mimo srovnávání dat k vyšetřování hledaného čísla přístroje a karty nesmějí být tato data použita a po ukončení opatření musí být bez prodlení smazána.

Toto opatření je možné nařídit proti obviněnému nebo proti osobě, u které se na základě určitých skutečností předpokládá, že pro obviněného přijímá určitá sdělení nebo přijímá a předává sdělení pocházející od obviněného. Rovněž může být nařízeno proti osobě, u které existuje předpoklad, že obviněný používá její připojení.

Příkaz vydává na návrh státního zastupitelství soud, přičemž při nebezpečí prodlení jej může vydat i státní zastupitelství. Takový příkaz však musí být do tří pracovních dnů potvrzen soudem, jinak se stává neúčinným. I tento příkaz musí být vydán v písemné formě. Pokud již nejsou dány podmínky pro vydání příkazu, je opatření bez prodlení ukončeno a o jeho výsledcích je vyrozuměn soud. Doba trvání příkazu je omezena na nejvýše šest měsíců. Prodloužení je zde možné, a to i opakovaně, vždy však maximálně o šest měsíců, pokud trvají podmínky uvedené v odstavci 1.

I v tomto případě mají poskytovatelé telekomunikačních služeb povinnost součinnosti, tudíž pokud je nařízeno opatření pro zjištění stanoviště mobilního telefonu za účelem zatčení nebo dopadení pachatele, vyplývá z toho povinnost poskytovatele telekomunikačních služeb sdělit číslo telefonu a karty.²⁰⁴

I proti tomuto příkazu je přípustná stížnost (více viz monitorování telekomunikací).

²⁰⁴ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 223.

Nově obsahuje německý trestní řád ještě ustanovení § 100j, které upravuje oprávnění požadovat zprávu o datech podle § 95 a 111 TKG. Těmi jsou data účastníka telekomunikace, která jsou získávána za účelem vzniku, změny nebo ukončení smlouvy o telekomunikační službě. Dále pak ještě telefonní číslo a jiná označení připojení, jméno a adresa majitele připojení, datum narození u fyzických osob, datum účinnosti smlouvy a u mobilního telefonu číslo takového přístroje. U pevné linky je to rovněž adresa připojení. Toto oprávnění je uplatněno vůči poskytovateli telekomunikační služby, pokud to vyžaduje zjištění skutkového stavu věci nebo pátrání po místě pobytu obviněného. Poskytovatel telekomunikační služby má povinnost takové údaje bez prodlení poskytnout. Pokud by poskytnutí takovýchto údajů odepřel, mohla by proti němu být uplatněna donucovací nebo pořádková opatření podle § 95 odst. 2 StPO. Vztahuje-li se žádost o takovou zprávu na data, prostřednictvím kterých je chráněn přístup ke koncovému zařízení nebo úložným zařízením, která jsou umístěna na takovém přístroji nebo mimo něj (např. PIN), může být zpráva požadována, pokud jsou splněny zákonné podmínky pro použití takových dat.

Taková zpráva může být požadována také na základě adresy internetového protokolu přiřazené k určitému časovému úseku.

Žádost může být vydána na návrh státního zastupitelství soudem. Při nebezpečí prodlení může příkaz vydat i státní zastupitelství nebo jeho vyšetřovatelé. V takovém případě musí soudní rozhodnutí bez prodlení následovat. Příkazu není třeba, pokud dotčená osoba již o této žádosti ví nebo je použití takových dat již povoleno soudním rozhodnutím, přičemž o tom musí být učiněn záznam do spisu.

Dotčená osoba je informována o možnosti přezkumu, a to v okamžiku, kdy tím nebude zmařen účel poskytnutí takové zprávy. Pokud by to odporovalo převažujícím zájmům třetí osoby nebo dotčené osoby, není informace o možnosti opravného prostředku poskytnuta vůbec. Důvody pro odložení nebo upuštění podání takové informace musejí být zaznamenány ve spise.

3.3 Informační povinnost a právní ochrana

Posledním důležitým ustanovením, které se vztahuje k těmto institutům, je § 101 StPO. Toto ustanovení upravuje jednotně pro všechna utajená opatření požadavky na

označení získaných údajů, informační povinnost a přezkumné řízení.²⁰⁵

Osobní data získaná prostřednictvím opatření uvedených v odstavci 1, mezi nimiž jsou i opatření podle § 100a a 100i StPO, jsou odpovídajícím způsobem označena a při jejich předání na jiné místo je toto označení zachováno. Toto ustanovení má své opodstatnění na základě faktu, že použití takto získaných poznatků v trestním řízení zpravidla závisí na tom, že takové opatření je možno nařídit pouze u zákonem uvedených trestných činů. Označením těchto údajů je tak dosaženo, že později nejsou tyto poznatky kvůli nedostatku znalostí o jejich původu použity k jiným účelům.²⁰⁶

Informační povinnost je pak upravena v odstavci 4. U opatření podle § 100a StPO je směřována vůči každému zúčastněnému na monitorované telekomunikaci, u opatření podle 100g StPO proti zúčastněnému na dotčené telekomunikaci a u opatření podle § 100i StPO proti cílové osobě. S informací je rovněž podáno poučení o možnosti dodatečné právní ochrany podle odstavce 7 a o lhůtě, ve které musí být taková ochrana uplatněna. Informace není podána, pokud proti ní stojí převažující legitimní zájmy dotčené osoby. V případě § 100a a 100g StPO rovněž není informace podána osobě, proti které nebylo opatření namířeno, pokud je tato osoba daným opatřením dotčena pouze nepodstatně a je předpokládáno, že nemá zájem na podání informace.²⁰⁷ Tato výjimka z informační povinnosti je však poměrně kritizována. Zejména je totiž nejasné, jak chtějí vyšetřovací orgány vlastně přezkoumávat, jestli má někdo na podání takové informace zájem.²⁰⁸

Šetření pro stanovení identity osoby, které má být taková informace podána, jsou provedena pouze tehdy, pokud je to vhodné s ohledem na intenzitu zásahu opatření do práv této osoby a s ohledem na náklady na zjištění její identity, stejně jako na omezení, která z nich vyplývají pro tuto nebo jiné osoby.

Zatímco český trestní řád stanovuje taxativní výčet důvodů, které odůvodňují nepodání takové informace, německý trestní řád umožňuje odložení splnění této povinnosti, a to do doby, jakmile je to možné bez ohrožení účelu vyšetřování, života, tělesné nedotknutelnosti, osobní svobody a důležitých majetkových hodnot. Je-li

²⁰⁵ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 225.

²⁰⁶ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 225.

²⁰⁷ Na příklad u telefonických objednávek donáškové služby.

²⁰⁸ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 226.

informace odložena, jsou důvody pro její odložení zaznamenány. Není-li odložená informační povinnost uskutečněna v rámci dvanácti měsíců od ukončení opatření, je potřeba pro další odložení vyžádat soudní souhlas. Soud určí zároveň dobu trvání dalších odložení. Pokud bylo v úzké časové souvislosti provedeno více opatření, začíná tato lhůta plynout ukončením posledního z nich, přičemž úzkou časovou souvislostí je v tomto případě míněno nanejvýš několik dní nebo týdnů.²⁰⁹ Soud může rovněž odsouhlasit definitivní upuštění od informační povinnosti, pokud lze s velkou pravděpodobností určit, že tyto podmínky pro její splnění nevzniknou ani v budoucnosti. K takovému rozhodnutí je příslušný soud, který je příslušný pro nařízení takového opatření, jinak soud, který sídlí v působnosti příslušného státního zastupitelství.

Osoby, kterým je podána informace, mohou u tohoto soudu po ukončení opatření navrhnout přezkum zákonnosti takového opatření a způsobu jeho provedení. Tento návrh musí podat do dvou týdnů od podání informace. Pokud je návrh na přezkum zákonnosti podán v přípravném řízení, je k rozhodnutí příslušný okresní soud. Po podání obžaloby je pro rozhodnutí příslušný soud, který se danou věcí zabývá, což je většinou zemský soud, přičemž takové rozhodnutí je součástí samotného rozhodnutí ve věci (rozsudku). Proti rozhodnutí soudu o přezkumu zákonnosti je přípustná stížnost.²¹⁰

Nejsou-li získaná osobní data pro trestní řízení a pro možné soudní přezkoumání již více potřebná, jsou pod dohledem státního zastupitelství bez prodlení zničena. O jejich zničení je učiněn záznam do spisu. Pokud je zničení odloženo pouze kvůli možnému soudnímu přezkumu opatření, smějí být tato data bez svolení dotčené osoby použita pouze za tímto účelem. Tato data jsou pak odpovídajícím způsobem blokována. Ke zničení dojde i při zastavení trestního řízení nebo pravomocném odsouzení.²¹¹

Příkaz k monitorování telekomunikace může být rovněž přezkoumán v rámci revize podle § 333 a násl. StPO. Podle § 344 odst. 2 StPO totiž může být namítáno porušení právních předpisů, způsobené tím, že hodnocení důkazu spočívalo na nepoužitelných poznacích. Podezření na trestný čin a dodržování subsidiarity

²⁰⁹ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 226.

²¹⁰ Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 226.

²¹¹ Srov. *Roxin, C., Schünemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012, s. 297.

přezkoumá však revizní soud pouze na základě toho, zdali bylo vydání příkazu k odposlechu odůvodněné a zdali orgán, který příslušný příkaz vydal, nepřekročil prostor pro uvážení. Mimoto je požadováno, aby bylo použití takovýchto důkazů namítáno již v průběhu hlavního líčení.²¹²

²¹² Srov. *Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011, s. 206-207.

4. Odposlech a záznam telekomunikačního provozu jako zásah do zaručených práv a svobod a úniky odposlechů

Odposlech a záznam telekomunikačního provozu patří mezi jeden z nejkritizovanějších právních institutů vůbec. Dalo by se říci, že společnost je v tomto ohledu rozdělena na dva tábory. Jedni poukazují na fakt, že odposlech a záznam telekomunikačního provozu je hrubým zásahem do lidských práv, který je nutné pokud možno omezit na nejnutnější případy, popřípadě úplně zrušit. Druhý tábor pak poukazuje na skutečnost, že moderní státy se potýkají s vysoce organizovanými kriminálními skupinami, které využívají při své činnosti nejvyspělejší technologie, a tudíž je nutné mít prostředky, které by mohly metody a postupy těchto organizovaných celků vypátrat a zachytit.

Abychom se mohli touto problematikou zabývat trochu podrobněji, je nutno si uvědomit pár základních faktů.

Je nepochybné, že aby stát zajistil veřejný pořádek a bezpečnost, ochranu života, zdraví, cti a majetku svých občanů, musí mít možnost zásahu do určitých lidských práv. Z toho vyplývá fakt, že trestní právo má již ze své podstaty kolizní povahu, kdy na jedné straně jsou především ústavní principy příkazující šetřit nedotknutelnost jedince v celé šíři jeho osobnosti, na druhé straně pak zpravidla společenským zájmem motivovaná a také zcela důvodná potřeba prolomením absolutní ochrany společenských zájmů předejít zvláště závažným důsledkům spojeným například s organizovaným zločinem. Jinak řečeno orgány činné v trestním řízení musí mít nástroje a prostředky k tomu, aby mohly reálně svá oprávnění vykonávat.²¹³

Jak jsem již uvedla výše, je v případě odposlechu a záznamu telekomunikačního provozu značně problematické porušování sféry lidských práv a svobod. Konkrétně se pak jedná o ochranu práva na listovní tajemství upraveného v čl. 13 Listiny,²¹⁴ které zaručuje i tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným

²¹³ Srov. *Souček, J.* Odposlech a záznam telekomunikačního provozu. Státní zastupitelství, 2008, č. 3, s. 22; *Šabata, K.* Zamyšlení o kolizní povaze trestního práva a nutnosti odposlechů. Státní zastupitelství, 2008, č. 3, s. 36.

²¹⁴ Článek 13 Listiny zaručuje však toto právo s výjimkou případů a způsobem, které stanoví zákon. To znamená, že je možné vytvořit zákonnou výjimku, která do tohoto práva bude za splnění předem stanovených podmínek zasahovat.

zařazením, a práva na respektování soukromého a rodinného života zaručeného v čl. 8 Úmluvy.²¹⁵

V judikatuře Ústavního soudu se v této souvislosti mluví i o tzv. právu na informační sebeurčení, které svou povahou i významem spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní, svobodou v prostorové dimenzi, svobodou komunikační a zajisté i dalšími ústavně garantovanými základními právy dotváří osobnostní sféru jedince. Toto právo lze dovodit z čl. 10 odst. 3 Listiny, garantujícího jednotlivci právo na ochranu před neoprávněným shromažďováním, zveřejňováním anebo jiným zneužíváním údajů o své osobě, a to ve spojení s právě již zmiňovaným čl. 13 Listiny.

Podle názoru Ústavního soudu, pokud ústavní pořádek České republiky připouští průlom této ochrany, děje se tak pouze a výlučně v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených základních práv a svobod jiných; sem spadá především nezbytnost daná obecným zájmem na ochraně společnosti před trestnými činy a dále tím, aby takové činy byly zjištěny a potrestány.²¹⁶ Na druhou stranu, aby nebyly překročeny meze nezbytnosti, musí existovat systém adekvátních a dostatečných záruk, skládající se z odpovídajících právních předpisů a účinné kontroly jejich dodržování. Tyto právní předpisy musí být přesné ve svých formulacích, aby daly občanům dostatečnou informaci o okolnostech a podmínkách, za kterých jsou státní orgány oprávněny k zásahu do soukromí. Přesně musí být definovány i pravomoci udělené příslušným orgánům a způsob jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování. V případě, že tyto zásady nebudou ze strany státní moci respektovány, jsou zásahy do uvedeného základního práva vyloučeny, a dojde-li k nim, stávají se protiústavními.²¹⁷

V této věci navazuje judikatura Ústavního soudu přímo na judikaturu Evropského soudu pro lidská práva, který se touto problematikou zabývá více než 30

²¹⁵ Srov. plenární nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/2010, uveřejněný pod č. 52 ve svazku 60 Sbirky nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 94/2011 Sb.

²¹⁶ Srov. plenární nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/2010, uveřejněný pod č. 52 ve svazku 60 Sbirky nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 94/2011 Sb.

²¹⁷ Srov. nález Ústavního soudu ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000, uveřejněný pod č. 11 ve svazku 21 Sbirky nálezů a usnesení Ústavního soudu České republiky.

let. Právě judikatura ESLP totiž stanovila základní principy, které musí vnitrostátní právní úprava splňovat, aby byla zajištěna ochrana práv zaručených Úmluvou.

ESLP ve své judikatuře opakovaně uvedl, že existence právní úpravy, kterou se vytváří možnost uplatnění tajného dohledu nad poštovními zásilkami a telekomunikacemi, je za výjimečných podmínek nevyhnutelná v demokratické společnosti v zájmu národní bezpečnosti a při předcházení nepokojům a zločinnosti. Zároveň však zformuloval požadavek, aby příslušný zákon představující zákonný základ pro opatření zasahující do soukromí osob byl dostatečně přístupný dotčené osobě, která by tak mohla předvídat důsledky jeho aplikace, a aby byl slučitelný s principem právního státu.

Také zdůraznil, že ani v případě, kdy je upřednostněna ochrana výše zmíněných zájmů před soukromou sférou jedince, nemají smluvní státy úplnou volnost při uplatňování dohledu nad osobami v jejich jurisdikci. V souladu s Úmluvou existuje pouze takový systém dohledu, v kterém existují adekvátní a účinné záruky proti zneužití. Za takové záruky ESLP ve své judikatuře považuje především definování kategorií osob, které mohou být odposlouchávány, či trestných činů, v souvislosti s kterými je možno realizovat odposlechy, časové vymezení odposlechů, kontrolu nezávislým soudním orgánem, postupy při vytváření záznamů obsahu odposlouchávaných hovorů, úpravu podmínek uchovávání vyhotovených záznamů a nahrávek a vymezení okolností, za kterých mohou být nahrávky smazány a zvukové nosiče nebo jiné záznamy zničeny.²¹⁸ Z toho mimo jiné vyplývá, že každé takovéto opatření představující zásah do práv zaručených Úmluvou musí být na úrovni národního práva přezkoumatelné, jinak by došlo k porušení ustanovení čl. 13 Úmluvy a opět by mohla být podána stížnost k ESLP. S tím úzce souvisí aplikace čl. 13 Úmluvy, který zaručuje každému, jehož práva a svobody přiznaná Úmluvou byla porušena, účinné právní prostředky nápravy před národním orgánem, i když se porušení dopustily osoby při plnění úředních povinností. Navíc je podle ESLP nutno se zabývat tím, zda řízení určená ke kontrole přijetí a použití omezujících opatření jsou způsobilá omezit zasahování vyplývající z inkriminovaného zákona na to, co je „nezbytné v demokratické společnosti“. K tomu, aby nebyly překročeny meze nezbytnosti ve smyslu čl. 8 odst. 2,

²¹⁸ Srov. *Bálintová, M.* Záruky proti zneužití odpočívání. *Justičná revue*, 2008, č. 10, s. 1352.

je navíc třeba v kontrolních řízeních co nejvěrněji respektovat hodnoty demokratické společnosti, jako je například zásada právního státu, která implikuje, že zasahování výkonné moci do práv jednotlivce musí podléhat účinné kontrole.²¹⁹

Na druhou stranu však ESLP uvedl, že pokud po ukončení sledování nebyla dotčená osoba o provedených opatřeních informována, není to v rozporu s ustanovením čl. 8 Úmluvy, když právě neinformování mohlo zajistit účinné fungování sledovacího systému.²²⁰

Z výše uvedeného tedy vyplývá, že samotná existence institutu narušujícího lidská práva a svobody není protizákonná, pokud splňuje požadavek minimalizace takových zásahů, požadavek subsidiarity takových opatření a požadavek záruk proti jejich zneužití. Právě naopak je žádoucí a v trestním právu nalezneme celou řadu institutů, které zasahují do práv a svobod mnohem intenzivněji, ale přesto nejsou zdaleka tolik kritizovány jako odposlechy.

Proč tomu tak tedy je? Proč je odposlech a záznam telekomunikačního provozu tak často diskutovaným tématem? Osobně v tom vidím dva důvody.

Prvním z nich jsou úniky odposlechů a jejich medializace, kdy zřejmě není třeba příliš připomínat veškeré kauzy, které za posledních několik let proběhly médii. Tyto kauzy vždy zas a znovu nastolily otázku, zdali jsou vůbec informace získané odposlechy dostatečně chráněny.

Z hlediska ochrany takovýchto informací je nejprve nutno rozlišovat v procesu jejich zpracovávání a dalšího využívání v rámci trestního řízení v zásadě dva základní režimy:

1. odfiltrování a fixaci dat, majících přímý vztah k předmětu trestního řízení, s jejich eventuálním pozdějším využitím v rámci důkazního řízení; tato data se musí zafixovat způsobem předepsaným v § 88 odst. 6 trestního řádu, jinak by k nim nebylo možno přihlédnout jako k důkazu, a v příslušné fázi trestního řízení se tak stávají součástí trestního spisu,
2. oddělení dat, která nemají přímý vztah k trestnímu řízení, nejsou tedy určena k využití v rámci dalšího důkazního řízení; ta je třeba uložit odděleně a nemají-

²¹⁹ Srov. rozsudek ESLP ze dne 8. 9. 1978, ve věci Klass a další proti Německu, stížnost č. 5029/71.

²²⁰ Srov. rozsudek ESLP ze dne 8. 9. 1978, ve věci Klass a další proti Německu, stížnost č. 5029/71.

li skutečně žádný vztah k vedenému trestnímu řízení, je nutno je předepsaným způsobem zničit, jak stanoví § 88 odst. 7 trestního řádu. Právě u těchto informací by nemělo nikdy dojít k jejich zveřejnění.²²¹

Trestní řád ukládá povinnost policejnímu orgánu záznamy, které nejsou užity jako důkaz v trestním řízení, spolehlivě uschovat tak, aby byla zajištěna ochrana před neoprávněným zneužitím záznamů, a v protokolu založeném do spisu poznamenat, kde jsou uloženy. Na zákonné úrovni mi tato úprava přijde dostatečná. Bohužel však nezabrání neprofesionálnímu jednání osob, které za vidinou zisku takovéto informace zpřístupní nepovolaným osobám. K únikům takovýchto záznamů tedy z mého pohledu nedochází kvůli nedostatečnosti úpravy, ale kvůli neprofesionalitě odpovědných osob.

Obecně takovéto osoby podléhají zákonné povinnosti mlčenlivosti. Vedle toho již existují interní úpravy, které zakládají povinnosti při nakládání s takovýmito informacemi. Příkladem takové úpravy je pokyn obecné povahy nejvyššího státního zástupce č. 7/2004, jímž se vydává kancelářský řád státního zastupitelství, ve znění pozdějších předpisů. Tento předpis obsahuje v § 126a až 126d pravidla pro nakládání s neutajovanými záznamy odposlechu.²²² Toto opatření má za účel zejména snížení rizika úniků informací v době, kdy se příslušné nosiče a ostatní dokumentace nacházejí v dispozici státního zastupitelství.

Záměrem této úpravy tedy je:

- minimalizovat počet případů, kdy se informace získané odposlechem dostávají na státní zastupitelství v samotném počátku nasazení odposlechu a kdy je riziko úniku a závažnosti jeho důsledků pro samu trestní věc i pro osoby, jejichž soukromí je takto prolamováno, největší,
- zabezpečit ochranu těchto informací, došlých na státní zastupitelství, od okamžiku jejich doručení způsobem, který vyloučí snadný přístup k jejich obsahu nepovolané osobě,
- zajistit, aby dispozice s těmito informacemi byla svěřena omezenému okruhu osob, tj. zásadně jen dozorovému státnímu zástupci, jeho nadřízeným, a u

²²¹ Srov. *Vondruška, F.* Odposlechy – věčné a (ne)vděčné téma současnosti. Státní zastupitelství, 2008, č. 3, s. 31.

²²² Tato hlava byla do pokynu zavedena novelou č. 1/2006 s účinností ode dne 1. června 2006.

kanceláře pak určené osobě, která dává záruku zachování důvěrnosti těchto informací,

- zajistit jejich bezpečné ukládání a kontrolu dispozice s nimi po dobu, po kterou se nacházejí u státního zastupitelství,
- stanovit postupy, které zabezpečí prokazatelné předávání těchto informací jiným orgánům (soudu, policii).²²³

Z výše uvedeného tedy vyplývá, že vhodným opatřením není novela zákonné úpravy, nýbrž zavádění takovýchto interních předpisů, které obsahují detailní úpravu nakládání s těmito informacemi a zároveň zohlední potřeby toho kterého orgánu činného v trestním řízení. Zároveň bych k tomu chtěla dodat, že i výběr takovýchto odpovědných osob by měl probíhat se zvýšenou pozorností a zároveň by tyto osoby měly být dostatečně finančně, popřípadě různými výhodami, ohodnoceny, aby jednoduše neměly potřebu prodávat tyto citlivé informace.

V tomto směru je nutné ještě poukázat na určitý nedostatek právní úpravy. Podle přílohy 1 k nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, totiž právní úprava zařadila informace o přípravě odposlechu a záznamu telekomunikačního provozu mezi informace utajované podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Vlastní obsah takto získaných informací však utajení podle tohoto zákona nepodléhá, ledaže by povinnost jejich utajování vyplynula z jejich vlastní povahy.²²⁴ Není bez zajímavosti, že utajení podobného institutu operativně pátracích prostředků je v té samé příloze věnováno mnohem více prostoru.

Druhým důvodem značné „nepopularity“ odposlechů je pak fakt, že odposlechy jsou institutem poměrně novým, úzce spjatým s rozvojem moderních technologií. Samozřejmě i dříve bylo možné narušit soukromí osob porušením listovního tajemství, popřípadě prostorovými odposlechy, ale v současné době tento institut nabírá úplně nových rozměrů. Technologické prostředky jsou totiž již na takové úrovni, že je

²²³ Vondruška, F. Odposlechy – věčné a (ne)vděčné téma současnosti. Státní zastupitelství, 2008, č. 3, s. 32.

²²⁴ Srov. Vondruška, F. Odposlechy – věčné a (ne)vděčné téma současnosti. Státní zastupitelství, 2008, č. 3, s. 31.

v podstatě možné odposlouchávat kohokoli a kdykoli, aniž by on o tom věděl.

Nelze samozřejmě opomenout, že tomu významnou měrou přispěla i změna lidského chování. Zatímco dříve docházelo k výměně informací zejména „tváří v tvář“, v současné době mají lidé tendenci komunikovat daleko více pomocí technologií jako jsou mobilní telefony nebo e-mail, což samozřejmě ale nahrává tomu, že někdo se může do takové komunikace poměrně snadno nabourat (a nemusí to být pouze stát). Dalo by se tedy říct, že problém není ani tak v samotném institutu, jako v lidském chování, kdy lidé neuváženě sdělují na internetu citlivé informace a pomocí e-mailů, SMS zpráv nebo sociálních sítí řeší problémy, které nejsou určeny cizím uším. Osobně bych řekla, že nejlepším řešením tohoto problému by byla dostatečná edukace a disciplína obyvatel v této oblasti, zároveň si však uvědomují, jak naivní je představa, že se lidé vzdají technologických vymožeností, které jim usnadňují každodenní komunikaci. Přece jen je daleko snazší někomu zavolat, než se s ním osobně sejít.

Zjednodušeně řečeno, lidé si sami na sebe ušili bič, když se rozhodli svěřit mezilidskou komunikaci do rukou techniky. Ostatně jako každý důležitý pokrok v lidských dějinách mají i technologické objevy svoji stinnou stránku, kterou nebyl předem nikdo schopen odhadnout. Dalo by se tedy říci, že současná doba se vyznačuje ztrátou soukromí, kdy každý, kdo k tomu má dostatečné prostředky a moc, popřípadě znalosti, se může nabourat do života kohokoliv, sledovat jeho každodenní činnost a samozřejmě toho i využít.

Je nepochybné, že taková ztráta soukromí je pro každého nepříjemná, a tudíž je i pochopitelné, že se mnozí lidé dovolávají alespoň přísného omezení odposlechů. Tomu hraje do karet i skutečnost, že odposlech a záznam telekomunikačního provozu je v současnosti často používanou operativní technikou v kriminalistické praxi i v trestním procesu, a nabízí se otázka, zdali orgány činné v trestním řízení nezneužívají odposlechů i v případech, kdy jejich použití není na místě, jednoduše proto, že je to snadný způsob získání potřebných informací. Odposlech totiž může být podle zákona použit pouze v případech, kdy již existuje podezření na konkrétní trestnou činnost páchanou určitou osobou, a výsledky získané jeho použitím slouží pouze k potvrzení takového podezření, popřípadě k doplnění mezer v dokazování, a jako takový by neměl sloužit k získávání informací, na základě kterých teprve takové podezření vzniká. Kritiky odposlechů je tak navrhováno, aby takovéto informace byly získávány jinými,

ne tolik invazivními důkazními prostředky. Je nutné si však uvědomit, že snižování počtu odposlechů vyžaduje, aby na druhé straně existovaly právě takové důkazní prostředky, které mohou informace získané odposlechy plnohodnotně nahradit, jinak by došlo k ohrožení akceschopnosti orgánů činných v trestním řízení.

Například se objevil názor, že odposlech a záznam telekomunikačního provozu může být nahrazen institutem tzv. korunního svědka podle anglosaského práva.²²⁵ Bohužel ani toto řešení by nebylo ideálním, protože i toto opatření narušuje základní lidská práva a svobody tím, že zakládá nerovnost osob před zákonem. Zjednodušeně řečeno se totiž jedná o slib mírného trestu za usvědčení jiné osoby.²²⁶ Navíc tento institut je plně závislý na existenci osoby, která může o daných skutečnostech vypovídat a která je na druhé straně prokazatelně usvědčitelná z jiného trestného činu. K tomu musí být navíc tato osoba ochotná s orgány činnými v trestním řízení spolupracovat. Je tedy nasnadě, že použití takového institutu je závislé na mnoha proměnných, které ne vždy jsou splněny, zatímco na druhou stranu je těžko představitelné, že pachatelé trestné činnosti by v dnešní době pro své aktivity nepoužívali žádnou komunikační technologii. Možnost nasazení odposlechu je tedy ve většině případů pouhou otázkou času.

V souhrnu se pak dá říci, že nahrazení odposlechu a záznamu telekomunikačního prostředku jinými důkazními prostředky by rozhodně nebylo bezproblémové. Osobně bych se však přikláběla k názoru, že odposlech je již ze své podstaty institutem nezastupitelným a pro vyšetřování určitých druhů kriminality nutným, protože informace, a to i informace závadové, se šíří rovněž telekomunikačním provozem. Tudíž nelze setrúvat u „zastaralých“ důkazních prostředků, ale je nutné je přizpůsobit metodám současných pachatelů trestné činnosti.

²²⁵ Šabata, K. Zamyšlení o kolizní povaze trestního práva a nutnosti odposlechů. Státní zastupitelství, 2008, č. 3, s. 36.

²²⁶ V českém právu existuje podobný institut spolupracujícího obviněného, který je zakotven v § 178a trestního řádu.

5. Úvahy de lege ferenda

Na základě výše uvedených skutečností musím říci, že právní úprava odposlechu a záznamu telekomunikačního provozu je podle mého názoru až na drobnější věci dostačující a rozhodně na základě této úpravy nedochází k nepřiměřeným zásahům do základních lidských práv a svobod. Co se týče institutu zjišťování údajů o telekomunikačním provozu, tam mi přijdou dané nedostatky již výraznější.

První připomínku bych měla k systematickému začlenění obou institutů, které považuji za sporné. Jak jsem již uvedla, jsou tato opatření zařazena do zajišťovacích institutů, jejichž smyslem je zajištění a opatření věcí a jiných majetkových hodnot důležitých pro trestní řízení, zejména z hlediska naplnění požadavku náležitého objasnění skutkového stavu věci.²²⁷ Naproti tomu však trestní řád upravuje i tzv. operativně pátrací prostředky, přičemž jejich účelem, stejně jako u odposlechu, je získání skutečností důležitých pro trestní řízení, které mohou být v dalším řízení za určitých podmínek použity jako důkaz. U institutu zjišťování údajů o telekomunikačním provozu je tato potřeba sice vyjádřena jako „*je-li třeba pro účely trestního řízení zjistit údaje o telekomunikačním provozu*“, ale vzhledem k tomu, že i výsledek uplatnění tohoto institutu se dá použít jako důkaz, není pochybností o tom, že i on se účelem shoduje s operativně pátracími prostředky. Tento fakt pak ještě podtrhuje skutečnost, že vůči operativně pátracímu prostředku sledování osob a věcí podle § 158d trestního řádu jsou oba tyto instituty v poměru speciality.²²⁸ Navíc jsou v praxi mnohdy i tak zařazovány mezi operativně pátrací prostředky.

²²⁷ Jelínek, J. a kol. Trestní právo procesní. 1. vyd. Praha: Leges, 2010, s. 316.

²²⁸ Podle důvodové zprávy k zákonu č. 273/2012 Sb. je dokonce analogie zjišťování údajů o telekomunikačním provozu k tomuto operativně pátracímu prostředku více na místě, než analogie k odposlechům podle § 88 trestního řádu, neboť je třeba si uvědomit, že podle § 88a trestního řádu není zjišťován obsah komunikace mezi osobami, ale pouze provozní a lokalizační údaje. Tento názor mi však nepřijde zcela správný, protože odposlechem lze získat stejné informace jako zjišťováním údajů o telekomunikačním provozu (např. datum a čas nebo délku hovoru). Srov. důvodová zpráva k návrhu zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Poslanecká sněmovna, 2012.

Dle mého názoru by tudíž bylo nejvhodnější vytvoření samostatné hlavy v části první trestního řádu, která by upravovala pouze operativně pátrací prostředky, mezi kterými by byl i odposlech a zjišťování údajů o telekomunikačním provozu. Takováto změna by totiž přispěla k větší přehlednosti trestního řádu a jasnému právnímu vymezení těchto institutů. Zároveň bych ráda podotkla, že provedení takovéto změny by mělo být zvažováno zejména v rámci rekodifikace trestního řádu.

Další nedostatek, který se rovněž týká obou institutů, se vztahuje k pojmu „úmyslný trestný čin, k jehož stíhání zavazuje vyhlášení mezinárodní smlouva“. Tomu je vytýkána zejména nejasnost a nepředvídatelnost právní úpravy. V tomto případě by řešením mohlo být uvedení taxativního výčtu trestných činů, přičemž by zároveň bylo i zváženo, na které trestné činy by se mohly mezinárodní závazky vztahovat. Ideálním řešením by pak mohlo být stanovení širšího pojetí trestných činů, korigované striktnějšími kritérii pro jejich posuzování v jednotlivých případech.

Rovněž úprava, která umožňuje odposlech nebo zjišťování údajů o telekomunikačním provozu se souhlasem uživatele podle § 88 odst. 5 a § 88a odst. 4 trestního řádu by mohla být doplněna určitými podmínkami, které by jasněji stanovily hranice jejího použití.

Především bych do tohoto ustanovení u obou institutů promítla zásadu subsidiarity, např. formulací „*při nebezpečí prodlení*“ nebo „*nesnese-li věc odkladu*“, doplněnou o dodatečný povolovací proces, kdy by soudce ve stanovené lhůtě takto vydaný příkaz dodatečně povolil, a pokud ne, musel by být takový odposlech ukončen. Výsledky jím získané by nemohly být v řízení použity a byly by bez prodlení zničeny.

Navíc by bylo vhodné doplnit ustanovení i o možnost odvolání souhlasu a o povinnost orgánu činného v trestním řízení poučit o tom dotčeného uživatele, který takovýto souhlas uděluje. Toto by však bylo podle mě bylo dostatečné i na úrovni interních normativních předpisů.

Za vůbec nejproblematictější však u úprav obou institutů považuji, že ani jedna z nich neobsahuje možnost vydání příslušného příkazu v případech, kdy jsou splněny podmínky pro jeho vydání, ale z důvodu časové tísně není tento postup vhodný, protože by mohlo dojít k značnému ztížení vyšetřování, nebo dokonce ke zmaření účelu vyšetřování. Tímto postupem by totiž mohly být při vyšetřování získány důležité informace (např. při pátrání po pachateli trestného činu po tzv. „horké stopě“).

Samozřejmě by u takového postupu musela být zdůrazněna zásada subsidiarity. Nařízení by vydával zřejmě policejní orgán nebo státní zástupce, v řízení před soudem pak soudce, přičemž ale toto nařízení by podléhalo dodatečnému přezkumnému a povolovacímu procesu soudu (nadřízeného soudu), kdy dodatečné povolení by muselo být vydáno v určité časové lhůtě. Pokud by povolení vydáno nebylo, stalo by se nařízení neúčinným a muselo by být bez prodlení ukončeno. Výsledky takovým nařízením získané by nemohly být nadále v trestním řízení nijak použity. Takováto úprava by dle mého mínění dokonce mohla nahradit i výše zmíněný postup, kdy dochází k nařízení pouze se souhlasem uživatele. Přesto se však nedá popřít, že i takováto úprava by v praxi mohla být problematická, zejména s ohledem na fakt, že policejní orgány by takovýmto postupem mohly obcházet řádný povolovací proces za účelem získání operativních poznatků nutných pro další postup ve vyšetřování.

U odposlechu bych pak dále pozměnila úpravu informační povinnosti podle § 88 odst. 8 trestního řádu, která se v současnosti vztahuje pouze na osobu uživatele podle § 88 odst. 2 věty třetí trestního řádu. Přitom zákon umožňuje zároveň použití záznamu odposlechu i v jiné trestní věci, než ve které byl odposlech nařízen. Záznam tak může být použit i vůči osobě, která nebyla primárně odposlouchávána, přesto se na ni však informační povinnost nevztahuje. To je dle mého názoru jak v rozporu se smyslem samotné informační povinnosti, tak samozřejmě i s ústavním pořádkem České republiky a Úmluvou, protože to zakládá nerovnost osob před zákonem. Tuto úpravu bych tudíž rozšířila i na osoby, proti kterým je vedeno trestní řízení, v rámci kterého jsou záznamy získané odposlechem použity jako důkaz.

U zjišťování údajů o telekomunikačním provozu bych pak v první řadě doplnila režim nakládání se zprávou získanou zjišťováním údajů o telekomunikačním provozu, zahrnující ukládání zpráv, které nejsou použity v trestním řízení jako důkaz, popřípadě jejich použití v jiném trestním řízení. To samé se týká i ničení zpráv, které nejsou použity jako důkaz v trestním řízení. Koneckonců tento nedostatek byl tomuto institutu vytýkán i ve výše zmiňovaném nálezu Ústavního soudu Pl. ÚS 24/2011 Sb., který mimo jiné uvedl, že není důvod pro uplatňování odlišných podmínek pro odposlech a záznam telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu, pokud

něco jiného nevyplývá z jejich povahy.²²⁹ Podle mého názoru by však nebylo ani nutné vytvářet pro tento institut zvláštní úpravu, ale stačilo by vytvořit normu, která by odkazovala na přiměřené použití ustanovení § 88 trestního řádu.

Dále by pak podle mě mělo být doplněno i ustanovení § 30 odst. 4 trestního řádu, které upravuje vyloučení soudce v souvislosti s řízením o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu. Toto ustanovení by se totiž mělo výslovně vztahovat i na soudce ohledně přezkumného řízení k příkazu ke zjišťování údajů o telekomunikačním provozu. Ačkoli je sice tato zákonná mezera překonána výkladem per analogiam, zdá se mi tento výklad na hranici přípustnosti. Ustanovení § 30 odst. 4 trestního řádu totiž obsahuje taxativní výčet případů, kdy je možné takové vyloučení soudce uplatnit, a to pouze ve vztahu k odposlechu a záznamu telekomunikačního provozu.

Poslední vytýkaný nedostatek se pak netýká trestního řádu, ale zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů, a nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. Na místě by totiž bylo zahrnout pod utajované informace minimálně i výsledky použití obou těchto institutů. U odposlechu bych však navrhovala zahrnout do seznamu utajovaných informací stejné skutečnosti jako u operativně pátracích prostředků.²³⁰

²²⁹ Srov. plenární nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/2011, uveřejněný pod č. 217 ve svazku 63 Sbírký nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 43/2012 Sb.

²³⁰ Těmi jsou informace o jejich přípravě, použití a výsledku, metody a postupy při jejich použití, informace o technických prostředcích a zařízeních zajišťujících jejich použití a informace o jejich výzkumu, vývoji a výrobě, včetně technické dokumentace. Nakonec jsou to i informace o finančním zabezpečení jejich pořizování a provozu.

Závěr

Není pochyb o tom, že využití odposlechu a záznamu telekomunikačního provozu i zjišťování údajů o telekomunikačním provozu v trestním řízení je nezbytnou součástí vyšetřování závažné kriminality.

V této práci jsem se věnovala zejména rozboru jejich právní úpravy v trestním řádu, popřípadě dalšími úpravami, které jsou obsaženy v interních normativních předpisech (pokyny obecné povahy nejvyššího státního zástupce, závazné pokyny policejního prezidenta apod.). Mým cílem bylo posoudit, zdali je tato úprava dostatečná a prostá větších zákonných mezer. Zároveň jsem brala v potaz i judikaturu Ústavního soudu a Nejvyššího soudu, která má na vývoj tohoto institutu nemalý vliv, a společně s judikaturou Evropského soudu pro lidská práva stanovuje základní principy a měřítka při používání těchto institutů.

U odposlechu a záznamu telekomunikačního provozu jsem se podrobně věnovala jak jednotlivým podmínkám, které jsou nutné pro jeho povolení, tak i jednotlivým fázím procesu jeho povolování, uskutečňování, vyhodnocování, ukládání a ničení získaných záznamů a nakonec i informační povinnosti orgánů činných v trestním řízení v souvislosti s přezkumným řízením. Zákon pamatuje i na případy, kdy je odposlech používán v rámci mezinárodního vyšetřování a upravuje tzv. přeshraniční odposlech.

U zjišťování údajů o telekomunikačním provozu jsem se pak věnovala podmínkám pro vydání příkazu k uplatnění tohoto institutu, procesem vydávání takového příkazu a jeho náležitostmi. Následně jsem rozebrala i informační povinnost a přezkumné řízení na ní navazující. Vedle toho jsem se věnovala i nařízení tohoto institutu se souhlasem uživatele.

Co se týče podmínek odposlechu i zjišťování údajů o telekomunikačním provozu, tam bych měla závažnější výhradu pouze proti formulaci „*jiné úmyslné trestné činy, k jejichž stíhání zavazuje vyhlášená mezinárodní smlouva*“, která nesplňuje podmínku jasnosti, přesnosti a předvídatelnosti právní úpravy v souladu s judikaturou Evropského soudu pro lidská práva i Ústavního soudu. Další výhrady pak mám ohledně obou institutů v případech, kdy lze jejich použití nařídit bez příkazu, pouze se souhlasem uživatele. Toto opatření by dle mého názoru mělo být doplněno o dodatečný povolovací proces a zároveň by mělo být omezeno podmínkou subsidiarity, která by

zajistila jeho použití pouze v těch nejnutnějších případech. Zcela pak u obou institutů schází úprava jejich použití v případech časové tísně, která by umožnila nařízení použití těchto institutů v co nejkratší době.

U odposlechu pak mám námitky proti úpravě informační povinnosti, kdy zákon neumožňuje její podání osobě, vůči níž nebyl sice odposlech nařízen, ale která byla jeho použitím dotčena, protože záznam takového odposlechu byl použit jako důkaz v rámci trestního řízení vedeného proti této osobě. Taková osoba pak nemá tudíž ani právo na zahájení přezkumného řízení u Nejvyššího soudu, což dle mého názoru zakládá nerovnost osob před zákonem. Celkově však jinak úpravu odposlechu a záznamu telekomunikačního provozu považuji za dostačující, prostou větších nedostatků, které by zásadním způsobem ovlivňovaly použití tohoto institutu v praxi. Nakonec i problémy, které jsem výše uvedla, se v praxi týkají marginálního počtu odposlechů.²³¹

To se však nedá říci o druhém institutu, zjišťování údajů o telekomunikačním provozu. Tento institut prošel v nedávné době podstatnou změnou, kdy Ústavní soud ustanovení § 88a trestního řádu zrušil v nálezu sp. zn. Pl. ÚS 24/2011 z důvodu jeho protiústavnosti. V návaznosti na to bylo do trestního řádu vloženo nové ustanovení § 88a, které stanovilo značně restriktivnější podmínky pro použití tohoto institutu. Přesto však této úpravě naprosto chybí postup při skladování a ničení výsledků získaných použitím tohoto opatření, které nejsou použity v trestním řízení jako důkaz. Novelou byla v tomto ustanovení zavedena i informační povinnost a možnost přezkumu zákonnosti příkazu k zjišťování údajů o telekomunikačním provozu, zákonodárce však opomněl rovněž novelizovat § 30 odst. 4 trestního řádu, který upravuje vyloučení soudce v souvislosti s tímto institutem, což by podle mě rovněž mělo být doplněno zákonnou novelou, vzhledem k tomu, že výklad per analogiam nepovažuji za dostatečný.

Poslední nedostatek, který by mohl být odstraněn, je nedostatečné zahrnutí obou institutů do utajeného režimu podle přílohy č. 1 k nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.

Vedle posuzování právní úpravy obou institutů jsem se rovněž v kapitole první

²³¹ Srov. Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2012. Policejní prezidium ČR, 2012.

této práce zabývala historií jejich vývoje od roku 1990, kdy byl do trestního řádu vložen institut odposlechu telefonních hovorů, až po současnost. Mým cílem bylo zejména postihnout nejdůležitější zákonné novely a judikáty Ústavního soudu a posoudit jejich přínos pro vývoj tohoto institutu.

Dále jsem se pak zabývala i obdobnými instituty podle německého práva, přičemž kvalita české právní úpravy se mi zdá srovnatelná s tou německou. Nakonec tyto úpravy se od sebe nějakým zásadním způsobem ani neliší, a ačkoli nemohu popřít, že v některých aspektech mi německá právní úprava přijde propracovanější, jinde je zase ta česká již o krok dál.

V předposlední kapitole jsem se pak obecněji věnovala vztahu institutu odposlechu a záznamu telekomunikačního provozu a ochrany lidských práv a svobod, a to i vzhledem k judikatuře ESLP. Do této kapitoly jsem zahrнула i problematiku úniků odposlechů, které byly v posledních letech „vděčným“ tématem nejrůznějších mediálních kauz.

Závěrem jsem v poslední kapitole uvedla i několik návrhů na zlepšení dosavadní právní úpravy, jejichž podstatu jsem shrнула výše.

Dle mého názoru neslouží právní úprava na zákonné úrovni k naprostému vyčerpání této problematiky. Spíše by měla stanovit zejména rámec použití těchto institutů, který zaručí jejich zákonnost. Určení detailů pak již spočívá na úpravě stanovené interními předpisy, které přece jen mohou daleko lépe vystihnout potřeby jednotlivých orgánů činných v trestním řízení, ale zároveň i vystihnout úskalí, která při používání těchto institutů v praxi nastávají, a na rozhodnutí soudů, zejména těch nejvyšších instancí, které svou judikaturou překlenují jednotlivé mezery v právní úpravě. Na úrovni Ústavního soudu a ESLP pak judikatura zároveň stanovuje i základní normy, které musí tato úprava splňovat.

Pokud by tomu bylo naopak a zákon by se opravdu pokusil postihnout i všechny tyto detailní problémy, byla by tato snaha již předem odsouzena k zániku. Za prvé není možné pomocí zákona postihnout veškeré situace, které v reálném životě nastanou, protože vždy se objeví situace, kterou zákonodárce nepředpokládal. Za druhé by taková úprava vedla ještě k větší komplikovanosti právní úpravy, která je již teď poměrně rozsáhlá a složitá. Ustanovení trestního řádu však zároveň nemohou být vágní vzhledem k požadavku jasnosti a přesnosti zákonného vymezení jednotlivých podmínek tak, aby

byly minimalizovány zásahy do práv a svobod osob zaručených ústavním pořádkem České republiky a Úmluvou. Je tedy nutné najít určitý kompromis mezi výše uvedenými požadavky. To se dle mého názoru u odposlechu a záznamu telekomunikačního provozu podařilo. U institutu zjišťování údajů o telekomunikačním provozu však již o něco méně.

Seznam zkratek

ESLP - Evropský soud pro lidská práva

GG – Základní zákon ze dne 23. 5. 1949

Listina - usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod

Odposlech - odposlech a záznam telekomunikačního provozu

Osoba - právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací

Soudní kancelářský řád – instrukce Ministerstva spravedlnosti č. j. 505/2001-Org, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy

Stát provádějící odposlech – členský stát, kde dotčená odposlouchávaná osoba využívá služeb svého telefonního operátora

StGB - německý trestní zákoník v publikovaném znění ze dne 13. 11. 1998

StPO - německý trestní řád v publikovaném znění ze dne 7. dubna 1987

TKG – německý telekomunikační zákon ze dne 22. 6. 2004

Trestní řád - zákon č. 141/1961 Sb., o trestním řízení soudním

Trestní zákoník - zákon č. 40/2009 Sb., trestní zákoník

Úmluva - Úmluva o ochraně lidských práv a základních svobod

Úmluva o pomoci v trestních věcech - Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie

Ústava – ústavní zákon č. 1/1993 Sb., Ústava České republiky

Ústavní soud – Ústavní soud České republiky

Uvědomovaný stát – členský stát, v jehož příhraničním území se odposlouchávaná osoba pohybuje

Útvar zvláštních činností – Útvar zvláštních činností služby kriminální policie a vyšetřování

Zákon o elektronických komunikacích - zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů

Zákon o soudnictví ve věcech mládeže - zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže

Zákon o telekomunikacích - zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů

Zákon o trestní odpovědnosti právnických osob - zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

ZPPP - závazný pokyn policejního prezidenta č. 30/2009 Sb., o plnění úkolů v trestním řízení

Literatura

Monografie:

- Fryšták, M.* Trestní právo procesní. 3. aktualiz. vyd. Ostrava: Key Publishing, 2012. ISBN 978-80-7418-160-3.
- Jelínek, J. a kol.* Trestní právo procesní. 1. vyd. podle novelizované právní úpravy účinné od 1. 1. 2010. Praha: Leges, 2010. ISBN 978-80-87212-30-1
- Jelínek, J. a kol.* Trestní právo procesní. 2. vyd. podle novelizované právní úpravy účinné od 1. 9. 2011. Praha: Leges, 2011. ISBN 978-808-7212-929.
- Jelínek, J.* Odposlech a záznam telekomunikačního provozu. Pocta prof. JUDr. Milanu Bakešovi, DrSc., k 70. narozeninám. 1.vyd. Praha: Leges, 2009. ISBN 978-808-7212-233.
- Jelínek, J. a kol.* Trestní zákoník a trestní řád s poznámkami a judikaturou. 2. aktualiz. vyd. podle stavu k 1. 12. 2011. Praha: Leges, 2011. ISBN 978-808-7212-998.
- Joecks, W.* Strafprozessordnung. Studienkommentar. 3. Auf. München: C. H. Beck, 2011. ISBN 978 3 406 61599 3
- Musil, J., Kratochvíl, V., Šámal, P. a kol.* Kurs trestního práva. Trestní právo procesní. 3. přeprac. a dopl. vyd. Praha: C. H. Beck, 2007. ISBN 978-807-1795-728.
- Novotný, O., Vokoun, R., Šámal, P. a kol.* Trestní právo hmotné. Zvláštní část. 6. vyd. Praha: Wolters Kluwer ČR, a. s., 2010. ISBN 978-80-7357-509-0
- Roxin, C., Schönemann, B.* Strafverfahrensrecht. Ein Studienbuch. München: C. H. Beck, 2012. ISBN 978 3 406 62597 8
- Šámal, P. a kol.* Trestní řád II. Komentář. 6. vyd. Praha: C. H. Beck, 2008. ISBN 978-80-7400-043-0
- Šámal, P. a kol.* Trestní řád I. § 1 až 156. Komentář. 7. vyd. Praha: C. H. Beck, 2013. ISBN 978-80-7400-465-0
- Šámal, P. a kol.* Trestní řád II. § 157 až 314s. Komentář. 7. vyd. Praha: C. H. Beck, 2013. ISBN 978-80-7400-465-0
- Šámal, P. a kol.* Trestní řád III. § 315 až 471. Komentář. 7. vyd. Praha: C. H. Beck, 2013. ISBN 978-80-7400-465-0
- Šámal, P., Novotný, F., Růžička, M., Vondruška, F., Novotná, J.* Přípravné řízení trestní. 2. vyd. Praha: C. H. Beck, 2003. ISBN 80-717-9741-3.

Články:

- Bálintová, M.* Záruky proti zneužití odpočívání. *Justičná revue*, 2008, č. 10.
- Koudelka, Z.* Rozhovor s místopředsedou Nejvyššího soudu Pavlem Kučerou. *Státní zastupitelství*, 2008, č. 3.
- Koudelka, Z.* Úniky odposlechů. *Státní zastupitelství*, 2008, č. 3.
- Sokol, T.* Odposlech. *Státní zastupitelství*, 2008, č. 3.
- Souček, J.* Odposlech a záznam telekomunikačního provozu. *Státní zastupitelství*, 2008, č. 3.
- Šabata, K.* Zamyšlení o kolizní povaze trestního práva a nutnosti odposlechů. *Státní zastupitelství*, 2008, č. 3.
- Vantuch, P.* Nová úprava odposlechu v trestním řádu od 1. 7. 2008. *Bulletin advokacie*, 2008, č. 10.
- Vondruška, F.* Odposlechy – věčné a (ne)vděčné téma současnosti. *Státní zastupitelství*, 2008, č. 3.

Zákony a právní předpisy:

- Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, dostupný na www.psp.cz.
- Zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů, dostupný na www.psp.cz.
- Zákon č. 178/1990 Sb., kterým se mění a doplňuje trestní řád, dostupný na www.psp.cz.
- Zákon č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů dostupný na www.psp.cz.
- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů, dostupný na www.psp.cz.
- Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů, dostupné na www.psp.cz.
- Zákon č. 292/1993 Sb., kterým se mění a doplňuje zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), zákon č. 21/1992 Sb., o bankách, a zákon č. 335/1991 Sb. o soudech a soudcích, dostupný na www.psp.cz.

Zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů, dostupný na www.psp.cz.

Zákon č. 265/2001 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, a některé další zákony, www.psp.cz.

Instrukce Ministerstva spravedlnosti č. j. 505/2001-Org, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy, ve znění pozdějších předpisů, dostupná v systému ASPI.

Výkladové stanovisko č. 25/2002 Sb. ve sbírce Nejvyššího státního zastupitelství, dostupné na www.nsz.cz.

Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů, ve znění pozdějších předpisů, dostupný na www.psp.cz.

Pokyn obecné povahy nejvyššího státního zástupce č. 7/2004, jímž se vydává kancelářský řád státního zastupitelství, ve znění pozdějších předpisů, dostupný v systému ASPI.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, dostupný na www.psp.cz.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnosti způsobilosti, ve znění pozdějších předpisů, dostupný na www.psp.cz.

Nářízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, dostupné na www.mvcr.cz.

Zákon č. 177/2008 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů, a zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, dostupný na www.psp.cz.

Pokyn obecné povahy nejvyšší státní zástupkyně č. 8/2009, o trestním řízení, ve znění pozdějších předpisů, dostupný na www.nsz.cz.

Závazný pokyn policejního prezidenta č. 30/2009 Sb., o plnění úkolů v trestním řízení, ve znění pozdějších předpisů, dostupný na www.policie.cz.

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, dostupný na www.psp.cz.

Zákon č. 41/2009 Sb., o změně některých zákonů v souvislosti s přijetím trestního zákoníku, www.psp.cz.

Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů, dostupný na www.psp.cz.

Zákon č. 459/2011 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony, dostupný na www.psp.cz.

Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a některé další zákony, dostupný na www.psp.cz.

Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, dostupný na www.psp.cz.

Základní zákon z 23. 5. 1949, ve znění pozdějších předpisů, BGBl. S. 1, dostupný na www.bgbl.de.

Německý zákon o organizaci soudů v publikovaném znění ze dne 9. 5. 1975, ve znění pozdějších předpisů, BGBl. I S. 1077, dostupný na www.bgbl.de.

Německý trestní řád v publikovaném znění ze dne 7. 4. 1987, ve znění pozdějších předpisů, BGBl. I S. 1074, ber. S. 1319, dostupný na www.bgbl.de.

Zákon o spolupráci spolku a zemí v záležitostech ústavní ochrany a o Spolkovém úřadu pro ústavní ochranu ze dne 20. 12. 1990, BGBl. I. S. 2954, 2970, dostupný na www.bgbl.de.

Německý trestní zákoník v publikovaném znění ze dne 13. 11. 1998, BGBl. I S. 3322, dostupný na www.bgbl.de.

Německý zákon k článku 10 Základního zákona ze dne 26. 6. 2001, omezující listovní, poštovní a telekomunikační tajemství, ve znění pozdějších předpisů, BGBl. I S. 1254, 2298, dostupný na www.bgbl.de

Německý telekomunikační zákon ze dne 22. 6. 2004, ve znění pozdějších předpisů, BGBl. I S. 3154, dostupný na www.bgbl.de.

Úmluva o ochraně lidských práv a základních svobod ze dne 4. 11. 1950, ve znění Protokolů č. 11 a 14, vyhlášená pod č. 209/1992 Sb., dostupná na www.echr.coe.int.

Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie ze dne 29. 5. 2000, vyhlášená pod č. 55/2006 Sb., dostupná na www.epravo.cz.

Soudní rozhodnutí:

Rozsudek ESLP ze dne 8. 9. 1978, ve věci Klass a další proti Německu, stížnost č. 5029/71, dostupný na hudoc.echr.coe.int.

Rozsudek ESLP ze dne 24. 8. 1998, ve věci Lambert proti Francii, stížnost č. 23618/94, dostupný na hudoc.echr.coe.int.

Rozsudek Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006, dostupný na www.nsoud.cz.

Stanovisko Nejvyššího soudu ze dne 5. 6. 2013, sp. zn. Tpjn 304/2012, dostupné na www.nsoud.cz.

Usnesení Nejvyššího soudu ze dne 8. 6. 2005, sp. zn. 7 Tdo 630/2005, dostupné na www.nsoud.cz.

Usnesení Nejvyššího soudu ze dne 24. 6. 2009, sp. zn. 5 Tdo 572/2009, dostupné na www.nsoud.cz.

Usnesení Nejvyššího soudu ze dne 14. 10. 2010, sp. zn. 4 Pzo 1/2010, dostupné na www.nsoud.cz.

Usnesení Nejvyššího soudu ze dne 13. 4. 2011, sp. zn. 4 Pzo 2/2010, dostupné na www.nsoud.cz.

Usnesení Nejvyššího soudu ze dne 26. 7. 2011, sp. zn. 4 Pzo 2/2011, dostupné na www.nsoud.cz.

Usnesení Nejvyššího soudu ze dne 30. 1. 2012, sp. zn. 4 Pzo 4/2011, dostupné na www.nsoud.cz.

Usnesení Nejvyššího soudu ze dne 9. 2. 2012, sp. zn. 4 Pzo 1/2012, dostupné na www.nsoud.cz.

Nález Ústavního soudu ze dne 27. 4. 1994, sp. zn. II. ÚS 6/93, uveřejněný pod č. 22 ve svazku 1 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupné na nalus.usoud.cz.

Nález Ústavního soudu ze dne 30. 11. 1995, sp. zn. III. ÚS 62/95, uveřejněný pod č. 78 ve svazku 4 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz.

Nález Ústavního soudu ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000, uveřejněný pod č. 11 ve svazku 21 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz.

Nález Ústavního soudu ze dne 13. 2. 2001, sp. zn. IV. ÚS 536/2000, uveřejněný pod č. 29 ve svazku 21 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz.

Nález Ústavního soudu ze dne 27. 8. 2001, sp. zn. IV. ÚS 78/2001, uveřejněný pod č. 123 ve svazku 23 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz.

Nález Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06, uveřejněný pod č. 88 ve svazku 45 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz

Nález Ústavního soudu ze dne 27. 9. 2007, sp. zn. II. ÚS 789/06, uveřejněný pod č. 150 ve svazku 46 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz.

Nález Ústavního soudu ze dne 27. 1. 2010, sp. zn. II. ÚS 2806/2008, uveřejněný pod č. 15 ve svazku 56 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz.

Nález Ústavního soudu ze dne 3.8.2010, sp. zn. IV. ÚS 1556/07, uveřejněný pod č. 152 ve svazku 58 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupný na nalus.usoud.cz.

Plenární nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/2010, uveřejněný pod č. 52 ve svazku 60 Sbírký nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 94/2011 Sb., dostupný na nalus.usoud.cz.

Plenární nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/2011, uveřejněný pod č. 217 ve svazku 63 Sbírký nálezů a usnesení Ústavního soudu České republiky, vyhlášený pod č. 43/2012 Sb., dostupný na nalus.usoud.cz.

Usnesení Ústavního soudu ze dne 18. 12. 2002, sp. zn. II. ÚS 616/01. 2002, dostupné na nalus.usoud.cz.

Usnesení Ústavního soudu ze dne 29. 4. 2004, sp. zn. IV.ÚS 554/03, uveřejněné pod č. 27 svazku 33 Sbírký nálezů a usnesení Ústavního soudu České republiky, dostupné na nalus.usoud.cz.

Nález Spolkového ústavního soudu ze dne 2. 3. 2010, BGBl. I S. 272, dostupný na www.bgbl.de.

Jiné zdroje:

- Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policíí ČR za rok 2012. Policejní prezidium ČR, 2012, dostupná na www.policie.cz.
- Důvodová zpráva k návrhu zákona č. 178/1990 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Federální shromáždění Československé socialistické republiky, 1990, dostupná na www.psp.cz.
- Důvodová zpráva k návrhu zákona č. 292/1993 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Poslanecká sněmovna, 1993, dostupná na www.psp.cz.
- Důvodová zpráva k návrhu zákona č. 177/2008 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Poslanecká sněmovna, 2007, dostupná na www.psp.cz.
- Důvodová zpráva k návrhu zákona č. 459/2011 Sb., kterým se mění zákon č. 141/1961 Sb., trestní řád. Poslanecká sněmovna, 2007, dostupná na www.psp.cz.
- Důvodová zpráva k návrhu zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Poslanecká sněmovna, 2012, dostupná na www.psp.cz.

Interception and recording of the telecommunication operation

Resumé

Tato diplomová práce se zabývá právní úpravou dvou trestně procesních institutů: odposlechu a záznamu telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu. Tyto instituty jsou obsaženy v zákoně č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (dále „trestní řád“). Cílem této práce je analýza této právní úpravy a jejího souladu s ochranou lidských práv, zejména práva na soukromí osob, přičemž na základě zjištěných nedostatků bych ráda navrhla možné změny této právní úpravy, které by takovým nepřiměřeným zásahům bránily.

Práce se sestává z úvodu, závěru a pěti kapitol. V úvodu se zabývám základními otázkami ohledně tohoto tématu, zejména vztahem mezi těmito instituty a lidskými právy a obecnými požadavky na jejich právní úpravu podle Listiny základních práv a svobod. Navíc je v této kapitole popsána struktura práce, její základní cíle a použitá literatura.

Kapitola první nastiňuje historii vývoje těchto institutů a skládá se ze dvou podkapitol. První podkapitola se zabývá historií odposlechu a záznamu telekomunikačního provozu, který je upraven v § 88 trestního řádu. Druhá podkapitola rozebírá vývoj příbuzného institutu zjišťování údajů o telekomunikačním provozu podle § 88a trestního řádu.

Kapitola druhá přezkoumává již relevantní českou právní úpravu a skládá se rovněž ze dvou podkapitol. První podkapitola se zabývá právní úpravou odposlechu a záznamu telekomunikačního provozu podle § 88 trestního řádu. Tato podkapitola je rozdělena do devíti částí. Část jedna se zaměřuje na podmínky pro nařízení tohoto institutu v trestním řízení. Část dvě se zaměřuje na příkaz k nařízení odposlechu a záznamu telekomunikačního provozu a jeho náležitosti. Část tři popisuje orgán odpovědný za provedení odposlechu, povinnosti takového orgánu během provádění odposlechu a způsob ukončení odposlechu. Část čtyři se pak zabývá odposlechem a záznamem telekomunikačního provozu, který je nařízen bez soudního příkazu, pouze se souhlasem uživatele odposlouchávané telekomunikační stanice. Část pět se vztahuje k použití záznamu odposlechu jako důkazu v trestním řízení. Následuje šestá část, která

popisuje uložení a zničení těch záznamů, které nebyly v trestním řízení použity jako důkaz. Sedmá část pak rozebírá informační povinnost orgánu činného v trestním řízení, jenž ukončil trestní řízení. Na takovou povinnost může navazovat zahájení přezkumného řízení ohledně příkazu k nařízení odposlechu a záznamu telekomunikačního provozu, a to na návrh uživatele odposlouchávané telekomunikační stanice. Toto přezkumné řízení je rozebráno v části osmé. Nakonec jsou v části deváté popsány základní aspekty použití odposlechu a záznamu telekomunikačního provozu v rámci tzv. přeshraničního odposlechu podle trestního řádu.

Druhá podkapitola se zabývá druhým institutem, kterým je zjišťování údajů o telekomunikačním provozu podle § 88a trestního řádu. Tato podkapitola má čtyři části, přičemž každá z nich pojednává o podobných aspektech jako u odposlechu a záznamu telekomunikačního provozu. První část popisuje podmínky pro vydání příkazu k zjišťování údajů o telekomunikačním provozu. Část dvě a tři pojednávají o informační povinnosti a na ní navazujícím přezkumném řízení. Poslední část se zabývá možností nařídit zjišťování údajů o telekomunikačním provozu i bez příkazu, pouze se souhlasem uživatele dotčené telekomunikační stanice.

Kapitola tři poskytuje přehled příslušných opatření podle německého práva. Tato kapitola se skládá ze tří podkapitol. Podkapitola jedna se zabývá opatřením, které je blízké českému odposlechu. Podkapitola dvě nastiňuje základních aspekty institutů odpovídajícím českému zjišťování údajů o telekomunikačním provozu. Podkapitola tři se zaměřuje na informační povinnost a přezkumné řízení.

Kapitola čtyři se zaměřuje na obecné problémy vyplývající ze vztahu odposlechu a záznamu telekomunikačního provozu a lidských práv. Tato kapitola rovněž obsahuje problematiku úniků odposlechlů.

Kapitola pět obsahuje návrhy na zlepšení české právní úpravy.

Shrnutí je pak obsaženo v závěru. Ten znova opakuje základní aspekty právní úpravy. Navíc hodnotí nutnost jejích změn vzhledem k návrhům uvedeným v předešlé kapitole.

Na základě těchto shrnutí bych u odposlechu a záznamu telekomunikačního provozu navrhla pouze menší legislativní úpravy. Obecně však považuji tuto úpravu za dostačující. U zjišťování údajů o telekomunikačním provozu bych ale navrhovala již podstatnější změny, protože tato úprava podle mého názoru neodpovídá požadavkům

stanoveným v judikatuře Ústavního soudu České republiky a nezaručuje dostatečnou ochranu lidských práv proti zásahům státních orgánů.

Abstract

This thesis describes legislation of two criminal procedure institutes: the interception and recording of telecommunication operation and the data identification of telecommunication traffic. These institutes are covered in the Code of Criminal Procedure. Purpose of this thesis is to analyze this legislation considering protection of human rights and suggest possible improvements of this legislation, which would prevent inappropriate interventions to human rights, particularly personal privacy.

The thesis is composed of introduction, conclusion and five chapters. Introduction explains basic issues of this topic. Primarily it concerns relation between these institutes and human rights and general requirements on such legislation given by The Charter of Fundamental Rights and Freedoms. Subsequently, it describes structure and basic aims of this thesis and secondary sources.

Chapter One explains history of development of these institutes. It consists of two subchapters. The first subchapter is concerned with the section 88 of the Code of Criminal Procedure, which governs the interception and recording of telecommunication operation. The second subchapter contains relating institute of the data identification of telecommunication traffic, which is included in the section 88a of the Code of Criminal Procedure.

Chapter Two examines relevant Czech legislation and consists of two subchapters. The first subchapter investigates the interception and recording of telecommunication operation and its legal aspects under the section 88. This subchapter is divided into nine parts. Part One focuses on basic conditions for use of this institute in criminal procedure. Part Two examines order to intercept and record telecommunication traffic and its requirements. Part Three describes responsible body, which carries out interception, duties of this body during the interception, and termination of the interception. Part Four investigates the interception and recording of telecommunication operation without order, just with consent of the user of tapped telecommunication station. Part Five relates to use of the record of telecommunication traffic as evidence in criminal procedure. Subsequently, Part Six describes storage and destruction of the

record of telecommunication traffic, which is not used as evidence. Part Seven describes information duty, which has body terminating criminal procedure. This duty can be followed by review procedure, which is opened on proposal of the user of tapped telecommunication station. This review procedure is illustrated in the Part Eight. Finally, Part Nine describes basic facts of use of the interception and recording of telecommunication operation abroad under the Code of Criminal procedure.

The second Subchapter looks at the second institute, the data identification of telecommunication traffic under the section 88a. This subchapter has four parts, each of them dealing with similar aspects as by the interception and recording of telecommunication operation. The first Part describes conditions for release of order to identify these data. Parts Two and Three deal with information duty and review procedure. Last, Part Four investigates possibility to order this institute without an order, just with consent of the user of telecommunication station.

Chapter Three provides an outline of relevant institutes under the German law. This chapter consists of three subchapters. Subchapter One deals with an institute, which is close to Czech interception. Subchapter Two illustrates three institutes, which are equal to the data identification of telecommunication traffic. Finally, subchapter Three is focused on information duty and review procedure.

Chapter Four concentrates in general on issues resulting from the relation between the interception and recording of telecommunication operation and human rights. This chapter is also concerned with the issue of leaks of the records of telecommunication traffic.

Chapter Five includes suggestions *de lege ferenda*, which should improve Czech legislation.

Finally, conclusion outlines more basic aspects of legislation. Moreover, it evaluates necessity of changes in this legislation, considering suggestions presented in the previous chapter.

On the ground of these conclusions, I would suggest just some small legislative changes by the interception and recording of telecommunication operation. But, in general, this legislation seems to be sufficient. On the other hand, when it comes to the data identification of telecommunication traffic, I would suggest more substantial improvements, since this legislation does not comply with judgments of the Czech

Constitutional Court and does not guarantee adequate protection of human rights against intervention of state power bodies.

Klíčová slova v češtině a v angličtině

Odposlech a záznam telekomunikačního provozu/ Interception and recording of the telecommunication operation

Zjišťování údajů o telekomunikačním provozu/ Data identification of the telecommunication traffic