Univerzita Karlova v Praze

Právnická fakulta

Štěpánka Kučerová

Odposlech a záznam telekomunikačního provozu

Diplomová práce

Vedoucí diplomové práce: JUDr. Bc. Jiří Říha, Ph. D.

Katedra trestního práva

Datum vypracování práce: 25. 6. 2017

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

V Praze dne

Děkuji vedoucímu své diplomové práce JUDr. Bc. Jiří Říhovi, Ph.D. za jeho vedení, čas věnovaný konzultacím a za cenné rady při zpracování.

Dále bych ráda poděkovala řediteli Útvaru zvláštních činností, plk. Ing. Vladimíru Šiborovi, a odborníkovi na IT zabezpečení Dr. Ing. Pavlu Kotykovi za čas věnovaný našim setkáním, zodpovězení mých otázek a zasvěcení do praxe v oblasti odposlechů.

V neposlední řadě děkuji své rodině za podporu po celý čas studia.

Obsah

Úvod

Odposlech a záznam telekomunikačního provozu (dále jen „odposlech“) představuje efektivní nástroj získávání důkazního materiálu a zároveň způsob odhalování a vyšetřování zejména organizované trestné činnosti. V praxi se proto jedná o hojně, a stále více využívaný institut, o čemž svědčí i statistiky nasazování odposlechů evidované Policií ČR. Uskutečnění odposlechu zároveň představuje zásah do základních práv občanů a je tedy důležité, aby právní úprava dostatečně stanovila mantinely pro jeho užití v trestním řízení a zároveň zajistila existenci následné kontroly garantující tak občanům možnost domáhat se svých základních práv v případě jejich porušení.

Ačkoli se práce věnuje zejména tématu odposlechu a záznamu telekomunikačního provozu, využívaného k zajištění *obsahu* komunikace, nelze opomenout ani úzce související institut zjišťování (provozních a lokalizačních) *údajů* o telekomunikačním provozu (dále jen „zjišťování údajů“). Instituty vykazují, spolu s operativně pátracím prostředkem sledování osob a věcí podle § 158d tr. řádu, celou řadu společných znaků. Cílem mé práce je provést komplexní rozbor zákonné i podzákonné právní úpravy odposlechu i zjišťování údajů, včetně jejího vývoje, který na území České republiky započal již v době bývalého režimu, kdy byly odposlechy hojně využívány zejména k dopadení a stíhání politických odpůrců. Vzhledem k již zmíněné podobnosti s operativně pátracím prostředkem sledování osob a věcí, věnuji samostatnou kapitolu komparaci s tímto institutem a stručnému rozboru povolovacího režimu sledování, který je nastaven mírněji než u odposlechu a zjišťování údajů, a to i přesto, že sledování může v některých případech představovat srovnatelný zásah do základních práv.

Institut odposlechu neodmyslitelně souvisí s technologickým rozvojem. Tento nástroj, který byl historicky využívaný především k odposlechu hlasové komunikace, se v dnešní době stále více využívá k zajišťování obsahu dat různé povahy přenášených v elektronických sítích. Odposlech tak s ohledem na specifika těchto dat představuje výzvu technickou i právní. Za účelem posouzení toho, jaké komunikace je možno odposlouchávat, příp. zajišťovat údaje o nich, se proto v další kapitole věnuji problematice legálního spojení *telekomunikačního provozu,* které se vzhledem ke zrušení zákona o telekomunikacích a jeho nahrazení zákonem o elektronických komunikacích, který s pojmem již nezachází, stalo překonaným ustanovením. Mým cílem je objasnit vztah pojmu telekomunikační provoz k zavedenému širšímu termínu elektronických komunikací a osvětlit způsob, jakým k samotnému odposlechu a zjišťování údajů na základě právních předpisů dochází. Jelikož se odposlech ve vztahu k moderním

elektronickým komunikacím setkává se specifiky různých forem přenášení zpráv, ráda bych osvětlila tato specifika odposlechu u velmi rozšířeného typu komunikace současné doby – sociálních sítí.

V poslední kapitole si kladu za cíl provést rozbor kontroly v oblasti odposlechu a zjišťování údajů. Náležitá a účinná kontrola v této oblasti je dle mého názoru stěžejním prvkem ochrany základních práv, do kterých je těmito instituty bezpochyby zasahováno. I přesto je kontrola ze strany Nejvyššího soudu prostřednictvím řízení o přezkumu příkazů k odposlechu a zjištění údajů relativně novým prvkem, zavedeným teprve novelami tr. řádu z let 2008 a 2012. Důležitým kontrolním orgánem v této oblasti je také *Stálá komise pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací*, zřízena Poslaneckou sněmovnou, jejíž působnosti a kontrolním mechanismům bych se v práci ráda věnovala. Jelikož v rámci soudního přezkumu odposlechu a zjištění údajů může dojít ze strany Nejvyššího soudu ke konstatování porušení zákona, zabývat se budu i potenciálním právem na náhradu škody, která nezákonným odposlechem vznikla.

Tato práce vychází z právní úpravy účinné ke dni 26. června 2017

1. Charakteristika odposlechu a zjišťování údajů podle trestního řádu

Trestní řád v souvislosti s telekomunikačním provozem obsahuje úpravu dvou zajišťovacích institutů: odposlechu a záznamu telekomunikačního provozu podle § 88 tr. řádu (dále jen „odposlech“) a od roku 2001 také institut zjišťování údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat podle § 88a tr. řádu (dále jen „zjišťování údajů o tel. provozu“).

Úprava obou ustanovení je systematicky zařazena mezi „předběžná opatření a zajištění osob a věcí“. V obou případech se jedná o zajišťovací instituty, které umožňují orgánům činným v trestním řízení za stanovených podmínek zasahovat do ústavně zaručeného tajemství zpráv podle čl. 13 Listiny základních práv a svobod (dále jen „Listina“) a případně i do práva na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů podle čl. 10 odst. 3 Listiny.[1] Česká republika vedle toho na sebe převzala závazek ochrany tajemství přepravovaných zpráv přijetím Úmluvy o ochraně lidských práv a základních svobod, která v čl. 8 zaručuje právo na respektování soukromého a rodinného života.

Základní rozdíl mezi úpravou § 88 a § 88a spočívá v povaze zajišťovaných dat, resp. informací. V případě odposlechu podle § 88 tr. řádu úprava směřuje ke zjištění samotného *obsahu* telekomunikačního provozu, který aktuálně probíhá nebo bude probíhat v budoucnosti. Postupem podle § 88a tr. řádu dochází ke zjištění *údajů* o telekomunikačním provozu, bez toho, aby byl současně zaznamenáván obsah komunikace. V souvislosti s odposlechem obsahu telekomunikačního provozu podle § 88 odst. 1 tr. řádu je potřeba zmínit, že citované ustanovení se netýká zásahu do svobody prostřednictvím tzv. prostorového odposlechu, kde se uplatní úprava obsažená zejména v § 158d tr. řádu.[2]

Údaji o telekomunikačním provozu se míní údaje provozní a lokalizační (např. čas a délka uskutečněného hovoru, informace o navštívených webových stránkách apod.) jak je v práci dále rozvedeno. Zjištění údajů lze realizovat jak do minulosti, tak do budoucnosti. To

[1] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C.H. Beck, 2013. s. 323; Fenyk, J., Hájek, R., Stříž, I., Polák, P. *Trestní zákoník a trestní řád. 2. díl – Trestní řád.* Praha: Linde, 2010. s. 303

[2] Šámal, P., Novotný, F., Růžička, M., Vondruška F., Novotná, J. *Přípravné řízení trestní.* Praha: C.H. Beck, 2003. s. 928

vyplývá z jazykového výkladu § 88a *„Je-li třeba zjistit údaje o telekomunikačním provozu…“*. Tento stav je přitom odlišný od předchozí právní úpravy, která obsahovala podmínku *„o uskutečněném telekomunikačním provozu“* a tedy nepředpokládala zjišťování údajů ve vztahu ke komunikaci, která teprve proběhne.[3]

Terminologie pak někdy zachází s pojmy aktivního a pasivního odposlechu, kdy aktivním odposlechem se má na mysli právě zjišťování obsahu komunikace, zatímco pasivním odposlechem dochází ke zjišťování údajů o telekomunikačním provozu.[4]

1.1. Odposlech jako zásah do základních práv

Před tím, než přistoupím k samotnému rozboru institutů odposlechu a zjišťování údajů, dovoluji si stručně rozebrat základní práva, se kterými tyto úkony nevyhnutelně přichází do konfliktu. Střet idejí liberálního státu a zaručenými svobodami jednotlivce na straně jedné a potlačování závažné kriminality na straně druhé je přitom hlavním sporem omezení některých základních práv z důvodu odposlechu v trestním řízení.

V případě aktivního i pasivního odposlechu dochází k tzv. „zákonem dovolenému zásahu“ do řady ústavně zaručených práv zakotvených v Listině základních práv a svobod (dále jen „Listina“). Jde zejména o čl. 7 zaručující nedotknutelnost osoby a jejího soukromí, dále čl. 10 odst. 2, 3 zaručující právo na ochranu před neoprávněným zasahováním do osobního a soukromého života.[5] K bezprostřednímu zásahu pak typicky dochází ve vztahu k čl. 13 Listiny zaručujícímu listovní tajemství i tajemství zpráv podávaných telefonem, telegrafem, nebo jiným podobným zařízením. Důležitost ústavní ochrany a garance tajemství písemnosti a různými způsoby dopravované zprávy je zřejmá, jelikož zpravidla vždy bývá úzce spojena s osobností jedince a s jeho intimní sférou v nejširším slova smyslu, které pro samotnou jejich povahu je třeba před zevním světem co nejúplněji chránit.

I přes to není možné, aby tato ochrana platila absolutně, ale “*jako výraz sebeobrany společnosti je prolomena způsobem (a v případech) stanoveným zákonem*.”[6] Podmínkou takového průlomu je, aby se tak stalo jen v takovém stupni a rozsahu, který je z hlediska sledovaného účelu nezbytný, a který šetří podstatu a smysl ústavně zaručeného práva. Přípustné

[3] Kolouch, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 443
[4] Fryšták, M. *Dokazování v přípravném řízení*, 2. vyd. Brno: Masarykova univerzita, 2015. s. 246
[5] Fryšták, M. *Dokazování v přípravném řízení*, 2. vyd. Brno: Masarykova univerzita, 2015. s. 247
[6] Ševčík, V. *Některé ústavní aspekty odposlechu a záznamu telekomunikačního provozu* (dvě části - část prvá), Bulletin advokacie č. 6-7/1996. s. 9

omezení – snížení ústavní ochrany nesmí být zneužívána k jiným účelům, než pro které byla stanovena.[7]

1.1.1. Vztah odposlechu a základního práva listovního tajemství

Základní právní úprava pro všechny způsoby předávání zpráv se nachází v čl. 13 Listiny, podle kterého „*Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.*“ Listovní tajemství upravené v čl. 13 Listiny je jedním ze základních práv a úzce souvisí s právem na ochranu soukromí (čl. 7 Listiny), stejně jako s právem na ochraně soukromého života (čl. 10 odst. 2 Listiny).

Objekt ochrany zahrnuje veškeré uvedené druhy tajemství. *Tajemství jiných písemností a záznamů* se tradičně vztahuje na všechny způsoby písemného projevu (deníky, zápisníky, adresáře, poznámky a jiné písemnosti držené v soukromí) a v souvislosti s rozvojem techniky i na nové formy záznamu informací, a to nejen v písemné, ale i v elektronické či jiné podobě (technické nosiče dat, paměť počítače, apod.).[8] Dikce čl. 13 Listiny uvádějící, že se mj. zaručuje také tajemství zpráv podávaných *„jiným podobným zařízením“* dává možnost rozšířit objekty ochrany tak, aby mohl být dostatečně reflektován rozvoj komunikačních technologií.

Ústavní soud ve svých nálezech sp. zn. IV. ÚS 78/01, sp. zn. II. ÚS 502/2000 a sp. zn. IV. ÚS 536/2000 konstatoval, 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.”*[9] V reakci na tyto nálezy byl zaveden institut zjišťování údajů o telekomunikačním provozu do trestního řádu.

Listina dále v čl. 13 umožňuje zásahy do tajemství výše zmíněných objektů, a to *„v případech a způsobem, které stanoví zákon“.* Vedle odposlechů podle tr. řádu umožňuje platná právní úprava zásahy do chráněných tajemství i dalšími zákony, jako zákonem č. 154/1994 Sb., o Bezpečnostní informační službě (§ 7 až § 12), zákonem č. 289/2005 Sb., o Vojenském zpravodajství (§ 9 až § 11) či zákonem č. 169/1999 Sb., o výkonu trestu odnětí svobody, který

[7] Čl. 4 odst. 3, 4 Listiny základních práv a svobod

[8] Pavlíček, V. a kol. *Ústavní právo a státověda,* 2. aktualizované vydání. Praha: Leges, 2015. s. 520

[9] Nález Ústavního soudu sp zn. IV. ÚS 78/01 ze dne 27.8.2001, Nález Ústavního soudu sp. zn. 502/2000 ze dne 22.1.2001, Nález Ústavního soudu sp. zn. 536/2000 ze dne 13.2.2001

umožňuje odposlech odsouzených ve výkonu trestu odnětí svobody. Ve všech těchto případech je odposlech operativně pátrací metodou provedenou podle jiného právního předpisu než trestního řádu a záznam o odposlechu v takových případech nelze použít jako důkaz v trestním řízení. Takový záznam má pouze operativní hodnotu a může případně sloužit pouze jako východisko pro další šetření.[10]

1.1.2. Článek 8 Úmluvy o ochraně lidských práv a základních svobod

Česká republika na sebe převzala závazek ochrany tajemství přepravovaných zpráv také přijetím *Úmluvy o ochraně lidských práv a základních svobod* (dále jen „*Úmluva*“).[11] Používání odposlechů a zjištění údajů o tel. provozu se dostává do střetu s čl. 8 Úmluvy, dle kterého *„má každý právo na respektování svého soukromého a rodinného života, obydlí a korespondence.“* Nejedná se přitom o práva absolutní povahy, jelikož Úmluva stanoví výjimky, za kterých státní orgán může do výkonu těchto práv zasahovat. Jedná se o případy, kdy je zásah v souladu se zákonem a nezbytný v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.[12] Mimo to čl. 8 Úmluvy není obsažen ve výčtu nederogovatelných práv uvedených v čl. 15 Úmluvy. Z toho vyplývá, že v případě naléhavé situace, jako je např. ohrožení státní existence či válečný stav, může stát od uvedených závazků odstoupit.

Ze znění čl. 8 Úmluvy je zřejmé, že jsou jím chráněny čtyři související zájmy: soukromý život, rodinný život, obydlí a korespondence. Ne vždy je přitom jednoduché rozlišit, do jakého z těchto zájmu bylo zasaženo, a to jak z důvodu jejich úzké souvislosti, tak z důvodu neexistence jednoznačných a vyčerpávajících definic obsahu pojmů.[13]

Záměrně zachází znění článku 8 Úmluvy s pojmem soukromého života, který je obsahově širší než pojem soukromí, užívaný například ve *Všeobecné deklaraci lidských práv.*[14] ESLP se v tomto směru vyjádřil, že soukromý život je *„široký pojem, který není poddajný vyčerpávající definici“*[15] Přesto ve své rozhodovací činnosti ESLP již mnohé zájmy výslovně

[10] Jelínek, J. a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*, 6. vyd. Praha: Leges, 2009. s. 363

[11] Sdělení o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících, č. 209/1992 Sb.

[12] Čl. 8 odst. 2 Úmluvy o ochraně lidských práv a základních svobod

[13] Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech: komentář*. 1. vyd. Praha: C.H. Beck, 2012. s. 862

[14] Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech: komentář*. 1. vyd. Praha: C.H. Beck, 2012. s. 863

[15] Např. *S a Marper proti Spojenému království*, rozsudek ESLP ze dne 4.12.2008, č. 30562/04, § 66

za součást práva na soukromý život označil. Ve vztahu k odposlechům a zjišťování údajů je nutné zmínit, že mezi zájmy prohlášenými ESLP za součást soukromého života jsou také otázky pořizování zvukových a obrazových záznamů hlasu, uchovávání osobních dat, komunikační provoz jako jsou telefonáty, e-maily, odposlouchávání soukromých rozhovorů, apod.[16] Odposlech a záznam telekomunikačního provozu vedle toho spadá i pod právo na ochranu korespondence podle čl. 8. Úmluvy, které chrání výměnu informací mezi lidmi a její důvěrnost, a to nejen výměnu prostřednictvím dopisů, jak by mohl pojem korespondence mylně napovídat, ale i prostřednictvím dalších prostředků komunikace, včetně telefonních hovorů a komunikace elektronické. Pojem nicméně nezahrnuje data o telekomunikačním provozu, která jsou v rámci čl. 8 Úmluvy sice chráněna, ale pouze v rámci ochrany soukromého života, nikoli v rámci ochrany korespondence.[17]

Dojde-li k zásahu do práva upraveného v čl. 8 Úmluvy, zkoumá Evropský soud pro lidská práva (dále jen „ESLP“) v zásadě splnění tří podmínek – podmínku legality, legitimity (tedy sledování jednoho z cílů taxativně vyjmenovaného v čl. 8 Úmluvy), a podmínku nezbytnosti v demokratické společnosti. V případě legality ESLP zkoumá, zda je zásah v souladu s vnitrostátním právním předpisem. Na dodržení této podmínky je přitom v oblasti používání tzv. „tajného sledování – „surveillance“), pod které ESLP řadí také používání odposlechů a zjišťování údajů o telekomunikačním provozu, kladen zvláštní důraz. V rámci přezkumu, zda v konkrétním případě existoval zákonný základ pro odposlech či zjištění údajů, se přezkoumává nejen samotná existence zákonného podkladu ve vnitrostátním právu, ale také jeho dostatečná kvalita. Aby byl zákonný podklad dostatečně kvalitní, musí být přístupný, předvídatelný, určitý a přesný.[18] Pokud zákon umožňuje v určité věci uvážení orgánů, je pro dodržení požadavku kvality zákona nutno jednoznačně uvést rozsah tohoto uvážení a způsob jeho výkonu, zvláště pak v situaci jako je tajné sledování, jehož uskutečnění ze samé podstaty nemůže být podrobeno kontrole dotčených osob.[19]

Zajímavým se může zdát, že současná judikatura ESLP použití důkazu získaného za porušení čl. 8 Úmluvy, nevylučuje. Nezákonný důkaz získaný porušením práva na soukromí není podle ESLP nutné vyloučit ze spisu, vnitrostátní soudy na něm dokonce mohou založit

[16] Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech: komentář*. 1. vyd. Praha: C.H. Beck, 2012. s. 863

[17] Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech: komentář*. 1. vyd. Praha: C.H. Beck, 2012., s. 877

[18] Ve svém rozhodnutím *Lüdi v. Švýcarsko*, č. 12433/86 (odposlech telefonu) ze dne 15. 6. 1992 ESLP konstatoval nezbytnost existence jasných a podrobných pravidel na základě kterých je možno k odposlechům přistoupit

[19] Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech: komentář*. 1. vyd. Praha: C.H. Beck, 2012., s. 921

svůj výrok o vině. Použití takového důkazu bude nicméně představovat jeden z faktorů, podle kterých ESLP posoudí spravedlivost celého trestního řízení, tedy soulad s čl. 6 Úmluvy upravujícího právo na spravedlivý proces.[20]

Jedna z prvních kauz, ve které se otázkou použitelnosti důkazu získaného porušením čl. 8 Úmluvy a dopadem takového důkazu na spravedlivost celého řízení, ESLP zabýval, byl případ *Schenk proti Švýcarsku*. Pan Schenk byl usvědčen na základě protizákonně získaného důkazu – nezákonného odposlechu, a jako stěžovatel se následně u ESLP domáhal konstatování nespravedlnosti celého trestního řízení a porušení čl. 6 Úmluvy. Tvrdil, že samotná skutečnost, kdy došlo k použití nezákonně získaného důkazu v trestním řízení, zakládá nespravedlnost celého tohoto řízení. ESLP nicméně dospěl k závěru, že čl. 6 Úmluvy porušen nebyl, neboť (i.) odposlech v daném případě nepředstavoval jediný důkaz zakládající odsouzení pana Schenka a navíc, a to především, (ii.) nebylo porušeno jeho právo na obhajobu, prostřednictvím kterého se mohl domáhat zpochybnění důkazu v rámci trestního řízení. Nad to ESLP konstatoval, že mu nepřísluší přezkoumávat přípustnost důkazů v trestním řízení, jelikož jeho pravomoc je omezena toliko na zásahy do práv a svobod zaručených Úmluvou, která nicméně přípustnost důkazů v trestním řízení nereguluje. Je nutné zmínit, že tento přístup se nesetkal s jednohlasným souhlasem, když čtyři disentující soudci namítli, že zákonnost důkazů má zcela zásadní význam pro posouzení spravedlivosti celého řízení. Klíčovou v dané věci je také skutečnost, že ESLP posuzoval použití nezákonných důkazů toliko na základě čl. 6 Úmluvy, tedy skrze soulad s právem na spravedlivý proces, nikoli z pohledu práva na soukromí zaručovaného v čl. 8 Úmluvy.[21]

ESLP následně i v dalších kauzách opakovaně konstatoval, že klíčovým faktorem pro posouzení spravedlivosti trestního řízení v případě použití nezákonného důkazu v rozporu s čl. 8 Úmluvy, je možnost obhajoby popřít pravost takového důkazu.[22] Naposledy v dubnu letošního roku ve věci *Matanovic proti Chorvatsku* shledal ESLP porušení čl. 6 Úmluvy z důvodu nedostatečného seznámení obhajoby se záznamy z utajeného sledování osob v průběhu vyšetřování. Soud v dané věci konstatoval, že je v zásadě na vnitrostátním právu, zda umožní obhajobě seznámit se přímo s pořízenými nahrávkami, nebo pouze s jejich přepisy. Obviněný se nicméně musí mít možnost se záznamy seznámit, a to i s takovými záznamy, které

[20] Nejedlý, J. *Zákonnost důkazů v trestním řízení ve světle Evropské úmluvy o ochraně lidských práv a základních svobod*, 1. vyd. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2013. s. 96

[21] *Schenk proti Švýcarsku,* č. 10862/84, rozsudek ESLP ze dne 12. července 1988

[22] Nejedlý, J. *Zákonnost důkazů v trestním řízení ve světle Evropské úmluvy o ochraně lidských práv a základních svobod*, 1. vyd. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2013. s. 96

byly v případu pořízené v obecnější rovině a týkaly se osob, které nebyly následně obviněny. V daném případě tyto záznamy nebyly součásti spisu a na žádost obviněného mu nebylo umožněno se s nimi seznámit. ESLP konstatoval, že přístup k těmto záznamům je relevantní, a státní orgány musí v dané situaci posoudit a poměřit právo na ochranu soukromí dotčených osob a právo na spravedlivý proces obviněného, který nepochybně musí mít možnost seznámit se s informacemi, které by mohly vést ke zproštění obvinění, nebo které by mohly ovlivnit výši uloženého trestu, případně by se týkaly přípustnosti či spolehlivosti důkazů. Chorvatský Nejvyšší soud záznamy nicméně obviněnému nezpřístupnil, když konstatoval, že je plně na státním zástupci, aby sám učinil výběr a rozhodl, které záznamy předloží soudu jako důkaz. Chorvatský Nejvyšší soud tak ani nepřistoupil k poměřování ochrany práva na soukromí dotčených osob s právem na spravedlivý proces obviněného. Takový postup byl dle ESLP zcela v rozporu s judikaturou, podle které *„v právních řádech, v nichž vyšetřující orgány jsou povinny brát v potaz skutečnosti svědčící jak v neprospěch, tak i ve prospěch obviněného, nemůže být v souladu s požadavky čl. 6 odst. Úmluvy systém, kdy vyšetřovací orgány samy vyhodnocují, co je a co není pro daný případ relevantní, aniž by zde byli jakékoli záruky pro práva obhajoby.“*[23]

1.2. Charakteristika institutu odposlechu podle § 88 tr. řádu

1.2.1. Předpoklady vydání příkazu k odposlechu

Vzhledem k zásahu do tajemství zpráv, ke kterému při odposlechu dochází, zákonodárce jasně vymezuje požadavky, které musí být k nařízení odposlechu splněny. Použití odposlechu přichází v úvahu pouze tehdy, 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 některý z taxativně vyjmenovaných trestných činů: 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, zjednání 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

[23] Kmec, J. *Evropský soud pro lidská práva – duben 2017,* Soudní rozhledy, č. 6/2017 s. 211; *Matanovic proti Chorvatsku*, č.2742/12, rozsudek ESLP ze dne 4. dubna 2017

c) jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva

Společnou podmínkou pro veškerou uvedenou trestnou činnost je, že se musí jednat o trestné činy spáchané úmyslně.[24] Z okruhu trestných činů, u nichž je odposlech umožněn, je přitom patrné, že tento je stanoven tak, aby institutu, který zasahuje do základních práv občanů, nebylo zneužíváno u méně závažné trestné činnosti.

Vedle okruhu trestných činů, u nichž odposlech může být nařízen, zákonodárce v § 88 odst. 1 tr. řádu stanoví další obecné požadavky, které musí být splněny. Jedná se zejména o požadavek *subsidiarity*, podle kterého je možné k odposlechu přistoupit pouze tehdy, nelze-li sledovaného účelu dosáhnout jinak anebo bylo-li by jinak jeho dosažení podstatně ztížené. Požadavek subsidiarity je formulován v souladu se zásadou přiměřenosti a zdrženlivosti vymezenou v § 2 odst. 4 tr. řádu.[25] Nejprve je tedy k získávání skutečností potřeba hledat způsoby, které nezasahují do základních práv a teprve v případě, kdy tato cesta s ohledem na smysl trestního řízení není možná, lze přistoupit k odposlechu.[26] Je nutné zejména v každém konkrétním případě zvážit, zda získání skutečností není možné docílit jinými důkazními prostředky uvedenými v trestním řádu (např. výslechy osob). Takto Nejvyšší soud ve svém rozhodnutí sp. zn. 4 Pzo 14/2016, v rámci přezkumného řízení nařízeného odposlechu judikoval, že „*není přípustné, aby teprve na základě a prostřednictvím povoleného odposlechu byly získávány informace o tom, zda se odposlouchávaná osoba dopustila protiprávního jednání. Takový poznatek musí vydání příkazu k odposlechu předcházet, přičemž je třeba, aby byl validní, což znamená, že musí pocházet ze spolehlivého zdroje a musí být dostatečně přesvědčivý. V žádném případě se nemůže jednat o pouhou spekulativní konstrukci, byť vedenou tzv. užitečným záměrem*.“[27] V daném případě NS nepřisvědčil správnosti postupu Okresního soudu, který odposlech nařídil. Shledal, že podezření ze spáchání trestné činnosti bylo možno prověřit jiným způsobem než nařízením odposlechu, konkrétně výslechem osob, jež mohly záležitost objasnit. K výslechům, které měly být realizovány na počátku řízení, bylo nicméně přistoupeno až v situaci, kdy odposlechy v daném směru nic neprokázaly. Nejvyšší soud se vyjádřil také k zákonnému požadavku subsidiarity, podle kterého sledovaného účelu nelze dosáhnout jinak, nebo podstatně ztíženě. Podmínku „podstatného ztížení“ nelze vykládat paušálně, tedy tak, že o ztížené dosáhnutí účelu by se mohlo jednat takřka v každém případě.

[24] Srov. § 15TrZ

[25] Usnesení Nejvyššího soudu sp. zn. 4 Pzo 10/2015 ze dne 20. ledna 2016; Fenyk, J., Hájek, R., Stříž, I., Polák, P. *Trestní zákoník a trestní řád 2. díl – Trestní řád.* Praha: Linde, 2010. s. 304

[26] Fryšták, M. *Dokazování v přípravném řízení*, 2. vyd. Brno: Masarykova univerzita, 2015. s. 247-248

[27] Usnesení Nejvyššího soudu sp. zn. 4 Pzo 14/2016 ze dne 15.11.2016

To vyplývá mimo jiné i ze skutečnosti, že příkaz k odposlechu lze vydat vzhledem k vyžadované povaze a trestnosti protiprávních jednání téměř výhradně v závažných a tím i často složitých případech.[28] Zcela shodně je požadavek subsidiarity vyjádřen také u zjišťování údajů o telekomunikačním provozu (§ 88a odst. 1 věta první tr. řádu) a obdobně u operativně pátracích prostředků v § 158 odst. 2 věta druhá tr. řádu.

Posledním požadavkem, jehož splnění je při nařízení odposlechu nutné dodržet, je existence důvodného předpokladu, že odposlechem budou získány významné skutečnosti pro trestní řízení. Těmi jsou především skutečnosti naznačené v § 89 odst. 1 písm. a) až c) tr. řádu za podmínky, že jsou pro trestní řízení významné.[29] Z předmětného ustanovení je možno dovodit, že se jedná zejména o dokázání skutečnosti, zda se stal skutek, v němž je spatřován trestný čin, zda jej spáchal obviněný, a dokázání dalších okolností majících vliv na posouzení povahy a závažnosti trestného činu.

Nedostatkem současné právní úpravy je dle prof. Jelínka skutečnost, že nevyjmenovává taxativně všechny trestné činy, o nichž je možné odposlech nařídit.[30] Stanovit takový okruh může pro adresáta právní normy činit problém zejména v souvislosti s odkazem na řízení o trestném činu, k jehož trestnímu stíhání zavazuje Českou republiku vyhlášená mezinárodní smlouva. Definici pojmu mezinárodní smlouvy nalézáme ve Vídeňské úmluvě o smluvním právu (č.15/1988 Sb.), která ve svém čl. 2 stanoví, že *„smlouvou je každá mezinárodní dohoda uzavřená mezi státy písemnou formou, řídící se mezinárodním právem, sepsaná v jediné nebo více věcně souvisejících listinách, ať je její název jakýkoli"* a tedy se definování tohoto pojmu nejeví být problematické. Stanovit ovšem okruh všech mezinárodních smluv, a tedy následně všech trestných činů, na něž se ustanovení § 88 odst. 1 tr. řádu vztahuje, dle mého názoru pro adresáty právní normy být problematické může. Při stanovení okruhu těchto trestných činů je nutné vycházet ze skutečnosti, že se nejedná jen o trestnou činnost, k jejímuž stíhání zavazuje přímo či bezprostředně vyhlášená mezinárodní smlouva[31], nýbrž i veškeré trestné činy, které mají v mezinárodní smlouvě podklad nebo na ni navazují, a to i tehdy, kdy se vnitrostátní postih provádí zásadně podle skutkových podstat trestných činů českého právního řádu. Není přitom rozhodující, zda je závazek stíhat nebo postihovat některá jednání ve vnitrostátní úpravě promítnut skrze speciální skutkovou podstatu [32] nebo skrze obecnou skutkovou podstatu, jako

[28] Usnesení Nejvyššího soudu sp. zn. 4 Pzo 14/2016 ze dne 15.11.2016

[29] Šámal, P. a kol.: *Trestní řád: komentář*. 7. dopl. a přeprac. vyd. Praha: C.H. Beck, 2013. s. 1192-1221

[30] Jelínek, J. a kol.: *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 6. vydání. Praha: Leges, 2016, s.737

[31] Např. trestání zločinu genocidia podle Úmluvy o zabránění a trestání zločinu genocidia – č. 32/1955 Sb.

[32] Např. trestný čin obchodování s lidmi podle § 168TrZ v návaznosti na Úmluvu a závěrečný protokol o potlačování obchodu s lidmi a vykořisťování prostitutce druhých osob ze dne 21. března 1950, Mezinárodní

je tomu např. u trestného činu obecného ohrožení nebo trestného činu ublížení na zdraví, k jehož stíhání v konkrétní podobě zavazuje mezinárodní smlouva.[33] Z toho důvodu je vždy potřeba zkoumat, zda z hlediska mezinárodních smluv nejde i u obecných trestných činů, jako je např. výše zmíněný trestný čin obecného ohrožení či ublížení na zdraví, o trestný čin, k jehož stíhání mezinárodní smlouva zavazuje. Při stanovení okruhu trestných činů, na něž se § 88 tr. řádu aplikuje, je tedy nutné vzít v úvahu i vnitrostátní normy, jež jsou plněním mezinárodního závazku. Pro potřeby státního zastupitelství vede přehled mezinárodních smluv včetně specifikace trestných činů, k jejichž stíhání zavazují, Mezinárodní odbor Nejvyššího státního zastupitelství.[34]

K vymezení okruhu trestných činů, u kterých je možné přistoupit k zásahu do práv osob tzv. tajným sledováním („*surveillance*“) zahrnujícím podle evropské judikatury také odposlechy, se ESLP vyjádřil ve věci *Kennedy proti Spojenému království*. V daném rozsudku konstatoval, že není třeba, aby trestné činy byly taxativně vyjmenovány, nýbrž postačuje pouze jejich druhové vymezení. Takový způsob, který jak bylo výše rozebráno, zvolila i česká právní úprava, je tedy v souladu s judikaturou ESLP.[35]

1.2.2. Nařízení odposlechu – příkazem / bez příkazu

Odposlech a záznam telekomunikačního provozu může za splnění všech náležitostí stanovených v § 88 tr. řádu nařídit příkazem předseda senátu v řízení před soudem, nebo soudce na návrh státního zástupce v řízení přípravném. V přípravném řízení tedy může odposlech nařídit v souladu s § 26 tr. řádu stanovujícím příslušnost soudu k úkonům v přípravném řízení jedině soudce okresního soudu, obvodního soudu v Praze, případně Městského soudu v Brně, v jehož obvodu je činný státní zástupce, který podal příslušný návrh. Tento soud je nadále příslušný k provádění všech úkonů pro celé přípravné řízení, nedojde-li k postoupení věci. V řízení před soudem se příslušnost soudu k vydání příkazu k odposlechu řídí obecnými ustanovením tr. řádu o věcné příslušnosti.[36] Příkaz má povahu rozhodnutí svého druhu a nejedná se tedy o usnesení ani opatření.[37] Z toho důvodu jej není možno napadnout opravným

úmluvu o potírání obchodu se ženami a dětmi (123/1924 Sb.) a Mezinárodní úmluvu o potírání obchodu se zletilými ženami (32/1936 Sb.)

[33] Srov. např. čl. 1 písm. c), d), e), f) Evropské úmluvy o potlačování terorismu – č. 552/1992 Sb.

[34] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR a.s., 2017, s. 802

[35] *Kennedy proti Spojenému království*, rozsudek ze dne 18.5.2010, § 34 a § 159

[36] Šámal, P., Púry, F., Urbánek, J. *Vzory podání a rozhodnutí v trestních věcech*, 3., přeprac. vyd. Praha: Linde, 2011.

[37] Usnesení Nejvyššího soudu sp. zn. Tzn 24/95 ze dne 27. 7. 1995; Fenyk, J., Hájek, R., Stříž, I., Polák, P. *Trestní zákoník a trestní řád. 2. díl – Trestní řád.* Praha: Linde, 2010. s. 304

prostředkem a jedinou možnou obranu představuje návrh na přezkum zákonnosti příkazu k odposlechu a záznamu v zvláštním řízení soudním, jehož úpravu nalézáme v ustanovení § 314l až § 314n tr. řádu a kterému je věnována samostatná kapitola této práce. Odposlechy bývají často nařizovány již před samotným zahájením trestního stíhání ve fázi prověřovací. V takovém případě se jedná o úkony, na které je pohlíženo jako na neodkladné či neopakovatelné podle § 160 odst. 4 tr. řádu.[38]

V příkazu, který musí být vydán písemně a s odůvodněním, je nutné uvést výslovně trestný čin, případně odkaz na mezinárodní smlouvu, o kterou se příkaz opírá (v případě odkazu na mezinárodní smlouvu je nutno uvést číslo Sbírky mezinárodních smluv a pokud možno i příslušnou část mezinárodní smlouvy zakotvující požadavek ke stíhání daného trestného činu).[39] V § 88 odst. 2, tr. řád stanoví další náležitosti, které příkaz musí obsahovat. Těmi jsou zejména uživatelská adresa či zařízení a osoba uživatele, pokud je jeho totožnost známa. Osobou uživatele se podle zákona č. 127/2005 Sb., o elektronických komunikacích (dále jen "ZoEK") rozumí každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací.

Podstatnou náležitostí je i stanovení doby odposlechu, která nesmí překročit 4 měsíce. Soud může stanovit i lhůtu kratší. Je možno dále tuto dobu prodloužit vydáním nového příkazu, a to i opakovaně, maximálně však o další čtyři měsíce. Vždy je přitom zapotřebí postupovat v souladu se zásadou zdrženlivosti (§ 2 odst. 4 tr. řádu) a v příkazu k prodloužení doby trvání uvést veškeré skutečnosti dle § 88 odst. 2.[40] Prodloužení doby se děje na základě vyhodnocení dosavadního průběhu odposlechu soudcem soudu vyššího stupně v řízení před soudem a v přípravném řízení na návrh státního zástupce soudcem krajského soudu. I toto rozhodnutí má povahu rozhodnutí svého druhu.[41] Návrh na prodloužení by měl být podán s dostatečným časovým předstihem tak, aby rozhodující soud mohl o případném prodloužení rozhodnout během původní čtyřměsíční lhůty. Není přípustné, aby státní zástupce navrhl soudci v přípravném řízení nařízení odposlechu až po uplynutí čtyřměsíční lhůty s odůvodněním, že v meziobdobí byly zjištěny nové skutečnosti odůvodňující opětovné nasazení odposlechu.

[38] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 186

[39] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR a.s., 2017, s. 803

[40] Jelínek, J. a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*. 6. vyd.. Praha: Leges, 2009. s. 738; Fenyk, J., Hájek, R., Stříž, I., Polák, P. *Trestní zákoník a trestní řád 2. díl – Trestní řád.* Praha: Linde, 2010. s. 304

[41] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 1192-1221; Toman, P. *Náležitosti příkazu k odposlechu a záznamu telekomunikačního provozu,* Bulletin advokacie 5/2017, s. 23

Takový postup by byl obcházením zákonné náležitosti, aby o prodloužení odposlechu rozhodoval soud vyššího stupně.[42]

Náležitostmi soudního příkazu k odposlechu a záznamu telekomunikačního provozu se blíže zabýval Ústavní soud ve svém nálezu sp. zn. II. ÚS 615/06. V něm mimo jiné uvedl, že příkaz musí být individualizován ve vztahu ke konkrétní osobě, proti níž se trestní stíhání vede, nebo vůči níž existuje důvodné podezření, že se trestných činů dopustila. V případě vydávání příkazu na základě důvodného podezření je navíc potřeba dostatečně vyložit, o jaké indicie se podezření opírá. *„Pouhé trestní oznámení samo o sobě, není-li doloženo alespoň indiciemi, z nichž lze důvodné podezření dovozovat, nepostačuje k nařízení odposlechů, neboť nepostačuje ani k zahájení řízení k objasnění a prověřování skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin podle § 158 tr. řádu.“*[43] Z výše uvedeného lze tedy dovodit, že by příkaz k odposlechu měl obsahovat následující:

a) vlastní příkaz k zahájení odposlechu
b) identifikátor zařízení a osoby, je-li známa,
c) označení trestného činu, pro který je vedeno trestní řízení (včetně případného odkazu na mezinárodní smlouvu),
d) stanovení doby, po kterou má být odposlech prováděn,
e) odůvodnění příkazu včetně popisu skutkového stavu,
f) účel odposlechu, tedy uvedení skutečností významných pro trestní řízení, které mají být prostřednictvím odposlechu získány,
g) vysvětlení, proč neexistuje jiný způsob, jak tyto informace získat, případně proč by bylo jejich získání jinou cestou podstatně ztíženo.

Příkaz se následně bezodkladně doručí policejnímu orgánu, v přípravném řízení pak jeho opis i státnímu zástupci. Děje se tak proto, aby státní zástupce mohl začít vykonávat potřebný dozor.

Bez příkazu k odposlechu jej může orgán činný v trestním řízení (dále jen „OČTŘ“) nařídit, případně sám provést, pouze v případě, kdy je vedeno trestní řízení pro taxativně vyjmenované trestné činy[44] a zároveň s tím uživatel odposlouchávané stanice souhlasí. Postačující je přitom souhlas vlastníka telefonu jako uživatele telekomunikačního zařízení, není

[42] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR a.s., 2017, s. 805
[43] Nález Ústavního soudu sp. zn. II. ÚS 615/2006 ze dne 23. května 2007
[44] Dle § 88 odst. 5 tr. řádu se jedná o trestné činy: obchodování s lidmi (§ 168 TrZ.), svěření dítěte do moci jiného (§ 169 TrZ.), omezování osobní svobody (§ 171 TrZ.), vydírání (§ 175 TrZ.), únosu dítěte a osoby stižené duševní poruchou (§ 200 TrZ.), násilí proti skupině obyvatelů a proti jednotlivci (§ 352 TrZ.), nebezpečného vyhrožování (§ 353 TrZ.), nebezpečného pronásledování (§ 354 TrZ.)

nutné obstarávat souhlas dalších účastníků telefonického hovoru.[45] Z povahy vyjmenovaných trestných činů vyplývá, že odposlech je v daném případě prováděn ve prospěch a v zájmu osoby, která k němu dala souhlas.[46] V daném případě může odposlech nařídit přímo policejní orgán, přičemž příkaz policejního orgánu by měl obsahovat obdobné náležitosti jako příkaz soudu.[47] V případě, kdy by již jednou udělený souhlas byl vzat zpět, je nutné odposlech okamžitě ukončit. Záznam učiněný po odvolání souhlasu nelze v trestním řízení použít.[48]

1.2.3. Provádění odposlechu a nakládání se zaznamenaným telekomunikačním provozem

Odposlech pro potřeby všech orgánů činných v trestním řízení provádí podle § 88 odst. 1 tr. řádu, stejně jako podle § 19 zákona o policii, Policie ČR. Konkrétně jej provádí specializovaný Útvar zvláštních činností (dále jen „ÚZČ"), do jehož působnosti vedle odposlechů spadá také sledování osob a věcí a další specializované úkony.[49] Konkrétní postupy stejně jako nástroje, které ÚZČ k provádění odposlechů používá, jsou utajované. Dochází k nim za součinnosti subjektů provozujících veřejné komunikační sítě nebo veřejně dostupné služby elektronických komunikací (dále jen „provozovatelé elektronických komunikací"), kteří mají mimo jiné povinnost na základě § 97 ZoEK zřídit a zabezpečit v určitých bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam. Zřízení a zabezpečení tohoto rozhraní se děje na náklady žadatele, kterým může být vedle Policie České republiky pro účely § 88 tr. řádu také Bezpečnostní informační služba a Vojenské zpravodajství pro účely stanovené zvláštními právními předpisy.[50]

V praxi k odposlechům dochází nejčastěji v přípravném řízení, v jehož rámci se zpravidla realizuje ve třech fázích.[51]

První fází je podání podnětu policejního orgánu státnímu zástupci. Dle závazného pokynu policejního prezidenta č. 103/2013 podává policejní orgán tento podnět až po konzultaci o technických možnostech provedení s Útvarem zvláštních činností, který provedení odposlechů

[45] Např. rozhodnutí Vrchního soudu v Praze sp. zn. 7 To 117/2001 ze dne 5. 2. 2002
[46] Fryšták, M. *Dokazování v přípravném řízení*, 2. vyd. Brno: Masarykova univerzita, 2015, s. 248
[47] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 188
[48] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR a.s., 2017, s. 806; Toman, P. *Náležitosti příkazu k odposlechu a záznamu telekomunikačního provozu,* Bulletin advokacie 5/2017, s. 23
[49] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 188
[50] Jedná se o § 6 až § 8 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů a § 9 a 10 zákona č. 289/2005 Sb., o Vojenském zpravodajství.
[51] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 1192-1221; Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR, a.s., 2017, s. 802

zajišťuje.[52] Státní zástupce následně postupuje v souladu s pokynem obecné povahy nejvyšší státní zástupkyně č. 8/2009 a nejdříve zkoumá, zda zásah do základních práv a svobod je v konkrétní věci odůvodněný, zákonný a přiměřený. V případě, kdy státní zástupce policejnímu orgánu nevyhoví, sdělí mu důvod takového postupu a učiní záznam do dozorového spisu.[53] Státní zástupce má nadále povinnost ověřit splnění všech zákonných podmínek pro odposlech (trestní řízení vedeno pro trestný čin, u kterého lze tento úkon nařídit, atd.) a zajistit aby návrh na vydání příkazu obsahoval veškeré náležitosti. Soudce po přezkoumání návrhu státního zástupce rozhodne, zda příkaz vydá či ne. Pokud je příkaz vydán, po doručení opisu příkazu k odposlechu vydaného soudcem státní zástupce předá neprodleně stejnopis policejnímu orgánu, který bude odposlech zajišťovat. V první fázi se také začíná samotná realizace odposlechu, přičemž v této fázi se s odposlechem nakládá jako s utajovanou informací, stupně utajení „vyhrazené“ nebo „důvěrné“.[54] V případě, kdy je odposlech prováděn ve fázích prověřování, je nutné, aby se jednalo o úkon neodkladný nebo neopakovatelný ve smyslu § 160 odst. 4 tr. řádu.[55]

Druhou fází je provádění samotného úkonu, tedy realizace příkazu Útvarem zvláštních činností. Po celou dobu provádění odposlechu policejní orgán vyhodnocuje, zda stále trvá důvod realizace odposlechu. Jestliže vyhodnotí, že důvody k vydání příkazu k odposlechu již pominuly, musí jej v souladu s § 88 odst. 3 tr. řádu okamžitě ukončit, a to i před skončením doby, na kterou byl odposlech nařízen. Dobu odposlechu lze rovněž prodlužovat, a to i opakovaně, nejdéle však vždy na dobu maximálně 4 měsíců. Zákon umožňuje nařídit, případně také prodloužit probíhající odposlech i v řízení před soudem. Dle Jelínka se pak ale nabízí otázka praktického využití poznatků získaných např. během probíhajícího hlavního líčení.[56] V této fázi provádění odposlechu již také není zcela vyloučeno, aby obviněnému byla předložena část záznamu k vyjádření.

Třetí fází se rozumí konečné vyhodnocení výsledku odposlechu a rozhodování o jeho další využitelnosti v trestním řízení. V této fázi, zejména bylo-li již vyšetřování uznáno za skončené a bylo umožněno prostudování spisu dle § 166 tr. řádu, má obviněný a jeho obhájce právo na seznámení se s obsahem záznamu odposlechu, který má sloužit jakožto důkaz v řízení. Toto právo má i poškozený.[57] Pokud policejní orgán při vyhodnocování dospěje k závěru, že

[52] Fryšták, M. *Dokazování v přípravném řízení*, 2. vyd. Brno: Masarykova univerzita, 2015, s. 248
[53] Pokyn obecné povahy nejvyšší státní zástupkyně ze dne 21. září 2009, o trestním řízení, čl. 27
[54] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 1192-1221
[55] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR, a.s., 2017, s. 802
[56] Jelínek, J. a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*. 6. vyd. Praha: Leges, 2009. s. 738
[57] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 1192-1221

odposlechem nebyly zjištěny skutečnosti významné pro trestní řízení, pak všechny získané záznamy se souhlasem soudu a v přípravném řízení se souhlasem státního zástupce po 3 letech od pravomocného skončení ve věci vyšetřovatel i ÚZČ zničí. O této skutečnosti je pořízen protokol, který je založen do spisu. Pokud záznamy potřebné informace obsahují, převezme tyto policejní orgán od ÚZČ a zbývající záznamy, neobsahující informace důležité pro trestní řízení, uloží a označí tak, aby nemohlo dojít k jejich zneužití.[58] Uschováním je povinen policejní orgán, který v protokolu založeném do spisu poznamená, kde jsou záznamy neobsahující informace důležité pro trestní řízení uloženy. K bezprostřednímu zničení záznamů nemůže být přistoupeno, jelikož nelze předjímat obsah obhajoby uplatněné obžalovaným ve stadiu projednání trestní věci před soudem, včetně využití mimořádných opravných prostředků.[59]

Nejvyšší soud ve stanovisku trestního kolegia sp. zn. Tpjn 304/2012 konstatoval, že podle § 88 odst. 1, 2. tr. řádu „*...lze 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 tr. řádu.“* Takový postup je dle NS ovšem možný pouze v případě, kdy pobyt odsouzeného a jeho dodání do výkonu trestu odnětí svobody není možno dosáhnout jinak nebo jen podstatně ztíženě. Zákonnost příkazu k odposlechu ve vykonávacím řízení je pak možné stejně jako u odposlechů prováděných v řízení přípravném a řízení před soudem, přezkoumat postupem za analogického využití § 88 odst. 8, 9 a § 314 písm. l až § 314 písm. n tr. řádu.[60]

1.2.4. Nepřípustnost odposlechu mezi obhájcem a obviněným

K základním lidským právům garantovaným ústavním pořádkem České republiky patří i právo na obhajobu. V čl. 40 Listiny upravujícím základní pravidla trestního stíhání, je stanoveno právo obviněného hájit se sám nebo prostřednictvím svého obhájce. Z pohledu obviněného je právo na obhajobu jedním z prostředků zajištění práva na spravedlivý proces, jež bezpochyby patří k základním pilířům právního demokratického státu. Ústavní soud ve své judikatuře hovoří o právu na obhajobu následovně: „*Ústavně zaručené právo na obhajobu (čl. 37 odst. 2, čl. 40 odst. 3 Listiny základních práv a svobod) spolu s presumpcí neviny (čl. 40*

[58] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 190

[59] Důvodová zpráva k zákonu č. 177/2008 Sb.

[60] Stanovisko trestního kolegia Nejvyššího soudu ze dne 5. 6. 2013, sp. zn. Tpjn 304/2012

odst. 2 Listiny) jsou základními podmínkami spravedlivého procesu (čl. 36 odst. 1 Listiny), v němž vina obviněného (obžalovaného) má být zjištěna.“[61]

Trestní řád ve spojitosti s právem na obhajobu garantuje důvěrnost informací mezi klienty a jejich obhájci mimo jiné tím, že podle § 88 odst. 1věta třetí až pátá, je provádění odposlechu mezi obhájcem a obviněným nepřípustné. Pokud je policejním orgánem dodatečně zjištěno, že došlo k odposlechu takové komunikace, je povinen výsledný záznam komunikace bezodkladně zničit. Přitom nesmí jakkoli použít informace, které se v této souvislosti dozvěděl (např. jako podnět ke kárnému řízení vůči obhájci). Protokol o zničení záznamu založí policejní orgán za účelem zajištění transparentnosti vzniklé situace do spisu.[62]

Důvodem této nepřípustnosti je zachování zvláštního vztahu důvěry mezi obviněným a obhájcem, který umožňuje klientovi (obviněnému) obracet se na advokáta bez rizika, že jeho trestnou činnost oznámí. Obsah sdělení mezi obhájcem a obviněným musí zůstat utajen pouze mezi nimi, čemuž odpovídá i povinnost mlčenlivosti advokáta obsažená v § 21 zákona č. 85/1996 Sb. o advokacii. Toto ustanovení ukládá advokátům povinnost mlčenlivosti o všech skutečnostech, o nichž se dozví při poskytování právních služeb; porušení této povinnosti se velmi přísně trestá v kárném řízení. Předmětem utajení přitom zůstávají nejen skutková sdělení, nýbrž i celá taktika obhajoby. Pokud by tyto informace vešly ve známost orgánům činným v trestním řízení, jednalo by se o zásadní zásah do základního práva obviněného na jeho obhajobu.[63]

Stát tento zvláštní vztah důvěry mezi advokátem a klientem respektuje a poskytuje mu ochranu. Jejím výrazem je mimo jiné právě zákaz odposlechu mezi obhájcem a obviněným. Ochranu však zákonodárce neposkytuje v případě komunikace mezi podezřelým a jeho obhájcem. Tím podle některých odborníků v oblasti trestního práva pozbývá celé ustanovení smyslu, neboť většina odposlechů bývá prováděna již ve fázi před zahájením trestního stíhání.[64]

I přesto, že se ustanovení o nepřípustnosti odposlechu mezi obhájcem a obviněným může jevit jako jednoznačné a postup podle něj bezproblémový, praxe podle Jelínka dokazuje opak. Policejní orgán k pořizování záznamu totiž často užívá speciální technické automatické zařízení, které automaticky zapne odposlech na odposlouchávané stanici obviněného na počátku rozhovoru a vypne jej po skončení telefonátu. Automatické zařízení není schopno

[61] Nález Ústavního soudu sp. zn.: III. ÚS 83/1996 ze dne 25. 9. 1996.
[62] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR, a.s., 2017, s. 803
[63] Jelínek, J., Uhlířová, M. *Obhájce v trestním řízení*. Praha: Leges, 2011. s. 258; VANTUCH, P. *Obhajoba obviněného*. 3., dopl. a přeprac. vyd. Praha: C. H. Beck, 2010. Beckovy příručky pro právní praxi. s. 47-60
[64] Např. Ježek, J. *K odposlechu advokáta*, Bulletin advokacie č. 9/2008, s. 32

zjistit, zda jedním z účastníků rozhovoru je obhájce a rozhovor je tedy nahrán bez ohledu na tuto skutečnost. Až z následného přehrání záznamu policejní orgán zjišťuje jeho obsah a případně i to, zda se jedná o komunikaci obviněného s obhájcem. Takový postup nicméně odporuje ustanovení tr. řádu, které vyžaduje *bezodkladné* zničení záznamu v případě, kdy během odposlechu policejní orgán zjistí, že se jedná o komunikaci mezi obhájcem a obviněným, nikoli jeho zničení až na základě následného vyhodnocování. V případech, kdy policejní orgán záznam zničí poté, co si jej přehraje, již disponuje informacemi o průběhu rozhovoru mezi obviněným a obhájcem, čemuž se zákonodárce snažil s ohledem na znění § 88 odst. 1 věta třetí tr. řádu zabránit. Stejný je postup v případech odposlechu a záznamu jiných forem komunikace, jako je např. obsah e-mailu, faxu apod., pokud záznamy zabezpečuje technické zařízení. I v těchto případech má kompletní obsah mezi obhájcem a obviněným k dispozici policejní orgán, který tak zná jejich obsah. V praxi tak podle Jelínka policejní orgán v případech, kdy používá technické automatické zařízení, nedostojí liteře zákona.[65]

Odposlech mezi obviněným a jeho obhájcem se stal aktuálně diskutovaným tématem v souvislosti s kauzou česko-íránského podnikatele Shahrama Abdullaha Zadeha, v jejímž rámci orgány činné v trestním řízení činily záznamy o komunikaci mezi obviněným Zadehem a jeho obhájci a tyto následně zařadily do trestního spisu. Ve věci dokonce podala svůj první podnět k postupu podle § 158 odst. 1 tr. řádu (dále jen „trestní oznámení“) Unie obhájců ČR, z. s. Česká advokátní komora v této souvislosti vydala stanovisko, ve kterém mimo jiné uvádí, že „*pokud se uvedené podezření potvrdí, půjde o bezprecedentní zásah do základních lidských práv osob na našem území, z něhož bude třeba vyvodit nejpřísnější důsledky…“*[66] Dle Nejvyššího státního zastupitelství došlo k „*závažnému pochybení policejního orgánu při nakládání se záznamy tel. provozu, které policejní orgán založil do spisu, aniž by provedl předchozí analýzu těchto záznamů z hlediska jejich obsahové a důkazní použitelnosti, včetně toho, zda neobsahují zákonem chráněnou komunikaci mezi obviněným a obhájcem v jiné trestní věci. “*[67] Vzhledem k tomu, že ve věci nebylo zatím nařízeno ani hlavní líčení, není jasné, jak se bude záležitost dále vyvíjet.

[65] Jelínek, J., Uhlířová, M. *Obhájce v trestním řízení*. Praha: Leges, 2011. s. 259; Vantuch, P.: *Nezákonný odposlech advokáta*, Bulletin advokacie č. 3/2008, s. 15

[66] Stanovisko České advokátní komory k podezření na nezákonné odposlechy telefonických rozhovorů mezi obviněným a jeho obhájci, dostupné na http://www.cak.cz/scripts/detail.php?id=17081

[67] Tisková zpráva Nejvyššího státního zastupitelství ze dne 5. května 2017, dostupná na: http://www.nsz.cz/index.php/cs/aktuality/1880-nsz-rozhodlo-v-pipadu-podezeni-z-ovlivovani-svdk-a-podplaceni-tlumonika

1.2.5. Záznam jako důkaz v trestním řízení

Má-li být záznam telekomunikačního provozu (dále jen „záznam“) použit jako důkaz v trestním řízení, je třeba k němu připojit protokol o uskutečnění odposlechu, který splňuje zákonem stanovené náležitosti. Těmi jsou podle § 88 odst. 6 tr. řádu:

- údaje o místě, času, způsobu a obsahu jeho provedení
- údaje o orgánu, který záznam pořídil

Nedostatek jejich splnění není dle názoru Vrchního soudu v Praze neodstranitelnou vadou a je možné jej napravit stejně jako v případě odstranění formálních nedostatků protokolu sepsaného o jakémkoli jiném úkonu trestního řízení, např. výslechem osob, které se provedení úkonu zúčastnily, popř. jej provedly, a to v postavení svědka. Takový postup nelze považovat za nepřípustnou manipulaci se záznamy a nevymyká se ani možnostem soudu, takže nevyžaduje další šetření.[68]

Vedle specifických náležitostí musí protokol obsahovat také obecné náležitosti protokolu, jejichž výčet upravuje ustanovení § 55 tr. řádu.[69] Jsou-li předmětem odposlechu data podrobena znaleckému zkoumání, může být vedle záznamu o provedeném odposlechu využit v trestním řízení také znalecký posudek jako listinný důkaz, resp. důkaz výpovědí znalce.[70] Vedle protokolu může být vyhotoven také přepis záznamu, který je neformální informační pomůckou.[71]

V jiné trestní věci, než je ta, v níž byl odposlech a záznam telekomunikačního provozu proveden, lze záznam jako důkaz užít tehdy, pokud je v této věci vedeno trestní stíhání pro trestný čin uvedený v odstavci 1 § 88 tr. řádu, nebo souhlasí-li s tím uživatel odposlouchávané stanice.

Co se týče hodnocení důkazů získaných odposlechem a zejména pak jejich ztotožnění, tedy přiřazení dat konkrétnímu zařízení nebo uživateli, je praxe v případě odposlechu telefonických hovorů v podstatě stabilizována. Takový záznam se jako důkaz v řízení před soudem provádí poslechem příslušné části záznamu.[72] Problematičtější je situace v případě záznamu elektronické komunikace, u které není možné data jednoduše ztotožnit analýzou hlasu

[68] Usnesení Vrchního soudu v Praze sp. zn. 4 To 3/01 ze dne 18. 1. 2001

[69] Jedná se zejména o pojmenování soudu, státního zástupce nebo jiného orgánu provádějícího úkon, identifikační údaje osob, stručné a výstižné vylíčení průběhu úkonu, návrhy stran, udělení poučení, popřípadě vyjádření osob a námitky stran nebo vyslýchaných osob proti průběhu úkonu nebo obsahu protokolu

[70] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 192

[71] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR, a.s., 2017, s. 806

[72] Draštík, A., Fenyk, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR, a.s., 2017, s. 806

komunikujících stran. Různé druhy nástrojů sloužících k ztotožnění elektronické komunikace jsou aplikovány v závislosti na konkrétních znalostech a zkušenostech vyšetřovatele. K nejběžnějším nástrojům ztotožnění elektronické komunikace řadíme znalecký posudek, využití metadat datového přenosu, ztotožnění skrze provozní a lokalizační údaje postupem dle § 88 písm. a) tr. řádu, elektronické identifikátory jako jsou např. elektronické podpisy a IP adresy, svědecké výpovědi, a tzv. časové značky.[73]

1.2.6. Následná informační povinnost

Informační povinnost, spočívající v povinnosti orgánu činného v trestním řízení, jehož rozhodnutím byla věc pravomocně skončena, informovat o nařízeném odposlechu osobu uživatele, je-li její totožnost známa, byla do trestního řádu zavedena novelou provedenou zákonem č. 177/2008 Sb. Informace musí obsahovat označení soudu, který vydal příkaz k odposlechu, délku trvání odposlechu a datum jeho ukončení. Součástí podané informace je poučení o právu podat ve lhůtě šesti měsíců Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k odposlechu.

Právo na informaci o provedeném odposlechu má v souladu s dikcí zákona tzv. *osoba uživatele*, jejíž osobní údaje a uživatelská adresa by měly být uvedeny v příkazu k odposlechu, pokud byla tato osoba v době vydání příkazu známa. Tyto údaje je možno zjistit i kdykoli později, zejména v průběhu trestního řízení.[74] Legální definice osoby uživatele je upravena v § 2 odst. 2 ZoEK, dle kterého se uživatelem rozumí *„každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací“*. Je nutné rozlišovat mezi pojmy uživatele a účastníka elektronických komunikací. Pojem osoby účastníka je totiž užší, když podle § 2 odst. 1 ZoEK je jím *„každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb.“*.

Trestní řád upravuje i tzv. *výjimky z informační povinnosti*, tedy situace, ve kterých příslušný orgán činný v trestním řízení (dále jen „OČTŘ“) informaci neposkytne. V souladu s ustanovením § 88 odst. 9 tr. řádu předseda senátu, státní zástupce, nebo policejní orgán nepodá informaci 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*

[73] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 194

[74] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 1214.

organizované zločinecké skupině, v řízení o trestném činu účasti na teroristické 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, jíž má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel trestního řízení, včetně řízení uvedeného v odstavci 6, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob."

Jedná se tedy o případy nejzávažnější trestné činnosti, popřípadě situace, kdy by poskytnutím takové informace mohl být zmařen účel trestního řízení a mohlo by dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob.[75] Dle ESLP totiž *„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 mohlo kompromitovat dlouhodobý cíl, kterým bylo původně nařízení sledování odůvodněno. Navíc takové upozornění by hrozilo přispět k odhalení pracovních metod zpravodajských služeb, pole jejich působnosti a případně i totožnosti jejich agentů."*[76] Dle názoru ESLP tak omezení informační povinnosti není v rozporu s čl. 8 EÚLP, když právě absence podání informace dotčené osobě zajišťuje účinnost uvedeného zásahu.

1.3. Zjišťování údajů o telekomunikačním provozu podle § 88a tr. řádu

Zatímco § 88 tr. řádu umožňuje odposlech samotného *obsahu* přepravovaných zpráv, novější institut zjišťování údajů o telekomunikačním provozu upravený v § 88a tr. řádu slouží k seznámení se s *údaji*, které nejsou samotným obsahem komunikace a které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat. Jedná se o provozní a lokalizační údaje evidované při registraci telekomunikačního provozu ve vztahu ke konkrétním osobám, které mohou vést zejména k dohledání a identifikaci zdroje a adresáta komunikace, a dále údaje vedoucí ke zjištění času, datu, způsobu a doby trvání komunikace apod.[77] Rozsah těchto údajů, způsob jejich uchovávání a postup při jejich poskytování oprávněným orgánům upravuje ZoEK a prováděcí právní předpisy k tomuto zákonu.

[75] Šámal, P. a kol. *Trestní řád. Komentář.* 7. vydání. Praha: C. H. Beck, 2013, s. 1215

[76] Rozsudek Evropského soudu pro lidská práva ve věci Klass a ostatní proti Německu č.. 5029/71 ze dne 6. září 1978

[77] Fenyk, J., Gřivna, T., Císařová, D. *Trestní právo procesní*, 6. aktual. vyd. Praha: Wolters Kluwer, 2015. s. 318

1.3.1. Zrušení původní ústavně nekonformní úpravy § 88a nálezem Ústavního soudu a zavedení nového znění

K zavedení institutu zjišťování údajů o tel. provozu došlo novelou tr. řádu provedenou zákonem č. 265/2001 Sb. Do původní úpravy nicméně zasáhl významným způsobem Ústavní soud nálezy *sp. zn. Pl. ÚS 24/10* a *sp. zn. Pl. ÚS 42/11*, kterými zrušil nejdříve ustanovení § 97 odst. 3, 4 ZoEK, prováděcí vyhlášku 485/2005 Sb. k zákonu, a konečně i celé ustanovení § 88a tr. řádu. Původní, zrušené ustanovení bylo následně nahrazeno novou právní úpravou § 88a tr. řádu, přijatou zákonem č. 273/2012 Sb., s účinností od 1. 10. 2012. Výše zmíněné ústavní nálezy si na tomto místě dovoluji stručně rozebrat.

Nejprve Ústavní soud ve svém nálezu *sp. zn. 24/2010* na návrh skupiny poslanců zrušil § 97 odst. 3 a 4 ZoEK a prováděcí 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. Obsahem zrušených ustanovení ZoEK byla povinnost provozovatelů elektronických komunikací uchovávat po stanovenou dobu provozní a lokalizační údaje a na žádost tyto údaje poskytnout oprávněným orgánům. Ústavní soud konstatoval, že ačkoli se stanovená povinnost týká pouze sběru informací a údajů o uživatelích (zejm. časech, místech a formách telekomunikačních spojení), a nikoli samotného obsahu sdělení, pakliže budou takové údaje sledovány po delší časový úsek, lze v jejich kombinaci sestavit detailní informace o společenské nebo politické příslušnosti, o osobních zálibách, sklonech nebo slabostech jednotlivých osob.[78] V předmětném nálezu se Ústavní soud proto podrobně zaobíral právem na informační sebeurčení a jeho vztahu ke zmíněnému ustanovení ZoEK. Právo na informační sebeurčení, garantované v čl. 10 odst. 3 Listiny, lze chápat jako právo každého svobodně rozhodovat o informacích z jeho osobní sféry a o tom, za jakých okolností a jakým způsobem mohou být tyto informace zpřístupněny jiným subjektům. Právo na informační sebeurčení je přitom aspektem práva na soukromí (čl. 10 odst. 2 Listiny), které jako jedno ze základních práv požívá dle Ústavního soudu „*zcela zvláštní respekt a ochranu*.“[79] Z ustálené judikatury vyplývá, že ochrana práva na informační sebeurčení ve smyslu čl. 13 a čl. 10 odst. 3 Listiny se vztahuje nejen k vlastnímu obsahu zpráv, ale i k doprovodným údajům, jako jsou údaje o volaných číslech, datu, čase hovoru apod.[80] Nadto Ústavní soud vycházel v předmětném nálezu i z judikatury ESLP, který právo na informační sebeurčení dovozuje z čl.

[78] K tomu též např. Hořák, J.: *Právo na soukromí versus bezpečnost ve sjednocené Evropě: zamyšlení nad problematikou „data retention“*, Acta UniversitatisCarolinae, Iuridica, č. 1/2006, s. 81

[79] Např. Nález Ústavního soudu sp. zn. II ÚS 2048/09 ze dne 2. 11. 2009

[80] Např. sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001, sp. zn. IV. ÚS 78/2001 ze dne 27. 8. 2001, sp. zn. II. ÚS 789/06 ze dne 27. 9. 2007

8 Úmluvy, a který již několikrát zdůraznil, že „*sběr a uchovávání údajů týkajících se soukromého života jednotlivce spadají pod rozsah čl. 8 Úmluvy, neboť výraz „soukromý život" nesmí být interpretován restriktivně*."[81]

Zásah do práva na informační sebeurčení z důvodu prevence a ochrany před trestnou činností není právní úpravou a priori vyloučen, může k němu však dojít jen při respektování ústavněprávních mantinelů zásahů do základních práv, skrze přesnou a ve formulacích zřetelnou zákonnou úpravu tak, aby potenciálně dotčené osoby měly dostatečnou informaci o okolnostech a podmínkách, za kterých je státní moc oprávněna k zásahu do jejich základních práv. V neposlední řadě musí zásah do základního práva obstát z hlediska uplatnitelné zásady proporcionality. K posouzení dodržení této zásady a přípustnosti zásahu, Ústavní soud užívá tzv. test *proporcionality* zahrnující tři kritéria:

- posouzení principu *vhodnosti*, podle něhož musí být příslušné opatření schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku,
- posouzení principu *potřebnosti*, podle kterého je povoleno použít pouze prostředek, který je nejšetrnější k dosažení požadovaného účelu (zásahu do základního práva)
- posouzení principu *přiměřenosti* (v užším smyslu), podle kterého újma na základním právu nesmí být nepřiměřená ve vazbě na zamýšlený cíl. Jinými slovy újma na základním právu nesmí svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních.

Napadená právní úprava nebyla podle Ústavního soudu schopna obstát v testu proporcionality, jelikož nedostála ústavněprávním požadavkům hned z několika důvodů. Nedostatkem úpravy bylo nejasné vymezení orgánů oprávněných si údaje od provozovatele elektronických komunikací vyžádat. Provozovatel měl povinnost na požádání poskytnout uchovávané údaje *„orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu*", přičemž tyto orgány nebyly konkrétně vymezeny ani v prováděcí vyhlášce, ani v samotném ZoEK. Takto vymezená úprava dle Ústavního soudu nesplňuje požadavky kladené na určitost a jasnost, když je na základě ní možné se pouze domnívat, o jaké oprávněné orgány se jedná. Za nejasný označil ÚS také účel, za kterým měly být údaje oprávněným orgánům poskytovány, což znemožnilo posouzení úpravy z hlediska kritéria potřebnosti. Možnost použití uchovávaných údajů nebyla vázána ani na podezření ze spáchání závažného trestného činu, ani nebyla upravena povinnost orgánů činných v trestním řízení následně dotčenou osobu

[81] Rozhodnutí ESLP Malone proti UK, č. 869/79 ze dne 2. 8. 1984

informovat. V neposlední řadě úprava neobsahovala pravidla zabezpečení uchovávaných údajů, ani záruky případně dotčených jednotlivců proti riziku zneužití údajů. Právní úprava nepromítala požadavek přiměřenosti zásahu do základního práva dostatečně a uvedená ustanovení stejně jako prováděcí vyhlášku nebylo možno považovat za ústavně konformní, neboť výrazným způsobem porušovali výše zmíněné ústavněprávní limity. V závěru svého nálezu se Ústavní soud stručně vyjádřil také k zjišťování údajů o tel. provozu podle § 88a tr. řádu, na které zrušené ustanovení § 97 odst. 3 ZoEK odkazovalo a u kterého shledal ÚS stejné nedostatky, tedy nerespektování ústavněprávních limitů a požadavků. Ustanovení § 88a tr. řádu nicméně nebylo předmětem řízení v dané věci, a Ústavní soud proto označil za nezbytné apelovat na zákonodárce, aby zvážil změnu ustanovení § 88a tak, aby bylo ústavně konformní.[82]

K tomu nicméně nedošlo, a ustanovení § 88a tr. řádu zůstalo beze změny až do jeho zrušení provedeném dalším nálezem ústavního soudu *sp. zn. Pl. ÚS 42/2011* ze dne 20. prosince 2011. Obvodní soud, který byl v dané věci navrhovatelem, dospěl v rámci trestního řízení u něj probíhajícího k závěru, že nemůže rozhodnout o návrhu na vydání příkazu ke sdělení údajů o uskutečněném telekomunikačním provozu podle § 88a tr. řádu z důvodu rozporu uvedeného ustanovení s ústavním pořádkem. Původní znění ustanovení § 88a totiž podmiňovalo přístup OČTŘ k údajům o telekomunikačním provozu pouze tím, že zjištění údajů slouží k objasnění skutečností důležitých pro trestní řízení. Takovou úpravu navrhovatel označil za protiústavní vzhledem k tomu, že neobsahovala dostatečné garance práv uživatelů služeb elektronických komunikací jako je tomu v případě odposlechu podle § 88, a procesní postup byl upraven značně benevolentně, což vedlo k inflaci návrhů podle § 88a. V důsledku takové úpravy bylo zasahováno do práva na ochranu tajemství zpráv ve smyslu čl. 13 Listiny, které jak již bylo zmíněno, se týká nejen vlastního obsahu zpráv, nýbrž i dalších údajů evidovaných při registraci telekomunikačního provozu. Ústavní soud se ztotožnil s názorem navrhovatele. V předmětném nálezu odkázal v obecných východiscích týkajících se práva na respekt k soukromému životu v podobě práva na informační sebeurčení na svůj předešlý nález sp. zn. 24/2010 jelikož i v tomto případě je právě ochrana soukromí jedince zásadní. Zopakoval, že zásah do tohoto práva je sice možný, nicméně musí pro něj být splněny podmínky vyplývající z ústavního pořádku, musí se jednat o omezení stanovené na základě zákona, jehož úprava je dostatečně zřetelná, a tedy splňující požadavek určitosti, a dostatečně předvídatelná. *„Zároveň musí omezení práva na informační sebeurčení sledovat ústavně aprobovaný účel, jímž je ochrana jiného základního práva nebo veřejného statku, přičemž posouzení vzájemné kolize*

[82] Nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011

těchto hodnot musí dbát imperativu minimalizace zásahů do základních práv a svobod, berouc přitom zřetel na jejich podstatu a smysl.“ Zásah do tohoto základního práva tak musí obstát z hlediska proporcionality, jejíž posouzení sestává dle judikatury Ústavního soudu z posouzení tří kritérií, již formulovaných u výkladu k prvému nálezu sp. zn. 24/2010 - jedná se o kritérium vhodnosti, potřebnosti, a přiměřenosti v tzv. užším smyslu.

V prvním kroku testu proporcionality Ústavní soud posuzoval vhodnost ustanovení a dospěl k závěru, že opatření je schopno dosáhnout sledovaného, ústavně aprobovaného účelu, kterým je v daném případě stíhání trestných činů, jejich předcházení, odhalování a vyšetřování, jakož i spravedlivé potrestání pachatelů. Ustanovení tedy v prvním kroku testu proporcionality obstálo.

Ustanovení nicméně neobstálo v druhém kroku testu proporcionality, tedy posouzení dle kritéria potřebnosti, a pro úplnost Ústavní soud uvedl, že by nebylo schopno obstát ani v kroku třetím, jehož podstatou je posouzení přiměřenosti v užším slova smyslu. V druhém kroku § 88 neobstál, jelikož zjišťování údajů ze strany OČTŘ nepodmínil požadavkem nezbytnosti a pro jeho aplikaci nestanovil účinné prostředky kontroly, jež by umožňovaly účinnou ochranu základního práva na informační sebeurčení dotčených uživatelů. V třetím kroku by pak ustanovení nebylo schopno obstát s ohledem na skutečnost, že nepřikládá žádný význam povaze a závažnosti trestného činu, pro který je trestní stíhání vedeno. Veřejnému zájmu totiž nelze přiznat v kolizi se základním právem přednost pokaždé, a to ani při současném splnění podmínky potřebnosti. Naopak je dle Ústavního soudu třeba vždy zvažovat, *„...zda vzhledem k významu objektu určitého trestného činu, jenž měl být spáchán, převáží zájem na jeho stíhání nad právem jednotlivce rozhodovat sám o tom, zda a komu zpřístupní svá osobní data“* Je přitom věcí zákonodárce, aby určil, tak jako učinil v § 88 tr. řádu, v případě jakých trestných činů tento zájem převažuje. Zákonodárce do napadeného ustanovení nepromítl požadavek proporcionality zásahu do základního práva s ohledem na sledovaný účel, neboť přístup k předmětným údajům upravil v podstatě jako běžný prostředek zaopatřování důkazů v trestním řízení, a to dokonce vedeného pro jakýkoli trestný čin. Tyto nedostatky dle Ústavního soudu nebylo možné odstranit ani prostřednictvím soudní kontroly, jelikož soudy při rozhodování o nařízení sdělení předmětných údajů sice mohou poskytovat ochranu základním právům, nicméně nemohou svou judikaturou nahrazovat absenci dostatečně určité zákonné právní úpravy, jež je ve smyslu čl. 4 odst. 2 Listiny předpokladem omezení základních práv a svobod. Ústavní soud z výše uvedených důvodů zrušil § 88a tr. řádu v celém rozsahu. Vzhledem k vyjádření Poslanecké sněmovny, podle kterého připravovala nové znění právní

úpravy, však odložil účinnost derogačního výroku na dobu do 30. září 2012, kterou považoval za dostatečnou pro dovršení legislativního procesu nového ustanovení.

Dnem 1. října 2012 následně nabyl účinnosti zákon č. 273/2012 Sb., jímž byl novelizován jednak ZoEK, jednak tr. řád, v jehož rámci bylo opětovně zavedeno ustanovení § 88a. Veškerý další výklad institutu zjištění údajů podle § 88a v této práci je věnován z pohledu současné právní úpravy, tedy úpravy „nové", zavedené v důsledku výše pospaných nálezů Ústavního soudu.

Uchováváním údajů o telefonických a datových přenosech se zabýval roku 2010 také německý ústavní soud. Ten v reakci na hromadnou stížnost téměř 35 000 občanů zrušil ustanovení zákona o telekomunikacích (dále jen „TKG") a tr. řádu (dále jen „StPO"). Napadené předpisy byly stejně jako v případě výše popsané zrušené české úpravy implementací směrnice Evropského parlamentu a Rady č. 2006/24/ES o uchovávání údajů z roku 2006 (dále jen „Směrnice o data retention"). Stejně jako v případě české úpravy obsažené v § 97 odst. 3 a 4 ZoEK, i německý TKG ukládal poskytovatelům služeb elektronických komunikací povinnost uchovávat preventivně a bez konkrétního podezření provozní a lokalizační údaje, a to bez splnění dostatečných ústavněprávních požadavků na bezpečnost dat, jasné vymezení účelu použití údajů, transparentnost a právní ochranu.[83] Spolkový ústavní soud tedy totožně jako Ústavní soud ČR uvedl, že uchovávání údajů o telekomunikačním provozu není a priori vyloučeno, nicméně zákonná úprava musí vyhovovat závažnosti takové zásahu a zásadě přiměřenosti.[84]

Národní implementace Směrnice o data retention upravující uchovávání provozních a lokalizačních údajů byly postupně podrobeny kritice a ústavnímu přezkumu v Bulharsku, Rumunsku, Polsku, Slovensku, a na Kypru.[85] Sama směrnice byla zrušena rozhodnutím Evropského soudního dvora Evropské unie (dále jen „SDEU") ve spojených věcech C-293/12 (Digital Rights Ireland Ltd) a C-549/12 (Kärntner Landesregierung). Předběžné otázky položené Irským *High Court* (věc C-293/12) a rakouským *Verfassungsgerichtshof* (věc C-594/12) byly obdobné a týkaly se souladu Směrnice o data retention s některými ustanoveními Listiny základních práv Evropské unie (dále jen „Charta") a s některými

[83] Rozsudek Spolkového ústavního soudu sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 ze dne 2. 3. 2010; Herczeg, J.: *Ústavněprávní limity monitoringu telekomunikačního provozu; konflikt mezi bezpečností a svobodou*, Bulletin advokacie 5/2010, s. 22

[84] DURICA, J., *Právo na soukromí versus posílení bezpečnosti: směrnice o uchovávání údajů o telekomunikačním provozu v nálezech ústavních soudů členských států EU,* Bulletin advokacie 6/2011, s. 19

[85] Harašta, J., Myška. M. *Budoucnost data retention*, Trestněprávní revue, 10/2015, s. 238; DURICA, J., *Právo na soukromí versus posílení bezpečnosti: směrnice o uchovávání údajů o telekomunikačním provozu v nálezech ústavních soudů členských států EU,* Bulletin advokacie 6/2011, s. 19

ustanoveními EÚLP.[86] Jádrem sporu bylo zejména posouzení otázky, zda je omezení práv obsažených v daných ustanoveních přiměřené vzhledem ke sledovanému cíli, kterým byla harmonizace vnitřního trhu a dále zpřístupňování údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů.[87] SDEU ve svém rozhodnutí došel k závěru, že Směrnice o data retention zasahovala do práv chráněných čl. 7 a 8 Listiny základních práv Evropské unie, tedy zasahovala do práva na respektování soukromého života a do práva na ochranu osobních údajů. Zároveň SDEU nicméně dodal, že v souladu s čl. 52 odst. 1 Listiny základních práv Evropské unie je omezení výkonu práv a svobod stanovených v Listině základních práv Evropské unie možné, pokud je „*stanoveno zákonem, respektuje podstatu práva či svobody a při dodržení zásady proporcionality jsou omezení těchto práv a svobod zavedena pouze tehdy, jsou-li nezbytná a odpovídají-li skutečně cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého*.“[88] Ačkoli SDEU konstatoval, že předmětná úprava je způsobilá k dosažení sledovaného cíle v obecném zájmu, kterým je objasnění a vyšetřování trestných činů, při přezkoumání dalšího z hledisek – přiměřenosti zásahu – dospěl k závěru, že úprava neodpovídá zásadě proporcionality. Uchovávání údajů podle Směrnice o data retention se vztahovalo globálně na všechny osoby, které využívají služeb elektronických komunikací bez nutnosti konkrétního podezření, že osoba páchá trestnou činnost. Dále Směrnice o data retention nestanovila žádné objektivní kritérium umožňující vymezit přístup příslušných vnitrostátních orgánů k údajům, nýbrž pouze odkázala v obecné rovině na závažné trestní činy vymezené každým členským státem v rámci jeho vnitrostátních právních předpisů. Dále Směrnice vymezila dobu pro uchovávání údajů jako ne kratší nežli šest měsíců a nejvýše dvacet čtyři měsíců. K tomu SDEU uvedl, že stanovení doby postrádá objektivní kritérium, na základě kterého by doba měla být stanovena, a jež by zaručovalo její omezení na nezbytné minimum. S ohledem na uvedené SDEU konstatoval, že „unijní zákonodárce překročil přijetím směrnice 2006/24 meze, jež ukládá požadavek na dodržování zásady proporcionality z hlediska článků 7 a 8 a čl. 52 odst. 1 Listiny základních práv Evropské unie.“ Na předběžné otázky proto SDEU odpověděl tak, že Směrnice o data retention je neplatná.[89]

[86] Jednalo se zejm. o posouzení souladu Směrnice o data retention s právem na respektování soukromého života stanoveným v čl. 7 Listiny základních práv Evropské unie, dále s právem na ochranu osobních údajů stanoveným v čl. 8 Listiny základních práv Evropské unie a s právem na respektování svobody projevy stanoveným v čl. 11 Listiny základních práv Evropské unie.

[87] Harašta, J., Myška. M. *Budoucnost data retention*, Trestněprávní revue, 10/2015, s. 238

[88] Harašta, J., Myška. M. *Budoucnost data retention*, Trestněprávní revue, 10/2015, s. 238

[89] Rozsudek Soudního dvora (velkého senátu) ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12; Molek, P. *Základní práva. Svazek první – Důstojnost.* Praha: Wolters Kluwer, 2017. s. 406

Zrušení Směrnice o data retention fakticky znamenalo, že se na Směrnici hledí, jako by nikdy nebyla.[90] Z toho důvodu by dle mého názoru bylo žádoucí novelizovat současnou českou právní úpravu, která do značné míry ze znění Směrnice o data retention vychází, tak, aby odpovídala uvedenému rozhodnutí SDEU.

1.3.2. Údaje jako předmět telekomunikačního tajemství anebo osobních a zprostředkovatelských dat

Podle ustanovení § 88a se postupuje a údaje podle něj se vyžadují jen v případě, kdy jsou tyto předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana zprostředkovatelských nebo osobních dat.

Předmět *telekomunikačního tajemství* je vymezen v § 88 a násl. ZoEK skrze stanovení povinností poskytovatele služby elektronických komunikací. Tato rozsáhlá definice v sobě zahrnuje zejména povinnost zajistit ochranu osobním údajům, ochranu důvěrnosti komunikací, a dále ochranu provozních a lokalizačních údajů. Poskytovatelé služeb mají povinnost přijmout odpovídající opatření, aby zajistili bezpečnost svých služeb, a dále povinnost informovat účastníky o jakémkoliv zvláštním riziku porušení bezpečnosti sítě.[91]

Ochrana osobních a zprostředkovatelských dat je poskytnuta nikoli pouze účastníkům telekomunikačního provozu, nýbrž i jeho uživatelům. Jinými slovy je tato ochrana poskytnuta nejenom ve vztahu k osobám, které uzavřely s poskytovatelem elektronických komunikací smlouvu na poskytování služeb (účastník dle § 2 písm. a) ZoEK), nýbrž každému, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací (uživatel dle § 2 písm. b) ZoEK).

Poskytování údajů, o něž se v těchto případech jedná, je upraveno v § 97 odst. 3 ZoEK. Dle tohoto ustanovení má provozovatel elektronických komunikací povinnost uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovány při zajišťování veřejných komunikačních sítí a při poskytování jejich veřejně dostupných služeb elektronických komunikací. Současně je provozovatel povinen zajistit, aby při plnění této povinnosti nebyl zároveň uchováván i obsah zpráv. Na požádání orgánů vyjmenovaných v předmětném ustanovení má provozovatel povinnost tyto údaje bezodkladně poskytnout.

[90] VLACHOVÁ, B. *Zákon o elektronických komunikacích: komentář*. Praha: C. H. Beck, 2017. s. 313-323
[91] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013, s. 1226

Jedná se mj. i o orgány činné v trestním řízení pro účely a při splnění podmínek stanovených v § 88a tr. řádu.[92]

1.3.3. Předpoklady vydání příkazu k zjištění údajů o telekomunikačním provozu

Trestní řád stanoví vedle povahy údajů jakožto předmětu telekomunikačního tajemství, příp. údajů, na něž se vztahuje ochrana osobních a zprostředkovatelských dat další podmínky, jejichž splnění je nutné k vydání příkazu k zjišťování údajů podle § 88a tr. řádu. Jedná se o podmínky:

a. Trestní řízení je vedeno
- pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky,
- pro některý trestný čin výslovně uvedený v § 88a odst. 1, [93]
- pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, přičemž

b. sledovaného účelu nelze dosáhnout jinak nebo by jinak bylo jeho dosažení podstatně ztížené, a

c. vydání údajů musí nařídit předseda senátu a v přípravném řízení na návrh státního zástupce soudce

Okruh trestných činů, pro které je možné nařídit zjišťování údajů o tel. provozu je odlišný od okruhu TČ stanoveného pro odposlechy podle § 88 odst. 1. Horní hranice trestní sazby úmyslných TČ, pro něž je možno zjišťování údajů nařídit, je v tomto případě nižší, když dle dikce zákona musí být minimálně tříletá. Podle důvodové zprávy k návrhu novely č. 273/2012 Sb. je okruh trestných činů stanoven tak, aby v něm byly zahrnuty ty trestné činy, které by bez provozních a lokalizačních údajů nemohly být vůbec objasněny, nebo by jejich objasnění bylo značně ztíženo. Jedná se o přitom o trestné činy, které jsou ve velké míře páchány prostřednictvím mobilních telefonů a prostřednictvím sítě internet.[94] Ohledně okruhu úmyslných TČ, k jejichž stíhání zavazuje mezinárodní smlouva, kterou je Česká republika

[92] Dalšími takovými oprávněnými orgány jsou podle § 97 odst. 3 ZoEK Policie České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti atd., Bezpečnostní informační služba, Vojenské zpravodajství a Čeká národní banka. A to vždy pro účely a za splnění podmínek stanovených zvláštním právním předpisem.

[93] Jedná se o následující trestné činy: *TČ porušení tajemství dopravovaných zpráv, TČ podvodu, TČ neoprávněného přístupu k počítačovému systému a nosiči informací, TČ opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, TČ nebezpečného vyhrožování, TČ nebezpečného pronásledování, TČ šíření poplašné zprávy, TČ podněcování k trestnému činu, TČ schvalování trestného činu*

[94] Důvodová zpráva k zákonu č. 273/2012 Sb.

vázána, lze odkázat na výklad věnovaný podmínkám vydání příkazu k odposlechu obsažený v kapitole 1.2.1., jelikož tato podmínka je totožná s podmínkou uvedenou v § 88 tr. řádu.

Shodně jako v případě odposlechu je pro zjišťování údajů formulována také zásada subsidiarity, dle které lze k úkonu přistoupit pouze *„nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené."*

1.3.4. Vydání příkazu k zjištění údajů a následná informační povinnost

Vydání údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovatelských dat, se zajišťuje *příkazem k zjištění údajů z telekomunikačního provozu*. V souladu s § 88a odst. 1 nařizuje zjištění údajů v přípravném řízení soudce na návrh státního zástupce. V příkazu soudce uloží provozovateli elektronických komunikací povinnost, aby sdělil požadované údaje buď státnímu zástupci, nebo v praxi nejčastěji přímo policejnímu orgánu provádějícímu úkony trestního řízení.[95] V řízení před soudem jejich vydání přímo soudu nařizuje předseda senátu (i odvolacího soudu) nebo samosoudce. Příkaz musí být vydán písemně a odůvodněn, včetně odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání mezinárodní smlouva zavazuje. Stejně jako v případě příkazu k odposlechu je i příkaz k zjištění údajů o tel. provozu rozhodnutím svého druhu a platí pro něj tedy stejná pravidla.

Obsah příkazu musí tedy vedle obecných náležitostí uvedených v § 134 tr. řádu obsahovat uložení povinnosti sdělení konkrétních údajů o uskutečněném tel. provozu, za jakou dobu mají být tyto údaje sděleny, dále údaje o osobě, ohledně nichž mají být příslušné skutečnosti sděleny a v neposlední řadě také účel zjišťování údajů zejména ve formě údajů o trestném činu.

Zjištění údajů je možné realizovat nejen ve vztahu do minulosti, jak tomu bylo podle předchozí právní úpravy[96], nýbrž lze vydat i příkaz ve vztahu do budoucnosti. Příkladem může být sledování přístupů k serveru obsahujícímu dětskou pornografii a následná identifikace počítačových systémů na základě těchto přístupů.[97]

Zákon, shodně jako u odposlechu a záznamu telekomunikačního provozu, vyžaduje jako obligatorní náležitost příkazu k zjištění údajů uvedení totožnosti uživatele služby elektronických komunikací, je-li tato známa a vztahuje-li se příkaz ke konkrétnímu uživateli.

[95] Fryšták, M. *Dokazování v přípravném řízení*, 2. vyd. Brno: Masarykova univerzita, 2015. s. 254
[96] V předchozí úpravě § 88a tr.řádu byla uvedena podmínka: „o uskutečněném telekomunikačním provozu"
[97] Kolouch, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 444

Příkazu není třeba, jestliže k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, k němuž se mají zjišťované údaje vztahovat. Je-li uživatelů jedné účastnické stanice více, je nutné, aby souhlas dal každý z nich.[98] Důkazem pro trestní řízení je následně *zpráva o zjištění údajů o uskutečněném telekomunikačním provozu.*

Trestní řád v § 88a odst. 2 a odst. 3 ukládá povinnost státnímu zástupci nebo policejnímu orgánu, v řízení před soudem předsedovi senátu (samosoudci), aby po pravomocném skončení věci informoval o nařízeném zjišťování údajů osobu uživatele, pokud je známa. Tento přístup je mimo jiné v souladu s judikaturou ESLP vztahující se k čl. 8 EÚLP, podle které vždy, kdy to je možné, a nepopírá to smysl tajného odposlechu, musí být osoba dodatečně informována o tom, že její komunikace byla odposlouchávána a musí mít k dispozici opravný prostředek, jímž může namítat nezákonnost takového odposlechu. Domnívám se, že analogicky se tento přístup vztahuje i na provozní a lokalizační údaje, nejen na odposlech obsahu zpráv.

Informace se v řízení před soudem podává bezodkladně po pravomocném skončení věci. V přípravném řízení je situace odlišná. Státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, podá informaci sice rovněž bezodkladně, avšak nikoli po právní moci svého rozhodnutí, ale až poté, co jeho rozhodnutí přezkoumá nejvyšší státní zástupce, jak ukládá § 174a tr. řádu. Zákon stanoví pro přípravné řízení i povinnost policejního orgánu, jehož rozhodnutím je věc pravomocně skončena, podat informace, a to bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem podle § 174 odst. 2 písm. e).[99]

Informace takto podávaná má zákonem předepsaný obsah. Musí obsahovat označení soudu, který příkaz vydal, údaj o období, jehož se příkaz týkal a poučení o právu podat Nejvyššímu soudu ve lhůtě 6 měsíců ode dne doručení informace návrh na přezkoumání zákonnosti tohoto příkazu.

Informaci příslušný orgán nepodává stejně jako u odposlechu v případě vymezeného okruhu trestných činů, dále v případě, kdy se na spáchání TČ podílelo více osob, přičemž alespoň ve vztahu k jedné z nich nebylo doposud trestní řízení skončeno, nebo pokud je proti osobě, již má být informace sdělena vedeno trestní řízení či by poskytnutím takové informace mohl být zmařen účel trestního řízení, příp. by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv nebo svobod osob.

[98] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C. H. Beck, 2013. s. 330
[99] Šámal, P. a kol., *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 1222-1237

1.3.5. Poskytnutí provozních a lokalizačních údajů podle zákona o Policii ČR

Nejenom podle ustanovení trestního řádu má Policejní orgán možnost získat provozní a lokalizační údaje. Stejné oprávnění stanoví také zákon č. 273/2008 Sb., o Policii České republiky (dále jen „PolČR“), konkrétně ustanovení § 68 odst. 2 a § 71 písm. a) předmětného zákona. Tato oprávnění Policie ČR jsou dle mého názoru velice zajímavým institutem, jelikož stejně jako v případě § 88a tr. řádu umožňují seznámit se s citlivými údaji o osobách, a prolamují tak základní právo na ochranu soukromí jednotlivců, nicméně přitom nepodléhají povolovacímu režimu soudu tak jak je tomu v případě získávání údajů podle tr. řádu.

Policie může v souladu s § 68 odst. 2 PolČR „*…žádat pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly poskytnutí provozních a lokalizačních údajů…“* a to přímo od provozovatele elektronických komunikací *„…způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak. Informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem*“.

Nezbytnost tohoto oprávnění policejního orgánu vyplývá z policejní praxe, ve které Policie v určitých případech potřebuje mít možnost získat provozní a lokalizační údaje i v případech netrestního charakteru, jako je pátrání po osobách pohřešovaných, u nichž je obava o jejich život a zdraví – typicky půjde o ztracené děti, pohřešované se zdravotními obtížemi, apod. [100] Může se ale také jednat o pátrání po pachatelích trestné činnosti jako po osobách hledaných, o osobu neznámé totožnosti, příp. mrtvolu neznámé totožnosti. Je nutné nezaměňovat získávání lokalizačních a provozních údajů podle ustanovení § 68 odst. 2 PolČR se získáváním totožných údajů podle § 88a tr. řádu, které může policie realizovat pouze v rámci trestního řízení a za podmínek stanovených trestním řádem. V případě hledané i pohřešované osoby se jedná o legálně definované pojmy.[101] V obecné rovině se definice pohřešované a hledané osoby mohou odlišit tak, že zatímco hledané osoby se dopustily určitého protiprávního jednání, osoby pohřešované se naopak mohly stát obětí protiprávního jednání, ohrožení života nebo zdraví. V obou případech je velmi důležitým aspektem pátrání rychlost, jelikož jakékoli zdržení může mít fatální následky.[102]

---

[100] Vangeli, B. *Zákon o Policii České republiky: komentář*, 2. vyd. Praha: C. H. Beck, 2014. s. 288-295

[101] *Hledanou osobou* se rozumí fyzická osoba, u které je dán některý ze zákonných důvodů omezení její osobní svobody, místo jejího pobytu není známo a policie po ní vyhlásila pátrání (§ 111 písm. c) PolČR). *Pohřešovanou osobou* se rozumí fyzická osoba, o níž se lze důvodně domnívat, že je ohrožen její život nebo zdraví, místo jejího pobytu není známo a policie po ní vyhlásila pátrání. (§ 111 písm. d) PolČR)

[102] Jamborová, K. *Provozní a lokalizační údaje, nález Ústavního soudu a § 88a TrŘ*, Trestněprávní revue 3/2012, s. 61

Povinnost provozovatele elektronických komunikací poskytnout pro účely pátrání policii lokalizační a provozní údaje vyplývá z ustanovení § 97 odst. 3 písm. b) ZoEK. V současné době má policie na základě zákona přístup k údajům dálkovým a nepřetržitým způsobem (tedy 24hodin, 7dní v týdnu), přičemž provozovatelé elektronických komunikací mají povinnost žádosti bezodkladně vyhovět, a tedy je nutné, aby za tímto účelem u nich byla zajištěna nepřetržitá služba. To Policii mimo jiné umožňuje neprodleně reagovat na objektivní potřebu údaje zajistit za účelem záchrany života a zdraví. Zákon o Policii z roku 1991 ustanovení § 68 neobsahoval, a možným prostředkem získávání údajů tak byl jedině postup dle 88a tr. řádu, tedy získávání údajů v rámci trestního řízení. Takový postup nicméně neumožňoval získat informace v případech, kdy existovala objektivní potřeba obdržet údaje co nejrychleji. Hrozila-li bezprostřední újma na zájmu chráněném trestním zákonem a nebylo možné odvrátit nebezpečí jinak, mohl policejní orgán postupovat taktéž v rámci podmínek krajní nouze a údaje si od provozovatelů elektronických komunikací vyžádat. Provozovatelé elektronických komunikací nicméně nemuseli být ochotni údaje poskytnout s ohledem na svou povinnost zajistit důvěrnost komunikací, která jim byla stanovena v § 89 ZoEK. [103]

Podle ustanovení § 68 odst. 2 PolČR, policie disponuje oprávněním vyžadovat lokalizační a provozní údaje pouze v rámci zahájeného pátrání. Zahajování pátrání upravují vnitřní předpisy policie, konkrétně závazný pokyn policejního prezidenta č. 135/2010. Pátrání je podle něj zahájeno započetím úkonů některého z forem pátrání, mezi které patří osobní pátrání, domovní a osobní prohlídky, kontroly podezřelých osob, apod.[104]

Informace získané postupem podle § 68 odst. 2 PolČR, lze využít pouze pro účely zjištění doby a místa pobytu osoby. Tyto informace nelze následně použít jako důkaz v trestním řízení. V případě, že by v rámci policejního pátrání vyvstalo podezření z páchání trestné činnosti a došlo by k zahájení úkonů trestního řízení, musela by policie pro účely zajištění údajů v rámci trestního řízení podat návrh na vydání příkazu k zajištění údajů v souladu s § 88a tr. řádu. Za příklad by mohl sloužit nález mrtvoly – utopence, u které je objeven mobilní telefon. Policie v domnění, že osoba zemřela následkem utonutí a nikoli následkem trestného činu, a ve snaze zajistit totožnost mrtvoly může postupovat podle § 68 odst. 2 PolČR a vyžádat si tak od provozovatele elektronických komunikací provozní a lokalizační údaje z předmětného mobilního telefonu za účelem zjištění totožnosti mrtvoly. Pokud nicméně v následné pitvě bude

[103] Vangeli, B. *Zákon o Policii České republiky: komentář*, 2. vyd. Praha: C. H. Beck, 2014. s. 288-295
[104] Závazný pokyn policejního prezidenta č. 135/2010

zjištěno, že k úmrtí došlo nikoli následkem utonutí nýbrž následkem trestného činu, bude nutné údaje z mobilního telefonu již vyžadovat postupem podle § 88a tr. řádu.

Je také potřeba zdůraznit, že policie může pátrat po osobách a věcech a popř. využívat oprávnění s tím související, pouze v rámci své působnosti, tedy v rámci úkolů v oblasti vnitřního pořádku a bezpečnosti. (nikoli např. pro účely občanskoprávního řízení).[105]

Oprávnění získávat provozní a lokalizační údaje mimo trestní řízení vyplývá také z ustanovení § 71 PolČR, a to v souvislosti se získáváním poznatků o terorismu. Dle tohoto ustanovení může útvar policie, jehož úkolem je boj s terorismem, za účelem předcházení a odhalování konkrétních hrozeb v oblasti terorismu a v nezbytném rozsahu žádat mj. od provozovatelů elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňující dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak. Ustanovení je specifikováno pouze pro účely boje s terorismem jakožto závažnou formou trestné činnosti, u nichž je nutné důkladně mapovat kontakty, organizační strukturu teroristických sítí a činnosti přímo související s udržováním existence těchto organizačních struktur, jako je např. jejich financování, apod. Odhalování této formy trestné činnosti vyžaduje spíše dlouhodobější sbírání poznatků, které se často nevyznačují dostatečnou konkrétností, jež by odůvodňovala zahájení trestního řízení, a proto tato činnost z povahy věci předchází trestnímu řízení.[106] Musí nicméně vždy být dána konkrétní hrozba, tedy hrozba podložena konkrétními poznatky o určitých osobách nebo činnostech – např. poznatky o financování terorismu, získávání zázemí pro tyto organizace a jejich příslušníky, související příprava a výcvik apod. Oprávněním dle tohoto ustanovení bude přitom disponovat pouze útvar, jehož úkolem je boj s terorismem a kterým je v současné době Útvar odhalování organizovaného zločinu Policie České republiky.

1.4. Dokazování e-mailem

Elektronická komunikace prostřednictvím e-mailové korespondence v praxi představuje právní výzvu ve smyslu určení ustanovení trestního řádu, podle nějž má být postupováno v případě potřeby zjištění obsahu e-mailových schránek. Z toho důvodu se v této kapitole stručně věnuji specifikům této oblasti. Není sporu o tom, že elektronická pošta, ačkoli uskutečňovaná prostřednictvím veřejné komunikační sítě, představuje soukromou komunikaci

[105] Jamborová, K. *Provozní a lokalizační údaje, nález Ústavního soudu a § 88a TrŘ*, Trestněprávní revue 3/2012, s. 61

[106] Důvodová zpráva k zákonu č. 273/2008, o Policii České republiky, k § 71

mezi konkrétními a předem určenými subjekty, a jedná se tedy o komunikaci důvěrnou.[107] E-mailové adresy, kterým chybí propojení s určitou osobou, stejné ochrany nepožívají, nicméně i jejich zneužití je zákonem zakázáno.[108]

Pro určení ustanovení trestního řádu, podle něhož bude při zjištění obsahu e-mailové schránky postupováno, je zejména důležité stanovit dobu, kdy k zjištění obsahu e-mailové schránky dochází, a dále rozlišit obsah e-mailové komunikace při jejím doručování od dat uložených v e-mailové schránce (jako jsou např. e-maily již přečtené, odeslané, rozepsané, apod.).

Dochází-li k zjištění obsahu e-mailové komunikace uskutečněné do doby, než se datový nosič dostal do moci orgánů činných v trestním řízení, může policejní orgán disponující datových nosičem ke zjištění obsahu takové elektronické komunikace patrně přistoupit bez nutnosti zvláštních příkazů, např. bez nutnosti příkazu soudce podle § 88 tr. řádu. Policejní orgán nicméně musí dodržet zákonnou úpravu postupu, kterým je možno datový nosič získat – typicky se bude jednat např. o vydání a odnětí věci podle § 78, § 79 tr. řádu, o postup při domovní prohlídce nebo při prohlídce jiných prostor a pozemků podle § 83 a § 83a tr. řádu či při osobní prohlídce podle § 83b tr. řádu. Vyloučené nejsou ani jiné legální způsoby získání datového nosiče jako je např. iniciativa oznamovatele, který sám policii datový nosič předá k podpoře svých tvrzení.[109]

Rozdílná je situace při zjištění obsahu e-mailové korespondence, uložené na datovém nosiči (např. v mobilním telefonu), a uskutečněné v době po zajištění datového nosiče orgány činnými v trestním řízení. V takovém případě již policejní orgán nemůže vstupovat do práv uživatele služeb elektronických komunikací a zajištění datového nosiče jako je např. počítač nebo mobilní telefon ho neopravňuje k tomu, aby v budoucnu bez dalšího využíval docházející e-maily jako důkazní materiál. Odesílání a přijímání e-mailových zpráv, tedy proces „doručování“ zpráv, je totiž stejně jako telekomunikační provoz, jednou z forem elektronické komunikace. Zjištění obsahu údajů doručených na zajištěný datový nosič v době po jeho zajištění orgány činnými v trestním řízení, je tedy pravděpodobně možné pouze postupem podle § 88 trestního řádu.[110] K tomuto názoru se již dříve přiklonil i Nejvyšší soud, který se

[107] Stanovisko trestního kolegia Nejvyššího soudu, sp. zn. Tpjn 300/2012, č. 20/2013 Sb. tr. rozh.

[108] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 118

[109] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 121

[110] *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek* ze dne 26. ledna 2015, Nejvyšší státní zastupitelství, 1 SL 760/2014

předmětnou problematikou zabýval na základě stížnosti pro porušení zákona podané ministrem spravedlivosti v případu, ve kterém došlo k zajištění mobilního telefonu policejním orgánem a následně k jeho kriminalistickému zkoumání, při němž měl být mimo jiné zajištěn registr SMS zpráv. Nejvyšší soud souhlasil s argumenty uvedenými ve stížnosti ministra spravedlnosti a ve prospěch obviněného rozhodl v tom smyslu, že „zjištění obsahu registru SMS zpráv" nesmí zahrnovat zprávy, které došly na zařízení až po jeho vydání.[111] Postup podle § 88 tr. řádu se jeví jako nevhodnější také v případě, kdy policejní orgán přímo nedisponuje s datovým nosičem s e-mailovou schránkou, a tedy potřebuje zjistit obsah e-mailové komunikace online. Naopak dle mého názoru nelze postupovat příkazem soudu vydaným na základě § 88a tr. řádu, jelikož ustanovení § 88a neumožňuje zásah do obsahu komunikace, nýbrž pouze zjištění provozních a lokalizačních dat, přičemž obsah zpráv elektronické pošty nespadá pod provozní a lokalizační údaje definované v ZoEK.

Otázkou je, jak přistupovat k datům uloženým v e-mailové schránce – těmi jsou např. zprávy uživatelem odeslané, rozepsané (tzv. koncepty), přečtené, ale i nepřečtené zprávy, zprávy odstraněné do tzv. koše apod. Vydání příkazu podle § 88 tr. řádu se v takovém případě nejeví jako vhodné řešení, a to s ohledem na technickou realizaci příkazu. Příkaz podle § 88 je totiž prováděn tak, že veškerá komunikace je od určitého okamžiku sledována a dostupná orgánům činným v trestním řízení – zprávy tedy mají od daného okamžiku dva adresáty (skutečného, tj. odposlouchávaného a policejní orgán). Takové technické provedení nicméně neumožňuje zajistit obsah dat v uložišti zpětně, tedy např. e-mailu doručeného do e-mailové schránky před datem vydání příkazu, tedy e-mailu, který je již ve schránce mezi uloženou poštou. Stejně tak by příkazem podle § 88 tr. řádu pravděpodobně nebylo možno zajistit obsah rozepsaných zpráv a jiných dat uložených v e-mailu, jelikož tato data není možné považovat za probíhající e-mailovou komunikaci v procesu „doručování". Podle názoru Nejvyššího státního zastupitelství by proto v případě zjištění obsahu dat uložených v e-mailové schránce, včetně již uskutečněné e-mailové komunikace, mělo být postupováno na základě povolení sledování osob a věcí soudem podle § 158d odst. 1, 3 trestního řádu.[112] Takový postup je v souladu s názorem Ústavního soudu, dle kterého *„Pořízení otisku elektronických dat lze povolit postupem podle*

[111] Usnesení Nejvyššího soudu sp. zn. 7 Tz 9/2000 ze dne 15. prosince 2000.

[112] *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek* ze dne 26. ledna 2015, Nejvyšší státní zastupitelství, 1 SL 760/2014

§ 158d odst. 3 tr. řádu, pokud jde o data na sledovaných počítačích již uložená, nikoli o data telekomunikačního provozu".[113]

V případě zjištění obsahu dat uložených v e-mailové schránce postupem podle § 158d odst. 3 tr. řádu je nicméně nutno si uvědomit, že § 158d odst. 3 sice umožňuje technické získání obsahu takto uložených dat, zároveň však neobsahuje dostatečné záruky zákonnosti zásahu do tajemství přepravovaných zpráv, tak jako je tomu v § 88 tr. řádu. Řešením zajišťujícím technickou možnost získání uložených dat v e-mailové schránce za současného zaručení zákonnosti zásahu a ochrany základního lidského práva na tzv. „listovní tajemství" by tak dle mého názoru mohlo být povolování zjištění obsahu uložených dat podle § 158d odst. 3 tr. řádu, ovšem za použití § 88 odst. 1 tr. řádu *per analogiam,* tedy pouze v případě, že je vedeno řízení pro trestný čin uvedený v § 88 odst. 1 a jsou splněny další podmínky k vydání povolení stanovené v § 88 odst. 1 tr. řádu.

[113] Usnesení Ústavního soudu sp. zn. III ÚS 3812/12 ze dne 3. 10. 2013

2. Vztah institutu sledování osob a věcí podle § 158d tr. řádu k odposlechu a zjišťování údajů

Operativně pátracími prostředky, které byly z původní úpravy obsažené v zákoně č. 283/1991 Sb., o Policii České republiky převzaté do trestního řádu novelou provedenou zákonem č. 265/2001 Sb., se rozumí:

a) předstíraný převod (§ 158c tr. řádu)
b) sledování osob a věcí (§ 158d tr. řádu)
c) použití agenta (§ 158e tr. řádu)

Ustanovení § 158 d) tr. řádu upravuje tři základní typy sledování osob a věcí:

a) *obecné sledování* (§ 158d odst. 1), které obsahuje charakteristiku sledování a stanoví povinnost policejního orgánu zničit záznam s obsahem komunikace, pokud při sledování zjistí, že se jedná o komunikaci mezi obhájcem a obviněným. Sledováním se rozumí *„získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky“.* V případě obecného sledování, o kterém nejsou pořizovány záznamy uvedené v odst. 2 ani nejde o případy uvedené v odst. 3 (sledování technickými prostředky se současným zásahem do některých základních práv) není třeba žádného povolení a sledování je tedy plně v pravomoci pověřeného policejního orgánu. Absence technické dokumentace skutečností získaných tímto typem sledování vede k tomu, že důkazy takto získané, budou sloužit převážně k operativním účelům, případně bude třeba v pozdějších stádiích trestního řízení vyslechnout policistu pověřeného sledováním jako svědka do protokolu.[114]
b) *sledování, při kterém mají být pořizovány zvukové, obrazové nebo jiné* záznamy (§ 158d odst. 2). Tyto záznamy lze pořídit pouze na základě písemného povolení státního zástupce.
c) sledování pomocí technických prostředků, při kterém dochází k zásahu do některých ústavně chráněných práv a svobod (§ 158d odst. 3), jako je nedotknutelnost obydlí, listovní tajemství a tajemství jiných písemností a záznamů uchovávaných v soukromí. Tento způsob sledování lze uskutečnit pouze na základě předchozího povolení soudce.

Zajišťovací úkony odposlech a zjišťování údajů jsou ve vztahu k operativně pátracímu prostředku sledování v poměru speciality.[115] Úprava § 158d speciální ustanovení jen doplňuje,

[114] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přepracované vyd. Praha: C. H. Beck, 2013. s. 2005
[115] Fryšták, M. *Dokazování v přípravném řízení*, 2. vyd. Brno: Masarykova univerzita, 2015. s. 254

nicméně nelze jejím prostřednictvím nahrazovat zásahy, ohledně nichž je stanoven zvláštní režim.[116] Pokud tak v případě sledování, při kterém bude věnována pozornost určité osobě či věci s předem neznámým výsledkem poznatků, bude potřeba provést zajišťovací úkon jako je odposlech či zjišťování údajů, pro který budou vytvořeny i další zákonné podmínky, bude nutné rozhodnout o nařízení odposlechu podle § 88 nebo zjišťování údajů podle § 88a odst. 1. Dosáhnout za těchto předpokladů účelu zajišťovacích úkonů pokračováním ve sledování nelze. To neznamená, že by samotné sledování muselo být jako celek ukončeno, v zákonných mezích může dále pokračovat.[117] Všechny tři instituty – odposlech, zjišťování údajů a sledování – přitom vykazují řadu společných rysů, zčásti jsou však rozdílné. Dále z toho důvodu provádím jejich komparaci.

Z hlediska druhu úkonů jsou zjišťování údajů a odposlech úkony zajišťovacími, zatímco sledování osob a věcí se řadí mezi operativně pátrací prostředky. Pro sledování tedy platí obecné podmínky použití operativně pátracích prostředků uvedené v § 158 b). Používání operativně pátracích prostředků je možno pouze v řízení o úmyslném trestném činu. Z uvedeného vyplívá, že okruh trestných činů, u kterých je možné přistoupit ke sledování je širší než okruh trestných činů uvedených v ustanoveních § 88 i v § 88a, které jsou vázány na zákonem vymezený okruh úmyslných trestných činů, zatímco sledování bez rozdílu na všechny úmyslné trestné činy. Další podmínkou společnou pro použití všech operativně pátracích prostředků je dodržení zásady subsidiarity, která je vyjádřena také u zajišťovacích úkonů odposlechu a zjišťování údajů. Použití operativně pátracích prostředků také nesmí sledovat jiný zájem než získání skutečností důležitých pro trestní řízení, přičemž práva a svobody je možno omezit jen v míře nezbytně nutné. Z ustanovení tedy automaticky nevyplívá možnost přistoupit ke sledování v každém trestním řízení o úmyslném trestném činu, a to právě s ohledem na zásadu subsidiarity a proporcionality, které je nutné v každém konkrétním případě použití sledování respektovat. Dle zásady subsidiarity stejně jako v případě odposlechu a zjišťování údajů platí, že ke sledování lze přistoupit až tehdy, pokud sledovaného účelu nelze dosáhnout jinak, nebo bylo-li by jeho dosažení jinak podstatně ztížené. Zásada proporcionality vychází z nutnosti v každém případě samostatně posoudit, zda zájem na ochraně základního práva (např. ochrana listovního tajemství) převažuje nad zájmem odhalit konkrétní trestnou činnost či nikoli. Záleží tedy na úvaze soudu, popřípadě státního zástupce, jestli v konkrétním případě sledování na základě této úvahy povolí či nikoli.

[116] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 2001-2011
[117] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C. H. Beck, 2013. s. 332

Také v případě sledování stanoví zákon provozovatelům elektronických komunikací povinnost poskytnout OČTŘ součinnost, a to umožněním připojení zařízení pro odposlech v určitých bodech provozovatelem za tímto účelem zřízených (§ 158d odst. 9). Na rozdíl od odposlechu a zjišťování údajů nicméně stanoví tuto povinnost i dalším subjektům, jako je např. pošta. Způsob a rozsah nezbytné součinnosti jsou stanoveny podle pokynů policejního orgánu, přičemž se povinný subjekt nemůže dovolávat mlčenlivosti v stanovené zvláštními zákony.[118]

Společné pro všechny tři instituty je, že mohou být prováděny v utajení. V případě sledování se utajovanost předpokládá. Vzhledem k tomu, že sledování vždy směřuje k získávání poznatků o osobách a věcech, bude se utajovanost typicky vztahovat k osobám, které jsou sledovány nebo nakládají se sledovanou věcí. Přitom musí policejní orgán dodržovat zásady utajení podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.[119] Dalším společným znakem je možnost osoby, do jejíchž práv je zasahováno, dát k úkonu souhlas (§ 158d odst. 6). Záznamy lze za splnění zákonných předpokladů stanovených v § 158d odst. 7 použít jako důkaz, podle odst. 10 je to pak možné i v jiné trestní věci, pokud je i v této věci vedeno trestní řízení o úmyslném trestném činu nebo souhlasí-li s tím osoba, do jejíchž práv a svobod bylo sledováním zasahováno. Pokud však nebyly zjištěny skutečnosti významné pro trestní řízení, musí policejní orgán záznamy předepsaným způsobem zničit. (§ 158d odst. 8).

Stejně jako u odposlechu a zjišťování údajů, i u sledování zákonodárce stanoví v § 158d odst. 1 větě druhé ochranu komunikace mezi obhájcem a obviněným *„Pokud policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky, které se v této souvislosti dozvěděl, nijak nepoužít.“*. Komunikace však v tomto případě není odposlouchávána dle § 88, ale např. jen za pomoci jednostranného poslechu telefonujícího obviněného nebo naopak obhájce anebo komunikace pomocí písemných zpráv přenášených kurýrem apod.[120] Stejně jako v případě odposlechu je stanovena ochrana komunikace pouze mezi *obviněným* a jeho obhájcem, a je tedy předpokladem takové ochrany zahájení trestního stíhání vydáním usnesení dle § 160 odst. 1 tr. řádu. Důvodem je důvěrný vztah mezi těmito osobami, který je předpokladem práva na obhajobu jako jednoho ze základních záruk práva na spravedlivý proces, jak již bylo popsáno výše v kapitole věnované nepřípustnosti odposlechu mezi obhájcem a obviněným. Pakliže

[118] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C. H. Beck, 2013. s. 331
[119] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 2005
[120] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 2001-2011

policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky získané v této souvislosti nijak nepoužít.

2.1. Povolovací režim sledování

Stejně jako u odposlechu a zjišťování údajů je i v případě sledování podle § 158d odst. 2 a odst. 3 zapotřebí písemného povolení státního zástupce, příp. soudce. Bez povolení státního zástupce podle § 158d odst. 2, je policejní orgán oprávněn provést sledování v případech, kdy věc nesnese odkladu, např. v případě, kdy má být sledována osoba nebo věc, která se na území ČR pravděpodobně bude zdržovat jen krátkou dobu. Policejní orgán musí následně o povolení státního zástupce dodatečně požádat a v případě, že státní zástupce do 48 hodin této žádosti nevyhoví, je policejní orgán povinen záznam o provedeném sledování zničit a informace, které se v této souvislosti dozvěděl, nijak nepoužít (§ 158d odst. 5). Takový postup policejního orgánu není za žádných okolností umožněn v případě sledování povolovaného soudcem podle § 158d odst. 3, a to patrně z důvodu základních práv, do nichž je tímto typem sledování zasahováno. Osoba, do jejíchž práv a svobod je zasahováno, může také stejně jako v případě odposlechu a zjišťování údajů o tel. provozu dát k provedení úkonu výslovný souhlas. V takovém případě policejní orgán povolení státního zástupce, příp. soudce vyžadovat nemusí.

Povolovací režim sledování může vzbudit určitou pozornost hned v několika ohledech. V souvislosti se sledováním, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy, nemusí být zcela zřejmé, z jakého důvodu zákonodárce svěřil povolovací režim do rukou státního zástupce, a nikoli soudce, jako je tomu u zajišťovacích institutů podle § 88 a § 88a, u nichž dochází ke srovnatelnému zásahu do soukromí občanů. V praxi taková úprava může dle mého názoru vést k nadužívání tohoto institutu stejně jako k rezignaci policejního orgánu na klasickou operativní činnost při vyhledávání, objasňování a vyšetřování trestných činů. Domnívám se, že sledování, při kterém dochází k pořizování zvukových a obrazových záznamů, představuje závažný zásah do soukromí občanů a proto by jeho povolování, stejně jako dohled nad samotným prováděním, neměl být výlučně v rukou státního zástupce stojícího na straně obžaloby a policie jako vyšetřovacího orgánu. Svěřením povolování do výlučné pravomoci soudu by sice došlo k většímu formalismu tohoto typu sledování, zároveň by však taková změna zvýšila garanci zákonnosti tohoto zásahu do práv občanů a zajistila nad ním náležitý dohled. Z toho důvodu také Stálá komise pro kontrolu použití odposlechů a záznamů telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací (dále jen „Kontrolní komise“) vydala 23. 2. 2017 usnesení, ve kterém žádá vládu,

aby předložila návrh zákona, který bude obsahovat změnu trestního řádu, a to tak, aby bylo vypuštěno oprávnění státního zástupce udělovat policejnímu orgánu písemné povolení ke sledování osob a věcí, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy podle § 158d odst. 2. Tato pravomoc by měla být svěřena výlučně soudu. Podle Komise neexistuje důvod, proč by měla v tomto směru existovat odlišná úprava povolovacího režimu 158d odst. 2 tr. řádu a § 88 a § 88a tr. řádu. Vedle toho Komise žádá vládu, aby byl náležitě zajištěn také funkční systém evidence a informování osob dotčených pořízením zvukového, obrazového nebo jiného záznamu podle § 158d tr. řádu v případech, kdy pořízením takového záznamu nebyly zjištěny skutečnosti důležité pro trestní řízení, a dále aby bylo zajištěno, že takové informace budou bezodkladně zlikvidovány. K usnesení se připojila i Stálá komise pro kontrolu činnosti GIBS. Vláda svým usnesením ze dne 31. 5. 2017 vzala na vědomí stanovisko ministra spravedlnosti k tomuto usnesení Kontrolní Komise, k návrhu zákona měnícího trestní řád však dosud nedošlo.[121]

V souvislosti s povolovacím režimem § 158d odst. 3 může dle Šámala vzbudit pozornost způsob zákonné úpravy sledování osob umístěním technických prostředků (odposlouchávacího zařízení) vstupem do obydlí. Je totiž s podivem, že přesto, že takovým úkonem dochází k zásahu hned do dvou základních práv – tedy práva na ochranu soukromí garantovaného čl. 10 Listiny a nedotknutelnosti obydlí podle čl. 12 Listiny, je úprava obsažená v § 158d odst. 3 nastavena mírněji, než je tomu v případě odposlechu a záznamu telekomunikačního provozu podle § 88.[122]

S tímto názorem souhlasím a domnívám se, že úprava povolovacího režimu podle § 158d) odst. 3 tr. řádu je nedokonalá. Jak již bylo zmíněno, sledováním podle § 158d odst. 3 tr. řádu dochází stejně jako v případě provádění odposlechu podle § 88 tr. řádu k zásahu do základních práv, zejména k zásahu do práva na ochranu soukromí, k zásahu do listovního tajemství a v případě sledování podle § 158d odst. 3 mimo to může dojít také k zásahu do nedotknutelnosti obydlí. V obou případech se tedy zjevně jedná o srovnatelný zásah do práv a svobod občanů, a proto není zřejmé, z jakého důvodu úprava § 158d odst. 3 postrádá ve srovnání s povolovacím režimem odposlechu určité záruky zákonnosti tohoto zásahu do základních práv. Předmětnými zárukami jsou zejména stanovení okruhu trestné činnosti určitého stupně závažnosti, která odůvodňuje případný zásah do soukromí, listovního tajemství,

121 Usnesení *Stálé kontrolní komise pro kontrolu použití odposlechů a záznamů telekomunikačního provozu, sledování osob a věcí a rušení elektronických komunikací*, č. 25 ze dne 23. února 2017, dostupné na: https://www.psp.cz/sqw/text/text2.sqw?idd=102715

122 Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C. H. Beck, 2013. s. 332

či jiného zasaženého práva. Ačkoli v případě provádění odposlechu trestní řád takový okruh trestné činnosti vymezuje, v případě sledování tomu tak není a může tedy teoreticky dojít k paradoxní situaci, kdy u trestného činu nespadajícího do výčtu § 88 nebude možno nařídit odposlech mobilního telefonu podezřelé osoby, nicméně zároveň bude možné nařídit sledování této osoby tzv. prostorovým odposlechem v jejím obydlí. Taková situace je dle mého názoru bez důvodu neproporční a úlohou zákonodárce by mělo být změnit ustanovení trestního řádu tak, aby srovnatelným zásahům do práv a svobod občanů odpovídaly srovnatelné záruky a podmínky jejich provedení. Povolení sledování podle § 158d odst. 3 není dále podmíněno, tak jak je tomu v případě odposlechu, splněním zásady subsidiarity, tedy skutečností, že sledovaného účelu nelze dosáhnout jinak nebo by jeho dosažení jiným způsobem bylo podstatně ztížené. Ani absence této podmínky přitom není vysvětlena v důvodové zprávě k trestnímu řádu a není zjevné, z jakého důvodu ustanovení podmínku opomíjí. V neposlední řadě chybí také podmínka, podle které by šlo stejně jako u odposlechu ke sledování přistoupit pouze v případě, kdy by bylo možné důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení uvedené zejména v § 89 odst. 1 písm. a) až c) tr. řádu.

Osobně za řešení zaručující dostatečnou ochranu základním lidským právům považuji povolování ke sledování osob a věcí podle § 158d odst. 3 za splnění omezujících podmínek uvedených v § 88 odst. 1 tr. řádu *per analogiam*. V budoucnu by přitom bylo na místě, aby zákonodárce zvážil změnu ustanovení § 158d odst. 3 a omezující podmínky do ustanovení vtělil.

3. Vývoj právní úpravy v oblasti odposlechu a zjišťování údajů

3.1. Vývoj na našem území před zavedením zákonné úpravy

Se zákonnou úpravou odposlechů se v České republice nesetkáváme do roku 1990, kdy byl novelou provedenou zákonem č. 178/1990 Sb. tento institut zaveden do tr. řádu. Přesto komunistický režim operativní techniku zahrnující technická zařízení umožňující skryté pořizování obrazových i zvukových záznamů, jako tajné fotografování, filmování, pozorování i odposlech telefonu či prostorový odposlech, znal a hojně využíval. Používání operativní techniky příslušníky Státní bezpečnosti (dále jen „StB“) bylo upraveno různými pokyny, předpisy a směrnicemi. „*Od r. 1954 se její nasazování řídilo "Směrnicemi o používání operativní techniky", označovanými od r. 1955 jako A-oper-IX-1, z let 1955, 1957 a 1959, od r. 1964 to pak byly směrnice A-oper-VI-1 z let 1964, 1969, 1972, 1980 a 1982.*“[123] Operativní technika měla dle těchto Směrnic sloužit k *„…odhalování a usvědčování nepřátelských protistátních živlů a boji s agenty imperialistických rozvědek.“*[124] Operativní technika tak dávala StB možnost získávat informace o náladách obyvatelstva, když v popředí zájmů byly zastupitelské úřady kapitalistických států a jejich pracovníci, příslušníci odboje, osoby politického spektra, ale i známé osobnosti, vědci, či běžní občané. Pravomoc pro schvalování použití operativně pátrací techniky se od počátku lišila dle významu sledované osoby a náročnosti způsobu provádění. V případě regionálního významu byla rozhodující pravomoc vložena do rukou krajských velitelů StB. Jednalo-li se však o tzv. zpravodajsko-technický úkon, jež svým významem či složitostí přesahoval regionální úroveň, povolovali jeho provedení velitelé sektorů StB, velitel StB, ministr vnitra a jeho náměstci.[125] Jak je zřejmé, úloha soudů v rozhodování o nasazení operativně pátrací techniky nehrála roli.

Jako zajímavost lze uvést, že nejstarší dochovaná směrnice pro odposlech telefonů, jakožto výseče veškeré nasazované techniky, pochází z 26. 9. 1949. Vedle doby, na niž bylo možno odposlechy provádět – 14dní s možným prodloužením, stanovila i 3 stupně důležitosti

[123] Povolný, D. *Operativní technika v rukou StB*. Praha: Úřad dokumentace a vyšetřování zločinů komunismu PČR, 2001, s. 33

[124] Tajný rozkaz ministra vnitra, jehož obsahem je Směrnice o používání operativní techniky /A-oper-IX-1/ ze dne 27. prosince 1955. Stať 1, čl. 1. Směrnice jsou dostupné online na webových stránkách Ústavu pro studium totalitních režimů: https://www.ustrcr.cz/uvod/rozkazy-smernice/smernice-k-cinnosti-zpravodajske-techniky/

[125] Povolný, D. *Operativní technika v rukou StB*. Praha: Úřad dokumentace a vyšetřování zločinů komunismu PČR, 2001, s. 33

nahraných zpráv dle jejich obsahu. V dalších letech pak byly přijímány směrnice nové, v různé míře upravující pravomoci osob povolujících odposlechy, včetně časových omezení. [126]

3.2. Zákonná úprava a její vývoj

3.2.1. Zákon č. 178/1990 Sb. zavádějící „Odposlech telefonních hovorů“

Znění trestního řádu bylo poprvé doplněno o zákonnou úpravu využití odposlechů v trestním řízení až novelou z roku 1990. Ta zavedla § 88 s názvem „Odposlech telefonních hovorů“ a nastavila tak základní právní mantinely tohoto institutu. Důvodem zavedení právní úpravy, která se zpočátku omezila pouze na odposlechy stacionárních telefonních stanic, byla snaha o posílení občanských práv a potřeba podřízení odposlechů kontrole justičních orgánů.[127] K zákonné úpravě odposlechu vedla zejména potřeba zajistit právní jistotu občanů, že k odposlechům nemůže nadále docházet na základě volné úvahy orgánů, a dále potřeba účinného prostředku v boji s pachateli *„nejzávažnějších trestných činů, organizované zločinnosti přesahující rámec naší republiky, obchodu s narkotiky, spekulačního obchodu v mezinárodním měřítku, mezinárodního terorismu, jakož i pachatelů trestných činů ohrožujících ústavní základy republiky a prokazování této trestné činnosti“*[128] kteří k jejich páchání často využívali nejnovějších vědeckých poznatků a nejmodernější techniky, na bázi vysoké konspirace a utajovaného spojení. Původní znění § 88 bylo vázáno na zvlášť závažné úmyslné trestné činy nebo jiné úmyslné trestné činy, k jejichž stíhání zavazovala mezinárodní smlouva. Zárukou zákonného užití odposlechů měla být i možnost pořízení odposlechů pouze na základě příkazu, vydaného buď předsedou senátu v řízení před soudem, nebo prokurátorem, příp. s jeho souhlasem vyšetřovatelem, v řízení přípravném.

Odposlech telefonních hovorů mohl být ve své původní úpravě prováděn jedině až po zahájení trestního stíhání. Právní úprava tedy nepočítala s operativním odposlechem před zahájením trestního stíhání a možným využitím jeho výsledků jako důkazu v trestním řízení, čímž se institut podstatně lišil od dnešního, kdy je odposlech za splnění stanovených podmínek považován za neodkladný či neopakovatelný úkon a může tedy prováděn již ve fázi prověřování před zahájením vlastního trestního stíhání. Ustanovení v odst. 1 stejně jako dnešní úprava pamatovalo i na odposlech komunikace mezi obhájcem a obviněným, když stanovilo, že *„Nelze*

[126] Povolný, D. *Operativní technika v rukou StB*. Praha: Úřad dokumentace a vyšetřování zločinů komunismu PČR, 2001, s. 34

[127] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C. H. Beck, 2013. s. 324

[128] Důvodová zpráva k novele trestního řádu provedené zákonu č. 178/1990 Sb.

však provádět odposlech telefonních hovorů mezi obhájcem a obviněným.“ Následné novelizace nicméně toto znění ještě několikrát změnily.

Ohledně náležitostí příkazu k odposlechu, i původní úprava tyto obsahovala, když stanovila, že příkaz musí být vydán písemně a odůvodněn, při současném stanovení doby, po kterou bude odposlech prováděn. Provedení odposlechu pak ve své původní podobě zajišťoval orgán Sboru národní bezpečnosti, který byl však již roku 1991 nahrazen sborem Policie. Stejně jako dnes pak bylo možné nařídit odposlech i pro jiné než vyjmenované trestné činy v tom případě, kdy k tomu účastník odposlouchávané telefonní stanice dal svůj souhlas.

Využití pořízeného záznamu jako důkazu v trestním řízení bylo v původní úpravě, stejně jako dnes, podmíněno tím, aby k němu byl připojen protokol s uvedením údajů o místě, čase, způsobu a obsahu provedeného záznamu, jakož i o osobě, která záznam pořídila. Z této úpravy, platné s jistými změnami dodnes, je zřejmá dvojí možná funkce odposlechu. Jednak jako zdroje informací využitelných při vyšetřování trestné činnosti, jednak jako důkaz v trestním řízení.[129]

První úprava byla tedy stručná a kusá, a to zejména v důsledku neznalosti potenciálních obtíží a nezkušenosti s uplatňováním institutu.

3.2.2. Následné novelizace provedené zákonem č. 558/1991 Sb., zákonem č. 292/1993 Sb., a zákonem č. 152/1995 Sb.

Na problémy, které začala kontinuálně přinášet trestněprávní praxe a s ohledem na nové technické prostředky v souvislosti s širokým rozšířením využívání sítí mobilních operátorů a zavádění internetu, reagovaly postupně další novely.

První novelizace § 88 provedená *zákonem č. 558/1991 Sb.* nebyla rozsáhlá a pouze upravila formulaci odst. 1, když stanovila, že odposlech mezi obhájcem a obviněným je nepřípustný (do té doby bylo znění formulace *„nelze však provádět odposlech mezi obviněným a obhájcem“*). Mimo to nově zavedla povinnost informovat o vydání příkazu organizaci obstarávající telekomunikační síť, v jejímž obvodu bude odposlech prováděn a v návaznosti na vznik sboru Policie České republiky svěřila provádění odposlechu do působnosti policejního orgánu. Následkem přijetí Listiny základních práv a svobod Českou národní radou (dále jen „ČNR“) platilo, že odposlech lze realizovat pouze, stanoví-li to zákon a v jeho mezích. Čl. 13 Listiny zakázal porušování listovního tajemství, zpráv podávaných telefonem nebo podobným zařízením, s výjimkou případů stanovených zákonem. ČNR navíc 21. 6. 1991 schvaluje zákon

[129] Sokol, T. *Odposlech*, Právní rádce 1/2005, s. 4

č. 283/1991 Sb., o Policii České republiky, jehož čtvrtý oddíl upravuje *„Oprávnění k používání operativně pátracích prostředků a operativní techniky“*. Ten mimo jiné zahrnoval i využití odposlechů. Použití operativní techniky povoloval ministr vnitra a kontrolu zajišťoval orgán ČNR složený z pěti poslanců, který záhy získal přezdívku „velké ucho“. Vznikla tak dvojí úprava odposlechu – jednak odposlech podle § 88 tr. řádu, nařizovaný po zahájení trestního stíhání, a jednak odposlech podle § 33 odst. 2 a § 35 písm. a) (původního) zákona o Policii ČR, který umožňoval povolit užití operativní techniky v podstatě kdykoliv *"při odhalování"*.[130] Mimo to původní zákon o Policii ČR zahrnoval ve své úpravě i možnost tzv. prostorových odposlechů, jejichž úpravu tr. řád v této době ještě neznal. Zákon o Policii České republiky ani trestní řád neřešily použitelnost informací získaných postupem podle zákona o Policii ČR jako důkazů v trestním řízení, což následně vedlo k celé řadě procesních pochybení. Novela provedená zákonem č. 265/2001 Sb. zrušila toto ustanovení zákona o Policii ČR upravující odposlech a pro potřeby trestního řízení byl od 1. 1. 2002 odposlech možný pouze podle trestního řádu.[131]

Následnou novelizací provedenou *zákonem č. 292/1993 Sb*. se název § 88 mění do dnešní podoby, když se místo odposlech telefonních hovorů poprvé objevuje zákonné spojení „odposlech a záznam telekomunikačního provozu“. To umožňuje nově provádět odposlech i u dalších komunikačních forem, jako je např. fax a mobilní telefonie (nikoli už jen stacionárních telefonních stanic). S ohledem na závažnost zásahu do osobních práv a v souladu s právní úpravou většiny států bylo nově rozhodování o vydání příkazu k odposlechu svěřeno do výlučné pravomoci soudů.[132] Podstatně se také rozšířila možnost nařídit odposlech, neboť v § 88 odst. 1 věta první byla formulace *"Po zahájení trestního stíhání…“ změněna* na formulaci *"Je-li vedeno trestní řízení…“,* což umožnilo provádění odposlechu i před zahájením trestního stíhání a následné použití záznamu z takového odposlechu jako procesně relevantní důkaz. Novela dále v § 88 odst. 4 zakotvila možnost použití záznamu jako důkazu v jiné trestní věci za předpokladu, že je i v této věci současně vedeno trestní stíhání pro trestný čin uvedený v § 88 odst. 1, anebo s tím účastník odposlouchané stanice souhlasí. Výklad pojmu *"současně"* vyvolával v praxi jistou obtíž, když nebylo zřejmé, zda se vztahuje k okamžiku provádění odposlechu nebo k okamžiku provádění důkazu. Dle Šámala se *"současnost"* vztahovala k okamžiku provádění důkazu. V důsledku takového výkladu je možno výsledky odposlechu použít i v trestní věci, v níž je vedeno trestní stíhání pro některý z trestných činů ze stanovených

[130] Sokol, T. *Odposlech*, Právní rádce 1/2005, s. 4
[131] Sokol, T. *Odposlech*, Právní rádce 1/2005, s. 4
[132] Důvodová zpráva k novele provedené zákonu č. 292/1993 Sb.

kategorií v době použití výsledků odposlechu k důkazu, aniž by bylo vyžadováno zahájení trestního stíhání podle § 160 odst. 1 tr. řádu již v okamžiku provádění takového odposlechu a záznamu telekomunikačního provozu.[133] Jelikož předmětné znění vyvolávalo v praxi obtíže a k jeho interpretaci se vyjádřil i Ústavní soud ve svém nálezu sp. zn. II ÚS 6/1993, rozhodl se zákonodárce situaci napravit a slovo „současně" novelou provedenou zákonem č. 265/2001 zrušil. V důvodové zprávě k předmětné novele se uvádí: *„Pokud trestní řád v této souvislosti uvádí, že trestní stíhání v jiné trestní věci je vedeno „současně", nemíní se tím časová, ale věcná souvislost. K odstranění pochybností v tomto směru se uvedené ustanovení upravuje."*[134] Slovenská právní úprava s termínem *současně* v příslušném ustanovení slovenského trestního řádu stále pracuje, což je kritizováno některými odborníky trestního práva procesního. Záhora kritizoval tuto nevhodnou formulaci slovenské právní úpravy na mezinárodní vědecké konferenci „Trestní právo procesní – minulost a budoucnost", která se konala v listopadu 2016, kde zejména poukázal na to, že na rozdíl od české právní úpravy, kde byla z příslušného ustanovení tr. řádu vypuštěna podmínka použitelnosti záznamu spočívající v tom, že trestní řízení v jiné trestní věci musí být vedeno současně, ve slovenském trestním řádu podmínka zůstala. V jejím důsledku tak řada představitelů především aplikační praxe zastává podle Záhory nesprávný názor, že trestní řízení musí být vedeno ve stejné době (jelikož termín současně chápe z časového hlediska).[135]

Novela provedená *zákonem č. 152/1995 Sb.* přinesla důležitou změnu v oblasti odposlechu obhájce a obviněného. Poslední věta dosavadního znění § 88 odst. 1: „*Použití odposlechu a záznamu telekomunikačního provozu mezi obhájcem a obviněným je nepřípustné*" byla nahrazena zněním novým „*Provádění odposlechu a záznamu telekomunikačního provozu mezi obhájcem a obviněným je nepřípustné…"* Z původní úpravy bylo totiž v praxi dovozováno, že odposlech komunikace mezi obhájcem a obviněným je možný, jeho záznam však nelze použít jako důkaz v trestním řízení. Problém odstranila předmětná novela, která odposlech a záznam mezi obviněným a obhájcem zcela zakázala. Pokud by navíc policejní orgán při odposlechu zjistil, že obviněný komunikuje se svým obhájcem, byl by povinen odposlech ihned přerušit, záznam o jeho obsahu zničit, a informace, které se takto dozvěděl, nijak nepoužít.[136]

---

[133] Šámal, P. *Odposlech a záznam telekomunikačního provozu ve světle judikatury*, Soudní rozhledy 3/2000, s. 67

[134] Důvodová zpráva k zákonu č. 265/2001 Sb.

[135] Stupková, L. *Konference „Trestní právo procesní – minulost a budoucnost",* Trestněprávní revue 1/2017, s. 16; Heranová. S. *Mezinárodní vědecká konference „Trestní právo procesní – minulost a budoucnost",* Bulletin advokacie 12/2016, s.

[136] Mandák, V. *Odposlech a záznam telekomunikačního provozu advokáta*, Bulletin advokacie 3/1995, s. 21

3.2.3. Zavedení institutu zjišťování údajů o telekomunikačním provozu do trestního řádu

Institut zjišťování údajů o telekomunikačním provozu byl do tr. řádu vložen novelou provedenou zákonem č. 265/2001 Sb. reagující tak zejm. na nálezy Ústavního soudu sp. zn. II. ÚS 502/2000 a sp. zn. IV. ÚS 536/2000, *"které vycházely z toho, že čl. 13 LPS 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."*[137] Pro hlubší pochopení zavedení a úpravy institutu zjišťování údajů jako reakci na předmětné ústavní nálezy, si dovoluji tyto podrobněji rozebrat:

a) IV. ÚS 536/2000

   V prvním z nálezů Ústavní soud dospěl k závěru, 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."* Mělo tomu tak být z toho důvodu, že *„pojem záznam se vztahuje také na údaje získané evidováním telekomunikačního provozu ve vztahu ke konkrétní osobě nebo osobám"* V předmětné věci byl stěžovatel odsouzen mj. na základě důkazu, kterým byl právě záznam obsahující identifikační a účastnické číslo mobilního telefonu, datum a čas počátku hovoru, dobu trvání hovoru, číslo volané stanice, označení základové stanice, která zachycovala hovor v okamžiku spojení, a označení základové stanice, která zprostředkovala hovor v okamžiku ukončení. Záznam byl obstarán policií od společnosti Eurotel, a to na základě ustanovení § 47 tehdejšího zákona o Policii, na jehož základě měla policie právo požadovat při plnění svých úkolů pomoc zejména ve formě potřebných podkladů a informací. Stěžovatel ve své ústavní stížnosti namítal nerespektování odst. 2 tohoto ustanovení, stanovujícího povinnost orgánů nebo osob poskytujících takovou pomoc, tuto poskytnout, pouze pokud jim v tom nebrání plnění nebo dodržování povinností podle jiných obecně závazných právních předpisů. Dle stěžovatele poskytnutí této pomoci v daném případě bránily s ohledem na ochranu soukromí a zákonná omezení s ní související zejména ustanovení Listiny základních práv a svobod, Mezinárodní paktu o občanských a politických právech a Úmluvy o ochraně lidských práv a základních svobod. Své tvrzení podepřel mimo jiné rozhodnutím Evropského soudu

[137] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013. s. 1223; Molek, P. *Základní práva. Svazek první – Důstojnost.* Praha: Wolters Kluwer, 2017. s. 404

pro lidská práva ve věci Malone vs. Spojené království, dle nějž je nutné považovat registrační údaje související s telekomunikačním provozem za součást komunikace, a tedy předmět práva na ochranu soukromí.[138] Ústavní soud tomuto tvrzení vyhověl a ztotožnil se s rozhodnutím ESLP ve věci Malone vs. Spojené království. Uvedl nutnost hodnotit veškeré údaje registrace telekomunikačního provozu, zvláště pak volaná čísla, jako nedílnou součást komunikace uskutečněné prostřednictvím telefonu. Čl. 13 tak dle Ústavního soudu nezakládá pouze ochranu tajemství vlastního obsahu zpráv, ale i výše uvedených složek. Jestliže je pak umožněn zásah do této ochrany, děje se tak pouze v zájmu ochrany demokratické společnosti či v zájmu jiných ústavně zaručených práv a svobod a to jen jde-li o zásah nezbytný. Nezbytnost takového zásahu musí mít jasně dané mantinely s dostatečnými zárukami v podobě úpravy právními předpisy a kontrolou jejich dodržování, které dávají občanům jasnou informaci o tom, za jakých okolností je státní orgán oprávněn k zásahu do základního práva občana – v daném případě do jeho soukromí. Přesně musí být stanovena i ochrana proti svévolnému zasahování do takového práva, které by zakládalo protiústavnost takového zásahu. Vzhledem ke skutečnosti, že český právní řád neznal v době rozhodování o ústavní stížnosti institut zjišťování údajů o telekomunikačním provozu, ale zároveň nebylo možné konstatovat, že by příslušné orgány nebyly oprávněny za žádných okolností tuto registraci provádět, dospěl Ústavní soud ústavně konformním výkladem k tomu, že OČTŘ musí při získávání těchto údajů postupovat přiměřeně podle § 88 trestního řádu, a to právě s ohledem na skutečnosti výše vyložené – tedy považujeme-li takové údaje ve světle judikatury ESLP za záznam jako předmět ochrany soukromí, pak je nutné zajistit stejnou ochranu tohoto institutu a chránit jej před svévolným zásahy.

b) ÚS 502/2000

V předmětném nálezu se Ústavní soud zabýval stížností navrhovatele, který byl rozsudkem Krajského soudu uznán vinným TČ loupeže a za tento byl odsouzen k TOS v trvání dvanácti let. Stěžovatel se mimo jiné dovolával protiústavnosti provedeného důkazu, a to výpisy z účtů mobilních telefonů, které poskytla

[138] Evropský soud ve svém rozhodnutí z roku 1984 ve věci *Malone vs. Spojené království* jednoznačně prohlásil, že registraci telekomunikačního provozu za součást chráněné komunikace považuje a že chybí-li ve vnitrostátním právu explicitní zmocnění za blíže určených podmínek tyto údaje požadovat, nemá na ně policie právo a telekomunikační společnost jí je bez souhlasu dotčené osoby nesmí poskytnout.

společnost Eurotel na žádost policejního orgánu již před sdělením obvinění. Dle stěžovatele Policie měla při pořizování tohoto důkazu postupovat dle § 33 až § 37 tehdejšího zákona č. 283/1991 Sb., O Policii České republiky upravujícího použití operativně pátracích prostředků, příp. dle § 88TrŘ., a to vzhledem k povaze získávaných údajů, na něž se vztahuje ochrana listovního tajemství, čl. 13 LZPS a tedy se touto povahou blíží právě zmíněným institutům. Ústavní soud stížnosti vyhověl. Své rozhodnutí, ve kterém znovu argumentoval mj. také rozhodnutím Malone v. Spojené království, odůvodnil skutečností, dle které je potřeba na údaje poskytnuté společností Eurotel (tedy zejm. číslo volané stanice, datum a čas počátku hovoru, doba jeho trvání, označení základové stanice, která hovor zajišťovala v momentu spojení a ukončení) za nedílnou součást komunikace uskutečněné prostřednictvím telefonu. Ústavní soud konstatoval, že *„Soukromí každého člověka si zaslouží zásadní (ústavní) ochranu nejen ve vztahu k vlastnímu obsahu podávaných zpráv, ale i ve vztahu k výše uvedeným údajům. Lze tedy konstatovat, že čl. 13 Listiny zakládá i ochranu tajemství volaných čísel a dalších souvisejících údajů, jako je datum a čas hovoru, doba jeho trvání, v případě volání mobilním telefonem i označení základových stanic zajišťujících hovor.“* Za přípustný zásah do tohoto práva, stejně jako v nálezu sp. zn. IV. ÚS 536/2000 ze dne 13. 2. 2001, popsaném výše, Ústavní soud označil pouze průlom do tohoto práva v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených práv a svobod jiných, a to pouze v případě, kdy se jedná o zásah nezbytný, provedený státní mocí. K tomu, aby nebyly překročeny hranice této nezbytnosti, pak mají sloužit právní předpisy a účinná kontrola jejich dodržování. S ohledem na existenci pravidel pro odposlech a záznam telekomunikačního provozu umožňující kromě dalších údajů pořídit především obsah předávaných zpráv, je možné postupovat podle těchto ustanovení i v případě pořizování či získávání těchto „dalších“ údajů, tj. při evidování telekomunikačního provozu.[139]

Následně byl zákonem č. 265/2001Sb. novelizujícím tr. řád zaveden institut zjišťování údajů o telekomunikačním provozu do tr. řádu do § 88a. Ustanovení však bylo předmětem dalších změn, resp. zrušení ústavním nálezem a opětovnému zavedení zákonem č. 273/2012 Sb.[140]

[139] Fryšták, M., Polišenská, P. *Dokazování v přípravném řízení: nejvýznamnější judikatura k vybraným tematickým okruhům*. Praha: Leges, 2014.
[140] Podrobněji k tomuto procesu viz. kapitola 1.3.1.

3.2.4. Novela provedená zákonem č. 178/2008 Sb.

Hlavním důvodem rozsáhlých změn trestního řádu provedených novelou z roku 2008 byla potřeba upřesnění podmínek pro povolování odposlechu, zvýraznění zásady přiměřenosti a zdrženlivosti jeho používání, jakož i zajištění následné informovanosti odposlouchávaných osob o provedeném odposlechu. [141]

Novelou byl také zaveden institut přezkumu odposlechu, který odposlouchávané osobě dává možnost podat návrh na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu Nejvyšším soudem. Je přitom ponecháno na úvaze odposlouchávané osoby, zdali této možnosti využije či nikoli. Přezkum příkazu k zjištění údajů o telekomunikačním provozu byl do trestního řádu zaveden až o pár let později, novelou provedenou zákonem č. 273/2012 Sb.

Ke zdůraznění principů přiměřenosti a zdrženlivosti, obecně formulovaných v tr. řádu v § 2 odst. 4, došlo doplněním ustanovení § 88 odst. 1 o formulaci, že k odposlechu a záznamu telekomunikačního provozu by mělo být přistoupeno teprve tehdy, „*jestliže získání skutečností důležitých pro trestní řízení není možno dosáhnout jinak nebo jen za podstatně ztížených okolností.“* Tehdejší ministr spravedlnosti JUDr. Jiří Pospíšil při odůvodňování návrhu zákona v Poslanecké sněmovně uvedl, že novela má zpřesnit a zpřísnit pravidla povolování odposlechu pro soudce, který v konkrétní věci rozhoduje, a to tak, že soudce nebude moct při povolování odposlechu postupovat ryze formálně, nýbrž bude muset věc fakticky zkoumat. Nová úprava tak měla přimět soudce zabývat se vždy tím, zda důkazy v dané věci není možno opatřit jinak než odposlechy a zda je odposlech přiměřeným prostředkem vzhledem k závažnosti trestného činu a k ostatním důkazům. Takovým postupem má být zamezeno tomu, aby byl odposlech a záznam telekomunikačního provozu užíván jako běžný způsob získávání informací.[142] S tím souvisí i pozměněné, resp. rozšířené náležitosti jak návrhu státního zástupce na vydání příkazu, tak i samotného příkazu k odposlechu. Od 1. 7. 2008 musí státní zástupci návrhy na povolení odposlechu odůvodnit výrazně lépe než před novelou, a to zejména vylíčením skutkových okolností případu vedoucích k návrhu a pokud je vedeno trestní řízení pro úmyslný TČ, k jehož stíhání zavazuje vyhlášená MS, musí být v návrhu zmíněna i tato smlouva.

Co se samotného příkazu k odposlechu týče, ten vedle dosavadních náležitostí musel nově obsahovat také konkrétní odkaz na vyhlášenou mezinárodní smlouvu v případě, kdy se

[141] Důvodová zpráva k návrhu zákona č. 177/2008 Sb.

[142] Odůvodnění vládního návrhu zákona, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), přednesené ministrem spravedlnosti JUDr. Jiřím Pospíšilem v Poslanecké sněmovně Parlamentu ČR při 1. čtení dne 9. 5. 2007

vede trestní řízení pro úmyslný trestný čin, k jehož stíhání taková MS zavazuje. Dále v příkazu měla být stanovena uživatelská adresa či zařízení a osoba uživatele, pokud je její totožnost známa a doba, po kterou odposlech bude prováděn a která nově nesměla přesahovat čtyři měsíce. Stejná doba byla stanovena i v případě prodloužení. V odůvodnění příkazu je nutné vylíčit skutkové okolnosti, které jeho vydání, včetně doby trvání, odůvodňují.

Vedle zdůraznění principu přiměřenosti a zdrženlivosti, bylo hlavní změnou zavedení institutu přezkumu zákonnosti odposlechu a zavedení informační povinnosti vůči osobě, u které byl odposlech nařízen. Dotčená osoba je po pravomocném skončení věci informována o odposlechu své uživatelské stanice a současně poučena o právu podat návrh Nejvyššímu soudu na přezkoumání zákonnosti příkazu k odposlechu. Předmětem přezkumu se stalo dodržení všech zákonných ustanovení o nařízení odposlechu a jeho provedení. Shledá-li Nejvyšší soud, že skutečně došlo k porušení zákona, pak dotčená osoba může volit další kroky, včetně požadování finančního zadostiučinění za způsobenou nemajetkovou újmu. [143] Přezkum Nejvyššího soudu se tak měl stát zárukou, že při zásahu do ústavních práv občana se tento zásah omezí jen na nejnutnější míru, že základní práva budou maximálně šetřena a zároveň se tak mělo zajistit sjednocení rozhodovací činnosti obecných soudů.[144] Co se práva na informaci týče, toto právo však ve své původní podobě nebylo, a stále není absolutní, když zákon stanoví, kdy informaci nelze poskytnout.

Další změnou bylo novelizované ustanovení § 88 odst. 1 věta třetí, podle kterého odpadla policejnímu orgánu povinnost v případě zjištění, že obviněný komunikuje se svým obhájcem, odposlech ihned přerušit. K této změně došlo v důsledku praxe, kdy ani před novelizací nebyl policejní orgán schopen zjistit a okamžitě přerušit odposlech komunikace mezi obviněným a jeho obhájcem, a to v důsledku používání automatického záznamového zařízení, které tento postup neumožňovalo. Tato úprava v nezměněné podobě zůstala až do současnosti, a to i přesto, že dává orgánům činným v trestním řízení příležitost seznámit se s obsahem důvěrného rozhovoru mezi obviněným a jeho obhájcem, což se z pohledu zabezpečení práva na obhajobu jeví nepřijatelné.[145]

Nově je policejnímu orgánu v § 88 odst. 3 uložena povinnost v průběhu trvání odposlechu průběžně vyhodnocovat, zda trvají důvody, které k vydání příkazu vedly Za předpokladu, že by důvody pominuly, je policejní orgán povinen odposlech ihned ukončit a uvědomit o tom předsedu senátu, který příkaz vydal, v přípravném řízení státního zástupce a

[143] Vantuch, P. *Nová úprava odposlechu v trestním řádu od 1. 7. 2008*. Bulletin advokacie. 10/2008, s. 28
[144] Důvodová zpráva k návrhu zákona č. 177/2008 Sb.
[145] Vantuch, P. *Nová úprava odposlechu v trestním řádu od 1. 7. 2008*. Bulletin advokacie. 10/2008, s. 28

soudce. Cílem tohoto ustanovení je, aby nedocházelo k odposlechu zbytečně v době, kdy již není zapotřebí. Stanoví se také 3letá lhůta, po jejímž uplynutí má policejní orgán povinnost zlikvidovat záznamy, kterými nebyly zjištěny skutečnosti významné pro trestní řízení. Tato lhůta počíná běžet od pravomocného skončení věci. Ke zničení záznamu může dojít teprve po souhlasu soudu a v přípravném řízení po souhlasu státního zástupce. Lhůta je takto stanovena s ohledem na možnost podání dovolání k Nejvyššímu soudu, nebo jiného mimořádného opravného prostředku. [146] Protokol o zničení záznamu o odposlechu je poté založen do spisu.

Oproti dřívější úpravě dochází také ke změně oprávněné osoby, která může dát souhlas k odposlechu podle § 88 odst. 5 tr. řádu, když touto osobou není účastník, nýbrž uživatel telefonu, či jiné telekomunikační služby.[147]

3.2.5. Novela provedená zákonem č. 459/2011 Sb.

Novela začlenila ustanovení o odposlechu a zjišťování údajů do hlavy IV. tr. řádu do části týkající se zajištění osob a věcí. Dle Šámala mohou vyvstat pochybnosti, zda byl tento krok správný s ohledem na to, že odposlechy nezajišťují osoby či věci, nýbrž pouze informace. Za správnější by se mohlo zdát zařazení institutů do hlavy páté k dokazování, případně mezi operativně pátrací prostředky, se kterými mají instituty mnoho společných rysů.[148]

V důsledku přijetí zákona č. 40/2009 Sb., trestní zákoník, došlo k nepřímé novelizaci řady různých typů institutů, mj. i procesního institutu odposlechu. Nový trestní zákoník přinesl rozdílnou kategorizaci trestných činů a zavedl tzv. bipartici – tedy dvě kategorie soudně trestných deliktů, a to přečinů a zločinů. Dosavadní úprava znala pouze monopartici, tedy podobu jednoho soudně trestného deliktu. Rozlišení mezi přečiny a zločiny se podle § 14 tr. zákoníku děje podle formálního hlediska, tedy podle formy zavinění a podle délky trestu odnětí svobody, který trestní zákon stanoví za konkrétní trestný čin. V kategorizaci zločinů dále určuje kritéria pro ty zločiny, které jsou považovány za zvlášť závažné.[149] Původní návrh trestního zákoníku vymezoval zvlášť závažné zločiny jako úmyslné TČ, na něž zákon stanoví TOS s horní hranicí trestní sazby nejméně osm let. Na to reagoval zákonodárce novelou trestního řádu provedenou zákonem č. 41/2009 Sb., když v § 88 odst. 1 vymezil okruh trestných činů, pro které může být odposlech nařízen právě jako „zvlášť závažné zločiny“ a s odkazem na výše uvedený původní návrh TZ předpokládal, že se bude jednat o úmyslné TČ na které zákon

[146] Důvodová zpráva k zákonu č. 177/2008 Sb.
[147] K rozdílu pojmů účastník a uživatel viz. kapitola 1.2.6.
[148] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C. H. Beck, 2013. s. 324
[149] Jelínek, J. *Pojem trestného činu a kategorizace trestných činů*, Bulletin advokacie 10/2009, s. 36

stanoví TOS s horní hranicí trestní sazby nejméně osm let. Následně však v Poslanecké sněmovně došlo ke změně vymezení zvlášť závažných zločinů tak, že hranice trestní sazby byla posunuta z osmi, na deset let. Oproti předchozí úpravě tak došlo k omezení počtu trestných činů, u kterých bylo možno odposlechy nařídit a u kterých je odposlech mnohdy klíčovým prostředkem k jejich odhalení. Z tohoto důvodu zákonodárce v novele z roku 2011 přistoupil k opětovné změně § 88 odst. 1.[150] Nové znění, podle kterého je odposlech možno nařídit u zločinů, na které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, dále pro taxativně vymezené TČ nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, zůstalo zachováno až dodnes.

Do výčtu trestných činů, u nichž je možno provést odposlech se souhlasem uživatele odposlouchávané stanice byl novelou zařazen trestný čin nebezpečného pronásledování, neboť nejčastější formou užívanou pachateli těchto trestných činů k systematickému terorizování oběti, bývá obtěžování prostřednictvím telefonu a internetu. Absence tohoto trestného činu v předmětném výčtu proto činila jeho dokazování obtížným.

[150] Důvodová zpráva k zákonu č. 459/2011 Sb.

4. Realizace odposlechu a zjištění údajů ve světle zákona o elektronických komunikacích; rozbor prováděcích právních předpisů

Zatímco právní úprava neposkytuje legální definice pojmů jako je *odposlech, záznam* a *telekomunikační provoz*, a to patrně za účelem zachování technologické neutrality, odborná literatura nabízí různé definice těchto pojmů. Ty se shodují v podstatných charakterizujících znacích, a na jejich základě je tak možné odposlech chápat jako „*záměrné, utajené a současné vnímání obsahu komunikace, zprostředkované telekomunikačními zařízeními (nebo sítěmi)"* a záznam jako *„souběžné zachycení obsahu probíhající komunikace na nosičích záznamu, které umožňují jeho uchování a následnou reprodukci"*[151]

Problematičtějším je jednoznačné definování pojmu *telekomunikačního provozu*, tedy, mluví-li dikce zákona o odposlechu telekomunikačního provozu, odposlech jakých komunikací lze pod tento pojem podřadit? Odpověď na tuto otázku se může zdát obtížná zejména s ohledem na neustálý technologický rozvoj komunikací. Tradičně byl pojem chápán jako *„komunikace realizovaná prostřednictvím mobilních či pevných telefonů, faxu, vysílaček a podobných přístrojů."*[152] Taková definice nicméně v současné době vzhledem k technologickému pokroku neobstojí. V této kapitole se proto mimo jiné věnuji vývoji tohoto pojmu a praktickým dopadům, které sebou v oblasti odposlechů přináší. Dále si dovolím podrobněji rozebrat úpravu vztahující se k § 88 a § 88a tr. řádu, obsaženou v zákoně o elektronických komunikacích a prováděcích vyhláškách k tomuto zákonu, jelikož ji pro pochopení institutů odposlechu a zjišťování údajů považuji za velmi důležitou.

4.1. Vymezení pojmu telekomunikačního provozu, elektronických komunikací, a některých souvisejících pojmů

S pojmem telekomunikačního provozu se v trestním řádu v souvislosti s odposlechy poprvé setkáváme při novelizaci § 88 tr. řádu novelou provedenou zákonem č. 292/1993 Sb., kdy bylo původní znění „odposlech telefonních hovorů" umožňující provádět odposlechy

[151] Novotná, J. *K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu*, Trestněprávní revue, 2003, č. 10, s. 290 a násl.; dále R. Polčák, F. Púry, and J. Harašta, *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 182

[152] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 183

pouze u stacionárních telefonních stanic změněno na „odposlech a záznam telekomunikačního provozu“.

Prováděcími předpisy konkretizujícími legální spojení *telekomunikačního provozu* byly až do roku 2005 zákon č. 110/1964 Sb. o telekomunikacích, následně zrušen a nahrazen (novým) zákonem č. 151/2000 o telekomunikacích. Ač ani jeden z uvedených předpisů legální definici pojmu telekomunikačního provozu neposkytoval, vymezovaly pojmy bezprostředně související jako telekomunikační zařízení[153], telekomunikační služba[154], a telekomunikační síť[155], na základě nichž by dle mého názoru bylo možné definovat telekomunikační provoz jako „*činnost telekomunikačních zařízení sloužících pro vysílání, přenos, směrování, spojování a příjem informací prostřednictvím elektromagnetických vln (např. telefon, fax, počítačová síť apod.), a to jak informací o obsahu komunikace (obsah zpráv, hovorů apod.), tak i souvisejících údajů.“*

Zákon č. 127/2005 Sb., o elektronických komunikacích nahrazující telekomunikační zákon, s dřívějšími pojmy již nezachází a zavádí místo nich pojmy jako síť elektronických komunikací a služba elektronických komunikací. Důvodem vedoucím k těmto změnám byla reakce na schválení nového regulačního rámce EU, který představoval zásadní změnu evropských telekomunikací. Regulační rámec obsahoval 5 směrnic, které nahradily desítky dřívějších předpisů. Velkou změnou bylo opuštění pojmu „telekomunikace“ a jeho nahrazení podstatně širším pojmem „elektronické komunikace“, které zahrnují kromě klasických služeb pevné a mobilní sítě i např. službu pronájmu okruhů, ISDN a samozřejmě služby internetu.[156] Za cíl si regulační rámec kladl zejména minimální rozsah regulace s cílem pružnějšího fungování. Důvodem nové úpravy byl pak zvláště dynamický technologický vývoj a s ním související zájem o využívání stále širšího sortimentu komunikačních služeb. [157]

Dle důvodové zprávy k návrhu ZoEK je úprava určena *„…pro všechny sítě elektronických komunikací (komunikační sítě) a služby založené na využití přenosu signálů elektronickým způsobem, které jsou a budou využívány ve všech sektorech ČR. Pro tyto*

---

[153] *Telekomunikačním zařízením se rozumí technické zařízení, včetně vedení, pro vysílání, přenos, směrování, spojování a příjem informací prostřednictvím elektromagnetických vln. (*§ 2 odst. 1 zákona č. 151/2000 Sb.)

[154] *Telekomunikační službou se rozumí služba, jejíž poskytování spočívá zcela nebo zčásti v přepravě nebo směrování informací telekomunikačními sítěmi třetím osobám. Touto službou je i pronájem telekomunikačních okruhů. (*§ 2 odst. 7 zákona č. 151/2000 Sb.)

[155] *Telekomunikační sítí se rozumí funkčně propojený soubor telekomunikačních zařízení k přepravě informací mezi koncovými body této sítě nebo soubor rádiových zařízení k přepravě informací nebo jejich vzájemná kombinace (*§ 2 odst. 2 zákona č. 151/2000 Sb.)

[156] Koenig, Ch. et al. EC Competition and Telecommunications Law. in: International Competition Law Sereies, Vol. 6, Kluwer Law International, The Hague, London, New York 2002.

[157] Důvodová zpráva k návrhu zákona č. 127/2005 o elektronických komunikacích

elektronické přenosy signálů, popř. pro vytvářející se novou přenosovou infrastrukturu, je zaveden společný pojem „elektronické komunikace“, který zahrnuje sítě a služby elektronických komunikací. Zahrnuty jsou všechny komunikační infrastruktury (tzn. telekomunikace, přenos v oblasti rozhlasového a televizního vysílání a v oblasti informačních technologií) a přiřazené prostředky, přičemž je uplatňován princip, že funkčně obdobné služby a komunikační sítě by měly podléhat jednomu regulačnímu režimu, bez ohledu na používané technologie.“[158]

Na rozdíl od tradičního pojetí, dle kterého byl telekomunikační provoz spojován s komunikací realizovanou prostřednictvím telefonů, faxu, vysílaček a podobných přístrojů, od přijetí zákona o elektronických komunikacích pod něj lze zahrnout veškeré druhy komunikace realizované prostřednictvím telekomunikačních sítí a sítí elektronických komunikací. Jedná se tedy i o komunikaci mezi počítači, jinými zařízeními, provoz prostřednictvím IP protokolů, a to nezávisle na tom, zda zahájení a obsah takové komunikace volí člověk, nebo počítač.[159] Taková definice pojmu elektronických komunikací navíc umožňuje v budoucnu pojmout i nově vznikající druhy komunikací, a tedy umožnit i jejich případný odposlech.

ZoEK se s terminologií typickou pro předešlou právní úpravu, (mj. i pojem telekomunikačního provozu), a jejím používáním ve zvláštních předpisech jako je mj. trestní řád, vyrovnal ve svých přechodných ustanoveních. Konkrétně v § 136 odst. 20 písm. a) ZoEK, dle kterého: *„Obsahuje-li zvláštní právní předpis ustanovení o*

a) telekomunikačním provozu, rozumí se tím přenášená zpráva podle tohoto zákona,

b) údajích o telekomunikačním provozu, rozumí se tím provozní a lokalizační údaje související s přenášenou zprávou podle tohoto zákona…“

Toto ustanovení je zároveň vůbec jediným místem, kde zákon definuje přímo telekomunikační provoz. Přenášenou zprávou se podle § 89 odst. 2 ZoEK rozumí *„jakákoli informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné služby elektronických komunikací, s výjimkou informace přenášené jako součást veřejného rozhlasového nebo televizního vysílání sítí elektronických komunikací, nelze-li ji přiřadit k určitelnému účastníkovi nebo uživateli, který tuto informaci přijímá.“*. Na základě těchto poznatků lze tedy telekomunikační provoz v současné podobě zjednodušeně definovat jako *jakoukoli formu komunikace přenášenou prostřednictvím veřejných sítí elektronických komunikací mezi konečným počtem uživatelů.*

[158] Důvodová zpráva k návrhu zákona č. 127/2005 Sb. o elektronických komunikacích

[159] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 183.

Provozní údaje jsou ustanovením § 90 ZoEK definovány jako jakékoli údaje zpracovávané za účelem přenosu zprávy sítí elektronických komunikací nebo za účelem účtování. Definice přitom odpovídá mezinárodním dokumentům jako je např. Úmluva o počítačové kriminalitě, která v čl. 1 písm. d) definuje provozní údaje jako *„jakákoli počítačová data vztahující se ke komunikaci prostřednictvím počítačového systému, vytvořená počítačovým systémem, jako součástí komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby“*[160] Jedná se např. o údaje o tom komu, jak dlouho a kdy bylo z určitého mobilního telefonu voláno, informace o navštívených webových stránkách a čase, který na nich uživatel strávil, jak dlouho trvalo připojení k internetu, s jakou IP adresou k připojení došlo, kolik dat bylo přeneseno, apod.

Lokalizačními údaji se dle § 91 ZoEK rozumí jakékoli zpracovávané údaje určující zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací. Jedná se např. o zeměpisnou šířku, délku a nadmořskou výšku koncového zařízení, informaci o směru pohybu a identifikaci síťové buňky, ve které je zařízení umístěno v určitém časovém bodu.[161] Díky lokalizačním údajům lze tedy velmi dobře monitorovat pohyb osoby, která má při sobě například mobilní telefon.

Výstižně popisuje výsledek spojení lokalizačních a provozních dat Novák v příkladu s mobilním telefonem, kdy při kombinaci lokalizace v ordinaci lékaři (údaj lokalizační) s následným vyhledáním informace o nemoci na internetu (údaj provozní), se stávají bezobsahové provozní a lokalizační údaje plně obsažnými.[162]

Přechodným ustanovením byl dle mého názoru rozšířen předmět úpravy § 88 a § 88a tr. řádu, když přestože terminologie telekomunikačního provozu zůstala v tr. řádu zachována, od přijetí ZoEK se obě ustanovení již vztahují na širší pojem elektronických komunikací. Z toho důvodu se domnívám, že by i v budoucnu bylo vhodnější formulovat znění § 88 tr. řádu *„odposlech a záznam elektronických komunikací“*, v případě § 88a tr. řádu pak v rámci přehlednosti zákona název změnit na *„zjištění lokalizačních a provozních údajů o elektronické komunikaci“*.

I přes vyčerpávající výklad k pojetí telekomunikačního provozu se tento pojem, resp. pojem elektronických komunikací, může stále zdát z pohledu vývoje všech v úvahu

[160] *Úmluva o počítačové kriminalitě* vyhlášená ve sbírce mezinárodních smluv pod č. 104/2013

[161] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 168

[162] Novák, J. *K uchovávání provozních a lokalizačních údajů v České republice ve světle rozhodnutí Soudního dvora Evropské unie.* Bulletin advokacie 5/2015, s. 36

přicházejících komunikací a v souvislosti s odposlechy problematický, a to zejména při nedostatku speciální úpravy pro různé formy elektronické komunikace. Obsahem dat v elektronických sítích totiž může být prakticky cokoli, od záznamů, dokumentů, až po kryptoměny, a specifika fungování jednotlivých sítí a obsahu, který je po nich přenášen, představují v souvislosti s odposlechem a záznamem stále technickou i právní výzvu.[163]

4.2. Realizace odposlechu ve světle zákona o elektronických komunikacích

Zákon o elektronických komunikacích konkretizuje povinnosti osob zajišťujících veřejnou komunikační síť ve vztahu k uživatelům a účastníkům sítí, jakož i povinnosti zabezpečení obsahu komunikací, provozních a lokalizačních údajů, a jejich případné vydávání oprávněným orgánům.

Podle § 89 ZoEK má provozovatel elektronických komunikací povinnost zajistit „*technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů"*. Zejména nesmí připustit odposlech, ukládání zprávy nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobám jiným, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak. Poslední sousloví „pokud zákon nestanoví jinak" je pro účely provádění odposlechu klíčové, jelikož právě trestní řád v § 88 výjimku z předmětné povinnosti zajistit důvěrnost komunikací představuje.

Pro účely provádění odposlechu pak § 97 ZoEK stanoví povinnost každého provozovatele elektronických komunikací zřídit a zabezpečit v určitých bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv, a to pro orgány k odposlechu oprávněné – tedy pro Policii ČR, Bezpečnostní informační službu, a Vojenské zpravodajství. Účely zřízení rozhraní pro odposlech jsou ve vztahu k jednotlivým orgánům definovány v příslušných předpisech.[164] ZoEK blíže nespecifikuje postup pro zabezpečení těchto bodů, a přenechává jej v § 97 odst. 9 ve spojení s § 150 odst. 4 ZoEK prováděcímu právnímu předpisu.

Tím je v daném případě *vyhláška č. 336/2005 Sb. o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a*

[163] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 181

[164] Viz. oprávnění Policie ČR podle § 88 tr.řádu, oprávnění BIS podle § 6- § 8 zákona č. 154/1994Sb. o Bezpečnostní informační službě, a oprávnění Vojenského zpravodajství podle § 9 a § 10 zákona č. 282/2005Sb. o Vojenském zpravodajství

provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv (dále jen „vyhláška č. 336/2005 Sb.“). V té je definován mj. pojem *uživatelské adresy* nutný pro interpretaci § 88 tr. řádu.[165] Rozsáhlá definice uživatelské adresy s výčtem možných identifikátorů koncového připojení nebo uživatele služby je přitom uvedena slovy „*zejména“,* což je důležité zohlednit při interpretaci zmíněného výčtu. Zákonodárce tak implikoval, že výčet není konečný a je tedy do budoucna schopen pojmout nové druhy komunikací. Zájmovou uživatelskou adresu vyhláška č. 336/2005 Sb. definuje jako konkrétní uživatelskou adresu určenou k odposlechu. Co se týče *rozhraní pro odposlech a záznam zpráv,* které má provozovatel povinnost zřídit, rozumí se jím buď

- *výstup* sloužící k přenosu provozních a lokalizačních údajů a obsahu komunikace zájmové uživatelské adresy ze sítě do zařízení oprávněného orgánu nebo
- *připojovací bod* pro zařízení oprávněného orgánu v místech předpokládaného výskytu projevů aktivity zájmové uživatelské adresy

Samotný odposlech se následně realizuje dvěma základními způsoby:

- *aktivací (příp. deaktivací)* odposlechu u zájmové uživatelské adresy, kdy informace o každé aktivitě zájmové uživatelské adresy se při tomto postupu přenáší na výstup, nebo
- *instalací (příp. odinstalováním)* zařízení oprávněného orgánu přímo v připojovacím bodě a jeho následnou aktivací

Oprávněný orgán ve spolupráci s provozovatelem tedy může volit ze dvou variant možného řešení. Prvním je zajištění rozhraní pro odposlech ve formě výstupu sloužícího k přenosu informací, který je následně aktivován či deaktivován. K aktivaci výstupu dochází pokynem z pracoviště oprávněného orgánu dálkovým přístupem.[166] Údaje o pokynech k aktivaci/deaktivaci provozovatel uchovává podle § 10 odst. 2 vyhlášky č. 336/2005 Sb. po dobu šesti měsíců za účelem kontroly. Druhé řešení, tedy instalaci připojovacích bodů pro zařízení oprávněného orgánu, se volí v takovém případě, ve kterém u sítě či služby není možné či účelné provádět odposlech s aktivací.

[165] Uživatelská adresa je definována jako identifikátor koncového připojení nebo uživatele služby, a to zejména jako: účastnické číslo, mezinárodní identifikátor mobilního účastníka – IMSI, mezinárodní identifikátor mobilní stanice – IMEI, uživatelské jméno nebo identifikátor přístupu k síti elektronických komunikací, adresa elektronické pošty, identifikátor poštovní schránky, identifikátor síťového zařízení používaný protokoly internetové vrstvy – IP adresa, identifikátor síťového zařízení používaný protokoly spojové vrstvy – MAC adresa, nebo identifikátor vytáčeného připojení.

[166] § 10 vyhlášky č. 336/2005 Sb.

4.3. Realizace zjištění údajů

Povinnost provozovatele elektronických komunikací zajistit důvěrnost komunikací podle § 89 ZoEK se vedle obsahu vztahuje taktéž na provozní a lokalizační údaje. Přesto zákon ukládá provozovateli elektronické komunikace povinnost uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Při plnění této povinnosti nesmí dojít k souběžnému uchovávání obsahu zpráv, ten nelze uchovávat za žádných okolností. (§ 97 odst. 3 ZoEK)

Provozovatel údaje uchovávající, je na požádání povinen vydat je oprávněnému orgánu – tím jsou dle ZoEK orgány činné v trestním řízení, Policie České republiky, Bezpečnostní informační služba, Vojenské zpravodajství a Česká národní banka, a to vždy za podmínek stanovených zvláštním právním předpisem. Lokalizačními a provozními údaji, jež má provozovatel povinnost uchovávat, jsou zejména „*údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí k zjištění data, času, způsobu, a doby trvání komunikace.“*[167] I v tomto případě zákonodárce podrobnější úpravu rozsahu, formy a způsobu předávání údajů oprávněným orgánům přenechává na prováděcích právních předpisech.

Tím je v daném případě zejména *vyhláška č. 357/2012 Sb. ze dne 17. října 2012 o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* (dále jen „vyhláška č. 337/2012 Sb.) Ve vyhlášce se stanoví rozsah uchovávaných údajů, a to vždy samostatným výčtem pro různé typy komunikací.[168] Vedle rozsahu uchovávaných údajů se stanoví i způsob jejich předávání, ke kterému dochází prostřednictvím kontaktních pracovišť oprávněného orgánu (ÚZČ) a provozovatele elektronické komunikace, a to při vzájemné informaci o způsobu prokazování autentičnosti žádosti o údaje, jakož i prokazování autentičnosti předaných údajů. Žádosti i údaje se předávají ve formě datového souboru.[169]

Povinnost likvidace údajů po stanovené době 6 měsíců uvedená v § 97 odst. 3 ZoEK, je konkretizována v § 4 vyhlášky č. 337/2012 Sb. dle které provozovatel po uplynutí doby zlikviduje údaje způsobem, které trvale znemožňují jejich obnovení. Výjimkou je nutnost uchovávat data po dobu, po kterou je možné vyúčtování poskytnutí služby právně napadnout

[167] § 97 odst. 4 ZoEK

[168] Podle § 2 vyhlášky č. 357/2012 Sb. se např. u služby přístupu k internetu z mobilního připojení se uchovávají údaje o typu připojení, telefonním čísle uživatele, identifikátoru mobilního zařízení, datum a čas zahájení a ukončení připojení k internetu, označení základové stanice Start a základnové stanice Stop, adresa IP a číslo portu, ze kterých bylo připojení uskutečněno

[169] § 3 vyhlášky č. 357/2012 Sb. ze dne 17. října 2012 o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

nebo tuto platbu právně vymáhat. Za účelem vyúčtování zůstávají data k dispozici minimálně po obecnou promlčecí lhůtu 3 let podle § 629 odst. 1 občanského zákoníku. V tomto ohledu je zajímavé zmínit, že tr. řád v § 88a neodkazuje na zákon o elektronických komunikacích jako na *lex specialis,* z čehož lze vyvozovat, že údaje o telekomunikačním provozu lze žádat zpětně i na dobu delší než 6 měsíců. Předpokladem úspěšnosti takové žádosti je ovšem reálná dispozice provozovatele elektronických komunikací s těmito údaji. Vzhledem ke zmíněným výjimkám z povinnosti údaje po 6 měsíční lhůtě zlikvidovat je tedy možné, aby orgán činný v trestním řízení úspěšně získal údaje o již proběhlém telekomunikačním provozu, které jsou starší než 6 měsíců.[170]

4.4. Šifrování

Zásadní překážku při využívání elektronických důkazů v trestním řízení a ztížení boje proti trestné činnosti může pro orgány činné v trestním řízení představovat stále rostoucí využívání šifrování dat. Jedná se o postup, kterým jsou data převedena do nečitelné podoby tak, aby je bylo možno převést zpět do čitelné podoby pouze za použití určitého klíče. Držitel dešifrovacího klíče si tak zajišťuje důvěrnost dat, ke kterým má po šifraci přístup pouze on. Existuje přitom celá řada možných způsobů šifrování a šifrovacích algoritmů, od těch zastaralejších, jejichž dešifrace může být pro policejní orgán relativně jednoduchá i bez dešifrovacího klíče, až po ty sofistikovanější, u nichž je získání přístupu k datům prakticky vyloučeno.[171]

Úpravu situací, kdy je nařízen odposlech komunikace upravené šifrováním, řeší ZoEK i vyhláška č. 336/2005 Sb. Pokud provozovatelé elektronických komunikací obsah zpráv šifrují nebo kódují, musí poskytovat příslušné dešifrovací klíče nebo musí zařízení pro odposlech instalovat do segmentů sítě, ve kterých komunikace neprobíhá šifrovaně. V případě, že k šifrování dochází mimo provozovatelovi sítě, je policii obsah zpráv zpřístupněn v takové formě, ve které je k dispozici.[172] Útvar zvláštních činností, který odposlech provádí, se následně může pokusit pomocí specializovaných technických nástrojů komunikaci dešifrovat. Specifika, která přitom používá, nicméně známa nejsou a podléhají režimu utajení. Za účelem dešifrování elektronické komunikace bývá záznam následně předmětem kriminalistické expertízy nebo

[170] Kolouch, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 443-444

[171] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 189

[172] § 8 odst. 4 vyhlášky č. 336/2005 Sb.

znaleckého zkoumání. Výstupem je v takovém případě znalecký posudek, který je využitelný jako důkaz v trestním řízení. Pokud dekrypce bez klíče není možná a klíč není možné získat, je pro Útvar zvláštních činností nemožné obsah dat zjistit. Jelikož v takovém případě neexistuje legální možnost získání přístupového hesla nebo klíče šifry od osoby obviněného, který nemá povinnost dešifrovací klíč policii vydat, lze se jednoduše dostat do situace, kdy data zločinců budou pro orgány činné v trestním řízení nedostupná.[173]

V tomto ohledu je dle mého názoru česká právní úprava zastaralá, jelikož se s šifrací dat prakticky nevyrovnává, když stanoví povinnost dešifrace dat pro účely trestního řízení pouze provozovatelům elektronických komunikací. Domnívám se, že taková úprava v praxi neobstojí, vzhledem k tomu, že např. v současné době masově využívaná komunikace skrze aplikační služby je šifrovaná *dodavatelem* aplikační služby (nikoli provozovatelem elektronických kom.), který ovšem nemá podle platné právní úpravy povinnost dešifrovací klíč vydat (za příklad mohou sloužit v současné době běžně používané aplikace jako je Whatsapp, Viber, apod.). Při vzniku situace, kdy dešifrovací klíč dobrovolně konkrétní subjekt – např. dodavatel aplikační služby, neposkytne, a policejní orgán sám nebude schopen komunikaci či data rozšifrovat, povede takový stav nevyhnutelně k nemožnosti data získat.

Za příklad právní úpravy v oblasti šifrace dat, která se mi jeví vhodnou, uvádím právní úpravu Velké Británie, obsaženou v zákoně o regulaci vyšetřovacích pravomocí (*„Regulation of Investigatory Powers Act"*). Předmětný zákon upravuje pravomoc vyšetřovacích orgánů vyžádat v případě šifrace dat potřebných pro vyšetřování klíč k jejich dešifraci. Tato pravomoc a jí odpovídající povinnost subjektů disponujících s daným klíčem přitom není, jako je tomu v případě naší legislativy, omezena pouze na provozovatele elektronických sítí. V případě, kdy k poskytnutí povinným subjektem nedojde dobrovolně, dopouští se navíc trestného činu.[174] Považuji v tomto ohledu za důležité, že britská úprava současně stanoví mantinely korigující zásah do práva na soukromí, ke kterému tímto postupem dochází. Zejména vymezuje situace, za kterých je možno dešifrovací klíč vyžadovat (jedná se o situace, kdy je získání dat nezbytné v zájmu národní bezpečnosti, ekonomického blahobytu nebo v zájmu prevence a odhalení trestné činnosti), dále možnost vyžadovat odtajnění šifrovaných dat pouze v případě, kdy tato

[173] Kodl, J., Smejkal, V., Sokol, T. *Šifry, státní zájmy a lidská práva*. CHIP, č. 4/1995, s. 34-37; Kodl, J., Smejkal, V., Sokol, T. *Smíme šifrovat?* CHIP, č. 5/1995, s. 30-32

[174] Campbell, L. *Organised crime and the law: a comparative analysis*. Oxford: Hart publishing, 2013. s. 87; dále Regulation of Investigatory Powers Act, čl. 49 a čl. 54, dostupné online na: http://www.legislation.gov.uk/ukpga/2000/23/contents

data byla získána v souladu se zákonem a v neposlední řadě úprava stanoví náležitosti příkazu k takovému odtajnění.

5. Exkurs - odposlech a zjištění údajů na sociálních sítích

Význam sociálních sítí v dnešní době je nepřehlédnutelný – podle průzkumů provedených statistickým portálem *Statista* v roce 2017 stoupl počet uživatelů sociálních sítí na 2,51 miliardy.[175] Termínem sociální sítě se označuje druh služby, pro kterou je typická interaktivnost jejích uživatelů. Uživatelé vytvářejí své osobní profily, které slouží k jejich prezentaci a prostřednictvím nichž mohou s ostatními uživateli sociální sítě komunikovat a sdílet vybrané údaje (často osobní povahy, jako je např. jméno, adresa, vzdělání, zájmy apod.), různá data, textový obsah, kontaktní list dalších uživatelů, apod. Množina těchto údajů představuje celistvý osobní profil uživatele. Osobní profil je dále propojený s provázejícími údaji, jako jsou např. záznamy místa a času přihlášení, IP adresy, délka spojení, atd., které jsou z větší části nedostupné pro běžného uživatele.[176]

Jak je zřejmé, webová prezentace je tedy nositelem informací, které nepochybně mohou sloužit jako vhodný důkazní materiál v trestním řízení. Desítky soudních rozhodnutí se dovolávají na digitální stopy sociálních sítí jako na elektronický důkaz, často nahrazený listinným výpisem z komunikace, fotografiemi apod.[177] Procesní způsob získávání těchto informací může nicméně činit potíže s ohledem na jejich různá specifika. Jedním ze způsobů zajištění dat ze sociálních sítí jako důkazu v trestní řízení je také odposlech a záznam tel. provozu, případně zjišťování údajů o tel. provozu (v takovém případě se zajišťují informace jako je např. IP adresa, čas a délka připojení apod.). Úprava těchto institutů při svém vzniku se sociálními sítěmi a jejich masovým využíváním nepočítala, a proto se až praxe musela a stále musí vypořádávat s možnostmi užívání této platformy k páchání, organizování či sdílení trestné činnosti.

Z právního hlediska je nejprve nutné zabývat se povahou sociální sítě, tedy zda se jedná o prostor soukromý, či veřejný. Ústavní soud se ve svém nálezu sp. zn. III. ÚS 3844/13 v tomto ohledu vyjádřil k povaze sociální sítě Facebook „*Povaha sociální sítě Facebook není jednoznačně soukromá či veřejná. Vždy záleží na konkrétních uživatelích, jakým způsobem si míru soukromí na svém profilu, případně přímo u jednotlivých příspěvků, nastaví.*“[178] Pokud uživatelé tedy zvolí komunikaci či sdílení jiného obsahu takovým způsobem, že k němu nemají přístup ostatní uživatelé sociální sítě, jedná se o komunikaci soukromou, byť uskutečňovanou skrze sociální síť využívanou miliardou uživatelů. S ohledem na takovou povahu komunikace

[175] Dostupné na: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/
[176] Kolouch, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s.151
[177] Polčák, R. Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 139
[178] Nález Ústavního soudu sp. zn. III. ÚS 3844/13 ze dne 30. října 2014

pak musí postupovat i orgány činné v trestním řízení, a při zjišťování komunikace respektovat obecné principy i zákonný rámec pro zásah do ústavně zaručených práv a svobod dotčených osob.[179] Při odposlechu soukromé komunikace na sociální síti a zjišťování souvisejících lokalizačních a provozních údajů musí tedy postupovat orgány činné v trestním řízení v souladu s § 88, příp. § 88a tr. řádu. A contrario lze dle mého názoru dovodit, že při nastavení osobního profilu na sociální síti jako veřejného, či při sdílení určitého obsahu veřejně, tedy tak, že v přístupu k uživatelem zveřejňovaným informacím nejsou omezeni ostatní uživatelé sociální sítě, může orgán činný v trestním řízení zajistit obsah a doprovodné údaje na tomto profilu zveřejněné bez nutnosti postupu podle § 88 či § 88a tr. řádu.

Významným aspektem pro dokazování daty ze sociálních sítí je také stát původů poskytovatele sociální sítě, resp. jurisdikce, pod kterou spadá a ochota tohoto poskytovatele s orgány činnými v trestním řízení spolupracovat při vydávání potřebných údajů. V případě, kdy je potřeba získat obsah, příp. související provozní a lokalizační údaje osobního profilu uložené na zahraničním serveru (jako je např. Google, Facebook, apod.), je potřeba, aby orgány činné v trestním řízení postupovaly cestou právní pomoci. Ta může být realizována na základě mezinárodní smlouvy anebo bez smluvního základu. V rámci Evropské Unie je v oblasti justiční spolupráce v tomto směru klíčová *Směrnice Evropského parlamentu a Rady č. 2014/41 ze dne 3. dubna 2014 o evropském vyšetřovacím příkaze ve věcech trestních*. Směrnice stanoví spolupráci v případě vyšetřovacího příkazu na zajištění důkazů, a to vč. elektronických důkazů v působnosti poskytovatele sociální sítě jiného členského státu. V případě Evropského vyšetřovacího příkazu, který obsahuje žádost o odposlech, má orgán, který příkaz vydal (vydávající orgán) povinnost poskytnout orgánu vykonávajícímu příkaz dostatečné informace, jako například údaje o vyšetřovaném trestném činu, aby vykonávajícímu orgánu umožnil posoudit, zda by daný vyšetřovací úkon byl povolen u obdobného vnitrostátního případu. Vykonávací stát může výkon evropského vyšetřovacího příkazu odmítnout, pokud by daný vyšetřovací úkon nebyl povolen v obdobném vnitrostátním případě. Svůj souhlas může také podmínit náležitostmi, které by musely být splněny v obdobném vnitrostátním případě.[180] Zahraniční poskytovatelé sociálních sítí se mohou nicméně rozhodnout spolupracovat dobrovolně, bez formálního postupu na základě mezinárodních smluv o právní pomoci.[181]

[179] Nález Ústavního soudu sp. zn. III. ÚS 3844/13 ze dne 30. října 2014

[180] Směrnice Evropského parlamentu a Rady č. 2014/41 ze dne 3. dubna 2014 o evropském vyšetřovacím příkaze ve věcech trestních, čl. 10 odst. 5

[181] Polčák, R., Púry, F., Harašta, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. s. 157

6. Kontrola v oblasti odposlechů

Odposlech, stejně jako zjišťování provozních a lokalizačních údajů se postupem času staly hojně využívanými nástroji k odhalování trestné činnosti. Jedná se přitom o razantní zásah do ústavně zaručených práv a svobod, což je třeba mít i při existující právní regulaci na paměti. Za velmi důležité je v oblasti odposlechů dle mého názoru nutno považovat nejen přísné dodržování požadavků zákona a pečlivé zvažování každého povolovaného případu, nýbrž také náležitou a účinnou kontrolu. Velké nebezpečí je podle Šámala skryto nejen v jednoinstančnosti rozhodování o odposlechu a zjišťování údajů, ale také v utajenosti jeho provádění a nedostatečné ověřitelnosti jak získaných informací, tak důvodů, o které se konkrétní příkaz opíral.[182] Na druhou stranu například utajenost provádění předmětných úkonů je jistě ve většině případů předpokladem jejich efektivnosti.

V následující kapitole se věnuji současným prostředkům kontroly v oblasti odposlechů, které považuji za velmi důležité. Okrajově se též zabývám otázkou náhrady škody ze strany státu v případě nezákonných odposlechů.

6.1. Řízení o přezkumu podle § 314l - § 314m tr. řádu

Příkaz k odposlechu, stejně jakožto příkaz k zjištění údajů o tel. provozu je rozhodnutím svého druhu a nelze jej tedy napadnout opravným prostředkem. Trestní řád nicméně umožňuje obranu v podobě institutu řízení o přezkumu zákonnosti příkazu, který je upraven v § 314l až § 314n tr. řádu.

Řízení o přezkumu příkazu k odposlechu telekomunikačního provozu bylo do tr. řádu zavedeno novelou provedenou zákonem č. 177/2008 Sb., a to v souvislosti se zavedením povinnosti informovat po pravomocném skončení věci o nařízeném odposlechu osobu uživatele, pokud je známa. Přezkum příkazu k zjištění údajů o telekomunikačním provozu byl následně zaveden novelou tr. řádu provedenou zákonem č. 273/2012 Sb. Úprava přezkumu obou institutů dle tr. řádu je přitom v zásadě stejná, z čehož budu vycházet, a tedy následující platí pro oba instituty stejně. Pojem „řízení o přezkumu“ tedy v následujícím výkladu zahrnuje obě řízení.

[182] Šámal, P. Musil, J., Kuchta, J. a kol. *Trestní právo procesní*. 4. přepracované vydání. Praha: C. H. Beck, 2013, s. 325

6.1.1. Zákonné předpoklady pro podání návrhu na přezkoumání zákonnosti příkazu

Řízení o přezkumu je možno zahájit pouze na návrh oprávněné osoby, nikoli z úřední povinnosti podle § 2 odst. 4 tr. řádu. Navrhovatelem, tedy osobou oprávněnou podat návrh na přezkum zákonnosti příkazu, se rozumí tzv. osoba uživatele, kterou je ve smyslu § 2 písm. b) ZoEK každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací pro účely mimo rámec své podnikatelské činnosti.[183] Nezbytným předpokladem, aby osoba uživatele návrh na přezkum mohla podat, je dodržení informační povinnosti ze strany orgánů činných v trestním řízení, kteří věc pravomocně skončily a mají vůči odposlouchávané osobě povinnost následné informace o provedeném odposlechu/zjišťování údajů a dále povinnost poskytnout odposlouchávané osobě poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti předmětného příkazu. Poučení je nezbytnou náležitostí podávané informace (§ 88 odst. 8, § 88a odst. 2 tr. řádu).

Informace se podává bezodkladně po pravomocném skončení věci, tj. v době kdy již nemohou být ohroženy výsledky trestního řízení. Podle Jelínka ovšem v praxi často k poskytnutí informace bezodkladně nedochází, případně k poskytnutí informace nedochází vůbec, čímž je osobě následně odepřeno i právo na obranu v podobě návrhu na přezkum k Nejvyššímu soudu.[184] Dalším předpokladem pro podání návrhu na přezkoumání zákonnosti příkazů je pravomocné skončení věci, v níž byl předmětný příkaz vydán. Návrh na přezkoumání zákonnosti příkazu tedy nelze k Nejvyššímu soudu podat před pravomocným skončením věci a bez následného zaslání informace uživateli telekomunikačního zařízení.[185] Pokud by byl návrh na přezkum přesto učiněn, Nejvyšší soud by ho podle § 265i odst. 1 písm. a) tr. řádu *per analogiam* odmítl jako nepřípustný.[186]

Ústavní soud se takto ve svém nálezu sp. zn. III. ÚS 3457/14 zabýval stížností, ve které navrhovatel namítal, že v jeho případě k poskytnutí informace o provedeném odposlechu nedošlo a o jeho provedení se dozvěděl až z médií. Navrhovatel se nejdříve domáhal svého práva u Nejvyššího soudu prostřednictvím návrhu na přezkum zákonnosti příkazu k odposlechu, nicméně Nejvyšší soud usnesením tento návrh odmítl z důvodu nepřípustnosti podle § 265i tr. řádu, jelikož dovodil, že právo podat návrh na přezkum má pouze osoba, která

[183] K pojmu osoby uživatele srov. kapitolu 1.2.6.
[184] Jelínek, J. a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*, 6. vyd. Praha: Leges, 2016. s. 739
[185] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. V Praze: C. H. Beck, 2013. s. 888
[186] Usnesení Nejvyššího soudu sp. zn. 4 Pzo 1/2010 ze dne 14. 10. 2010

byla po pravomocném skončení věci o odposlechu v souladu s § 88 odst. 8 tr. řádu řádně informována. Stěžovatel o poskytnutí informace o případném odposlechu jeho osoby, o kterém se měl dozvědět až z médií, sice požádal, avšak jeho žádosti nebylo tehdejším Útvarem pro odhalování organizovaného zločinu vyhověno (dále jen „ÚOOZ“) a informován tedy nebyl. Stěžovatel v ústavní stížnosti konstatoval, že se tak dostal do situace, kdy neměl k dispozici žádný právní prostředek k ochraně svých základních práv a z toho důvodu se dovolával ochrany přímo u Ústavního soudu. Domníval se, že k porušení jeho práv došlo i ze strany ÚOOZ, neboť dle něj bylo pravděpodobné, že mu orgán neposkytl informaci v rozporu se zákonem, aby tak cíleně zabránil jeho dalšímu možnému postupu návrhem na přezkum zákonnosti příkazu. Ústavní soud ve svém nálezu nejdříve konstatoval, že soudní přezkum nařízených odposlechů ex ante, je nezbytnou zárukou jejich přípustnosti a za neméně důležitou záruku ústavnosti odposlechů označil také povinnost OČTŘ informovat dotčenou osobu o provedeném odposlechu/zjištění údajů, nejde-li o některou z výjimek z této informační povinnosti upravenou v tr. řádu. K postupu Nejvyššího soudu se Ústavní soud vyjádřil tak, že z *„dikce § 314l ve spojení s § 88 odst. 8 tr. řádu vyplívá, že zákonným předpokladem pro podání návrhu na přezkoumání zákonnosti příkazu je jednak pravomocné skončení věci, v níž byl příkaz vydán, a jednak skutečnost, že příslušný orgán dotčenou osobu informoval o provedeném odposlechu.“* NS tedy nemohl pochybit, když zamítl stěžovatelův návrh na přezkum, jelikož postupoval v souladu s právními předpisy. Tím ovšem není stěžovateli do budoucna odepřena možnost domáhat se svého práva v případě, kdy bude o odposlechu dle § 88 odst. 8 tr. řádu vyrozuměn. Ústavní soud nezjistil pochybení ani na straně ÚOOZ, který informaci nepodal v souladu se zákonem, jelikož předmětné řízení ještě nebylo ukončeno. Pokud by ovšem ÚS zjistil, „*že informační povinnost byla OČTŘ opomenuta, přestože již bylo trestní řízení pravomocně skončeno a ve věci nemohly být uplatněny výjimky ve smyslu § 88 odst. 9 trestního řádu, musel by nutně dospět k závěru, že došlo k zásahu do základních práv stěžovatele, neboť by tak stěžovateli byla upřena možnost domáhat se ochrany před Nejvyšším soudem*.“[187]

6.1.2. Průběh řízení o přezkumu

Přezkoumání zákonnosti vydání a provedení příkazu provádí Nejvyšší soud v neveřejném zasedání, v senátě složeném z předsedy senátu a dvou soudců. Platí, že soudce, který se účastnil rozhodování v předchozím řízení, je vyloučen z řízení o přezkumu příkazu. Stejně tak je v souladu s § 30 odst. 4 tr. řádu vyloučen z dalšího rozhodování soudce, který se

[187] Nález Ústavního soudu sp. zn. III ÚS 3457/14 ze dne 26. dubna 2016

účastnil rozhodování v řízení o přezkumu.[188] Dle zákonné úpravy Nejvyšší soud přezkoumává nejen zákonnost vydání příkazu, nýbrž i zákonnost jeho provedení.

Shledá-li Nejvyšší soud, že vydání příkazu a jeho provedení bylo v souladu s podmínkami uvedenými v § 88 odst. 1 nebo § 88a odst. 1 tr. řádu, vysloví usnesením, že zákon porušen nebyl. I přesto, že zákon výslovně vyžaduje pouze dodržení podmínek § 88 odst. 1, je nutné vykládat jej spolu s dalšími odstavci, které konkretizují některé další podstatné okolnosti vztahující se k příkazu, prodlužování doby odposlechu, případné provádění odposlechu se souhlasem uživatele odposlouchávané stanice apod. To podle Šámala "*vyplývá i z toho, že v § 314m odst. 1 žádný odkaz na příslušný odstavec § 88 uveden není, a proto je možno vyslovit porušení zákona z hlediska celé zákonné úpravy příkazu a provedení odposlechu a záznamu*".[189] Nebylo by tedy možné vyslovit zákonnost odposlechu v případě, kdy by např. doba trvání odposlechu byla v příkazu stanovena na delší dobu než čtyři měsíce (srov. § 88 odst. 2). Podobně je tomu také u příkazu k zjištění údajů o telekomunikačním provozu, kde § 314n odst. 1 vyžaduje k zákonnosti příkazu pouze soulad s podmínkami uvedenými v § 88a odst. 1, nicméně podstatné okolnosti vztahující se k příkazu a jeho provedení jsou uvedeny i v odstavci 4 podle kterého *„příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat."* Proto je nutné § 88a odst. 1 vykládat i ve spojení s ustanovením odstavce 4 § 88a, což vyplívá i ze skutečnosti, že v § 314m odst. 1 žádný odkaz na příslušný odstavec § 88a uveden není, a je tedy možné vyslovit porušení zákona z hlediska celé úpravy § 88a.[190] O zákonnosti příkazu Nejvyšší soud vždy rozhoduje formou usnesení, proti němuž není přípustný žádný opravný prostředek, a to řádný ani mimořádný.

Situace, kdy NS shledá rozpor příkazu k odposlechu nebo zjištění údajů, je upravena v § 314m tr. řádu. V takovém případě Nejvyšší soud vysloví porušení zákona usnesením, proti kterému se stejně jako v případě vyslovení zákonnosti nelze bránit opravným prostředkem. Zákon přitom neupravuje žádné další podrobnosti rozhodování ani případný další postup a důsledky vyplívajících z uvedeného rozhodnutí. Zřejmé přitom je, že ani závěr o porušení zákona nemá vliv na již provedené dokazování za použití přezkoumávaného příkazu.[191]

[188] Jelínek, J. a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*, 6. vyd. Praha: Leges, 2016. s. 738
[189] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013.s. 3628
[190] Šámal, P. a kol. *Trestní řád: komentář*, 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013.s. 3628
[191] Fenyk, J., Gřivna, T., Císařová, D. *Trestní právo procesní*, 6., aktualiz. vyd. Praha: Wolters Kluwer, 2015. s. 798

Pozitivní usnesení o porušení zákona má tedy v podstatě pouze deklaratorní charakter, neboť nemá přímý vliv na meritorní rozhodnutí v dané věci.[192]

6.2. Náhrada škody způsobené nezákonným odposlechem

V souvislosti se zmíněným usnesením Nejvyššího soudu o porušení zákona v řízení o přezkumu příkazu dle § 314l - § 314n tr. řádu, se dále krátce věnuji možnému vymáhání náhrady škody, pro něž je předmětné deklaratorní rozhodnutí zásadní. Náhrada škody způsobené nezákonným rozhodnutím nebo nesprávným úředním postupem je na ústavní úrovni garantována čl. 36 odst. 3 Listiny, na zákonné úrovni zákonem č. 82/1998 Sb., o odpovědnosti státu za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem (dále jen OdpŠk), který dále provádí nařízení vlády ČR č. 116/1998 Sb.

Stát podle tohoto zákona odpovídá za škodu, která byla způsobena rozhodnutím vydaným v občanském soudním řízení, ve správním řízení, v řízení podle soudního řádu správního a v trestním řízení, přičemž se musí jednat o rozhodnutí nezákonné. Za to se v souladu s § 8 odst. 1 OdpŠk považuje takové pravomocné rozhodnutí, které bylo pro nezákonnost (zejm. v důsledku podání mimořádného opravného prostředku, ale též ústavní stížnosti[193]) zrušeno nebo změněno příslušným orgánem, přičemž takovým rozhodnutím je soud rozhodující o náhradě škody v civilním řízení vázán. *„Judikatura civilních soudů ovšem (správně) dospěla k závěru, že stejný význam může mít i pouhý tzv. akademický výrok Nejvyššího soudu ke stížnosti pro porušení zákona, že byl porušen zákon, aniž by současně došlo ke zrušení rozhodnutí (nebylo-li možno rozhodnutí zrušit, neboť zákon byl porušen ve prospěch obviněného - § 268 odst. 2 a § 269).“*[194]

K povaze nezákonného rozhodnutí se vyjádřil Nejvyšší soud ve svém rozhodnutí sp. zn. 30 Cdo 4286/2013 kterým rozhodoval o dovolání žalobce, domáhajícího se náhrady škody, jež mu měla být způsobena mimo jiné také provedením odposlechu jeho telefonních hovorů. Nejvyšší soud v citovaném rozhodnutí uvedl, že „*nezákonným rozhodnutím ve smyslu zákona č. 82/1998 Sb., je též rozhodnutí orgánu činného v trestním řízení, jehož nezákonnost byla deklarována v rozsudku Nejvyššího soudu vydaného na základě stížnosti pro porušení zákona, aniž zároveň došlo ke zrušení takového rozhodnutí. Rovněž deklaratorní rozhodnutí je tudíž způsobilé naplnit podmínku dle ustanovení § 8 odst. 1 OdpŠk, tudíž daný závěr lze vztáhnout i*

[192] Šámal, P., Musil, J., Kuchta, J. *Trestní právo procesní*, 4., přeprac. vyd. Praha: C. H. Beck, 2013. s. 888
[193] Jelínek, J. a kol. *Trestní právo procesní*, 4. vyd. Praha: Leges, 2016. s. 778
[194] Jelínek, J. a kol. *Trestní právo procesní*, 4. vyd. Praha: Leges, 2016. s. 778, poznámka pod čarou č. 5

na rozhodnutí dle ustanovení § 314m tr. řádu." Je přitom povinností žalobce prokázat existenci tohoto deklaratorního rozhodnutí. Je tedy nezbytným předpokladem, aby byla rozhodnutím Nejvyššího soudu deklarována nezákonnost vydání příkazu nebo provedení odposlechu dle § 314l a násl. trestního řádu. Pokud by žalobce nemohl uplatnit postup dle § 314l a násl. tr. řádu., např. z důvodu, že v rozporu s § 88 odst. 8 a 9 tr. řádu nebyl o odposlechu řádně informován, šlo by zde o nárok odvozovaný od nesprávného úředního postupu, nikoli odvozovaný od nezákonného rozhodnutí.[195]

6.3. Stálá komise pro kontrolu použití odposlechů

Další prostředek kontroly v oblasti odposlechů představuje *Stálá komise pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací* (dále jen „Komise"). Ta je jednou z komisí zřízených Poslaneckou sněmovnou na základě jejího jednacího řádu, který umožňuje Poslanecké sněmovně ze svých poslanců a dalších osob, které nejsou poslanci, zřizovat stálé nebo dočasné komise a stanovit jim v rámci své působnosti úkoly. Předsedou komise je vždy poslanec, kterého volí Sněmovna[196] a kterým je v současné době pro Komisi poslanec Daniel Korte. Komise byla zřízena dne 10. 12. 2013 na 4. schůzi Poslanecké sněmovny jejím usnesením a na stejné schůzi byl usnesením schválen také Statut Komise. Činnost Komise tedy probíhá v souladu se zákonem o Policii, Jednacím řádem Poslanecké sněmovny a Statutem Komise.[197]

Dle § 98 odst. 1 PolČR. *„Kontrolu použití odposlechu a záznamu telekomunikačního provozu a použití sledování osob a věcí podle jiného právního předpisu a rušení provozu elektronických komunikací vykonává Poslanecká sněmovna, která k tomu účelu zřizuje kontrolní orgán. Kontrolní orgán se skládá z poslanců určených Poslaneckou sněmovnou."* Činnost Komise tedy spočívá na rozdíl od předchozí úpravy obsažené v zákoně č. 283/1991 Sb., o Policii České republiky, již nejen v kontrole odposlechu a záznamu telekomunikačního provozu a použití sledování osob a věcí podle tr. řádu, ale také v kontrole nového institutu rušení provozu elektronických komunikací. Naopak oproti úpravě platné do novely provedené zákonem č. 341/2011 Sb. o Generální inspekci bezpečnostních sborů a změně některých zákonů

[195] Rozhodnutí Nejvyššího soudu sp. zn. 30 Cdo 4286/2013 ze dne 4. 12. 2014

[196] Zákon č. 90/1995 Sb. ze dne 19. dubna 1995 o jednacím řádu Poslanecké sněmovny, § 47 – Komise sněmovny

[197] Zpráva o činnosti Stálé komise PS pro kontrolu použití odposlechů, záznamů telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací z roku 2016, dostupná online na webových stránkách Poslanecké sněmovny Parlamentu ČR

(dále jen „Zákon o GIBS“), se již nepočítá s kontrolou činnosti Inspekce policie, když v důsledku zmíněného zákona došlo k jejímu zrušení.

6.3.1. Kontrolní mechanismy Komise

Samotná kontrola pak může mít celou řadu podob. Zákon o Policii ČR ukládá v § 98 odst. 2 povinnost ministru vnitra předložit Komisi minimálně dvakrát ročně *zprávu o použití prostředků odposlechu, sledování osob a věcí, a rušení provozu elektronických komunikací*. Zprávu vypracovává přímo Útvar zvláštních činností, který ji následně předává ministrovi, který zprávu předkládá Komisi.

Komise vedle toho může využít svého práva a vyžádat si od ministra další informace o využití těchto prostředků. Podle § 98 odst. 3 PolČR ministr jednou ročně předkládá *analýzu použití úkonů odposlechu, sledování osob a věcí, a rušení provozu elektronických komunikací,* a to příslušnému výboru Poslanecké sněmovny a Komisi.

Dále disponuje Komise oprávněním požadovat informace a účast na jejích jednáních od jiných osob, jako jsou např. policisté, ale i civilní osoby a po předchozím vyrozumění ministra vnitra může zvolit kontrolu přímo prostřednictvím návštěvy příslušného ÚZČ. Vzhledem k tomu, že novelou provedenou zákonem č. 64/2014 Sb., kterým se mění některé zákony v souvislosti s přijetím kontrolního řádu, bylo do PolČR vloženo ustanovení, dle kterého se na postup Komise nepoužije kontrolní řád, samotný postup těchto kontrol tak není zákonem nikde upraven.[198] Dle důvodové zprávy k této novele z roku 2014 je tomu tak proto, že se *„jedná o zcela specifický druh kontroly vykonávaný orgánem moci zákonodárné vůči orgánu moci výkonné”*[199] Podle Zprávy o činnosti Komise za rok 2016 kontrola probíhá u náhodně vybraných případů ze Zprávy Policie ČR o použití odposlechu a z výroční Informace pověřených celních orgánů o použití odposlechu a dále na základě podnětů – žádostí fyzických i právnických osob o prověření domnělého odposlechu. V roce 2016 v žádném z kontrolovaných případů nebylo zjištěno porušení zákona ze strany Policie ČR a žadatelé o kontrole byli v tomto smyslu informováni.[200]

[198] Vangeli, B. *Zákon o Policii České republiky: komentář*. 2. vyd. Praha: C. H. Beck, 2014. Beckovy komentáře. s. 379-380

[199] Důvodová zpráva k zákonu č. 64/2014 Sb., kterým se mění některé zákony v souvislosti s přijetím kontrolního řádu

[200] Zpráva o činnosti Stálé komise PS pro kontrolu použití odposlechů, záznamů telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací za rok 2016

Zajímavou možností kontroly je dle mého názoru kontrola podle ustanovení § 10 odst. 2 již zmíněné prováděcí vyhlášky k ZoEK č. 336/2005, podle které „*provozovatel komunikační sítě po dobu šesti měsíců uchovává za účelem kontroly pokyny k aktivaci a deaktivaci odposlechu a informace o jejich provedení, a to způsobem nedovolujícím jejich změnu.*“ Toto ustanovení tak umožňuje Komisi provádět kontrolu přímo v součinnosti s provozovatelem komunikační sítě, od kterého si může vyžádat údaje o pokynech k aktivaci či deaktivaci odposlechu ze strany Útvaru zvláštních činností. Tímto způsobem Komise patrně může i prověřit údaje, které již obdržela od ÚZČ za účelem potvrzení jejich správnosti.

7. Úvahy de lege ferenda

Na základě poznatků prezentovaných v této práci jsem dospěla k názoru, že právní úprava odposlechu a záznamu telekomunikačního provozu vykazuje určité nedostatky, které by bylo na místě zákonodárcem zvážit a případně dát prostor k diskuzi o novelizaci trestního řádu. Tyto nedostatky neshledávám pouze u institutu odposlechu, nýbrž také u institutu zjišťování údajů o telekomunikačním provozu a u blízkého institutu sledování osob a věcí, kterým se práce z důvodu úzké spojitosti také částečně věnovala.

Ve své práci jsem se mimo jiné zabývala terminologií trestního řádu, konkrétně legálním spojením *telekomunikačního provozu*, se kterým trestní řád v § 88 stejně jako v § 88a pracuje, a to i přesto, že tento termín je v současné době již překonaný. Ke změně v terminologii došlo přijetím zákona č. 127/2005 Sb., o elektronických komunikacích, v reakci na schválení nového regulačního rámce EU, jež definitivně opustil pojem telekomunikace a nahradil je podstatně širším pojmem elektronických komunikací. Ty zahrnují kromě klasických telekomunikačních služeb i nové druhy komunikací, jako jsou např. služby pronájmu okruhů, mobilní sítě, ISDN a služby Internetu. ZoEK se vyrovnává s terminologií typickou pro předešlou právní úpravu, (mj. i s pojmem telekomunikačního provozu), a jejím používáním ve zvláštních předpisech jako je mj. trestní řád, ve svých přechodných ustanoveních, podle kterých *„Obsahuje-li zvláštní právní předpis ustanovení o telekomunikačním provozu, rozumí se tím přenášená zpráva podle tohoto zákona.“* V případě, že obsahuje zvláštní právní předpis ustanovení o údajích o telekomunikačním provozu *„rozumí se jím provozní a lokalizační údaje související s přenášenou zprávou podle tohoto zákona.“*

Na základě ZoEK a prováděcích předpisů k němu došlo tedy k nahrazení pojmu telekomunikací a souvisejících pojmů, a to obsahově širším pojmem elektronických komunikací. Domnívám se, že zákonodárce by měl tuto změnu reflektovat a novelizovat znění § 88 a § 88a tr. řádu nahrazením zastaralých pojmů výrazy současně platnými. Název § 88 tr. řádu by dle mého názoru měl znít:

„Odposlech a záznam elektronických komunikací“, případně:
„Odposlech a záznam přenášené zprávy elektronických komunikací“

V případě § 88a tr. řádu se domnívám, že by bylo vhodné zavést název:
„Zjištění provozních a lokalizačních údajů souvisejících s přenášenou zprávou“

Ačkoli hlavním tématem mé práce nebyl rozbor operativně pátracího prostředku sledování osob a věcí, částečně jsem se v druhé kapitole tomuto institutu věnovala, a to z důvodu některých společných znaků se zajišťovacími instituty upravenými v § 88 a § 88a tr. řádu.

V rámci provedené komparace zmíněných institutů jsem se mimo jiné zabývala povolovacím režimem sledování osob a věcí, při kterém mají být pořizovány obrazové, zvukové nebo jiné záznamy podle § 158d odst. 2 tr. řádu. Tento typ sledování podléhá schválení státního zástupce a nikoli soudce, jako je tomu u zajišťovacích institutů odposlechu a zjišťování údajů, a to i přesto, že oba instituty představují srovnatelně závažný zásah do soukromí občanů. V praxi taková úprava může dle mého názoru vést k nadužívání tohoto institutu stejně jako k rezignaci policejního orgánu na klasickou operativní činnost při vyhledávání, objasňování a vyšetřování trestných činů. Vzhledem k závažnosti zásahu do soukromí, jež tento typ sledování představuje, by jeho povolování, stejně jako dohled nad samotným prováděním, neměl být dle mého názoru výlučně v rukou státního zástupce stojícího na straně obžaloby a policie jako vyšetřovacího orgánu. Svěřením povolování do výlučné pravomoci soudu by sice došlo k většímu formalismu tohoto typu sledování, zároveň by však taková změna zvýšila garanci zákonnosti tohoto zásahu do práv občanů a zajistila nad ním náležitý dohled. V této věci již jednala *Stálá komise pro kontrolu použití odposlechů*, která vydala 23. 2. 2017 usnesení, ve kterém žádá vládu, aby předložila návrh zákona, který bude obsahovat změnu trestního řádu, a to tak, aby bylo vypuštěno oprávnění státního zástupce udělovat policejnímu orgánu písemné povolení ke sledování osob a věcí, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy podle § 158d odst. 2. tr. řádu, a aby tato pravomoc byla svěřena výlučně soudu. Podle Komise neexistuje důvod, proč by měla v tomto směru existovat odlišná úprava povolovacího režimu 158d odst. 2 tr. řádu a § 88 a § 88a tr. řádu. S tímto názorem Komise souhlasím a taktéž se domnívám, že by bylo vhodné povolovací režim sledování podle § 158d odst. 2 svěřit do výlučné pravomoci soudu a změnit ustanovení předmětné následovně:

„*Sledování, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy, lze uskutečnit pouze na základě předchozího písemného povolení soudce.“*

Úprava povolovacího režimu dle mého názoru není vyhovující ani v případě sledování, při kterém má být zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků podle § 158d odst. 3 tr. řádu. Sledováním podle § 158d odst. 3 tr. řádu dochází stejně

jako v případě provádění odposlechu podle § 88 tr. řádu k zásahu do základních práv, zejména k zásahu do práva na ochranu soukromí, k zásahu do listovního tajemství a mimo to může dojít také k zásahu do nedotknutelnosti obydlí. V obou případech se tedy zjevně jedná o srovnatelný zásah do práv a svobod občanů, v případě sledování se v určitých případech může jednat dokonce o zásah závažnější (např. pokud je nasazen prostorový odposlech v obydlí osoby, dochází tak nejen k zásahu práva na soukromí, ale také k zásahu do nedotknutelnosti obydlí). Proto není zřejmé, z jakého důvodu úprava § 158d odst. 3 postrádá ve srovnání s povolovacím režimem odposlechu určité záruky zákonnosti tohoto zásahu do základních práv. Předmětnými zárukami jsou zejména stanovení okruhu trestné činnosti určitého stupně závažnosti, která odůvodňuje případný zásah do soukromí, listovního tajemství, či jiného zasaženého práva. Ačkoli v případě provádění odposlechu trestní řád takový okruh trestné činnosti vymezuje, v případě sledování tomu tak není. Taková situace je dle mého názoru bez důvodu neproporční a úlohou zákonodárce by mělo být změnit ustanovení trestního řádu tak, aby srovnatelným zásahům do práv a svobod občanů odpovídaly srovnatelné záruky a podmínky jejich provedení. Povolení sledování podle § 158d odst. 3 není dále podmíněno, tak jak je tomu v případě odposlechu, splněním zásady subsidiarity, tedy skutečností, že sledovaného účelu nelze dosáhnout jinak, nebo by jeho dosažení jiným způsobem bylo podstatně ztížené. Ani absence této podmínky přitom není vysvětlena v důvodové zprávě k trestnímu řádu a není zjevné, z jakého důvodu ustanovení zásadu subsidiarity opomíjí. V neposlední řadě ustanovení neobsahuje podmínku, podle které by šlo stejně jako u odposlechu ke sledování přistoupit pouze v případě, kdy by bylo možné důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení uvedené zejména v § 89 odst. 1 písm. a) až c) tr. řádu. Osobně za řešení zaručující dostatečnou ochranu základním lidským právům považuji povolování sledování osob a věcí za použití § 88 odst. 1 tr. řádu *per analogiam*, tedy za splnění podmínek uvedených v § 88 odst. 1 tr. řádu. V budoucnu by přitom bylo na místě, aby zákonodárce zvážil změnu ustanovení § 158d odst. 3 a omezující podmínky do ustanovení vtělil. Znění ustanovení § 158d odst. 3 by následně mohlo být:

„Pokud má být sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků, lze je uskutečnit jen je-li vedeno trestní řízení pro zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, 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,

zjednání 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 pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Příkaz může být vydán pouze na základě předchozího povolení soudce v případě, kdy lze důvodně očekávat, že jím budou získány významné skutečnosti pro trestní řízení a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené. Při vstupu do obydlí nesmějí být provedeny žádné jiné úkony než takové, které směřují k umístění technických prostředků.“

Za uvážení by dle mého názoru stálo taktéž sjednocení maximální možné délky doby sledování podle § 158d odst. 2 a odst. 3, jež může být podle současné úpravy stanovena maximálně na šest měsíců, ačkoli není zřejmé, z jakého důvodu je tato doba stanovena mírněji než v případě zajišťovacího prostředku odposlechu podle § 88 tr. řádu, který lze nařídit vždy nejvýše na dobu čtyř měsíců.

V rámci rozboru technické realizace odposlechu jsem se zaobírala také otázkou šifrace dat jako potenciální překážkou úspěšného provedení obou zajišťovacích úkonů podle § 88 a § 88a tr. řádu. Šifrování dat dle mého názoru představuje zásadní problém, a to vzhledem k neexistenci právní úpravy, která by odpovídajícím způsobem na tento druh „utajení“ dat jejich převedením do nečitelné podoby s možností jejich odtajněním pouze za pomoci dešifrovacího klíče reagovala. Právní úprava sice ukládá povinnost odtajnit šifrovaná data provozovatelům elektronických komunikací, nicméně nepamatuje na samotné dodavatele různých druhů elektronických komunikací, jako jsou např. dodavatelé aplikačních služeb jako je Whatsapp, Viber, apod. Právě dodavatelé komunikačních služeb jsou přitom zejména ti, kteří data šifrují. Vzhledem k tomu, že dodavatelé nemají zákonnou povinnost poskytnout policejnímu orgánu dešifrovací klíč a provozovatel elektronické komunikace s ním ve většině případů nedisponuje, dostává se policejní orgán do situace, kdy buď může spoléhat na dobrovolné poskytnutí šifrovacích klíčů ze strany dodavatelů, případně se může pokusit poskytnutá data dešifrovat sám prostřednictvím vlastních metod. Domnívám se, že předmětná situace není vhodná a zákonodárce by měl proto po vzoru některých zahraničních právních úprav stanovit pravidla pro spolupráci subjektů disponujících s dešifrovacím klíčem s policejním orgánem (příp. dalších oprávněných orgánů) a zároveň stanovit sankce za porušení takové povinnost spolupráce v trestním řízení. Jako inspirace úpravy, která se mi jeví vhodná, mi v předkládané práci posloužila britská úprava obsažena v zákoně o regulaci vyšetřovacích pravomocí

(*„Regulation of Investigatory Powers Act“*). Předmětný zákon upravuje pravomoc vyšetřovacích orgánů vyžádat v případě šifrace dat potřebných pro vyšetřování klíč k jejich dešifraci. Tato pravomoc a jí odpovídající povinnost subjektů disponujících s daným klíčem přitom není, jako je tomu v případě naší legislativy, omezena pouze na provozovatele elektronických sítí. V případě, kdy k poskytnutí povinným subjektem nedojde dobrovolně, dopouští se navíc trestného činu. Považuji v tomto ohledu za důležité, že britská úprava současně stanoví mantinely korigující zásah do práva na soukromí, ke kterému tímto postupem dochází. Zejména vymezuje situace, za kterých je možno dešifrovací klíč vyžadovat (jedná se o situace, kdy je získání dat nezbytné v zájmu národní bezpečnosti, ekonomického blahobytu nebo v zájmu prevence a odhalení trestné činnosti), dále možnost vyžadovat odtajnění šifrovaných dat pouze v případě, kdy tato data byla získána v souladu se zákonem a v neposlední řadě úprava stanoví náležitosti příkazu k takovému odtajnění.

Dle mého názoru by bylo vhodné po vzoru zmíněné britské úpravy stanovit povinnost odtajnění komunikace poskytnutím dešifrovacího klíče nebo jiným způsobem na vyžádání policejního orgánu, i jiným subjektům (než pouze provozovatelům elektronických komunikací), u kterých typicky k šifraci dochází. V případě zavedení takové úpravy považuji zároveň za vhodné stanovit rozumné mantinely stanovení dešifrovací povinnosti, jako je např. zásada subsidiarity vyžádání takových údajů.

Ve své práci jsem rozebrala také kontrolu v oblasti odposlechů, která je svěřena samotným soudům disponujícím uvážení při povolení každého konkrétního odposlechu či zjištění údajů, dále Nejvyššímu soudu v rámci přezkumu příkazů k úkonům upraveným § 88 a § 88a tr. řádu, a v neposlední řadě také *Stálé komisi pro kontrolu použití odposlechů*, jejichž činnost je vykonávána nezávisle podle vnitřních předpisů, Jednacího řádu Poslanecké sněmovny a PolČR. Úprava kontroly v této oblasti mi přijde dostačující.

Závěr

Svou diplomovou práci jsem pojala jako rozbor nejen účinné právní úpravy, nýbrž i jejího vývoje. V první kapitole jsem se věnovala vztahu zajišťovacích institutů odposlechu a zjištění údajů k základním právům, do nichž je těmito úkony zasahováno. Dále jsem detailně analyzovala současnou právní úpravu obou těchto zajišťovacích úkonů, podmínky jejich provedení, a jejich následné využití jako důkazů v rámci trestního řízení. Z důvodu podobnosti s operativně pátracím prostředkem sledování osob a věcí, upraveným v § 158d tr. řádu, jsem v samostatné kapitole provedla komparaci všech tří institutů. Dále jsem se zabývala povolovacím režimem sledování, který je v určitých ohledech mírnější než povolovací režim stanovený pro postup podle § 88 a § 88a tr. řádu, a to i přesto, že se v některých případech jedná o srovnatelný zásah do základních práv občanů.

V práci jsem se dále věnovala procesu realizace obou zajišťovacích úkonů ve světle tr. řádu, zákona o elektronických komunikacích a prováděcích předpisů k tomuto zákonu. V rámci analýzy realizace odposlechu a zjišťování údajů jsem provedla rozbor některých stěžejních pojmů, jako je telekomunikační provoz, elektronické komunikace apod. Na úvod své práce jsem si dala za cíl tímto postupem zjistit, jaké druhy komunikací mohou být v dnešní době odposlouchávány a zdali současná právní úprava odráží technický pokrok v oblasti elektronických komunikací a s ním související nové druhy a formy způsobu přenosu zpráv. Na základě rozboru příslušných předpisů jsem dospěla k závěru, že odposlech, stejně jako zjištění údajů o telekomunikačním provozu, je z právního hlediska reálný u jakéhokoli druhu elektronické komunikace. Znění právní úpravy nijak nebrání odposlechu moderních druhů komunikací, a naopak zůstává prostřednictvím úpravy jednotlivých pojmů otevřeno jejich rozvoji a formám novým. I přesto v praxi může docházet k situacím, kdy zaznamenaná data nejsou tzv. čitelná, a to z důvodu šifrace. Vzhledem k tomu, že dešifrovací postupy, které Útvar zvláštních činností u jednotlivých typů komunikací využívá, včetně jejich potenciální úspěšnosti, jsou z pochopitelných důvodů v režimu utajení, nebylo v mých možnostech zjistit formy a úspěšnost dešifrace dat u konkrétních forem komunikace. V rámci dostupné literatury jsem se věnovala otázce šifrování a odposlechu vč. zjišťování dat na sociálních sítích. Dospěla jsem k závěru, že rozhodné u přenosu informací v rámci této formy komunikace je nastavení přístupnosti profilu na sociální síti jejím uživatelem, prostřednictvím něhož uživatel určuje charakter sítě buďto jako veřejné, nebo jako soukromé. V případě nastavení profilu jako veřejného lze dle mého názoru data uživatele zajišťovat bez nutnosti postupu podle § 88 a § 88a tr. řádu, zatímco v opačném případě, tedy v případě nastavení profilu jako soukromého, kdy

dochází ke sdílení informací pouze s limitovaným okruhem osob, se již patrně jedná o zásah do tajemství zpráv a postup dle § 88, případně § 88a tr. řádu, je nutný.

Ve své práci jsem rozebrala také kontrolu v oblasti odposlechů, která je svěřena soudům disponujícím uvážením při povolení každého konkrétního odposlechu či zjištění údajů, dále Nejvyššímu soudu v rámci přezkumu příkazů k úkonům upraveným v § 88 a § 88a tr. řádu, a v neposlední řadě také Stálé komisi pro kontrolu použití odposlechů, jejichž činnost je vykonávána nezávisle podle vnitřních předpisů, Jednacího řádu Poslanecké sněmovny a zákona o Policii. Úprava kontroly v této oblasti mi přijde dostačující. Zároveň ji však vnímám jako nástroj relativně jednoduše zneužitelný, jelikož, jak jsem se přesvědčila při studiu tohoto tématu, většina postupů v rámci kontroly zůstává utajena a veřejnosti nepřístupná.

Seznam zkratek

ESLP – Evropský soud pro lidská práva

Jednací řád Poslanecké sněmovny - zákon č. 90/1995 Sb. o jednacím řádu Poslanecké sněmovny

Komise/Kontrolní komise – Stálá komise pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací

LZPS – 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

OČTŘ – orgán činný v trestním řízení

Odposlech/aktivní odposlech – Odposlech a záznam telekomunikačního provozu podle § 88 tr. řádu

PolČR, Zákon o Policii – zákon č. 273/2008 Sb., o Policii České republiky

Poslanecká sněmovna/PS – Poslanecká sněmovna Parlamentu České republiky

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

Směrnice o data retention - směrnice Evropského parlamentu a Rady č. 2006/24/ES o uchovávání údajů z roku 2006

StB – útvar Státní bezpečnosti fungující v letech 1945-1990

TČ – trestný čin

TOS – trest odnětí svobody

TrZ/Tr. zákoník – zákon č. 40/2009Sb., trestní zákoník

TrŘ/Tr. řád – zákon č. 141/1961Sb., trestní řád

ÚZČ – Útvar zvláštních činností služby kriminální policie a vyšetřování

ZoEK – zákon č. 127/2005Sb., o elektronických komunikacích

Zákon o telekomunikacích – zákon č. 110/1964Sb., o telekomunikacích

(nový) Zákon o telekomunikacích – zákon č. 151/2000Sb., o telekomunikacích

Zákon o odp. za škodu/OdpŠk – zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), v účinném znění

Zjištění údajů/zjišťování údajů/pasivní odposlech - zjištění údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat podle § 88a tr. řádu

Seznam pramenů a použité literatury

Literatura

- CAMPBELL, L. *Organised crime and the law: a comparative analysis*. Oxford: Hart publishing, 2013, 435 p. ISBN 9781849461221
- DRAŠTÍK, A., FENYK, J. a kol. *Trestní řád. Komentář. 1. díl.* Praha: Wolters Kluwer ČR, a.s., 2017, s. 1412 ISBN 978-80-7552-600-7
- FENYK, J., GŘIVNA, T., CÍSAŘOVÁ, D. *Trestní právo procesní*. 6. aktualiz. vyd. Praha: Wolters Kluwer, 2015, 848 s. ISBN 978-80-7478-750-8
- FENYK, J., HÁJEK, R., STŘÍŽ, I., POLÁK, P. *Trestní zákoník a trestní řád. 2. díl – Trestní řád.* Praha: Linde, 2010, ISBN 978-80-7201-803-1
- FRYŠTÁK, M. *Dokazování v přípravném řízení*. 2. vyd. Brno: Masarykova univerzita, 2015, 392 s. ISBN 978-80-210-7687-7
- FRYŠTÁK, M., POLIŠENSKÁ, P. *Dokazování v přípravném řízení: nejvýznamnější judikatura k vybraným tematickým okruhům*. Praha: Leges, 2014, 118 s. ISBN 978-80-87576-85-4
- JELÍNEK, J a kol. *Trestní právo procesní*. 4. vyd. Praha: Leges, 2016, 848 s. ISBN 978-80-7502-160-1
- JELÍNEK, J. a kol. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*. 6. vyd. Praha: Leges, 2016, 1280 s. ISBN 978-80-7502-106-9
- JELÍNEK, J., UHLÍŘOVÁ, M. *Obhájce v trestním řízení*. Praha: Leges, 2011, 416 s. ISBN 978-80-87212-88-2
- KMEC, J., KOSAŘ, D., KRATOCHVÍL, J., BOBEK, M. *Evropská úmluva o lidských právech: komentář*. 1. vyd., Praha: C.H. Beck, 2012, 1696 s. ISBN 978-80-7400-365-3
- KOENIG, Ch. et al. *EC Competition and Telecommunications Law*. Vol. 6. New York: Kluwer Law International, The Hague, 2002, 776 p. ISBN 9789041125644
- KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016, 522 s. ISBN 978-80-88168-15-7
- MOLEK, P. *Základní práva. Svazek první – Důstojnost.* Praha: Wolters Kluwer, 2017. 552 s. ISBN 978-80-7552-167-5

- NEJEDLÝ, J. *Zákonnost důkazů v trestním řízení ve světle Evropské úmluvy o ochraně lidských práv a základních svobod*. 1. vyd. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2013, 205 s. ISBN 78-80-87146-71-2
- PAVLÍČEK, V. a kol. *Ústavní právo a státověda*. 2. aktualizované vydání. Praha: Leges, 2015, 364 s. ISBN 978-80-7502-053-6
- POLČÁK, R., PÚRY, F., HARAŠTA, J. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, 253 s. ISBN 978-80-210-8073-7
- POVOLNÝ, D. *Operativní technika v rukou StB*. Praha: Úřad dokumentace a vyšetřování zločinů komunismu PČR, 2001, 111 s. ISBN 80-902885-3-7
- ŠÁMAL, P. a kol. *Trestní řád: komentář*. 7. dopl. a přeprac. vyd. Praha: C.H. Beck, 2013, 4720 s. ISBN 978-80-7400-465-0
- ŠÁMAL, P., MUSIL, J., KUCHTA, J. a kol. *Trestní právo procesní*. 4. přeprac. vyd. Praha: C.H. Beck, 2013, 1056 s. ISBN 978-80-7400-496-4
- ŠÁMAL, P., NOVOTNÝ, F., RŮŽIČKA, M., VONDRUŠKA, F., NOVOTNÁ, J. *Přípravné řízení trestní.* Praha: C.H. Beck, 2003. 1471 s. ISBN 80-7179-741-3
- ŠÁMAL, P., PÚRY, F., URBÁNEK, J. Vzory *podání a rozhodnutí v trestních věcech*. 3. přeprac. vyd. Praha: Linde, 2011, 767 s. ISBN 978-80-7201-829-1
- VANGELI, B. *Zákon o Policii České republiky*: komentář. 2. vyd. Praha: C.H. Beck, 2014, 488 s. ISBN 978-80-7400-543-5
- VANTUCH, P. *Obhajoba obviněného*. 3. dopl. a přeprac. vyd. Praha: C.H. Beck, 2010, 666 s. ISBN 978-80-7400-321-9
- VLACHOVÁ, B. *Zákon o elektronických komunikacích: komentář*. Praha: C.H. Beck, 2017. ISBN 978-80-7400-632-6.

Odborné články

- DURICA, J. *Právo na soukromí versus posílení bezpečnosti: směrnice o uchovávání údajů o telekomunikačním provozu v nálezech ústavních soudů členských států EU.* Bulletin advokacie, 6/2011, s. 19
- HARAŠTA, J., MYŠKA. M. *Budoucnost data retention*. Trestněprávní revue, 10/2015, s. 238

- HERANOVÁ. S. *Mezinárodní vědecká konference „Trestní právo procesní – minulost a budoucnost“.* Bulletin advokacie, 12/2016, dostupné na: http://www.bulletin-advokacie.cz/mezinarodni-vedecka-konference-trestni-pravo-procesni-minulost-a-budoucnost
- HERCZEG, J. *Ústavněprávní limity monitoringu telekomunikačního provozu; konflikt mezi bezpečností a svobodou*. Bulletin advokacie, 5/2010, s. 22
- HOŘÁK, J. *Právo na soukromí versus bezpečnost ve sjednocené Evropě: zamyšlení nad problematikou „data retention“*. Acta UniversitatisCarolinae, Iuridica, 1/2006, s. 81
- JAMBOROVÁ, K. *Provozní a lokalizační údaje, nález Ústavního soudu a § 88a TrŘ*. Trestněprávní revue, 3/2012, s. 61
- JELÍNEK, J. *Pojem trestného činu a kategorizace trestných činů*. Bulletin advokacie, 10/2009, s. 36
- JEŽEK, J. *K odposlechu advokáta*. Bulletin advokacie, 9/2008, s. 32
- KMEC, J. *Evropský soud pro lidská práva – duben 2017.* Soudní rozhledy, 6/2017, s. 211
- KODL, J., SMEJKAL, V., SOKOL, T. *Smíme šifrovat?.* CHIP, 5/1995, s. 30-32
- KODL, J., SMEJKAL, V., SOKOL, T. *Šifry, státní zájmy a lidská práva*. CHIP, 4/1995, s. 34-37
- MANDÁK, V. *Odposlech a záznam telekomunikačního provozu advokáta*. Bulletin advokacie, 3/1995, s. 21
- NOVÁK, J. *K uchovávání provozních a lokalizačních údajů v České republice ve světle rozhodnutí Soudního dvora Evropské unie.* Bulletin advokacie, 5/2015, s. 36
- NOVOTNÁ, J. *K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu*. Trestněprávní revue, 10/2003, s. 290
- SOKOL, T. *Odposlech*. Právní rádce, 1/2005, s. 4
- STUPKOVÁ, L. *Konference „Trestní právo procesní – minulost a budoucnost“.* Trestněprávní revue, 1/2017, s. 16
- ŠÁMAL, P. *Odposlech a záznam telekomunikačního provozu ve světle judikatury*. Soudní rozhledy, 3/2000, s. 67
- ŠEVČÍK, V. *Některé ústavní aspekty odposlechu a záznamu telekomunikačního provozu* (dvě části - část prvá). Bulletin advokacie, 6-7/1996, s. 9
- TOMAN, P. *Náležitosti příkazu k odposlechu a záznamu telekomunikačního provozu.* Bulletin advokacie, 5/2017, s. 23

- VANTUCH, P. *Nezákonný odposlech advokáta*. Bulletin advokacie, 3/2008, s. 15
- VANTUCH, P. *Nová úprava odposlechu v trestním řádu od 1. 7. 2008*. Bulletin advokacie, 10/2008, s. 28

Judikatura

- *Klass a ostatní proti Německu*, č. 5029/79, rozsudek ESLP ze dne 6. září 1978
- *Malone v. Spojené království*, č. 8691/79, rozsudek ESLP ze dne 2. srpna. 1984
- *Schenk proti Švýcarsku,* č. 10862/84, rozsudek ESLP ze dne 12. července 1988
- *Lüdi proti Švýcarsku*, č. 12433/86, rozsudek ESLP ze dne 15. 6. 1992
- Usnesení Nejvyššího soudu sp. zn. Tzn 24/95 ze dne 27. 7. 1995
- Nález Ústavního soudu sp. zn. III. ÚS 83/1996 ze dne 25. 9. 1996
- Usnesení Nejvyššího soudu sp. zn. 7 Tz 9/2000 ze dne 15. 12. 2000
- Usnesení Vrchního soudu v Praze sp. zn. 4 To 3/01 ze dne 18. 1. 2001
- Nález Ústavního soudu sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001
- Nález Ústavního soudu sp. zn. IV. ÚS 536/2000 ze dne 13. 2. 2001
- Nález Ústavního soudu sp zn. IV. ÚS 78/01 ze dne 27. 8. 2001
- Rozhodnutí Vrchního soudu v Praze sp. zn. 7 To 117/2001 ze dne 5. 2. 2002
- Nález Ústavního soudu sp. zn. II. ÚS 615/2006 ze dne 23. 5. 2007
- Nález Ústavního soudu sp. zn. II. ÚS 789/06 ze dne 27. 9. 2007
- *S a Marper proti Spojenému království*, č. 30562/04, rozsudek ESLP ze dne 4. prosince 2008
- Nález Ústavního soudu sp. zn. II. ÚS 2048/09 ze dne 2. 11. 2009
- Rozsudek Spolkového ústavního soudu sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 ze dne 2. 3. 2010
- *Kennedy proti Spojenému království*, č. 26839/05, rozsudek ESLP ze dne 18. května 2010
- Usnesení Nejvyššího soudu sp. zn. 4 Pzo 1/2010 ze dne 14. 10. 2010
- Nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011
- Nález Ústavního soudu sp. zn. Pl. ÚS 42/2011 ze dne 20. 12. 2011
- Stanovisko trestního kolegia Nejvyššího soudu sp. zn. Tpjn 304/2012 ze dne 5. 6. 2013
- Usnesení Ústavního soudu sp. zn. III. ÚS 3812/12 ze dne 3. 10. 2013

- Rozsudek Soudního dvora (velkého senátu) ve spojených věcech C-293/12 a C-594/12 ze dne 8. dubna 2014
- Nález Ústavního soudu sp. zn. III. ÚS 3844/13 ze dne 30. 10. 2014
- Rozhodnutí Nejvyššího soudu sp. zn. 30 Cdo 4286/2013 ze dne 4. 12. 2014
- Usnesení Nejvyššího soudu sp. zn. 4 Pzo 10/2015 ze dne 20. 1. 2016
- Nález Ústavního soudu sp. zn. III. ÚS 3457/2014 ze dne 26. 4. 2016
- Usnesení Nejvyššího soudu sp. zn. 4 Pzo 14/2016 ze dne 15. 11. 2016
- *Matanovic proti Chorvatsku*, č. 2742/12, rozsudek ESLP ze dne 4. dubna 2017

Právní předpisy

- Vídeňská úmluva o smluvním právu (č.15/1988 Sb.)
- Vyhláška ministra zahraničních věcí č. 32/1955 Sb. o Úmluvě o zabránění a trestání zločinu genocidia
- Směrnice Evropského parlamentu a Rady č. 2014/41 ze dne 3. dubna 2014 o evropském vyšetřovacím příkaze ve věcech trestních
- Směrnice Evropského parlamentu a Rady č. 2006/24/ES o uchovávání údajů
- Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění účinném od 1. 3. 2015
- Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění účinném od 18. 3. 2017 do 30. 6. 2017
- Zákon č. 110/1964 Sb., o telekomunikacích, ve znění účinném od 1. 4. 1995 do 30. 6. 2000
- Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění účinném od 1. 1. 2016
- Zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění účinném od 1. 1. 2014
- Nařízení vlády ČR č. 116/1998 Sb., kterým se provádí zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem
- (nový) Zákon č. 151/2000 Sb., o telekomunikacích, ve znění účinném od 1. 4. 2005 do 30. 4. 2005

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění účinném od 1. 10. 2016 do 30. 6. 2017
- Zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění účinném od 1. 7. 2016
- Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění účinném od 19. 9. 2016 do 30. 6. 2017
- Vyhláška č. 336/2005 Sb., o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění účinném od 18. 3. 2017 do 12. 8. 2017
- Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
- Zákon č. 273/2008 Sb., o Policii České republiky, ve znění účinném od 1. 1. 2017 do 30. 5. 2017

Další prameny

- Tajný rozkaz ministra vnitra, jehož obsahem je Směrnice o používání operativní techniky /A-oper-IX-1/ ze dne 27. prosince 1955.
- Důvodová zpráva k zákonu č. 178/1990 Sb.
- Důvodová zpráva k zákonu č. 292/1993 Sb.
- Důvodová zpráva k zákonu č. 265/2001 Sb.
- Důvodová zpráva k zákonu č. 127/2005 Sb., o elektronických komunikacích
- Odůvodnění vládního návrhu zákona, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), přednesené ministrem spravedlnosti JUDr. Jiřím Pospíšilem v Poslanecké sněmovně Parlamentu ČR při 1. čtení dne 9. 5. 2007
- Důvodová zpráva k zákonu č. 177/2008 Sb.
- Důvodová zpráva k zákonu č. 273/2008 Sb., o Policii České republiky
- Pokyn obecné povahy nejvyšší státní zástupkyně ze dne 21. září 2009, o trestním řízení
- Závazný pokyn policejního prezidenta č. 135/2010
- Důvodová zpráva k zákonu č. 459/2011 Sb.
- Důvodová zpráva k zákonu č. 273/2012 Sb.
- Stanovisko trestního kolegia Nejvyššího soudu, sp. zn. Tpjn 300/2012, č. 20/2013 Sb. tr. rozh.

- Závazný pokyn policejního prezidenta č. 103/2013
- Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek ze dne 26. ledna 2015, Nejvyšší státní zastupitelství, 1 SL 760/2014
- Zpráva o činnosti Stálé komise Poslanecké sněmovny pro kontrolu použití odposlechů, záznamů telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací za rok 2016
- Usnesení Stálé kontrolní komise pro kontrolu použití odposlechů a záznamů telekomunikačního provozu, sledování osob a věcí a rušení elektronických komunikací, č. 25 ze dne 23. února 2017, dostupné na: https://www.psp.cz/sqw/text/text2.sqw?idd=102715
- Tisková zpráva Nejvyššího státního zastupitelství ze dne 5. května 2017, dostupná na: http://www.nsz.cz/index.php/cs/aktuality/1880-nsz-rozhodlo-v-pipadu-podezeni-z-ovlivovani-svdk-a-podplaceni-tlumonika
- Stanovisko české advokátní komory k podezření k nezákonným odposlechům telefonických rozhovorů mezi obviněným a jeho obhájci, ze dne 14. 2. 2017, dostupné na: http://www.cak.cz/scripts/detail.php?id=17081

Wiretapping and Interception of communication

Abstract

This thesis analyzes legal framework as well as other issues regarding monitoring and intercepting the substance of communication under Section 88 of the Criminal Procedure Act. Also, the characteristics of logging and accessing data relating to communication (such as times, patterns, locations and parties involved) under Section 88a are described. These institutes in certain instances represent lawful interfere with the right to respect for private life and other human rights and both are of critical importance in the investigation of many types of crimes.

The thesis is systematically divided into seven chapters.

Chapter One presents both concepts in their relationship to the affected basic human rights and describes characteristics, major principles as well as the procedure of issuing a wiretap and data retention warrants.

As both concepts have similar features with conception of Surveillance of persons and items under the Section 158d of the Czech Criminal Procedure Act, comparison with this institute is provided in the second chapter.

The third Chapter is devoted to the evolution of Wiretapping legislation and its changes due to particular amendments. The first legal regulation of Wiretapping was adopted in the Czech Criminal Procedure Act in 1991 as a response to the political revolution followed by the need for explicit legislation providing human rights as well as conditions on which it is permitted to interfere with these rights.

Chapter Four focuses on performance of Wiretapping and data retention itself. Implementing legislation is particularly important at this stage. For better understanding, legal definitions of telecommunications, electronic communications and other terms used in relevant legislation are outlined. Topic of encrypting as a potential obstacle in obtaining information through the wiretapping and data retention is also presented.

The next chapter follows the topic of wiretapping of modern communications since it focuses on a specific kind of widely used communication form, social sites. It is evident that using different kinds of social networks where people can easily share not only private information, but also other content, can as well be used for criminal activities.

Control mechanisms as an important guaranty of legitimacy of wiretapping are analyzed in the sixth chapter. There are two main mechanisms in Czech legislation guarantying lawful conduct of wiretapping and data retention. Supreme Court examine the legality of the order for the interception and recording of telecommunication traffic upon a petition of the person whose communication was recorded. Another type of control comes under the competence of The

Permanent Commission established by the Chamber of Deputies and conducts general control over wiretapping and data retention.

Last chapter provides proposals for legislative improvement, which are based on the research conducted in this study.

Resumé

Diplomová práce se zabývá právní úpravou a související problematikou odposlechu a záznamu telekomunikačního provozu upraveného v § 88 tr. řádu jakožto i problematikou úzce souvisejícího institutu zjišťování údajů o telekomunikačním provozu upraveného ustanovením § 88a tr. řádu. Oba tyto zajišťovací instituty a zároveň významné způsoby získávání důkazů v rámci trestního řízení představují za splnění stanovených podmínek dovolený zásah do základního práva na respektování soukromého života a některých dalších základních práv.

Práce je systematicky rozdělena do sedmi kapitol.

Kapitola první se věnuje komplexnímu rozboru obou institutů z pohledu základních lidských práv, s nimiž přichází do konfliktu, detailní charakteristice, vůdčím principům a úpravě procedury nařizování odposlechu a zjištění údajů.

Vzhledem k řadě společných znaků, které zajišťovací úkony podle § 88 a § 88a tr. řádu vykazují ve vztahu k operativně pátracímu prostředku sledování osob a věcí podle § 158d tr. řádu, je v následující kapitole provedena komparace těchto institutů.

Třetí kapitola je věnována vývoji právní úpravy odposlechu a změnám, ke kterým došlo v rámci jednotlivých novelizací. První zákonná úprava odposlechu byla do trestního řádu zavedena v roce 1991, a to v důsledku politických změn vedoucích k potřebě výslovného zakotvení základních práv občanů, a podmínek, za nichž je možné do těchto práv zasahovat.

Čtvrtá kapitola se zaměřuje na analýzu postupu realizace odposlechu a zjištění dat obsaženého z velké části v prováděcích právních předpisech a interních aktech orgánů činných v trestním řízení. Pro lepší porozumění jsou rozebrány legální pojmy jako telekomunikace, elektronické komunikace a další související termíny užívané příslušnou legislativou. V předmětné kapitole je prezentováno také téma šifrování, představující potenciální překážku v získávání informací skrze odposlech a zjištění údajů.

Následující, pátá kapitola, volně navazuje na předešlou v tématu realizace odposlechu, nicméně již ve vztahu ke konkrétnímu typu přenosu informací skrze sociální sítě. Je zřejmé, že tento v současné době široce využívaný způsob komunikace, prostřednictvím něhož může docházet ke sdílení informací a dalších dat, může sloužit též k páchání trestné činnosti.

V šesté kapitole si kladu za cíl provést rozbor kontroly v oblasti odposlechu a zjišťování údajů jako stěžejního prvku garance zákonnosti prováděných odposlechů a zjišťování údajů o telekomunikačním provozu. Tento prvek je v rámci české legislativy zastoupen zejména kontrolou ze strany Nejvyššího soudu prováděné prostřednictvím řízení o přezkumu zákonnosti

příkazů k odposlechu či zjištění údajů a dále Stálou komisí pro kontrolu použití odposlechů, zřízenou Poslaneckou sněmovnou.

V poslední kapitole této práce se věnuji úvahám de lege ferenda, ke kterým jsem dospěla na základě provedené analýzy vybraného tématu.

Klíčová slova v češtině a angličtině

Odposlech / Wiretapping

Zjišťování údajů / Data retention

Elektronické důkazy / Electronic evidence