

Poř. č. 25/2002

Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů při výkonu působnosti státního zastupitelství k problematice způsobu zjišťování údajů z telekomunikačního provozu, zejména ke způsobu zjišťování místa pohybu a totožnosti pachatele trestného činu prostřednictvím údajů z mobilního telefonu

I. Údaje chráněné podle zákona č. č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů (telekomunikačního zákona), ve znění pozdějších předpisů, které jsou předmětem telekomunikačního tajemství jako data související s poskytováním telekomunikační služby, zejména údaje o účastnících telekomunikačního spojení (§ 84 odst. 3 písm. c) telekomunikačního zákona), anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat (§ 84 odst. 5 citovaného zákona), lze pro účely trestního řízení vyžadovat v přípravném řízení

a) na základě příkazu soudce podle 88a odst. 1 trestního řádu nebo – jde-li o sledování osob a věcí – na základě předchozího povolení soudce podle § 158d odst. 3 trestního řádu, nebo

b) postupem podle § 88a odst. 2 trestního řádu, tj. se souhlasem oprávněného uživatele telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat, pokud mají být tyto údaje získány ve vztahu k mobilnímu telefonu, který se dostal do moci třetí osoby jinak než s přivolením tohoto oprávněného uživatele mobilního telefonního přístroje. Stejně je třeba vykládat i podmínku výslovného souhlasu toho, do jehož práv a svobod má být sledováním zasahováno, uvedenou v ustanovení § 158d odst. 6 trestního řádu.

II. Údaje, které nejsou chráněny jako předmět telekomunikačního tajemství nebo jako osobní či zprostředkovací data, lze při sledování osob a věcí a pro jeho účely získávat se souhlasem státního zástupce udělovaným podle § 158d odst. 2 trestního řádu.

K obsahu jednotlivých podnětů k vydání stanoviska:

Nejvyšší státní zastupitelství obdrželo v posledním období několik podnětů, které se obsahově týkají podobné nebo totožné problematiky - způsobu zjišťování

údajů z telekomunikačního provozu, zejména zjišťování místa pohybu a totožnosti pachatele trestného činu prostřednictvím údajů z mobilního telefonu.

Základním problémem, který má být řešen, je zejména to, na základě jakého právního institutu, jenž je zakotven v trestním řádu, mají být tyto údaje vyžadovány. Tedy zda (kromě ustanovení § 88 tr. ř., kde zjišťování příslušných údajů tohoto charakteru bude zřejmě pravidlem) jím může být jen ustanovení § 88a tr. ř., nebo zda k tomu lze využít i ustanovení § 158d odst. 2 a odst. 3 tr. ř. o sledování osob a věcí, podle kterého lze takové údaje patrně také získávat, a pominout nelze ani případný vztah ustanovení § 47a zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, podle něhož je policie při sledování osob a věcí oprávněna žádat v rozsahu potřebném pro plnění konkrétního úkolu policie od právnických a fyzických osob, které zajišťují telekomunikační činnost, předávání dat souvisejících s poskytováním telekomunikační služby způsobem umožňujícím dálkový a nepřetržitý přístup, k trestnímu řádu, zvláště k ustanovení § 158d odst. 2 a odst. 3 tr. ř.

Dalším problémem úzce souvisejícím s těmito otázkami je otázka vymezení rozsahu údajů, které lze podřadit pod pojem „telekomunikační tajemství“ včetně výkladu obsahu ochrany osobních a zprostředkovacích dat z telekomunikačního provozu.¹ V jednotlivých podnětech byla tato problematika popsána následujícím způsobem:

Krajské státní zastupitelství v Ústí nad Labem požádalo o stanovisko k uplatňování ustanovení § 158d odst. 2 tr. ř. vzhledem ke způsobu zjišťování údajů z telekomunikačního provozu s poukazem na to, že v praxi policejních orgánů se vyskytl způsob podání podnětu podle tohoto ustanovení i v případech žádosti o aktivní nebo pasivní výpis volání, který lze nepochybně vyžadovat pouze postupem podle § 88a tr. ř. Policejní orgány se přitom řídí závazným pokynem Policejního prezidia ČR č. 149/2001.² Druhý problém, který se zde zmiňuje, je otázka správného postupu při zjišťování čísla IMEI v určitých dnech, tedy zjištění, jaké konkrétní telefonní číslo v určitých dnech bylo u daného telefonního přístroje používáno.³

¹ Samostatně byla ještě řešena otázka postupu při odposlechu a záznamu telekomunikačního provozu v době po přečíslování české veřejné telekomunikační sítě, k němuž má dojít plošně v době z 21. na 22. 9. tohoto roku. Žádost o stanovisko v této věci vneslo Městské státní zastupitelství v Brně s tím, že po přečíslování se změní formát telefonních čísel a vydané příkazy k odposlechu tak vlastně budou obsahovat jiné číslo (bude vypuštěna nula z předvolby příslušného operátora či telefonního obvodu nebo se číslo zcela změní). Tato změna by však neměla mít na platnost vydaných příkazů žádný vliv, protože jde o záležitost čistě technického charakteru. Proto bylo sděleno Městskému státnímu zastupitelství v Brně stanovisko Nejvyššího státního zastupitelství, že v daném případě nejsou dány důvody pro změnu původních příkazů k odposlechu a záznamu telekomunikačního provozu ani pro vydávání příkazů nových. To bylo zasláno na vědomí též oběma vrchním státním zastupitelstvím a Útvaru zvláštních činností Policie ČR.

² Závazný pokyn policejního prezidenta č. 149 ze dne 18. 12. 2001, kterým se upravuje postup při vyžadování použití sledování osob a věcí pro účely trestního řízení, byl uveřejněn v částce č. 180/2001 Sbírky interních aktů řízení Policejního prezidia ČR. V Příloze č. 3 tohoto závazného pokynu je předtištěn formulář nazvaný „Žádost o výpis aktivního a pasivního volání“, v něm se v úvodní části uvádí: „Pro plnění úkolů Policie České republiky v souladu s § 158d odst. 2 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a § 47a odst. 3 zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, vyžaduji výpis volání....“. V části VIII. se předpokládá, že tato žádost bude schválena státním zástupcem.

³ Oba problémy signalizovalo Okresní státní zastupitelství v Ústí nad Labem a k tomuto posledně zmíněnému uvádí: „...připojuji i tabulku, kterou centrum společnosti EUROTEL rozšířilo po svých regionálních střediscích a kde se vykládá trestní řád a to mnohdy nesprávně či nepřesně. Například kroužkem označená řádek „Určení čísla IMEI v určitých dnech“ zcela jistě automaticky podřadit pod

Obdobný problém řešilo již Vrchní státní zastupitelství v Olomouci⁴ a zaujalo k němu vlastní stanovisko. Podle něj je-li důvodem činnosti orgánů Policie ČR pouze identifikace pachatele trestného činu prostřednictvím mobilního telefonu, např. zjišťováním zda je mobilní telefon v provozu, kde se nachází a kdo je jeho současným držitelem, je na místě postup podle § 158d tr. řádu. Obecně je sice možno postupovat podle § 88a tr. řádu, toto ustanovení však v plném rozsahu dopadá pouze na údaje o telekomunikačním provozu již uskutečněném. Mají-li být však zjišťovány údaje, které umožní zjistit provoz a identifikaci přístroje, resp. jeho držitele v přítomnosti nebo v budoucnu a slouží toliko ke zjištění místa výskytu a pohybu mobilního telefonu a tím i totožnosti držitele přístroje, lze aplikovat postup podle § 158d tr. řádu. Za takové údaje je třeba považovat např. číslo SIM karty nebo IMEI, uživatelské telefonní číslo, apod. Za předpokladu, že vlastník přístroje dá souhlas ke zjištění uvedených údajů umožňujících identifikaci současného držitele, resp. místa jeho pohybu, poskytne policejním orgánům potřebná data, anebo dá souhlas k jejich obstarání, je možno postupovat podle § 158d odst. 6 tr. ř. a v takovém případě není zapotřebí souhlasu státního zástupce nebo soudce. Jinak je třeba postupovat podle § 158d odst. 3 tr. řádu a vyžádat předchozí povolení soudce.

Obstaráním a využitím těchto údajů při sledování by mohlo být zasaženo do tajemství zpráv podávaných telefonem (do něhož náleží též ochrana údajů o telekomunikačním provozu) ve vztahu k vlastníkovi přístroje a k jeho prolomení je proto namístež vyžádat souhlas soudce. Naproti tomu osoba, která není vlastníkem ani oprávněným uživatelem přístroje, tedy pachatel trestného činu, který se zmocnil přístroje proti vůli vlastníka, takové ochrany nepožívá. V případě aplikace § 158d odst. 3 tr. řádu ovšem nelze postupovat podle § 158d odst. 5 tr. řádu a zahájit sledování i bez povolení.

V prakticky shodné záležitosti předložil odbor bezpečnostní politiky Ministerstva vnitra dne 28. 5. 2002 analytickému a legislativnímu odboru Nejvyššího státního zastupitelství vlastní návrh stanoviska k zákonným možnostem Policie ČR získávat tzv. data související s poskytováním telekomunikační služby. Týká se sice v první řadě oprávnění policie uvedeného v ustanovení § 47a zákona o policii, ale souvisí úzce s touto problematikou a je do určité míry v protikladu s předchozími názory státních zastupitelství. Vychází z toho, že Policie ČR může získávat tzv. data související s poskytováním telekomunikační služby na základě dvou různých

pojmem sledování osob a věcí ve smyslu § 158d trestního řádu, např. v situaci, kdy policejní orgán údaj o konkrétním telefonním čísle potřebuje pro následný postup podle § 88, popř. § 88a trestního řádu nejde o případ sledování osob a věcí, nýbrž o prosté poskytnutí součinnosti v trestním řízení podle § 8 odst. 1 trestního řádu. V dané situaci totiž policejní orgán nežadá informaci o uskutečněném telekomunikačním styku a ani sám nehodlá realizovat nelegální odposlech příslušné telefonní stanice, dosud nesleduje ani konkrétní osobu, ani konkrétní věc a o žádném sledování nehodlá pořizovat žádný záznam.“.

⁴ Šlo o podnět OSZ v Bruntále a KSZ v Ostravě, podstatou byla otázka zjišťování pohybu a totožnosti pachatele trestného činu prostřednictvím údajů z odcizeného mobilního telefonu, který má pachatel u sebe. OSZ v Bruntále k konkrétní trestní věci obdrželo žádost Policie ČR, Služby kriminální policie a vyšetřování o udělení písemného povolení ke zjištění údajů telekomunikačního provozu podle § 158d odst. 2 tr. řádu. Prostřednictvím těchto údajů měla policie v úmyslu zjistit, zda je odcizený mobilní telefon používán a identifikovat tak pachatele tr. činu. Číslo SIM karty a výrobní číslo přístroje (IMEI) dal policii k dispozici majitel telefonního přístroje. OSZ Bruntál navrhovaný postup odmítlo a postupovalo podle § 88a odst. 1 tr. řádu podáním žádosti Okresnímu soudu v Bruntále. Krajské státní zastupitelství v Ostravě se v teoretické rovině s tímto postupem ztotožnilo s výhradou, že v dané konkrétní věci nebylo podání žádosti okresnímu soudu na místě, neboť bylo zřejmě účelnější opatřit souhlas majitele telefonu. KSZ v Ostravě v zásadě odmítá postup podle § 158d tr. řádu, neboť se jedná o zjišťování údajů související s telekomunikačním provozem a jediný možný je postup podle § 88a tr. řádu.

právních titulů - podle ustanovení § 47a odst. 3 zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, a podle ustanovení § 88a tr. ř. Ačkoli jde v obou případech o získání těchto údajů, jsou pokaždé získávány z jiného důvodu (pravděpodobně i v rozdílném rozsahu), proto se uvedená zákonná ustanovení nevyklučují, naopak se doplňují a stojí vedle sebe jako dvě autonomní oprávnění příslušných orgánů činných v trestním řízení. Oprávnění podle § 88a tr. ř. vylučně slouží k získání těchto údajů jako důkazů v trestním řízení (jež jsou získávány primárně za účelem objasnění skutečností důležitých pro trestní řízení). Ustanovení § 47a odst. 3 zákona o policii naproti tomu fakticky představuje technické oprávnění policie, které umožňuje získávat výše popsané údaje výhradně pro účely efektivní realizace trestně-procesního institutu sledování osob a věcí (srov. § 158b a 158d tr. ř.). V praxi jde zejména o případy, kdy policie s využitím těchto údajů monitoruje pohyb sledované osoby. Např. ztratí-li se sledovanou osobou kontakt, je možné s využitím údajů týkajících se provozu jejího mobilního telefonu s touto osobou kontakt obnovit a ve sledování úspěšně pokračovat. Tyto instituty (stejně jako data související s poskytováním telekomunikační služby získaná podle § 47a zákona o policii) neslouží primárně k získání informací důležitých pro trestní řízení, ale k bezproblémovému využívání trestně procesních institutů, které již tyto informace přinášejí. Vzhledem k charakteru oprávnění podle § 47a odst. 3 zákona o policii nepřichází žádný předběžný justiční souhlas v úvahu.

Analytický a legislativní odbor Nejvyššího státního zastupitelství k tomuto navrhovanému výkladu dodal, že samozřejmě obě úpravy mají svůj samostatný okruh společenských vztahů, v nichž se uplatňují (úprava v trestním řádu v trestním řízení a úprava v zákoně o policii při činnostech podle zákona o policii v rozsahu vymezeném v daném ustanovení), ale nelze zcela vyloučit, že by v trestním řízení při vyžadování údajů podle § 88a tr. ř. bylo využito i úpravy obsažené v zákoně o policii, a to zejména tak, že by údaje z telekomunikačního provozu byly získávány způsobem umožňujícím dálkový a nepřetržitý přístup. Lze jen doporučit, aby policejní orgány na to, že se budou zjišťovat údaje z telekomunikačního provozu způsobem vyplývajícím z § 47a odst. 3 zákona o policii, upozornily jak státního zástupce (bude-li návrh podáván jím), tak zejména soudce, aby to bylo mohlo být případně zohledněno ve vydaném příkazu.

Na gremiální poradě Nejvyššího státního zastupitelství byla z podnětu mezinárodního odboru NSZ ze dne 25. 2. 2002 posuzována otázka, zda - pokud dochází ke sledování pohybu věci (mobilního telefonu) prostřednictvím buněk operátora, a přitom nejde o odposlech nebo zjišťování, komu je z mobilního telefonu voláno, ale jde pouze o sledování pohybu osoby, která má mobilní telefon u sebe - je třeba k tomuto sledování povolení státního zástupce podle § 158d odst. 2 tr. ř. nebo povolení soudce podle § 158d odst. 3 tr. ř. Mezinárodní odbor dospěl předběžně k závěru, že k této formě sledování postačí souhlas státního zástupce podle § 158d odst. 2 tr. ř., neboť souhlasu soudce podle § 158d odst. 3 tr. ř. je třeba, pouze pokud má být sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí. Rovněž není třeba žádat soudce o rozhodnutí podle § 88 tr. ř., neboť se nejedná o odposlech a záznam telekomunikačního provozu. Rozhodnutí soudce podle § 88 tr. ř. (nebo případně podle § 88a tr. ř.) je třeba pouze v těch případech, kdy je zjišťován buď obsah konkrétních zpráv sdělovaných telekomunikačními prostředky nebo informace o tom, na která čísla bylo z konkrétní telekomunikační stanice voláno či zasílány zprávy. V tomto případě se jedná pouze o sledování pohybu osoby na základě toho, že tato osoba má u sebe přístroj vysílající takové impulsy, které je

možné sledovat. Není zjišťován ani obsah jednotlivých telefonních hovorů uskutečněných prostřednictvím mobilního telefonu ani čísla, na která bylo tímto mobilem telefonováno. S ohledem na vymezení předmětu telekomunikačního tajemství podle § 84 odst. 3 telekomunikačního zákona sledováním pohybu věci (mobilního telefonu) prostřednictvím buněk operátora nedochází k porušení telekomunikačního tajemství, neboť žádným způsobem nejsou zjišťovány údaje týkající se účastníků telekomunikačního provozu.

K bodům I. a II. stanoviska:

Jak je patrné, vyskytlo se na tutéž problematiku celkem pět různých názorů. Všechny vycházejí ze shodného předpokladu, že se jedná zejména o sledování pohybu osoby pomocí mobilního telefonu, který má taková osoba u sebe, jde o předpokládaného pachatele trestného činu a jde o odcizený mobilní telefon. Bylo by možno řešit ještě řadu jiných situací, zejména co do rozsahu sledovaných zjišťovaných a sledovaných údajů z pohledu vymezení předmětu telekomunikačního tajemství v podobě zákonem stanovené povinnosti mlčenlivosti (§ 84 zákona o telekomunikacích) a také ale i ústavně chráněného tajemství telefonem a jiným zařízením dopravovaných zpráv ve smyslu čl. 13 odst. 1 Listiny, ale z praktického hlediska je možno podstatu problému omezit (a tím vymezit) takto:

Jde-li o zjištění místa pohybu (identifikaci) mobilního telefonu (a tím i vytvoření předpokladů pro odhalení místa pohybu pachatele trestného činu a jeho zjištění a zajištění), je k tomu třeba:

- 1. příkazu soudu ke zjištění údajů o telekomunikačním provozu podle § 88a odst. 1 tr. ř. nebo souhlasu majitele (resp. oprávněného uživatele) mobilního telefonu podle § 88a odst. 2 tr. ř., nebo**
- 2. souhlasu soudce ke sledování osob a věcí podle § 158d odst. 3 tr. ř., nebo**
- 3. souhlasu státního zástupce ke sledování osob a věcí podle § 158d odst. 2 tr. ř., nebo**
- 4. souhlasu státního zástupce ke sledování osob a věcí podle § 158d odst. 2 tr. ř. v kombinaci s oprávněním policie vyplývajícím z ustanovení § 47a odst. 3 zákona o policii, resp.**
- 5. není třeba vůbec žádného zvláštního procesního institutu, jde-li jen o zjištění IMEI kódu mobilního telefonu, neboť se zde jedná jen o zjištění skutečností potřebných pro užití prostředků uvedených v § 88, resp. § 88a tr. ř., a pak stačí uplatnit pouze povinnost plynoucí z ustanovení § 8 odst. 1 tr. ř.**

Úvodem je třeba zmínit, že k předmětu telekomunikačního tajemství bylo již řečeno v jiné souvislosti:⁵ „Předmětem telekomunikačního tajemství je nyní bez jakýchkoli pochybností nejen obsah zpráv přepravovaných nebo jinak zprostředkovaných telekomunikačními zařízeními a sítěmi s výjimkou zpráv, určených veřejnosti. Jsou jimi i provozní doklady, z jejichž obsahu je zjevný obsah přepravovaných zpráv (§ 84 odst. 3 písm. b) nového zákona o telekomunikacích), ale i data související s poskytováním telekomunikační služby,

⁵ V rámci přípravy výkladového stanoviska poř. č. 28/2000 Sb. v. s. NSZ k postupu při zjišťování informací z telekomunikačního provozu o jeho účastnících (mimo obsahu dopravovaných zpráv), které již nelze použít vzhledem k pozdějšímu ústavnímu nálezu sp. zn. II. ÚS 502/2000 (a dalším obdobným nálezům), avšak co do vymezení rozsahu předmětu telekomunikačního tajemství a zejména také odpovědi na otázku koho, resp. čí údaje má chránit, lze na něj v této souvislosti navázat (viz spis sp. zn. SL 737/99).

zejména údaje o účastnících telekomunikačního spojení.“ (§ 84 odst. 3 písm. c) cit. zák.).⁶ Chráněna jsou však obdobným způsobem i osobní a zprostředkovací data ostatních uživatelů telekomunikačních služeb, kteří nejsou současně jejími účastníky.⁷ Zde jim ochranu poskytuje zvláštní povinnost mlčenlivosti zdůrazněná v ustanovení § 84 odst. 5 telekomunikačního zákona.⁸ Rozlišování těchto dvou skupin

⁶ Podle § 2 odst. 9 zák. č. 151/2000 Sb., o telekomunikacích, se účastníkem rozumí uživatel telekomunikační služby, který je s jejím poskytovatelem ve smluvním vztahu.

⁷ Podle § 2 odst. 8 cit. zák. se uživatelem telekomunikační služby rozumí fyzická osoba nebo právnická osoba, které je poskytována telekomunikační služba.

⁸ Lze souhlasit se stanoviskem odboru legislativy MV z 19. 7. 2000 v příloze podání ZTÚ SKP - PČR, které rozlišuje data o účastnících telekomunikačního provozu chráněná telekomunikačním tajemstvím podle § 84 odst. 3 písm. c) cit. zák. a pojem osobních a zprostředkovacích dat o uživatelích telekomunikačního provozu chráněná zvláštní povinností mlčenlivosti podle § 84 odst. 5 tohoto zákona. Rozbor v textu uvedeném v prvním odstavci na str. 2 tohoto materiálu shledává vzhledem k obsahu § 86 odst. 1 zákona o telekomunikacích rozpor mezi okruhem těchto údajů vymezených podle § 84 odst. 3 písm. c) a § 84 odst. 5 telekomunikačního zákona posuzovaných v kontextu ustanovení § 86 odst. 1 cit. zák. na straně jedné a okruhem taxativně vypočtených údajů uvedených v § 84 odst. 5 téhož zákona, posuzovaného však izolovaně na straně druhé. Lze oprávněně usuzovat, že tu jde o legislativní nonsens. Jak totiž vyplývá z návrhu věcného záměru zákona o telekomunikacích (viz k tomu zdejší spis sp. zn. SL 323/98), ale i z návrhu paragrafovaného znění tohoto zákona (k tomu viz zdejší spis sp. zn. SL 350/99), předkladatel původně definoval telekomunikační tajemství tak, že jeho předmětem je: „a) obsah zpráv přepravovaných nebo jinak zprostředkovaných telekomunikačními zařízeními a sítěmi, b) jsou provozní doklady, z jejich obsahu by mohl být zjevný obsah přepravovaných zpráv.“ Od takto definovaného telekomunikačního tajemství oddělil ochranu osobních a zprostředkovacích dat, která definoval jako: „a) jméno a příjmení, popř. obchodní jméno, rodné číslo, popř. identifikační číslo organizace, akademický titul, adresa, popř. sídlo, b) data související s poskytováním telekomunikační služby.“ Předmětem vlastního telekomunikačního tajemství (v užším smyslu) proto tyto údaje neměly původně vůbec být a měly být chráněny zvláštní povinností mlčenlivosti obdobně, jak je tomu dnes v ustanovení § 84 odst. 5 telekomunikačního zákona. Jejich ochrana neměla vyplývat přednostně z ústavou zaručeného práva na ochranu dopravovaných zpráv (čl. 13 Listiny základních práv a svobod). Ta měla být poskytována obsahu dopravovaných zpráv a dokladům, z nichž by mohl být tento obsah patrný. Ochrana těchto dat byla odvozována od práva na ochranu osobních údajů (na ochranu soukromí - viz čl. 7 odst. 1 a čl. 10 Listiny základních práv a svobod), což vyplývá jak z odůvodnění návrhu věcného záměru zákona, tak i z důvodové zprávy k němu (viz str. 24 důvodové zprávy). Tam se výslovně uvádí: „Zákon stanoví telekomunikační tajemství a povinnosti osob k zajištění jeho dodržování odlišně od dosavadního zákona o telekomunikacích a v širším měřítku (a konkrétněji), než jak je stanoveno v čl. 13 Listiny základních práv a svobod, která je součástí ústavního pořádku, a v dalších předpisech. To je dáno zejména snahou transformovat tuto instituci v rozsahu daném Směrnicí 95/43/EC, ve znění Směrnice 97/66/EC, o nakládání s osobními daty a ochraně soukromí v odvětví telekomunikací, do českého právního řádu a upravit normativně (s taxativním výčtem povinností osob vykonávajících telekomunikační činnosti - pro podporu právní jistoty dotčených osob) i ochranu osobních a zprostředkovacích dat týkající se zpracování osobních dat a ochrany soukromí v telekomunikacích.“ Jde vlastně o uvedení této normy nejen do souladu s citovanými směrnici orgánů EU, ale i do souladu s předtím již vydaným zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Nicméně v legislativním procesu došlo k narušení tohoto logického uspořádání, takže částečně se ochrana těchto dat dostala do obsahu telekomunikačního tajemství ve formulaci uvedené v § 84 odst. 3 písm. c) zákona o telekomunikacích, a to pokud jde o účastníky telekomunikačního provozu výslovně, pokud jde o ostatní uživatele, lze ji dovodit výkladem (viz slůvko „...zejména...“), částečně zůstala v obecné podobě (tedy obecně pro všechny uživatele telekomunikačních služeb) v ustanovení § 84 odst. 5 téhož zákona, z něhož však - a v tom je třeba především spatřovat legislativní nonsens - zase vypadla ve výčtu jednotlivých dat zprostředkovací data. Ustanovení se tak tváří, jako by podávalo taxativní výčet údajů v něm obsažených (asi to jinak ani vykládat nepůjde), nicméně v předchozí větě stanovená povinnost mlčenlivosti se má vztahovat na „osobní a zprostředkovací data“ ... Přitom v následujícím výčtu zůstala uvedena pouze data mající charakter osobních údajů. Proč tomu tak je, nelze blíže objasnit. Ačkoli celý tento díl 12 zákona nese název „Telekomunikační tajemství a ochrana osobních a zprostředkovacích dat“ a ustanovení § 84 podává definici těchto pojmů, zprostředkovací data tak zde vlastně přímo definována nejsou a význam tohoto pojmu nutno odvozovat od demonstrativního výčtu

dat z hlediska řešeného problému však není podstatné.⁹ Nicméně za podstatné je třeba považovat to, že výslovná ochrana osobních údajů uživatelů (nikoli tedy pouze účastníků) telekomunikačních služeb podléhající zvláštní povinnosti mlčenlivosti znamená, že chrání kohokoli, kdo je uživatelem telekomunikačních služeb. Konkrétně to tedy ...znamená, že chrání nejen uživatele oprávněného, ale stejným způsobem chrání i uživatele neoprávněného. ...Jinak řečeno, ani pachatele krádeže mobilního telefonu nelze jednoduše identifikovat, aniž by bylo nutno prolomit tuto zvláštní povinnost mlčenlivosti.¹⁰ To je i odpověď na případné úvahy o tom, jakým jiným, jednodušším než zákonem stanoveným postupem, dovolujícím prolomit tuto povinnost mlčenlivosti, lze získat ona osobní a zprostředkovací data, týkající se pachatelů trestné činnosti této povahy.¹¹ "

V souvislosti s řešením otázky případné trestněprávní odpovědnosti operátorů mobilních telefonních sítí za nezablokování mobilního telefonu při jeho ohlášeném odcizení (viz sp. zn. 1 NZn 2672/2000) byly dotazem u Českého telekomunikačního úřadu (ČTÚ) zjišťovány také bližší podrobnosti k technické podstatě stránce provozu a používání mobilního telefonu (včetně povahy IMEI kódu).¹² Navíc tu byla znovu otevřena otázka ochrany dat účastníků, resp. uživatelů telekomunikačních služeb, neboť původní úvaha v zadání vycházela z názoru (byť vyjádřeného jen v poznámce pod čarou), podle něhož „identifikace či vyřazení odcizeného mobilního telefonu nemůže podléhat mlčenlivosti, neboť pachatel není ve smluvním vztahu s poskytovatelem a není tak účastníkem telekomunikačního spojení; tento vztah nenastane ani případným vložením nové GO či TWIST karty, neboť vložení takové karty do mobilního telefonu je učiněno v rozporu s vůlí jeho vlastníka - jde o neplatný právní úkon.“ Jedná se o podobnou úvahu, kterou učinilo i Vrchní státní zastupitelství v Olomouci ve vztahu ke zjišťování příslušných údajů o mobilním telefonu, který byl odcizen, pokud k tomu dá souhlas jeho původní vlastník (uživatel).

I když tento výklad nelze považovat za jednoznačný a bezproblémový, jak by se na první pohled zdálo (vždyť je logické, že zákon nemá chránit pachatele a bránit tak oprávněnému vlastníku odcizené věci, aby k ní mohl uplatnit svá zákonná

údajů, uvedených až v ustanovení § 86 odst. 1 zákona o telekomunikacích. Bude na praxi, jak si s tímto problémem poradí.

⁹ V obou případech jde o zvláštní státem stanovenou (uznanou) povinnost mlčenlivosti. Telekomunikační zákon pro prolomení tajnosti těchto informací nestanoví žádné odlišné podmínky. Proto ani její rozlišování z hlediska podmínek pro její prolomení pro potřeby orgánů činných v trestním řízení resp. orgány Policie ČR nemá žádný praktický význam.

¹⁰ Samozřejmě s výjimkou případů zvláštní oznamovací povinnosti podle trestního zákona.

¹¹ Výjimka, která přímo prolomuje ochranu tajnosti těchto dat, je uvedena v ustanovení § 84 odst. 9 telekomunikačního zákona, které stanoví, že provozovatelé veřejných telekomunikačních sítí a poskytovatelé veřejných telekomunikačních služeb si mohou vzájemně předávat data uvedená v odstavci 3 písm. c), je-li to nezbytné pro zajištění propojení a přístupu k síti, ke vzájemnému vyúčtování a k identifikaci zneužívání sítě a služeb. Jde tedy jen o předávání takových dat mezi subjekty podílejícími se na poskytování telekomunikačních služeb, nikoli navenek.

¹² ČTÚ mj. uvedl, že šifrovací algoritmy standardu GSM používané všemi operátory mobilních sítí v ČR zajišťují jak důvěrnou autentifikaci klientů, tak šifrování přenášených dat, a v neposlední řadě též ověření typu a stavu mobilního telefonního přístroje. Každý mobilní telefonní přístroj GSM je vybaven SIM kartou (Subscriber Identity Modul), která je proti zneužití přístroje a proti neoprávněnému přihlášení k síti chráněna číslem PIN (Personal Identification Number) a její blokování proti zneužití provádějí všichni operátoři na přání účastníka. Dále je každý mobilní telefon vybaven ve své elektronice IMEI - International Mobile Equipment Identity – což je 15-ti místný kód, prvních 6 číslic tohoto kódu TAC (Type Approval Code) identifikuje zemi, ve které byl telefon schválen k provozu a číslo schválení tohoto zařízení. proto telefony téhož typu mají tuto část kódu stejnou. Zbývajících 9 míst slouží k identifikaci konkrétního přístroje. Většina mobilních telefonů zobrazí IMEI po zadání příkazu *#06#...

práva...), je ve výsledku třeba tomuto názoru přisvědčit. Je tu ale třeba dodat ještě argumenty, které takový výklad podpoří a současně upozornit na to, že nelze uvést, že by postavení takového uživatele telekomunikačních služeb nepodléhalo mlčenlivosti **vůbec**. Problém lze spatřovat - jak bylo na to upozorněno již výše - ve výkladu obsahu povinné mlčenlivosti, tzn. telekomunikačního tajemství - pokud jde o jeho osobní dosah, tedy vyjasnit na **které osoby, která zařízení a v jakém rozsahu** se vlastně vztahuje. Zda se vztahuje pouze na *účastníky* telekomunikačního provozu, na *všechny uživatele* telekomunikačních služeb (lépe řečeno zde telekomunikačního zařízení) nebo jen na *oprávněné uživatele* a samozřejmě i (oprávněné) účastníky telekomunikačního provozu.

Zákon o telekomunikacích tuto otázku výslovně neřeší, upravuje telekomunikační tajemství obecně a podle znění jeho ustanovení by se měla tato povinnost mlčenlivosti proto vztahovat zásadně na všechny uživatele telekomunikačních služeb (tyto osoby podle definice telekomunikačního zákona nemusí být s poskytovatelem telekomunikačních služeb ve smluvním vztahu). Pokud jde o průlom do ní, není v něm nikde žádné ustanovení, které by pro průlom stanovilo odlišné podmínky z hlediska postavení dané osoby ve vztahu k poskytovateli telekomunikačních služeb. Obecně proto musí platit, že nerozhoduje - pro uplatnění omezení plynoucí z telekomunikačního tajemství a tedy *a contrario* i pro průlom do něj - zda jde o uživatele telekomunikačních služeb legálního či nelegálního. Ledaže jsou naplněny výslovně zákonem stanovené podmínky pro takový průlom (jako je tomu např. v případě oznamovací povinnosti podle § 168 tr. zák.). To ovšem platí principiálně z pohledu *telekomunikačního zákona* a váže samozřejmě poskytovatele telekomunikačních služeb z jeho pohledu jako obecné normy, která upravuje (v režimu práva povahy převážně administrativní) jím poskytované služby vůči veřejnosti, a v rámci nich povinnost mlčenlivosti platí zásadně *erga omnes*. Ale *speciální norma*, kterou je zde *trestní řád*, stanoví *zvláštní podmínky pro průlom do uvedené povinnosti mlčenlivosti*.¹³ A tak - ačkoli zákon o telekomunikacích, který zásadně z hlediska konstrukce jím stanovené povinnosti mlčenlivosti nerozlišuje mezi postavením uživatele poskytované telekomunikační služby z hlediska zákonného či nezákonného vztahu k telekomunikačnímu zařízení, které užívá, tento vztah je důležitý v případě, kdy je užito institutu trestního řádu pro průlom do telekomunikačního tajemství. Zejména se uplatní (a proto je třeba se touto otázkou podrobněji zabývat) v případech, kdy se má aplikovat ustanovení § 88a odst. 2 tr. ř. (a totéž pak platí obdobně i pro ustanovení § 158d odst. 6 tr. ř.). Podle konstrukce telekomunikačního tajemství je totiž i nelegální uživatel telekomunikačních služeb *navenek* chráněn touto povinností mlčenlivosti. Avšak pro **účely trestního řádu** lze tuto povinnost prolomit nejen na základě příkazu soudu, který má v jistém smyslu „objektivní“ charakter a nikdo nezpochybňuje, že působí skutečně *erga omnes*, tedy že v jakémkoli případě probíhajícího telekomunikačního provozu (s výjimkou toho, kde to zákon výslovně vylučuje - což je komunikace mezi obviněným a obhájcem) lze tyto údaje získat na jeho základě. Pro **účely trestního řízení** však postačí k průlomu do tohoto tajemství i **souhlas původního oprávněného uživatele telekomunikačních služeb k tomu, aby jejich poskytovatel byl povinen poskytnout orgánům činným v trestním řízení příslušné údaje**.

¹³ Tak, jako je stanoví § 168 trestního zákona obecně z hlediska konstrukce oznamovací povinnosti ohledně vyjmenovaných trestných činů, která až na dvě zákonem stanovené výjimky - povinnou mlčenlivost advokáta a zpovědní tajemství - prolamuje všechny ostatní zákonem stanovené či zákonem uznané povinnosti mlčenlivosti.

Pro pochopení významu tohoto tvrzení je nutno si uvědomit, že v řadě případů v praxi nepůjde zdaleka jen o zcela „jasné případy“ sledování zlodějů mobilních telefonů, ale v řadě případů může být takový úkon zahájen proti novému jeho držiteli, jenž navíc (aspoň teoreticky) mohl tento přístroj získat od obchodníka, na něhož přešlo vlastnické právo k tomuto přístroji v důsledku uplatnění § 446 obchodního zákoníku.¹⁴ Tam již pak s prostým poukazem na to, že majitel telefonu dává souhlas ke sledování pachatele trestného činu za pomoci jeho vlastního přístroje, nelze vystačit. Ačkoli § 88a odst. 2 tr. ř. hovoří stejnými pojmy (a to zcela záměrně a jistě opodstatněně) jako telekomunikační zákon (a stejně je tomu tak i v případě § 88 odst. 3 tr. ř.), důsledky, které vyplývají z uplatnění tohoto institutu jsou takové, že k průlomu do telekomunikačního tajemství postačí v tomto případě souhlas původního oprávněného uživatele telefonního přístroje, jenž jej byl zbaven trestným činem, a není tu nutno dále zkoumat, kdo je jeho současným držitelem, a tedy i uživatelem (nebo dokonce účastníkem) telekomunikačních služeb. Lze proto akceptovat v tomto směru stanovisko Vrchního státního zastupitelství v Olomouci, pokud jde o výklad podmínky uvedené v § 88a odst. 2 tr. ř., tedy souhlasu uživatele telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním zařízení vztahovat. Má se vykládat tak, že tu nejde o souhlas uživatele zařízení, ke kterému – coby k zařízení, k věci samotné - se mají tyto údaje vztahovat, ale údajů, které se mají vztahovat k (původnímu) oprávněnému uživateli telekomunikačního zařízení a tím i telekomunikačních služeb. Jinak řečeno – jde o údaje o uživateli, nikoli o údaje o zařízení, které se vyžadují a k nimž se dává souhlas. Protože **ochrana údajů** chráněných podle telekomunikačního zákona se vztahuje primárně na ochranu údajů **o uživateli**, a nikoli na ochranu údajů **o zařízení, které užívá**. Samo zařízení je z tohoto pohledu vlastně indiferentní – tyto úkony jsou realizovány vždy vůči určitým osobám (ať už známým či neznámým), cíleně mají odhalit údaje o osobách, byť se tak děje **skrze sledování zařízení** samotného. Tuto skutečnost je třeba si náležitě uvědomit, protože podle toho pak se musí posuzovat to, jaké údaje o zařízení vlastně vypovídají o jeho uživateli a jakým způsobem umožňují jeho identifikaci, a jaký je takřikajíc i „osobní rozsah“ telekomunikačního tajemství (zjednodušeně řečeno, tj. včetně všech druhů zde uplatňovaných povinností mlčenlivosti).

Tedy – a nyní už výlučně z pohledu institutů trestněprávních – lze problém uzavřít následovně:

Nenalezne se patrně údaj, který by v daném případě, tj. v případě identifikace uživatele mobilního telefonu, nepodléhal ochraně v podobě zákonné povinnosti mlčenlivosti vyplývající z telekomunikačního tajemství (v širším smyslu, včetně ochrany různých druhů dat a tajemství telefonem, aj. dopravovaných zpráv ve smyslu ústavní svobody, zakotvené v čl. 13 odst. 1 Listiny základních práv a svobod). I takové technické údaje, jako je identifikační údaj charakterizující samotný přístroj - kód IMEI (nejen tedy telefonní číslo účastnické mobilní telefonní stanice), jsou chráněnými údaji ve smyslu těchto ustanovení, protože podle toho, co bylo řečeno ve zmiňovaném nálezu Ústavního soudu, od něhož se začala odvíjet problematika posuzování ochrany telekomunikačního tajemství a osobních a zprostředkovaných dat účastníků telekomunikačního provozu, a co bylo posléze pro účely trestního řízení potvrzeno vcelku bez jakýchkoli pochybností novelou trestního řádu provedenou zákonem č. 265/2001 Sb., která vložila za § 88 ustanovení § 88a, jež

¹⁴ Kupující nabývá vlastnické právo i v případě, kdy prodávající není vlastníkem prodávaného zboží, ledaže v době, kdy kupující měl vlastnické právo nabýt, věděl nebo vědět měl a mohl, že prodávající není vlastníkem a že není ani oprávněn zbožím nakládat za účelem jeho prodeje.

v této podobě předtím v trestním řádu nebylo,¹⁵ všechny tyto údaje patří (váží se) ke konkrétní osobě uživatele uvedeného telekomunikačního zařízení a slouží - ať už po „technické“ stránce jsou zjišťovány jakkoli použitým postupem - k její identifikaci. Obvykle tedy slouží k jejímu zjištění, mnohdy zaměření, sledování a posléze i ke zjištění její osobní identity. Bez toho totiž by takové úkony neměly smyslu – jak bylo řečeno, hlavním účelem a konečným cílem sledování věci není zjistit a odhalit identitu **věci**, vždy jde o prostředek, jímž má být odhaleno určité **jednání určité osoby**, tak či onak angažované v trestné činnosti. Jde totiž o trestní řízení, které se vede proti osobám pro podezření z trestného činu a jen v rámci odhalování, zjišťování a dokazování této trestné činnosti, tedy prokazování konkrétního jednání konkrétních osob se tyto instituty užívají. To plyne ze stávající právní úpravy a nemá smyslu s tímto tvrzením příliš polemizovat.

Z uvedených důvodů nelze přisvědčit těm názorům, které tvrdí, že uvedené údaje lze získávat (např. jen pro účely „zaměření“ pohybu dotyčné osoby) volně, tedy jen na podkladě povinnosti k součinnosti, vyplývající z ustanovení § 8 odst. 1 tr. ř.¹⁶

¹⁵ Namítá se někdy – a to vcelku opodstatněně - že samotný nálezn Ústavního soudu sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001 (viz zejména: „Soukromí každého člověka je hodno ochrany ve smyslu čl. 13 Listiny základních práv a svobod nejen ve vztahu k vlastnímu obsahu zpráv podávaných telefonem, ale i ve vztahu k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie o základových stanicích zajišťujících hovor. Tyto údaje jsou nedílnou součástí komunikace uskutečněné prostřednictvím telefonu. Jestliže ústavní pořádek České republiky připouští průlom této ochrany, děje se tak pouze a výlučně v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených základních práv a svobod jiných; sem spadá především nezbytnost daná obecným zájmem na ochraně společnosti před trestnými činy a na tom, aby takové činy byly zjištěny a potrestány. Přípustný je tedy pouze zásah do základního práva nebo svobody člověka ze strany státní moci, jestliže jde o zásah nezbytný ve výše uvedeném smyslu. K tomu, aby nebyly překročeny meze nezbytnosti, musí existovat systém adekvátních a dostatečných záruk, skládající se z odpovídajících právních předpisů a účinné kontroly jejich dodržování. S ohledem na to, že jsou stanovena pravidla pro odposlech a záznam telekomunikačního provozu ze strany státních orgánů, která umožňují kromě dalších údajů pořídit především obsah telefonické zprávy, je možné postupovat podle těchto pravidel i při pořizování či získávání těchto „dalších“ údajů, tj. při evidování telekomunikačního provozu...“) nebyl v obsahu svého odůvodnění tak striktní, aby požadoval pro zjišťování **těchto údajů** přímo **souhlas soudce**, ale spíše „jen“ upozorňoval na neexistující dostatečnou právní úpravu takového postupu, a proto pro její nedostatek (a v zájmu umožnění takových zjištění do legislativní nápravy tohoto nedostatku) analogicky odkázal na ustanovení § 88 tr. ř. o odposlechu a záznamu telekomunikačního provozu, u něhož je udělení souhlasu soudu nezbytnou podmínkou. Z toho se podává, že není důvodu nutně svazovat postupy, jimiž se tyto údaje získávají, vždy jen s takovým postupem, u něhož se předpokládá předchozí souhlas soudu. Problém takového výkladu spočívá v tom, že jednak **obsahově**, ač se v citovaném ústavním nálezu konstatuje i nedostatek podrobné právní úpravy, jsou už tímto nálezn „navždy“ takové údaje svázány s tajemstvím pomocí telefonu aj. dopravovaných zpráv a **zásah do tohoto tajemství** upraveného v čl. 13 odst. 1 Listiny je přípustný **jen se souhlasem soudu**, a navíc – tuto skutečnost dnes navenek deklaruje i ustanovení § 88a tr. ř., které z takového obsahového hodnocení uvedených údajů vlastně samo vychází.

¹⁶ Určité úvahy, od nichž se pak odvíjí posuzování toho, kdy operátoři provozující mobilní telefonní sítě mohou sdělovat příslušné údaje přímo policii, aniž by k tomu bylo třeba souhlasu státního zástupce či soudu, se odvíjejí od technických zvláštností provozu mobilních telefonů. Konkrétně se v důsledku nich hledá prostor pro vymezení provozu zapojeného mobilního telefonního přístroje, aniž by však šlo ještě o telekomunikační provoz, s nímž je spojena zvláštní ochrana poskytovaná telekomunikačním tajemstvím. Hovoří se např. o době, kdy nejde o přímou komunikaci mezi účastníky, ale o pouhé mechanické (automatické) přihlášení telefonu do sítě příslušného operátora po jeho zapnutí. I tady je třeba mít na paměti – aniž by tu stanovisko bylo způsobilé řešit technickou stránku provozu tohoto

Veźme-li se toto tvrzení za východisko, pak je zřejmé, že tu stojí vedle sebe dva instituty, které umožňují zasahovat do sféry osobní svobody toho, kdo používá mobilní telefonní přístroje, přičemž Ministerstvo vnitra vedle toho předkládá ještě třetí konstrukci, která ovšem také vychází ze „souběžné“ aplikace jednoho z nich - z ustanovení § 158d tr. ř. Jde o:

1. zjišťování těchto údajů postupem podle § 88a tr. ř., kde o charakteru úkonu a jeho výsledku nemůže být pochyb, a to za předpokladu, že se přijme názor, že v případě postupu podle odstavce 2 citovaného ustanovení tu postačí souhlas jen původního, legálního uživatele telekomunikačních služeb (zpravidla tedy původního vlastníka či uživatele mobilního telefonního přístroje),
2. institut sledování osob a věcí podle § 158d tr. ř., kde je nutno posoudit, ve kterém „stupni“ sledování lze tohoto postupu užít (v úvahu připadají jen ustanovení odstavce 2, 3 a 6, přičemž pro posledně uvedený postup platí totéž, co pro postup podle § 88a odst. 2 tr. ř.), a
3. z pohledu Ministerstva vnitra i zjišťování těchto údajů pomocí dálkového přístupu podle § 47a zákona o policii ve spojení s § 158d tr. ř., jde-li o potřebu získání takových údajů jen v rozsahu aktuální a nezbytné potřeby pro zabezpečení sledování osob a věcí, nikoli pro opatřování těchto údajů jako skutečností, které mají samy o sobě být užity v trestním řízení jako důkaz či důkazní prostředek (totéž by mohlo platit i o vztahu tohoto § 47a odst. 3 zákona o policii a § 88a odst. 1 tr. ř.).

Z toho, co bylo vyvozeno o povaze uvedených údajů a rozsahu ochrany, která je poskytována telekomunikačnímu tajemství (v uváděném širším smyslu), nutno učinit závěr, že jediným možným postupem, jde-li o **trestní řízení**, ať už je upraven po „technické“ stránce trestním řádem v jakékoli podobě, je takový postup, u něhož se k jeho provedení předpokládá udělení **předchozího souhlasu soudce**. Jen v rámci prováděného sledování osob a věcí, jde-li o takové úkony, jimiž se nezasahuje do práv chráněných článkem 13 Listiny základních práv a svobod a prolomitelných jen postupem podle § 88a tr. ř. (nepředpokládá se tu samozřejmě ani odposlech ani záznam telekomunikačního provozu podle § 88 tr. ř.), pak postačí k takovému postupu i souhlas státního zástupce podle § 158d odst. 2 tr. ř. Jsou to ovšem případy, kdy nejde o získávání údajů podléhajících telekomunikačnímu tajemství ani se na ně nevztahuje ochrana osobních a zprostředkovacích dat.

K otázce vztahu ustanovení § 47a zákona o Policii ČR a trestního řádu tu nelze uvést nic jiného, než znovu opakovat, že Nejvyššímu státnímu zastupitelství nepřísluší posuzovat postupy policie v případech, kdy nejde o činnost, která se dotýká působnosti státního zastupitelství, a nepřísluší mu ani podávat výklad právních předpisů nad rámec oprávnění daného nejvyššímu státnímu zástupci ustanovením § 12 odst. 2 zákona č. 283/1993 Sb., o státním zastupitelství, ve znění pozdějších předpisů. Nepřísluší mu tedy oprávnění podávat výklad ustanovení § 47a

zařízení – že takový provoz může být jistě monitorován policií, pokud však nejde o zjišťování těch údajů, které jsou předmětem telekomunikačního tajemství. Jde-li tak či onak o identifikaci konkrétních účastníků, resp. o zjišťování chráněných údajů, prostřednictvím nichž lze teprve přístroje identifikovat, může být takový postup později z hlediska důkazní hodnoty zpochybňován. Bude-li takto postupováno bez souhlasu příslušného orgánu, mělo by být vždy náležitě doloženo, že o legálnosti takového postupu nemohou být pochybnosti. Pokud by je nebylo možno přesvědčivě odstranit, je vhodnější příslušný souhlas k tomu kompetentního orgánu vyžádat předem, čímž se zabrání možné ztrátě významného důkazu.

zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, jako takového. Proto Nejvyšší státní zastupitelství již od samého počátku, kdy se začaly objevovat problémy kolem použití postupu policie vázaného na ustanovení § 47a odst. 3 zákona o policii, tvrdilo (a na tom se nic nemění ani nyní), že jde o institut, který stojí vedle institutu upraveného v ustanovení § 88a tr. ř. (a také v § 158d tr. ř.), a že je věcí policie, pokud pro účely svého vlastního postupu plynoucího z úkolů uložených policii příslušnými ustanoveními zákona o policii (zejména § 2), využívá tohoto ustanovení; a že je jen na ní, jakým způsobem tak činí. Jde-li však o postup **v trestním řízení**, je policie povinna postupovat podle trestního řádu a respektovat ty procesní instituty, které jí trestní řád v tomto směru dává. Tedy, jde-li o získávání uvedených údajů, musí pro tento účel zásadně postupovat podle ustanovení § 88a tr. ř. nebo – a v tomto směru také nebude jistě pochyb o zákonnosti takového postupu – v případě sledování osob a věcí, podle ustanovení § 158d odst. 3 (nebo odst. 6) tr. ř.¹⁷ Resp. při sledování osob a věcí nepochybně může využívat technických možností daných provozem mobilních telefonů a sítěmi operátorů a vyžadovat k úspěšnému provedení sledování příslušné údaje i za souhlasu státního zástupce podle § 158d odst. 2 tr. ř., avšak jak už bylo řečeno - jen za podmínky, že nejde o zásah do těch údajů, které chrání (negativně – tím že stanoví podmínky průlomu) ustanovení § 88a tr. ř. anebo ustanovení § 158d odst. 3 tr. ř. Souhlas státního zástupce nemůže ani při sledování osob a věcí nahradit souhlas soudu, je-li tento souhlas soudu podmínkou k získání takto chráněného údaje.

Lze proto považovat stanovisko Vrchního státního zastupitelství v Olomouci k této problematice za správné, stejně jako postup těch státních zástupců, kteří pro účely vyžádání údajů z telekomunikačního provozu (včetně osobních a zprostředkovaných dat o jeho účastnících a telekomunikačního tajemství ve smyslu zákona o telekomunikacích) odmítají udělit policejnímu orgánu svůj souhlas podle § 158d odst. 2 tr. ř. a odkazují na povinnost vyžádat v takovém případě souhlas soudu ve smyslu § 158d odst. 3 tr. ř.¹⁸

¹⁷ Úprava v § 158d odst. 3 tr. ř. pro připomenutí vychází z toho, že 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 na základě předchozího povolení soudce. Při vstupu do obydlí nesmějí být provedeny žádné jiné úkony než takové, které směřují k umístění technických prostředků. Ve smyslu § 158d odst. 6 tr. ř. bez splnění podmínek podle odstavců 2 a 3 lze sledování provést, pokud s tím výslovně souhlasí ten, do jehož práv a svobod má být sledováním zasahováno. Je-li takový souhlas dodatečně odvolán, sledování se neprodleně zastaví.

¹⁸ Nelze pochybovat o tom, že tam, kde bylo povoleno sledování osob a věcí soudem podle posledně uvedeného ustanovení, lze vyžadovat i údaje z telekomunikačního provozu bez dalšího, dodatečného či rozšiřujícího souhlasu soudu, a to přímo v průběhu sledování, vyskytne-li se taková potřeba. Je pak ale lhostejné, zda mají tyto údaje sloužit výlučně jen jako „technická podpora“ k zabezpečení úspěšného průběhu vlastního sledování nebo se event. mají stát také samostatným důkazem či důkazním prostředkem. Samozřejmě se nebrání policii, aby pro své vlastní účely a postupem podle zákona o policii a dalších pro ni závazných předpisů, si takové údaje dále opatřovala, pokud má za to, že institut uvedený v § 47a zákona o policii jí k tomu opravňuje. Ustanovení § 47a zákona o policii však není procesním institutem trestního řízení a proto jeho užití **v trestním řízení** je možno připustit jen jako skutečně **technický postup**, užitý při legálně povoleném získávání těchto údajů. Tehdy, pokud s povolením soudu (vydaným podle § 88a nebo podle § 158d odst. 3 tr. ř.) nebo se souhlasem oprávněných osob (podle § 88a odst. 2, § 88 odst. 3 nebo § 158d odst. 6 tr. ř.) tyto údaje bude policie získávat za pomoci technického prostředku – dálkového připojení, které se v ustanovení § 47a zákona o policii předpokládá.

Toto stanovisko se vydává podle § 12 odst. 2 zák. č. 283/1993 Sb., o státním zastupitelství, ve znění pozdějších předpisů.

Nejvyšší státní zástupkyně:
Mgr. Marie Benešová, v.r.